Veritas NetBackup™ Appliance Administrator's Guide

Release 5.3

VERITAS™

Veritas NetBackup™ Appliance Administrator's Guide

Last updated: 2023-11-27

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

Documentation feedback

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

APPL.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

Overview

This chapter includes the following topics:

About NetBackup appliances

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

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

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

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

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

A 53xx appliance is configured as a media server by default. You can choose to configure a 53xx appliance as follows:

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

---

Note: The 53xx compute node does not have internal disk space available for backups or storage. The space available from the Primary Storage Shelf and up to five Expansion Storage Shelves can be used for backups.

This appliance version allows for easy expansion of existing NetBackup environments that have NetBackup 10.3 or greater installed. The appliance also includes its own browser-based interface. This interface is used for local administration of the network, internal disk storage, tape libraries and much more.

NetBackup appliances support the following features:

- Three interfaces for appliance configuration and management:
  - The NetBackup Appliance Web Console is a web-based graphical user interface that lets you monitor and manage a specific appliance. This interface works best with Google Chrome 96.0 and later, Microsoft Edge 96.0 and later, and Mozilla Firefox 95.0.2 and later.
  - The Veritas Appliance Management Console is a web-based graphical user-interface that helps you to centrally manage multiple NetBackup appliances from a single interface. The Appliance Management Console lets you upgrade and install EEBs on multiple appliances. You can always log on to a dedicated appliance and use the NetBackup Appliance Web Console for all the other tasks.
    See the *Appliance Management Guide* for details.
  - The NetBackup Appliance Shell Menu is a command line driven interface. For a complete description of all appliance commands, refer to the following document:
    NetBackup Appliance Command Reference Guide

- Configuration H of the NetBackup 5240 appliance supports iSCSI connections. All configurations of the NetBackup 5340 appliance support iSCSI. See the *NetBackup Appliance iSCSI Guide* for reference.
- Copilot enables Oracle database administrators to work with NetBackup appliance administrators to perform a streamlined backup and restore process of Oracle databases.
- A NetBackup 5350 appliance supports 1 Primary Storage Shelf and up to 3 Expansion Storage Shelves.
  For more information on the hardware enhancements, refer to the *NetBackup 5350 Appliance Product Description Guide*.
- A NetBackup 5340 appliance supports 1 Primary Storage Shelf and up to 3 Expansion Storage Shelves.
  For more information on the hardware enhancements, refer to the *NetBackup 5340 Appliance Product Description Guide*.
- Starting with NetBackup appliance version 2.7.1, you can use the fully qualified domain name (FQDN) as the appliance host name.
- Starting with NetBackup appliance version 2.7.3, the NetBackup Cloud Storage of data backups and restores are enabled by default on the NetBackup appliances.
  For complete details, refer to the *NetBackup Cloud Administrator's Guide*
- Backup of VMware virtual machines. NetBackup appliance supports direct backup of VMware virtual machines. The appliance can back up virtual machines without a separate Windows system as backup host.
- Symantec Data Center Security (SDCS) integration. The SDCS agent is installed and configured when you initially configure your appliance. By default, SDCS operates in unmanaged mode and helps secure the appliance using host-based intrusion prevention and detection technology. In managed mode, this agent ensures that the appliance audit logs are sent to an external SDCS server to be validated and verified.
- BMR integration. When the appliance is configured as a primary server, you can enable Bare Metal Restore (BMR) from the NetBackup Appliance Web Console.
- IPv4-IPv6 network support. The NetBackup appliances are supported on a dual stack IPv4-IPv6 network. The NetBackup appliance can communicate with, back up, and restore an IPv6 client. You can assign an IPv6 address to an appliance, configure DNS, and routing to include IPv6 based systems. The NetBackup Appliance Web Console can be used to enter information about both IPv4 and IPv6 addresses.

- ACSLS Support. This feature facilitates configuration of NetBackup ACS robotics on the NetBackup appliance. The appliance administrator can change the ACSLS entries in the `vm.conf` file on the local appliance.
- NetBackup SAN Client and Fibre Transport. SAN Client is a NetBackup optional feature that provides high-speed backups and restores of NetBackup clients. Fibre Transport is the name of the NetBackup high-speed data transport method that is part of the SAN Client feature. The backup and restore traffic occurs over a SAN, and NetBackup server and client administration traffic occurs over the LAN.
- Starting with software version 2.7.3, you can duplicate data between NetBackup 52xx or 53xx appliances using Fibre Transport. The supported data transfer methods are optimized duplication and Auto Image Replication. To use this feature, both the source host and target host must use the appliance software version 2.7.3 or later.
- NetBackup preinstalled. Simplifies the deployment and integration into an existing NetBackup environment.

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

- Tape out option. The appliance includes a gigabit, dual-port Fibre Channel host bus adapter (HBA).
  Multiple FC ports can be used for tape out, as long as they are solely dedicated to the tape out function. For more information, refer to the *Veritas NetBackup Appliance Network Ports Reference Guide*.
- Hardware component monitoring. The appliance can monitor key hardware components such as the CPU, disks, memory, power supply modules, and fans. In addition, the appliance provides an optional Call Home feature that allows proactive monitoring and messaging of these NetBackup components.
- The NetBackup appliances support the core NetBackup software agents. The NetBackup agents optimize the performance of critical databases and applications.
  See the *NetBackup Administrator's Guide Volume I* for more information about the policy types that are supported for each software agent. And for the latest NetBackup appliance compatibility information, refer to the Hardware Compatibility List on the Support website.
  www.netbackup.com/compatibility

- Flexible hardware configuration. The appliance can be ordered in a variety of configurations to provide the necessary Ethernet ports. Along with the built-in Ethernet ports on the motherboard, expansion cards can be specified to provide additional 1 GB or 10 GB Ethernet ports. Dual-port and quad-port expansion cards are supported.

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

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

Replace unsupported media servers	Replace an existing media server that runs on a platform that is not supported in NetBackup 10.3.
Add deduplication capability	■ Add the appliance to an existing NetBackup environment or replace an existing media server that does not support deduplication. ■ Configure MSDP partition on the Appliance for deduplication capability.
Use AdvancedDisk for non-deduplicated backups	■ AdvancedDisk can provide faster restore operation but is not space-optimized like MSDP. This is a good solution for backups that include strict tape out schedules. Backups can be expired after duplication to MSDP and space on AdvancedDisk freed up for next day backups.
Add more storage capability	Add storage capability to existing NetBackup 10.3 and greater environments. ■ Built-in appliance disk storage for 52xx appliances The internal disks can be used for additional backup storage on a 52xx appliance. **Note:** The 53xx appliances do not have internal disk space available for backups or storage. The space available from the Primary Storage Shelf and Expansion Storage Shelves can be used for storage. ■ Additional external storage The Storage Shelf is an external unit that provides additional disk storage space. You can add up to six of these units to a NetBackup 5240 or 5250 appliance. If you need or want to add a Storage Shelf to an existing or an operational NetBackup appliance, your appliance may first require a hardware and/or a memory upgrade. For more information, contact your NetBackup appliance representative about your expansion needs.

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

About the Primary Server role

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

Note: The NetBackup 53xx appliance is a media server by default and is not supported for the primary server role configuration.

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

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

About the media server role

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

A NetBackup 53xx appliance is a media server by default. The internal storage in a 53xx appliance cannot be used for storing any data or taking any backups. The internal storage is used for storing the operating system, checkpoints, and logs.

Media server appliances use a simplified administrative interface for the local network and for disk storage management. However, the majority of NetBackup administration such as backup management is performed on the primary server.

When you configure an appliance as a media server, you must specify the primary server it needs to communicate with. The software version on the media server cannot be a later version than what is currently used on the primary server. For example, if the media server is at version 4.0, the primary server must be a NetBackup 52xx appliance with software version 4.0 or later, or a traditional NetBackup primary server with version 9.0 or later.

About accessing the NetBackup Appliance Web Console

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

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

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

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

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

Web browsers supported by the appliance

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

- The NetBackup Appliance Web Console and the IPMI console use pop-up menus. If you use pop-up blockers with your Web browser, some of these menus may not display properly. You must disable pop-up blocking or add the Appliance Web address to the list of acceptable sites in your browser.
- The web browser should have active scripting (ActiveX and JavaScript) enabled.
- The NetBackup Appliance Web Console is best viewed with 1280 * 1024 or a higher screen resolution.

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

Table 1-1 Web browsers supported by the appliance

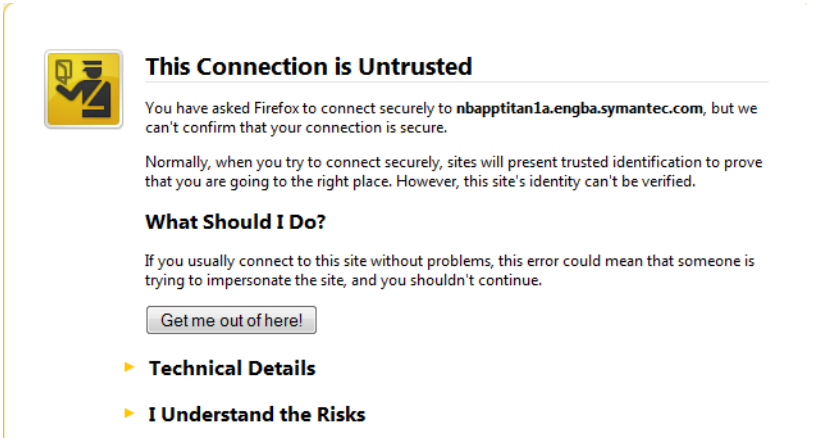
Web browser	Supported Versions	Notes
Mozilla Firefox	95.0.2 and later **Note:** If you try to access the NetBackup Appliance using earlier versions of Firefox and reset the password using `Settings > Password`, the page may hang.	Mozilla Firefox may display an **Untrusted Connection** page when you access the NetBackup Appliance Web Console. See "Disabling the Untrusted Connection page in Mozilla Firefox" on page 16.

Table 1-1 Web browsers supported by the appliance *(continued)*

Web browser	Supported Versions	Notes
Google Chrome	96.0 and later	Google Chrome may display a **The site's security certificate is not trusted!** page when you access the NetBackup Appliance Web Console. Select **Proceed anyway** to access the console.
Microsoft Edge	96.0 and later	

Disabling the Untrusted Connection page in Mozilla Firefox

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



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

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

To disable the Untrusted Connection page in Mozilla Firefox

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

About the NetBackup Appliance Shell Menu

The NetBackup Appliance Shell Menu is an interactive shell that is available on the appliances through SSH. This menu interface enables you to perform most of the administration functions that are necessary to administer the appliances.

You can use the NetBackup Appliance Shell Menu in place of the NetBackup Appliance Web Console for many operations. In addition, anyone who is limited to only SSH because of firewall restraints should use this shell menu.

The *NetBackup Appliance Commands Reference Guide* contains detailed information about the NetBackup Appliance commands. Each command contains a brief description of the primary function of the command, a synopsis, and descriptions of the options that are listed in the synopsis. Some commands also contain notes and usage examples.

Note: It is possible that changes may occur after the documents have been initially released. The electronic versions of these documents on the Support website contain the most up-to-date information. You should refer to these documents for the latest information about the appliance. The documents are provided so that you can download and print them at any time.

NetBackup Appliance Documentation page

Logging in to the NetBackup Appliance Shell Menu

The following procedure explains how to log in to the NetBackup Appliance Shell Menu (shell menu).

To log in to the shell menu

1. Connect to the shell menu.
2. Log in by using one of the following methods:

- Username/Password - You can login with a valid username/password.
- Smart card login - If the appliance has been configured and enabled for smart card login, you can log in using smart card. Ensure that you have configured the smart card. For details, see the *NetBackup Appliance Security Guide*.

3 After a successful login, the cursor is alongside the **Main_Menu** prompt.

4 Press the ? key to display the available commands and shell views.

Note: If you log in to the appliance shell menu using the Terminal utility application on an Apple Mac machine, some commands may not work because of a conflict with a locale setting. To avoid this issue, disable the **Set locale environment variables on startup** option in the Terminal application. In an active Terminal session, select **Terminal > Preferences > Profiles > Advanced**. The option appears in the "International" section.

Starting with release 5.0, if Call Home is disabled or not working properly, a warning message appears after login asking users to ensure that Call Home is enabled and working.

- If Call Home is disabled, the following warning message is displayed:

  Warning: It has been detected that you have not enabled Call Home.

  It is strongly recommended that you enable Call Home. Enabling Call Home helps to connect your appliance with the Veritas AutoSupport server and upload software information. Veritas Support uses this information to resolve any issues that you may report.

- If Call Home is not working, the following warning message is displayed:

  Warning: It has been detected Call Home is not working on this appliance.

  It is strongly recommended that you ensure that Call Home is working correctly. Enabling Call Home helps to connect your appliance with the Veritas AutoSupport server and upload software information. Veritas Support uses this information to resolve any issues that you may report.

  To resolve this issue, ensure the system can reach the Veritas Call Home server through correct name resolution or proxy server setting.

Limitations of the NetBackup Appliance Shell Menu

Note the following about the NetBackup Appliance Shell Menu interface:

- The NetBackup Appliance Shell Menu user interface cannot input or modify multi-byte characters, and they are not localized to any language for this release.
- Non-English characters are not shown on the NetBackup Appliance Shell Menu user interface after you finish appliance configuration. This issue occurs when you use the NetBackup Appliance Web Console during the initial configuration of a NetBackup appliance.
- The Secure Shell(SSH) sessions have a limited idle time due to security limits on the Red Hat Enterprise Linux (RHEL) Operating System. You may experience the following issues:
  - The user is logged out automatically if the SSH session remains idle up to the current session time limit.
  - Commands fail to complete if they require more time than the current session time limit. One example where you may experience this issue is when you add a large number of LDAP or AD users and user groups.

  To help avoid these issues, keep the session alive for a longer duration by increasing the session time limit in the SSH client. For detailed configuration instructions, refer to your SSH client documentation.

Command limitations on appliances that are not configured

Before an appliance can be managed, it must first be configured. The commands that are used for initial configuration are the only valid commands that can be executed on a new appliance, or a factory reset appliance. Commands other than those used for the initial configuration can exhibit unexpected or undesired behavior. To prevent this situation, Veritas recommends that you avoid using any management commands until after the appliance initial configuration has been completed.

For information on valid commands for appliances that are not configured, refer to the following documents:

NetBackup Appliance Initial Configuration Guide

NetBackup Appliance Commands Reference Guide

About appliance console components

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

About using the links on the title bar

On the title bar of the NetBackup Appliance Web Console, the **Connected To** value shows the name of the appliance, the hardware model such as 5240, and the role in which it has been configured. In case the appliance is configured as a media server, the primary server that it is connected to is also displayed.

Example: Connected To: Primary 5240: nb-appliance

Here the hostname of the appliance is nb-appliance and it is a 5240 appliance that has been configured as a primary server.

Example: Connected To: Media 5240: nb-appliance | Primary: app-primary

Here the hostname of the appliance is nb-appliance and it is a 5240 appliance that has been configured as a media server. It is connected to a primary server named app-primary.

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

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

- To access online help, click **?**. An enhanced context-sensitive help system is available with the Appliance. The help system is a browser-based Help delivery system with advanced search, autosuggest, and filtering capabilities. The help system lets you search from a much larger appliance content set.
  More information about online Help is available.
  See "Accessing and using help" on page 20.
- To disconnect from the NetBackup Appliance Web Console and to end your session, click **Logout**.
- To see Appliance product version and copyright information, click **About**.

Accessing and using help

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

To access and use the Help system

1. Click **?** on the upper-right corner of the NetBackup Appliance Web Console. This opens a new browser window that displays context-sensitive help for the specific page.
2. You can type the text or phrase that you want to search for, in the text box. You can also type in a query like 'About Appliance', ‘configuring NetBackup Appliance’ etc.

Note: Starting version 3.1, the NetBackup content is no longer available with the Help system.

About using Web browser bookmarks

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

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

Avoiding CSRF (Cross Site Request Forgery)

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

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

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

- If you are currently logged on to the NetBackup Appliance Web Console and try to start a new session from a new tab, only the new session is considered

as current and active. Any task you perform in the older session may display the CSRF error page.

- If you try to access any page with an incorrect security token, a bookmarked old token, or a modified token that does not match the server-side token for the same session, the CSRF error page is displayed.

See "About the NetBackup Appliance Web Console login page" on page 22.

About the NetBackup Appliance Web Console login page

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

Section	Description
Product Information	This section provides the following links where you can access NetBackup appliance information and documentation: ■ **What is new in Version 5.3?** ■ **Release Notes** ■ **Appliance Documentation Set** ■ **View Compatibility Lists** ■ **View Veritas Services and Operations Readiness Tools**

Section	Description
Download Packages	This section indicates whether there are NetBackup client packages stored on the appliance that can be installed on clients. Client packages also include the NetBackup Administration Console. You can select to install all listed client packages or select a specific package to install. Note the following important points about downloading client packages: ■ If you want to store clients on the appliance, a separate client package is available to download. If a client package does not exist on the appliance, the following message appears when you select to download it: `No packages found.` The client packages are posted on the Veritas Services and Operations Readiness Tools (SORT) site (https://www.veritas.com/support/en_US/downloads). Client versions that are stored on the appliance do not have to match the NetBackup version that is currently installed on the appliance. ■ To install the NetBackup Administration Console client, you must first download the Windows client package. This client is required to access the NetBackup Administration Console. ■ You can install the vCentre Plug-in to use vSphere Client to monitor virtual machine backups and recover a virtual machine from a backup.
Browser Recommendation	This section verifies and displays a confirmation if the NetBackup Appliance Web Console supports your browser. This interface works best with Google Chrome 96.0 and later, Microsoft Edge 96.0 and later, and Mozilla Firefox 95.0.2 and later.
Notifications	This section provides notifications or alerts about the current appliance services and components, such as Call Home functionality.

Logging into the NetBackup Appliance Web Console

There are two options for logging in to the Appliance Web Console

- Username/Password - You can login with a valid username/password.

- Smart Card Login - If the appliance has been configured and enabled for smart card login, you can log in using smart card. Ensure that you have configured the smart card. For details, see the *NetBackup Appliance Security Guide*.

To log on to the NetBackup Appliance Web Console

1 Enter the following URL in the web browser:

https://*ip*|*hostname*/appliance

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

Note: If you use Microsoft Edge 96.0 or higher to access the NetBackup Appliance Web Console, security certificate warnings appear when you access a pop-up menu. Select **Continue to this website (not recommended)** to log into the appliance. Once you select this option, the security certificate warnings do not appear on the pop-up menus.

The browser displays the NetBackup Appliance Web Console login page.

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

---

2 To log on with user name and password:

- Enter your user name in the **Username** field. The default user name is **admin**.
- Enter your password in the **Password** field. The default user password is **P@ssw0rd**, where 0 is the number zero.
- Click on **Log in with username and password**, or press the return button of the keyboard.

Note: If you log on as an `AMS` user on the login page on the AMS, you are redirected to the Appliance Management Console. If you log on as an Administrator, you are directed to the NetBackup Appliance Web Console.

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

---

3 To log in with a smart card:

- Ensure that the appliance has been configured and enabled for smart card authentication. Make sure that your smart card is connected to your computer.
- You may be prompted to select a certificate. A pop-up dialog may appear and show certificates that are cached in your browser. Select the certificate you want to use for smart card authentication. You can click **Cancel** if you do not want to log in with a smart card.

  Note: You can use your username and password if you select a certificate.

- If you selected a certificate, click on the **Log in with Smart Card** button. It may take up to 30 seconds to complete the login.

The browser remembers your selection. If you selected a certificate, you can log in again with that same certificate. If you did not select a certificate, you **can** log in with your user name and password. **If you want to change your authentication choice to use a certificate or a different certificate, it is necessary to terminate the browser and start it again. Refer to your browser's documentation.**

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

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

To change the system locale	Details
1. Browse the locales on your system	Log on to the shell menu and run `Settings> SystemLocale List` *`language_code`*. **Example**: Run `Settings> SystemLocale List` *`ja`* to browse the available locales in Japanese language. The following locales can be displayed: ■ ja_JP ■ ja_JP.UTF-8 ■ ja_JP.eucJP ■ ja_JP.eucjp ■ ■ ja_JP.ujis ■ ja_JP.utf8
2. Set the preferred locale along with its format	Run `Settings > SystemLocale Set` *`language_code`* command. **Example**: Run `Settings> SystemLocale Set` *`ja_JP.UTF-8`* to set the `ja_JP.UTF-8` locale to the Appliance.

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

5 Click **Login**.

The appliance displays either of the following:

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

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

- NetBackup Appliance home page - After you have successfully configured your appliance, the **Home** page is displayed. More information about the **Home** page is available.
  See "NetBackup appliance home page" on page 28.

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

Table 1-2 lists the reasons due to which login failure can occur.

Table 1-2 Troubleshooting login failures

Error message	Reasons	Troubleshooting
`User authentication failed. Please enter valid user name and password. If problem persists contact your System Administrator.`	■ If the provided user name and password are 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.
`Login was unsuccessful, click ? for details.`	■ 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 instances of the NetBackup Appliance Web Console. ■ View the UI logs to view the exceptions stack and trace all programmatic statements. You can find the UI logs at the following location: `/log/webgui/webserver`
`The connection has timed out`	If the web server is not responsive the login page is not displayed.	Contact your system administrator for more assistance.
`Unable to connect`	If the web server has been shut down.	Contact your system administrator for more assistance.

NetBackup appliance home page

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

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

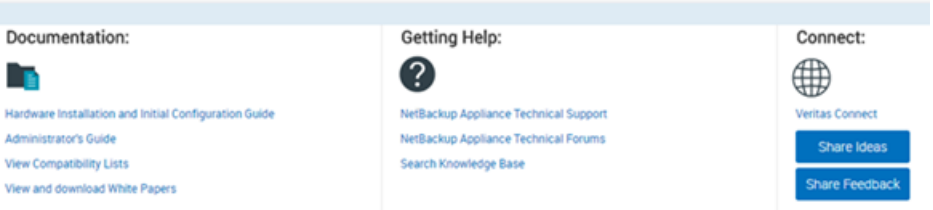
Table 1-3 Home page description

Element	Displays	Helps to	Links to the page
Storage	Displays the used storage space across the appliance. The information is dynamically updated to display the current storage utilization. It displays the **Used** and **Available** space within your storage system and is calculated as follows: ■ **Used** = Sum of used space on all configured partitions. ■ **Available** = Sum of available space on all configured partitions. When you log into the appliance the home page displays the status of the **Used** and **Available** storage space.	Determine the available storage space. It enables you to take the required steps if the storage space has been used to the maximum.	**Manage > Storage** For more information See "Manage > Storage" on page 64.
Deduplication Summary	Displays the current deduplication ratio pertaining to all the backups taken so far across all the media servers.	Determine the quality of the data backed-up using deduplication. Lower the ratio, lower is the amount of data being stored using Deduplication. Deduplication ratio = total number of bytes backed up (without Deduplication) / number of bytes changed and backed up (with Deduplication)	This element is not linked to any specific page. For information on how to set the deduplication parameters See "About configuring deduplication solutions" on page 131.

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

Element	Displays	Helps to	Links to the page
Hardware	Displays the performance of all the monitored hardware devices.	Determine if the hardware is running and a failure has been detected. An error message is displayed, in case a hardware component malfunctions.	**Monitor > Hardware** For more information See "Monitor > Hardware options" on page 36.
Notifications	Displays the latest notifications for your appliance. These notifications include: ■ Latest software updates available for your appliance. It displays the new software updates available on the support site. ■ Connectivity status for the Call Home server ■ NetBackup license key status	Identify the following: ■ Latest software upgrades available from the Support site. ■ If Call Home is functional. ■ Expiring, expired, or missing NetBackup license key.	**Manage > Software Updates** For more information See "Software release updates for NetBackup Appliances" on page 178.

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



Common tasks in NetBackup appliance

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

Table 1-4 Quick links for common appliance tasks

Appliance functions	Tasks	Go to this topic
Monitoring	Monitor hardware, services, and Symantec Data Center Security (SDCS)	See "Monitor > Hardware options" on page 36. See "About hardware monitoring and alerts" on page 35. See "About Symantec Data Center Security on the NetBackup appliance" on page 45.
Managing the appliance	Configure data buffer and deduplication settings of the appliance Add or remove license keys Run migration utility Manage software updates	See "About configuring deduplication solutions" on page 131. See "Configuring data buffer parameters" on page 127. See "Managing license keys on the NetBackup appliance" on page 161. See "Manage > Software Updates" on page 178.
Storage management	Resize or move partitions Add or remove disks View disk status View the partition distribution on a disk	See "About storage configuration" on page 60. See "Manage > Storage" on page 64.
Restoring an appliance	Create a checkpoint Rollback to a checkpoint	See " Manage > Appliance Restore" on page 136.
Configuring appliance settings	Alert and Call Home Network Date and Time User authentication and management Password management	See "About modifying the appliance settings" on page 231.
Troubleshooting	Troubleshoot appliance issues	See "Gathering device logs on a NetBackup appliance" on page 311.

About the NetBackup appliance documentation

The following documents help to ensure that you can successfully install, configure, and use your appliance. In addition, you can find information about the appliance hardware documents from the following table.

All these documents are posted on the NetBackup Appliance Documentation page.

Table 1-5 NetBackup Appliance Software documentation

Guide	Description
NetBackup™ 52xx Initial Appliance Configuration Guide	This document guides you through the 52xx configuration process from the NetBackup Appliance Web Console or from the NetBackup Appliance Shell Menu.
NetBackup™ 53xx Initial Appliance Configuration Guide	This document guides you through the 53xx configuration process from the NetBackup Appliance Web Console or from the NetBackup Appliance Shell Menu.
NetBackup Appliance Upgrade Guide	This document guides you through the required steps to upgrade a NetBackup appliance.
NetBackup™ Appliance Administrator's Guide	The *NetBackup™ Appliance Administrator's Guide* contains the following types of information: ■ Deployment information ■ Administering your appliance ■ Monitoring information
NetBackup™ Appliance Command Reference Guide	The *NetBackup™ Appliance Command Reference Guide* provides a complete list of the commands that are available for you to use through the NetBackup Appliance Shell Menu.
Appliance Management Guide	This document helps you to use the Veritas Appliance Management Console to centrally manage multiple appliances. The Veritas Appliance Management Console provides enterprise-wide monitoring and management of NetBackup appliances. With 3.1 and later, you can manage software upgrades or install EEBs on multiple appliances.
NetBackup Appliance Release Notes	This document contains information about this version of NetBackup Appliance. It contains brief descriptions of new features within the release, operational notes that apply to the release update, and any known issues.

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

Guide	Description
NetBackup Appliance Troubleshooting Guide	This document provides a general overview of how to troubleshoot NetBackup appliance issues and an explanation of the appliance troubleshooting tools and log files. If you need more specific troubleshooting information about a particular issue, go to the NetBackup Appliance page on the Veritas Support website. You can use the search function to look for articles relating to specific issues.
NetBackup Appliance Capacity Planning and Performance Tuning Guide	This document contains information on how to optimize your backup environment and your NetBackup appliance. It helps you to analyze your backup requirements and design a system that best fits your needs.
NetBackup Appliance Security Guide	This document describes the security features in NetBackup Appliance and how to use those features to ensure that your appliance environment is secure.
NetBackup Appliance Fibre Channel Guide	This document describes the supported Fibre Channel (FC) capabilities and configurations for NetBackup appliances.
NetBackup Appliance iSCSI Guide	This document describes how iSCSI works on the NetBackup appliance.
NetBackup Appliance Decommissioning and Reconfiguration Guide	This document describes how to decommission and reconfigure a NetBackup appliance.
NetBackup Appliance SNMP Trap Reference Guide	This document provides a complete list of the NetBackup Appliance SNMP traps. It describes what each trap means and the recommended actions for when an error occurs.
NetBackup Copilot for Oracle Configuration Guide	This document outlines how to configure Copilot using NetBackup and the NetBackup Appliance.
NetBackup Appliance Third-party Legal Notices	The *NetBackup Appliance Third-party Legal Notices* document lists the third-party software that is included in this product, and it contains attributions for the third-party software. This document is available from the following website: https://www.veritas.com/about/legal/license-agreements

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

Guide	Description
NetBackup™ Appliance AutoSupport 2.0 Reference Guide	This document contains the information about the AutoSupport 2.0. It helps you to understand the deployment of the AutoSupport infrastructure, and how does the AutoSupport infrastructure analyzes the Call Home data from each appliances.
NetBackup™ 53xx Appliance High Availability Reference Guide	This document contains the information about the High Availability (HA) solution. It helps you to understand the deployment of the high availability configuration.

Table 1-6 NetBackup Appliance Hardware documentation

Guide	Description
NetBackup™ 5240 Appliance Product Description	This guide introduces you to the NetBackup 5240 Appliance and Storage Shelf.
NetBackup™ 5250 Appliance Product Description	This guide introduces you to the NetBackup 5250 Appliance and Storage Shelf.
NetBackup™ 5340 Appliance Product Description	This guide introduces you to the NetBackup 5340 Appliance and the 5U84 Storage Shelves.
NetBackup™ Appliance Safety and Maintenance Guide	This document provides safety maintenance information for the following hardware: ■ NetBackup 52xx appliances ■ NetBackup 53xx appliances ■ Veritas 3U16 24TB/36TB Storage Shelves ■ Veritas 2U12 49TB Storage Shelf ■ Veritas 5U84 Storage Shelves

Chapter 2

Monitoring the NetBackup appliance

This chapter includes the following topics:

About monitoring the NetBackup appliance

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

Table 2-1 describes the components that you can monitor using the **Monitor** menu:

Table 2-1 Monitor tab

Monitor	Lets you...	Topic
Hardware	Monitor the hardware, the storage devices, and all the components that are associated with them.	See "About hardware monitoring and alerts" on page 35.

Table 2-1 Monitor tab *(continued)*

Monitor	Lets you...	Topic
SDCS Events	Monitor the Symantec Data Center Security (SDCS) events that occur on the appliance. The SDCS agent is installed and configured when you initially configure your appliance. This agent operates in unmanaged mode by default, but can be connected to an external SDCS server to validate and verify your appliance's audit logs.	See "About Symantec Data Center Security on the NetBackup appliance" on page 45.

Appliance monitoring from the System Health Insights portal

System Health Insights is a global appliance monitoring and insights portal that delivers telemetry-driven information to help you understand the health and operational state of your appliances. Use System Health Insights to monitor storage use across appliances, monitor the hardware metrics, and reduce upgrade planning with automatic upgrades. The automatic upgrade feature is available only through System Health Insights. Automatic upgrades are supported for appliances that use software versions 5.3 and later. For complete details, see the *System Health Insights User Guide*.

About hardware monitoring and alerts

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

- Hardware monitoring and alerting from the NetBackup Appliance Web Console.
  See "Monitor > Hardware options" on page 36.
- Sending an email to the local administrator.
  See "About Email notification from a NetBackup appliance" on page 44.
- Sending an alert to the SNMP manager.
  See "About SNMP" on page 241.
- Sending a notification to Veritas using Call Home.
  See "About Call Home" on page 242.

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

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

Monitor > Hardware options

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

The **Monitor > Hardware** page on the NetBackup Appliance Web Console lets you monitor the hardware, the storage devices, and all of the components that are associated with them. If Call Home is enabled, this information is also automatically sent to Veritas Support in the case of a serviceable event. The hardware monitoring information allows Veritas to provide proactive service and helps lead to a faster resolution of any hardware issues.

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

Table 2-2 Hardware components monitored in 52xx appliances

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

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

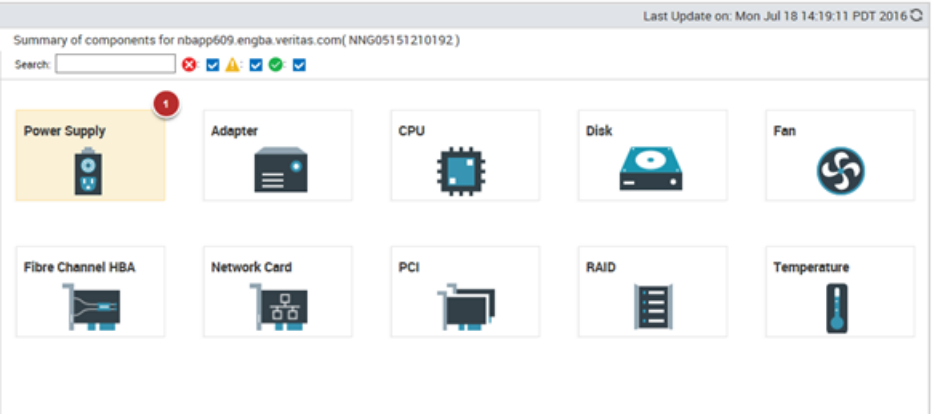


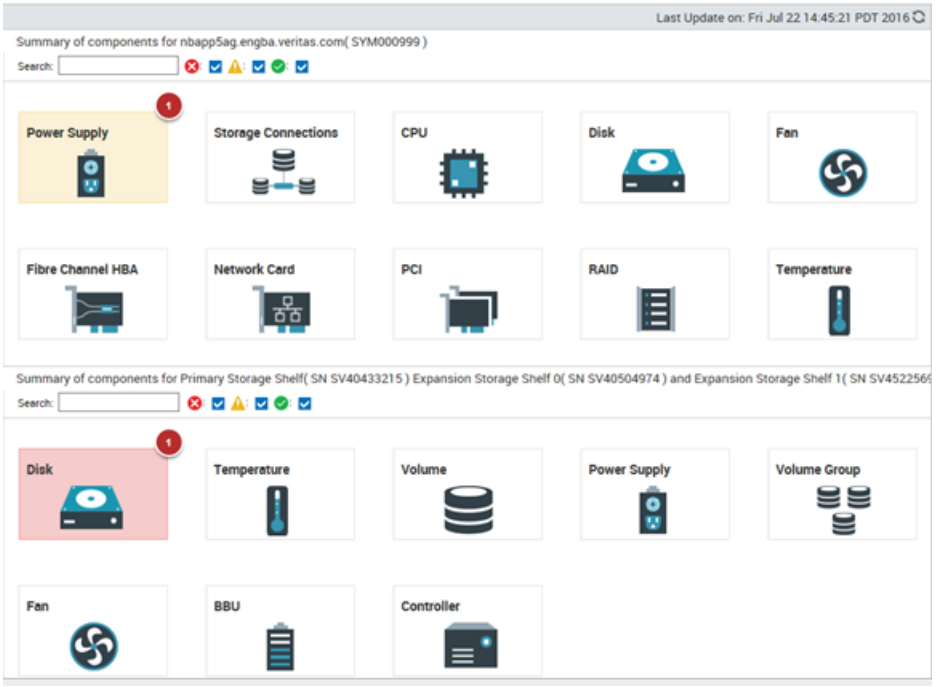
Table 2-3 Hardware components monitored in the 53xx appliance

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

Table 2-3 Hardware components monitored in the 53xx appliance *(continued)*

Primary storage shelf	**Disk**, **Fan**, **Battery Backup Unit (BBU)**, **Controller**, **Volume**, **Volume Group**, **Power Supply**, **Temperature**
Expansion storage shelf	**Disk**, **Fan**, **Power Supply**, **Temperature**

Figure 2-2 Hardware components monitored in 53xx series appliances



The left pane of the **Monitor > Hardware** page lists **Appliance** and **Storage**. The right pane displays the **Summary of components** for the appliance and for the attached storage. The storage devices can include a 52xx storage shelf, a 53xx primary storage shelf, or a 53xx expansion storage shelf. Click on any of the components for further information, including health status and any errors or warnings.

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

Interpreting errors or warnings

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

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

Monitoring storage connections

On a 53xx series appliance, you can view the connections between hardware components to check the connection status. Click **Storage Connections** under **Summary of components for appliance**. The following pop-up window appears:

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

Flashing a beacon

On a 52xx appliance, the **Disk** component for the appliance and the storage shelf includes an option to flash a beacon. The beacon helps to locate a disk within the 52xx appliance or the storage shelf.

On a 5340 appliance, the storage shelves include an option to flash a beacon. When the beacon option is set to flash *Enclosure* the individual disks inside a storage shelf are not flashed. When the beacon option is set to flash an individual disk or a disk group with a WWID, that specific ID is flashed.

Note: For a 5340 appliance, the beacon option is available from the NetBackup Appliance Shell Menu. The option is not available from the NetBackup Appliance Web Console.

To flash a beacon from the Monitor > Hardware page

1 Do the following based on the appliance model:

- For a 52xx appliance, click the **Disk** icon under **Summary of components for appliance** or **Summary of components for storage shelf**.

2 In the pop-up window that appears, select the disk ID that you want to flash and click **Beacon**.

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

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

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

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

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

Hardware components that are monitored

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

Table 2-4 NetBackup 52xx and 53xx appliance hardware that is monitored

Hardware monitored	Data collected
CPU	■ 52xx: **Processor**, **Status**, **Voltage**, **Low Watermark**, **High Watermark**, **BIOS Firmware** ■ 53xx: **Processor**,**Status**, **Voltage**, **Low Watermark**, **High Watermark**, **BIOS Firmware**
Disk	■ 52xx: **Slot number**, **Status**, **HotSpare Type**,**Foreign state**, **Firmware version**, **Serial number**, **Capacity**, **Type**, **Enclosure ID** ■ 53xx: **Slot number**, **Status**, **Foreign state**, **Firmware version**, **HotSpare Type**,**Serial number**, **Capacity**, **Type**, **Enclosure ID**

Table 2-4 NetBackup 52xx and 53xx appliance hardware that is monitored *(continued)*

Hardware monitored	Data collected
DIMM*	■ **Name**, **Status**, **Manufacturer**, **Part Number**, **Serial Number**, **Type**, **Size**, **Speed**, **Uncorrectable Error Count**, **State** **Note:** The **Uncorrectable Error Count** represents the number of times a DIMM has encountered an uncorrectable error. The **Status** column can have values like Uncorrectable Error, Optimal, and Not Populated. Note that if the **Status** is Uncorrectable Error, the **State** of the DIMM is Failed. In this scenario, the DIMM needs to be replaced. If the alerts are configured, you will receive an alert if the DIMM has uncorrectable errors. You can monitor the DIMM from the NetBackup Appliance Shell Menu by running the `Monitor > Hardware ShowHealth Appliance DIMM` command. To reset the uncorrectable error count, run the `Support > Cleanup > ResetDIMMErrors` command. See the *NetBackup Appliance Commands Guide* for reference.
SSD (5250 and 5350)	■ **Device Path**, **Firmware Version**, **Capacity**, **Serial Number**, **Status**, **State**
Fan	■ **Name**, **Status**, **Speed**, **Low watermark**
Power Supply	■ **Status**, **Wattage**, **High watermark**
RAID	■ **WWID**, **Name**, **Status**, **Capacity**, **Type**, **Disks**, **Write policy**, **Enclosure ID**, **Hotspare availability** **Note:** The WWID in the RAID table is a unique device ID of the disk. Clicking a WWID in the RAID table directs you to the **Disk** tab on the **Manage > Storage** page of the NetBackup Appliance Web Console. The console highlights the disk that corresponds to the WWID that is clicked. Clicking the highlighted Disk ID (or the WWID) on the **Manage > Storage** page opens a **RAID status details** window. The RAID details window provides status information about the RAID and the highlighted storage disk.

Table 2-4 NetBackup 52xx and 53xx appliance hardware that is monitored *(continued)*

Hardware monitored	Data collected
Temperature	■ **Type**, **Temperature**, **Low watermark**, **High watermark** **Note:** The temperature readings for the P1 Therm Margin sensor and the P2 Therm Margin sensor are shown as negative values. The negative values indicate how hot (in degrees C) it can get before the CPU reaches the maximum heat tolerance. The low watermark and highwater mark for these sensors is -15 degrees C and -128 degrees C respectively.
Adapter	■ 52xx: **Adapter model**, **Adapter status**, **BBU status**, **Rebuild Rate %**,**BBU Learn Cycle active**, **Charge**, **Charging status**, **Voltage**, **Temperature**, **Manufacturing date** ■ 53xx: N/A
PCI	■ 52xx: **Slot**, **Details** ■ 53xx: **Slot**, **Details**, **Firmware**
Fibre Channel HBA	■ **Status**, **Mode**, **PCI slot**, **Port World Wide Name (WWN)**, **Speed**, **Remote Port** **Note:** Fibre Channel HBA ports that are marked with **Initiator*** mode indicate that they are configured for target mode when the SAN Client Fibre Transport media server is active. However, these ports are currently running in initiator mode, which implies that the SAN Client is disabled or it is inactive.
Network Card	■ **Port name**, **PCI slot**, **Card model**, **Serial number**, **Port speed**, **MAC address**, **Link state**
Storage Connections	■ 52xx: N/A ■ 53xx: **Appliance port**, **Expansion Storage Shelf port**, **Status**

Table 2-4 NetBackup 52xx and 53xx appliance hardware that is monitored *(continued)*

Hardware monitored	Data collected
Storage Status*	■ 52xx: N/A ■ 53xx: **Status** **Note:** The **Storage Status** component monitors the health of the storage array as a whole. If a **Storage Status** error or warning message appears, the error cannot be acknowledged to suppress notifications. If you have Call Home enabled, Veritas is notified of the error, and a Support ticket is opened on your behalf. Veritas Support contacts you shortly afterward. If you do not have Call Home enabled and you receive a **Storage Status** error, contact Veritas Support for assistance.
Partition Information*	■ **Partition**, **Total size**, **Used percentage**, **Status** **Note:** In the MSDP partition, the value that is displayed for the **Used** space may be different from the backup space that is available or used on the MSDP partition. The backup space statistics for the MSDP partition can be obtained by checking the MSDP disk pool sizes from the NetBackup Administration Console.
MSDP*	■ **Queue size**, **Oldest tlog creation date**

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

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

Hardware monitored	Data collected
Disk	■ **Slot number**, **Status**, **Foreign state**, **HotSpare Type**,**Firmware version**, **Serial number**, **Capacity**, **Type**, **Storage shelf ID**
Fan	■ **Name**, **Status**, **Speed**, **Low watermark**
Power Supply	■ **Status**

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

Hardware monitored	Data collected
Temperature	■ **Type**, **Temperature**, **High watermark** Temperature monitoring includes the following temperature sensors that are located on the storage shelf: ■ I/O Module1 (1) ■ I/O Module1 (2) ■ I/O Module2 (1) ■ I/O Module2 (2) ■ Backplane1 ■ Backplane2 ■ PSU1 (1) ■ PSU1 (2) ■ PSU2 (1) ■ PSU2 (2)

Table 2-6 53xx Primary Storage Shelf hardware that is monitored

Hardware monitored	Data collected
Disk	■ **Location**, **Status**, **Capacity**, **Associated Volume Group**, **Firmware version**, **Serial number**
Fan	■ **Location**, **Status**
Power Supply	■ **ID**, **Location**, **Status**
Temperature	■ **Location**, **Status**
BBU	■ **Location**, **Status**
Controller	■ **Location**, **Status**, **Data Cache**, **Controller Firmware**, **NVSRAM Firmware**
Volume	■ **LUN**, **Status**, **Associated Volume Group**, **WWID**, **Capacity**
Volume Group	■ **Volume Group name**, **Status**, **Associated Volume Group**, **RAID level**, **Capacity**, **Disks**

Table 2-6 53xx Primary Storage Shelf hardware that is monitored *(continued)*

Hardware monitored	Data collected
Storage Connections	■ **Primary Storage Shelf port**, **Expansion Storage Shelf port**, **Status** **Note:** This option is only displayed under the Primary Storage Shelf from the NetBackup Appliance Shell Menu. On the NetBackup Appliance Web Console, the connections information is included in the **Storage Connections** icon under the appliance.

Table 2-7 53xx Expansion Storage Shelf hardware that is monitored

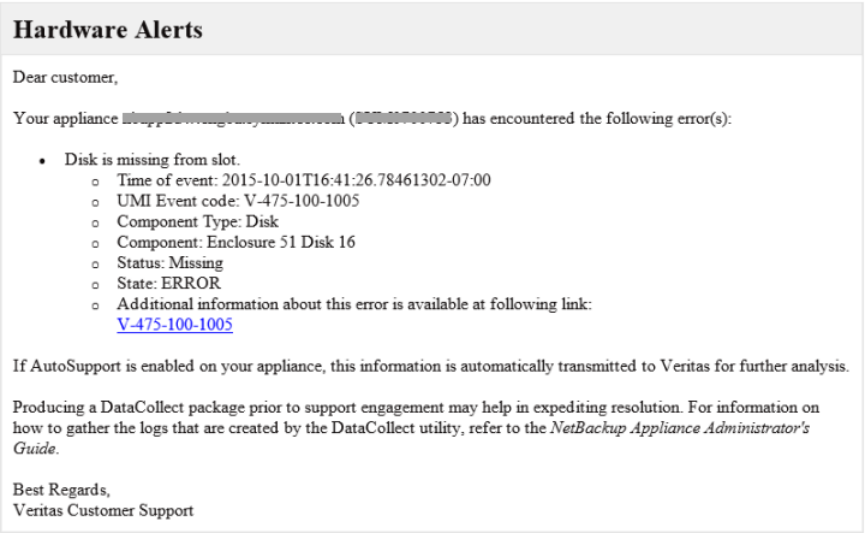
Hardware monitored	Data collected
Disk	■ **Location**, **Status**, **Capacity**, **Associated Volume Group**, **Firmware version**, **Serial number**
Fan	■ **Location**, **Status**
Power Supply	■ **Location**, **Status**
Temperature	■ **Location**, **Status**

About Email notification from a NetBackup appliance

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

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

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



Hardware Alerts

Dear customer,

Your appliance [redacted] has encountered the following error(s):

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

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

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

Best Regards,
Veritas Customer Support

About Symantec Data Center Security on the NetBackup appliance

Note: After an upgrade, the appliance SDCS agent is automatically set to unmanaged mode. If an appliance was running in managed mode before upgrade, make sure to reset that appliance back to managed mode after the upgrade is completed.

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

Symantec Data Center Security: Server Advanced (SDCS) is a security solution offered by Symantec to protect servers in data centers. The SDCS software is included on the appliance and is automatically configured during appliance software installation. SDCS offers policy-based protection and helps secure the appliance using host-based intrusion prevention and detection technology. It uses the least-privileged containment approach and also helps security administrators centrally manage multiple appliances in a data center. The SDCS agent runs at startup and enforces the customized NetBackup appliance intrusion prevention

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

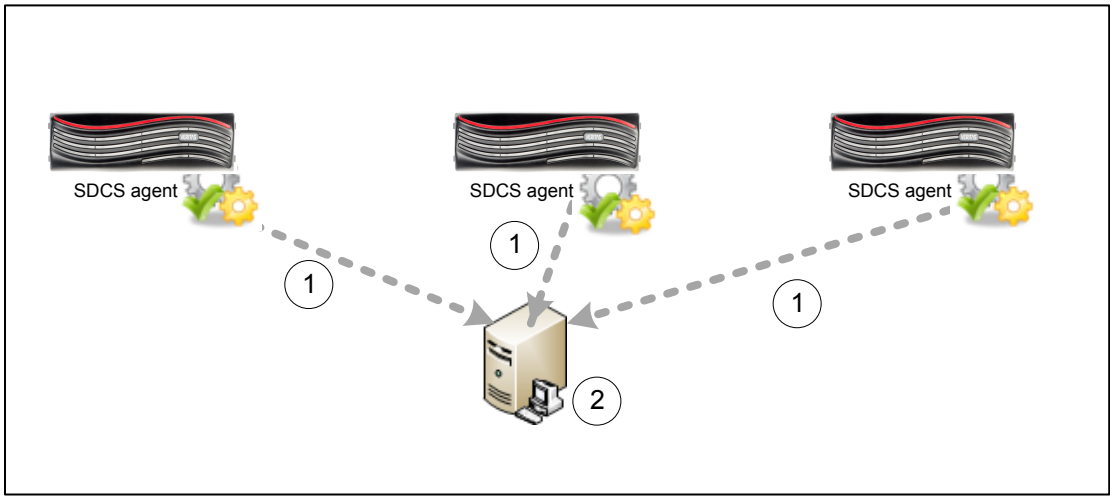
- Hardened Linux OS components
  Prevents or contains malware from harming the integrity of the underlying host system as a result of OS vulnerabilities.
- Data protection
  Tightly limits appliance data access to only those programs and activities that need access, regardless of system privileges.
- Hardened appliance stack
  Appliance application binaries and configuration settings are locked down such that changes are tightly controlled by the application or trusted programs and scripts.
- Expanded detection and audit capabilities
  Provides enhanced visibility into important user or system actions to ensure a valid and complete audit trail that addresses compliance regulations (such as PCI) as a compensating control.
- Centralized managed mode operations
  Lets you use a central SDCS manager for an integrated view of security across multiple appliances as well as any other enterprise systems managed by SDCS.

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

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

Figure 2-3 illustrates SDCS in managed mode.

Figure 2-3 SDCS implementation in managed mode



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

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

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

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

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

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

Monitor > SDCS Events

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

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

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

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

Note: If you need the SDCS console and server software, you can download them from https://my.veritas.com.

Note: You can manually implement third-party certificates on web service support using the Java keystore repository of security certificates.

Table 2-8 describes the event attributes for each sortable column of the SDCS event viewer.

Table 2-8 SDCS event attributes

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

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

Columns	Description
Severity	The severity of each event in the log. For example, an event like the **Server Error** would be of **Critical** severity. The following severity types are displayed: ■ **Information** - Information about normal system operation. ■ **Notice** - Information about normal system operation. ■ **Warning** - Unexpected activity or problems that have already been handled by SDCS. These events might indicate that a service or application on a target computer is functioning improperly with the applied policy. After investigating the policy violations, you can configure the policy and allow the service or application to access the specific resources if necessary. ■ **Major** - Activity with more effect than **Warning** and less effect than **Critical**. ■ **Critical** - Indicates activity or problems that might require administrator intervention to correct.
Message	The message that describes the logged event.
Details	Details of each logged event. Click the **Log Details** pop-up window icon to view the details of the logged event. For a list of all the possible details that can be deisplayed, refer to the SDCS documentation.

Viewing SDCS audit log details

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

You can view the detailed information for each Symantec Data Center Security (SDCS) logged event using the `Main_Menu > Monitor > SDCS > Audit View` command. Table 2-9 describes the various details that displayed in the command output.

Table 2-9 SDCS log details description

Detail	Description
Event Severity	The severity of the logged event. The following severity types are displayed: ■ **Information** - Information about normal system operation. ■ **Notice** - Information about normal system operation. ■ **Warning** - Unexpected activity or problems that have already been handled by SDCS. These events might indicate that a service or application on a target computer is functioning improperly with the applied policy. After investigating the policy violations, you can configure the policy and allow the service or application to access the specific resources if necessary. ■ **Major** - Activity with more effect than **Warning** and less effect than **Critical**. ■ **Critical** - Indicates activity or problems that might require administrator intervention to correct.
Process ID	The ID assigned to the process.
Rule Name	The name of the policy rule that generated the event.
Process	The name of the policy applied to the agent that triggered the event.
Event Date	The date and time (YYYY-MM-DD HH:MM:SS) that the event occurred.
Event Type	The event type for the logged event. For a detailed list of all the event types and their descriptions, refer to the SDCS documentation.
Sequence Number	The sequence number of the logged event.
Event Priority	The priority (0-100) assigned to the event.
Facility	The login mechanism for the event.
Description	The detailed or consolidated description of the event.
User Name	The name of the user that was logged in when the event took place.
File Name	The path and name of the affected file.
New Size	The size of the affected file after the logged event.
Old Size	The size of the affected file before the logged event.
Operation	The type of operation that was performed on the affected file.

Filtering SDCS audit logs

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

To filter SDCS audit logs

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

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

   The **Filters** dialog box is displayed.
4. Use the following fields to enter the filter criteria:

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

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

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

Setting the SDCS audit log retention specification

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

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

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

To set the audit log retention

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

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

   ---

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

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

5 You can set the retention using the following fields:

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

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

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

About Symantec Data Center Security Downloads

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

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

- A management server running the Symantec Data Center Security: Server Advanced 6.5 or later.

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

If you need the SDCS console and server software, you can download them from https://my.veritas.com.

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

Downloading the IPS and IDS policies from the NetBackup appliance

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

To download NetBackup appliance IPS and IDS policies:

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

   The `SDCSSPolicies.zip` file is downloaded to your local folders.
4. Extract the contents from the `SDCSSPolicies.zip` file.

   The `SDCSSPolicies` folder contains the following:

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

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

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

See "Connecting to the SDCS server" on page 55.

For instructions on how to apply policies using the SDCS management console, refer to the *Symantec Data Center Security: Server Advanced Administrator's Guide* at the following location: http://www.symantec.com/docs/DOC7979

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

Connecting to the SDCS server

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

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

To connect an SDCS server

1 Log in to the NetBackup Appliance Web Console.

2 Click **SDCS Events**.

3 Under **Connect to SDCS server**, click **Connect**.

The **Connect to SDCS Server** dialog box appears.

4 Enter a valid host name or IP address of the SDCS server in the **Host Name / IP** field.

5 Enter the port number of the SDCS server in the **Port** field.

6 Select either **Download authentication certificate from the SDCS server** or **Provide the location for the existing certificate**.

The appliance displays the certificate details.

7 Click on **Accept Certificate** to accept the certificate.

The appliance displays the **Certificate issued** message.

8 Click **Connect** to connect to the SDCS server.

The appliance has connected to the SDCS server successfully when the following message appears:

Connected successfully to SDCS server.

Revert SDCS to unmanaged mode on a NetBackup appliance

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

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

1 Log in to the NetBackup Appliance Web Console.

2 Click **Monitor > SDCS Events**.

3 Under **Connect to SDCS server**, click **Connect**.

The **Connect to SDCS Server** dialog box appears.

4 Enter **127.0.0.1** or **localhost** in the **Host Name / IP** field.

5 Enter the port number of the appliance in the **Port** field.

6 Click **Connect**.

The appliance reverts to the unmanaged mode.

Chapter 3

Managing a NetBackup appliance from the NetBackup Appliance Web Console

This chapter includes the following topics:

About the Manage views

The NetBackup Appliance enables you to use the NetBackup Administration Console to manage your clients, create policies, run backups, and perform other administration functions. For information on how to perform these functions from the NetBackup Administration Console, you must refer to your NetBackup core documentation set. If you want to download the latest versions of this documentation set, you can do so from the Support website. For help using the NetBackup Administration Console, refer to the *NetBackup Administrator's Guide, Volume I* on the Support website.

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

Table 3-1 describes the tabs included in the **Manage > Host** menu:

Table 3-1 Manage > Host

Manage	Lets you...	Topic
Data Buffer	Configure the data buffer parameters using Data Buffer tab in the NetBackup Appliance Web Console.	See "Manage > Host > Data Buffer options" on page 125.
Lifecycle	View and change the lifecycle parameters using this tab when the appliance is configured as a primary server.	See "Manage > Host > Lifecycle options" on page 127.
Deduplication	View and change the deduplication parameters using this tab.	See "About configuring deduplication solutions" on page 131.
Advanced	Enable Bare Metal Restore (BMR) from this tab when the appliance is configured as a primary server.	See "About BMR integration" on page 134.
IPMI	Reset the IPMI. The reset operation involves restarting the IPMI.	See "Manage > Host > IPMI options" on page 135.

Table 3-2 describes the **Manage > Storage** menu:

Table 3-2 Manage > Storage

Manage	Lets you...	Topic
Capacity Distribution section	View a graphical representation of the storage partitions within your appliance. The donut chart shows the storage partitions that are configured.	See "Manage > Storage" on page 64.
Capacity Chart section	View an overview of storage capacity usage ranges for specific periods of time.	
Partitions section	View details about all the partitions that are configured on the Appliance.	
Disks section	View a tabular representation of the storage disks that comprise your appliance and the storage shelves that are attached to it.	

Table 3-3 describes the **Manage > Migration Utility** menu:

Table 3-3 Manage > Migration Utility

Manage	Lets you...	Topic
Configure Migration	Select the start time, the migration window (duration), the source disk pool where the current backup images reside, and the destination (target) disk pool where you want the images migrated.	See "About the Migration Utility" on page 164.
Migration Job Status	View the status and the result of all the scheduled migration jobs.	

Table 3-4 describes the individual following sub-menus under the **Manage** menu:

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

Manage	Lets you...	Topic
Appliance Restore	Reset the appliance to a specific state. That state can be a state that is determined through the use of checkpoints.	See " Manage > Appliance Restore" on page 136.
License	Review, add, and delete license keys through the administrative web UI.	See "Manage > Appliance License " on page 160.

Table 3-4 Manage > Appliance Restore, License, Software Updates, Additional Servers, Certifications, File Manager *(continued)*

Manage	Lets you...	Topic
Software Updates	View, install, or delete a software update on your appliance. This screen contains two tables that show the software updates that are available for you to download for your appliance and the software updates that you can choose to install or delete. This screen also displays the NetBackup Appliance software version that is currently installed on your appliance.	See "Software release updates for NetBackup Appliances" on page 178.
Additional Servers	Add or delete additional servers. This tab lets you add an entry to the NetBackup `bp.conf` file. The `bp.conf` file allows communication to occur between the appliance and the Windows NetBackup Administration Console, so you can manage your appliance through that console. **Note:** This tab is only displayed for an appliance configured as a primary server.	See "Manage > Additional Servers" on page 194.
File Manager	Manage all uploaded files on the appliance. You can upload certificate files and other similar files.	See "Manage > File Manager" on page 196.

About storage configuration

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

The NetBackup 52xx appliances are available for use with up to four storage shelves. The storage shelves provide you with additional disk storage space. After you have physically connected the storage shelves, use the NetBackup Appliance Web Console to manage the storage space.

The NetBackup 53xx appliance must be connected to one Primary Storage Shelf. The storage space can be expanded by using up to five Expansion Storage Shelves. After you have physically connected the Expansion Storage Shelf, use the NetBackup Appliance Web Console to manage the storage space.

Note: The 53xx appliance (base unit) does not have internal disk space available for backups or storage. It only stores the OS, logs, checkpoints etc. The space available from the Primary Storage Shelf and the Expansion Storage Shelf can be used for backups.

If you have NetBackup 53xx appliances with an Expansion Storage Shelf, the following restrictions apply:

- Moving an Expansion Storage Shelf or disks from one 5340 appliance to another 5340 appliance is not supported.
- Moving an Expansion Storage Shelf or disks from one 5350 appliance to a 5340 appliance is not supported.
- Moving disk drives within an Expansion Storage Shelf is not supported.

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

Figure 3-2 provides a bird's-eye view of how storage space is configured within your 5340 appliance.

Figure 3-1 NetBackup 52xx Appliance storage space

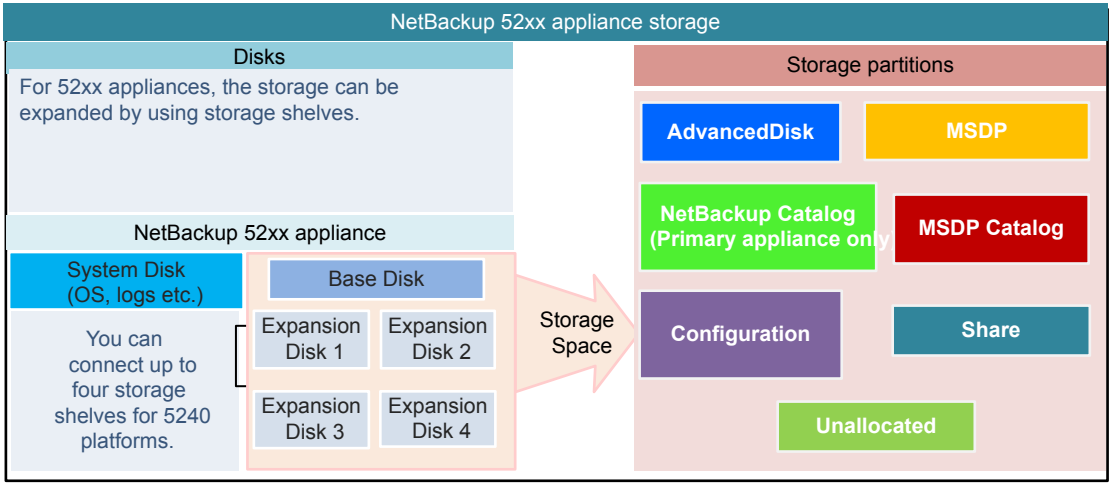


Figure 3-2 NetBackup 5340 Appliance storage space

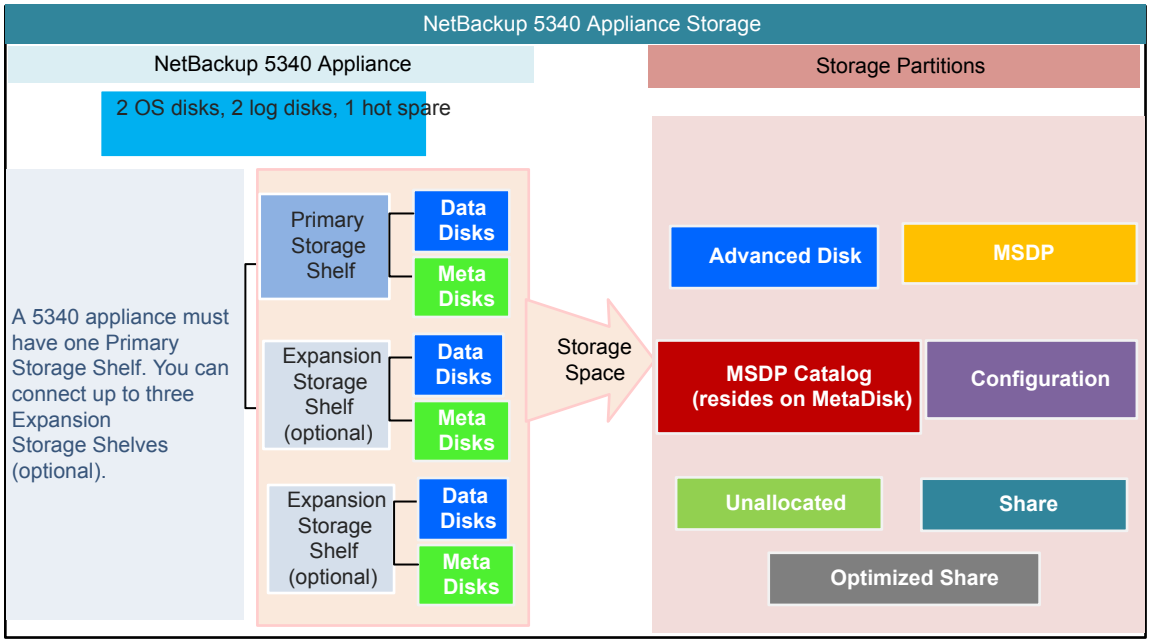
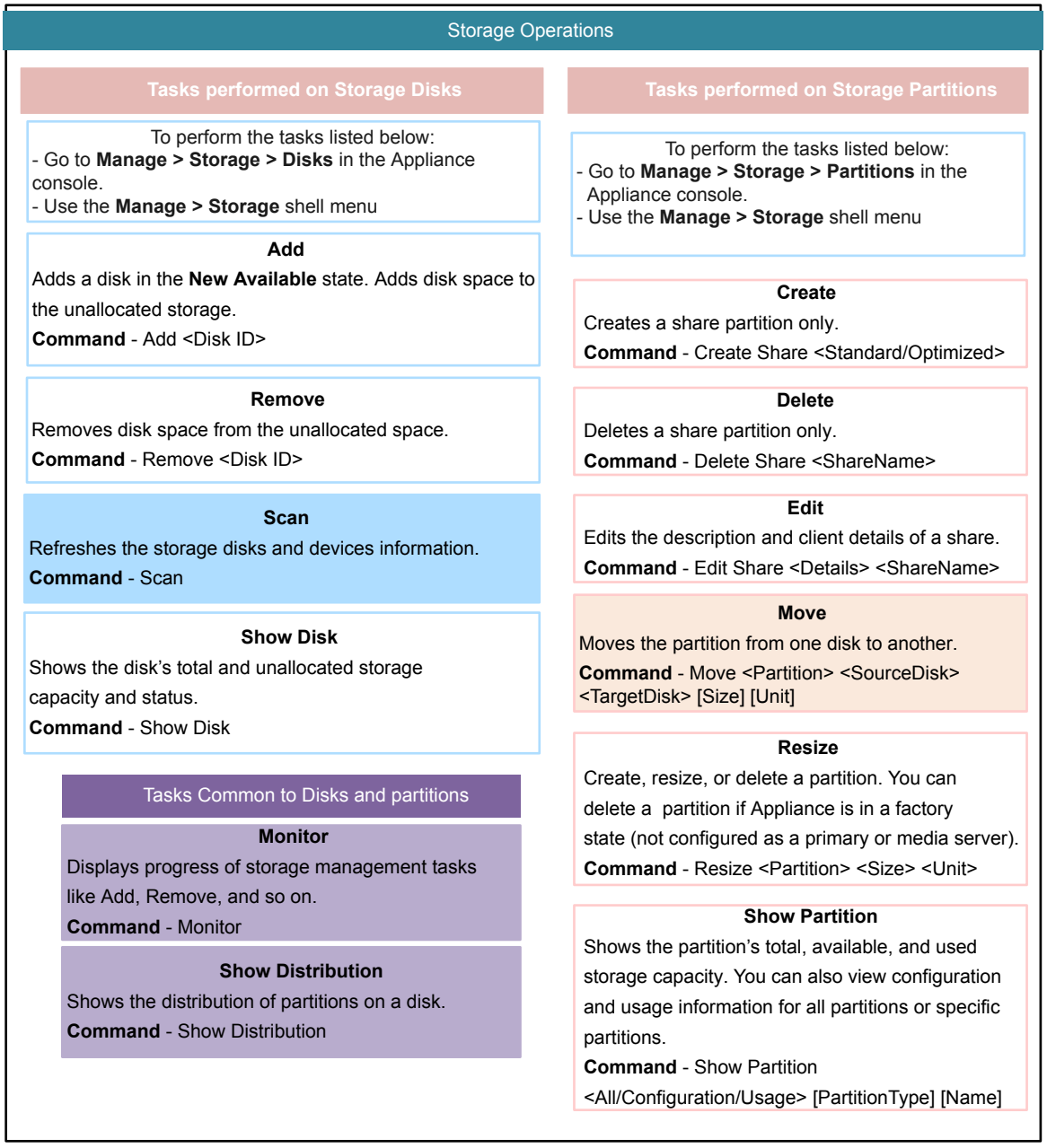


Figure 3-3 lists the tasks that you can perform on the appliance storage space.

Figure 3-3 Storage Operations



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

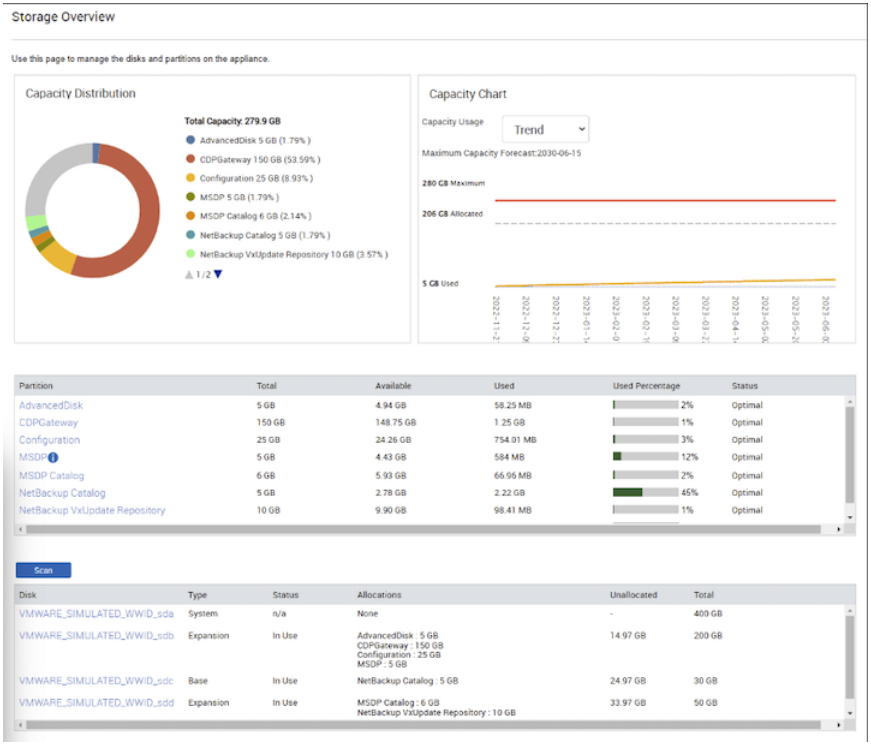
For more information about `Main > Manage > Storage` commands, refer to *NetBackup™ Appliance Command Reference Guide*.

Manage > Storage

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

Figure 3-4 shows an example of the **Manage > Storage** page for a 52xx appliance.

Figure 3-4 Storage Overview example



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

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

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

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

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

CDPGateway A CDPGateway partition lets you rapidly make copies of backups for VMware virtual machines (VMs) ,without stunning the VMs. You can make recent copies of backups and use NetBackup to retain and restore the backups as required.

To create a CDPGateway partition, log in to the NetBackup Appliance Shell Menu and use the `Manage > Storage > Create` command. For complete details, see the *NetBackup Appliance Commands Reference Guide*.

NetBackup Catalog This partition contains metadata for NetBackup which includes information regarding backups, storage devices, and configuration. The NetBackup Catalog partition can reside only on a Base disk of a NetBackup 52xx appliance primary server.

Note: To ensure good backup and recovery performance, Veritas recommends as a best practice that you keep the catalog size under 4 TB. The size of the environment and the length of backup image retention may cause catalogs to grow in excess of 4 TB. A catalog size beyond 4 TB is not an issue for NetBackup. However, operational issues may result for the environment with regard to the time it takes to perform backups and recoveries. In the event of a disaster, the catalog size also directly affects the recovery time of the environment.

Configuration A storage partition that stores configuration information.

MSDP	The allocated space for Media Server Deduplication (or MSDP) on your appliance. On 52xx appliances, the MSDP partition should reside on an expansion disk for optimum performance. See "Moving the MSDP partition from a base disk to an expansion disk for optimum performance" on page 82.
MSDP Catalog	This partition contains metadata for MSDP which includes information regarding MSDP backups. On the 52xx appliances, the MSDP Catalog partition can either exist on the base or the expansion disk. On a 53xx appliance, the MSDP Catalog partition is located on a dedicated disk that called the Metadisk. The Metadisk contains the MSDP Catalog partition only.
NetBackup VxUpdate Repository	This partition is used to store downloaded VxUpdate formatted packages of NetBackup clients, NetBackup add-on packages, and EEBs or hotfixes for NetBackup clients.
NDMP Log	This partition contains logs that are generated when NDMP is enabled during the backup operation. The NDMP Log partition is only available to a physical appliance media server. The NDMP Log partition size is fixed and cannot be resized.
Standard Share	This partition contains all of the shares that have been allocated for database backups (Copilot).
Optimized Share	This partition contains all of the optimized shares that have been allocated for database backups (Copilot).
Unallocated	The storage space that has not been allocated to the other partitions (includes all partitions that are displayed except Unallocated). When you expand the storage space for partitions like MSDP, AdvancedDisk, it is used from the Unallocated space. When you add a disk, the size of the Unallocated space increases. The size of the MSDP, AdvancedDisk, and any other partition remains the same.

See the NetBackup documentation for more information on partitions.

Table 3-5 lists the supported sizes and platforms for each partition.

Table 3-5 Appliance storage partitions

Partition Name	Minimum supported size	Maximum supported size	Supported platforms
AdvancedDisk	1 GB	Maximum available capacity	52xx 53xx
CDPGateway	101 GB	Sum of remaining space	5250, 5350
NetBackup Catalog	250 GB (Primary server)	Maximum available Base disk capacity (Primary server)	52xx (primary server only)
NetBackup VxUpdate Repository	100 GB	Maximum available capacity	52xx (primary server only)
NDMP Log	100 GB (Media server)	Maximum available capacity	52xx 53xx
Configuration	100 GB	500 GB	52xx 53xx
MSDP	10 GB	Maximum available capacity	52xx
	10 GB	960 TB	53xx
MSDP Catalog	5 GB	25 TB	52xx, 53xx
Standard Share (Copilot)	5 GB	Maximum available capacity The limit for each individual share is 250 TB	5240, 5250, 53xx
Optimized Share (Copilot)	5 GB	114 TB or 228 TB	53xx
Universal Share	5 GB	Maximum available capacity	52xx 53xx

Note: To view the exact numbers for supported sizes, see the *NetBackup Appliance Product Description Guide* for the appropriate model.

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

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

Note: The sizes that are displayed for the MSDP partition on the **Manage > Storage** page or by using the **Manage > Storage > Show** command on the NetBackup Appliance Shell Menu may not be the full space that is available or used by the MSDP partition. This is because space is reserved by the file system and also by MSDP. The file system reserves space for it's own use. In addition, MSDP reserves 4 percent of the storage space for the deduplication database and transaction logs. For more information, see the *NetBackup Deduplication Guide*

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

Table 3-6 describes the various partition status that is displayed next to the partition type.

Table 3-6 Partition Type Status

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

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

Table 3-7 describes the various partition states.

Table 3-7 Partition Name Status

Status	Description
Mounted	The partition is currently mounted.
Not Mounted	The partition is not currently mounted. If the partition is not mounted, the status can either be Degraded or Not Accessible. See Table 3-6 for more information.
I/O Error	There is an I/O error with the partition. If the partition has an I/O error, the status can either be Degraded or Not Accessible. See Table 3-6 for more information.

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

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

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

If you want to expand storage and attach a storage shelf or an expansion system to an appliance, see the *NetBackup Appliance Hardware Installation Guide* for the appropriate model. Once these storage shelves or expansion systems are properly connected to the appliance, you must scan for the newly available disks from the **Disks** section. The new disks have the **New Available** status. Once the newly

available disks are displayed, these disks must be added so the additional space can be used.

See “Adding the storage space from a newly available disk” on page 92.

The following columns are displayed in the table:

Column names	Description
Disk	Displays the ID that is associated with the disk. **Example:** 50001FAFA000000F5B0519CB4
Type	Displays the type of disk. **Example:** Base Table 3-8 describes each disk type.
Status	Displays the status of the disk. **Example:** In Use Table 3-9 describes each status.
Allocations	Lists the partitions that exist on each disk. Also lists the size of each partition. **Example:** AdvancedDisk: 18 TB
Unallocated	Displays the available space within the disks. **Example:** 1.9172 GB
Total	Displays the total storage space within the disk. **Example:** 4.5429 TB

Table 3-8 lists the disk types that can appear depending on your appliance model.

Table 3-8 Disk Types

Type	Description	Supported Platforms
System	This category tells you the storage that is occupied by the appliance operating system, logs etc.	52xx 53xx
Base	This category tells you the storage that is available with the appliance base unit.	52xx
Expansion	A storage shelf that is connected to a 52xx appliance.	52xx

Table 3-8 Disk Types *(continued)*

Type	Description	Supported Platforms
Data	All partitions, except MSDP Catalog, exist on the Data disk. Examples of partitions that exist on the data disks are MSDP, AdvancedDisk, Configuration, etc. There can be six data disks for a Primary Storage Shelf and six for an Expansion Storage Shelf.	53xx
Meta	The MSDP Catalog partition exists only on the Meta disk. There can be one Meta disk for a Primary Storage Shelf and one for an Expansion Storage Shelf.	53xx
Unknown	This category appears when appliance cannot determine the disk type like when the disk is not accessible.	Not Applicable

Table 3-9 describes the various status that is displayed in the **Status** field.

Table 3-9 Disk Status

Status	Description
Foreign	Denotes that the disk has storage configuration information, and may contain data. The **Remove** link is displayed next to all **Foreign** disks. You can remove any pre-existing data from a **Foreign** disk. After you remove a **Foreign** disk, the status of the disk is **New Available**. Disk status is displayed as **Foreign**, when: ■ A disk that was **In Use** was physically disconnected, later reconnected. In this case, restarting the appliance would bring the disk status back to its previous state. ■ A disk that was **In Use** was physically disconnected. The Appliance was reimaged and reconfigured and the disk is connected back. Or ■ A disk that was connected to another system still has configuration information of the old system
In Use	Denotes that the disk is currently in use. The **Remove** link is displayed if the disk does not have any partition.

Table 3-9 Disk Status *(continued)*

Status	Description
n/a	Denotes that no commands or operations can be performed on disks with this status. An example of a disk that has an n/a status is System. An example of a disk that has an n/a status is Operating System.
New Available	Denotes that the disk is available to be added to the storage space. The **Add** link is displayed to add the storage disk to the storage space.
Not Accessible	Storage disk that was **In Use** is not accessible any more.

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

Manage > Storage > Shares

The **Manage > Storage > Shares** page enables you to view and manage your Shares.

Share summaries

The top portion of the page displays a Share summary in the following ways:

Total Shares The total number of Standard Shares and Optimized Shares on the appliance.

By Share Type The types of Shares on the appliance.

Optimized Share Reserve Displays a summary of the following:

- **Total** - The maximum size of the Optimized Share Reserve.
- **Allocated** - The amount of space currently used.
- **Unallocated** - The amount of space currently unused.

Standard Shares Displays a summary of the following:

- **Total** - The amount of space currently used.
- **Total Unallocated** - The maximum size available for Share creation.

Share operations

From this page you can perform the following actions:

- Create Shares
  See "Creating a Share" on page 98.
- Create Optimized Share Reserve
  See "Creating the Optimized Share Reserve" on page 105.
- Delete Optimized Share Reserve
  See "Deleting the Optimized Share Reserve" on page 106.
- Move Shares
  See "Moving a Share" on page 104.
- Edit Shares
  See "Editing a Share" on page 101.
- Delete Shares
  See "Deleting a Share" on page 103.

Share list

Clicking on a Share opens a pane where you can view all of the Share details, as well as edit or delete the Share.

The Shares page displays details about all the Shares that are configured on the appliance. The following columns are displayed in the Share table:

Column Name	Description
Share Name	Displays the name of the share. **Example:** share1234
Share Type	Displays the type of the share. **Example:** Optimized
Total	Displays the total space that is allocated to the share. **Example:** 3 TB
Available	Displays the free space within the total share capacity. **Example:** 1.90 TB
Used	Displays the used space within the total share capacity. **Example:** 2.10 TB

Column Name	Description
Used Percentage	Displays the percentage of used space in the share. **Example:** 2%

Share details pane

Click any Share from the share section to go to open the Share details pane. The following information is displayed:

Detail	Description
Share Name	Displays the name of the share. **Example:** share1234
Application	Displays the type of application being exported on this share. **Example**: Oracle
Storage Layout	Displays the type of share. **Example:** OPTIMIZED
Description	Displays the description of the share that was provided during share creation. **Example:** This share is dedicated to Oracle.
Capacity Details	Displays the capacity details for the share using the following details: ■ **Total** - The total space that is allocated to the share. ■ **Available** - The free space within the total share capacity. ■ **Used %** - The percentage of used space in the share.
Location on Disk	Displays the location of the share using the following details: ■ **Shelf** - The ID of the storage shelf. ■ **Disk ID** - The ID of the disk.
Clients	Displays the clients that connect to the share using the following details: ■ **Client** - The name of the client. ■ **Options** - The options that are provided for the client.
Instructions	Displays the instructions for how to mount the share on the server.

See “About Copilot functionality and Share management” on page 96.

See “About Optimized Shares and the Optimized Share Reserve” on page 98.

Refer to the *NetBackup™ Copilot™ for Oracle Configuration Guide* for more information on configuring Oracle database backups.

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

About Universal shares migration

Starting with NetBackup Appliance 5.0, the NetBackup Appliance Web Console does not support Universal Shares. You cannot create, modify, view or delete the Universal Shares from the NetBackup Appliance Web Console. You can use the NetBackup Web Console to manage the universal shares.

The Universal Shares interface has been removed from the NetBackup Appliance Web Console.

Refer to the *NetBackup Web UI Administrator's Guide* to create, modify, view, and delete NFS and CIFS (SMB) shares.

If you upgrade to NetBackup Appliance 5.0 from previous versions and if NFS or CIFS shares are already created using the NetBackup Appliance Web Console, the shares will be migrated from the NetBackup Appliance to NetBackup during upgrade. After upgrade, the old universal shares will be managed by NetBackup.

If the migration of universal shares fails during upgrade, contact Veritas Support to migrate the remaining shares manually to NetBackup.

About NFS Kerberos Universal shares

Starting with appliance release 5.3, the use of NFS Kerberos Universal shares is supported, including for high availability (HA) setups. For complete configuration details, see the following article:

https://www.veritas.com/support/en_US/article.100060273.html

Checking partition details

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

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

the past storage capacity usage, and calculates when the available storage is fully used.

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

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

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

Table 3-10 Operations to manage the appliance storage partitions

Operation	Description	Partition
`Resize`	Creates, resizes, or deletes a selected partition. Review the following considerations: ■ You can create a partition using Resize only if the Appliance is configured as a primary or a media server. ■ You can resize a partition to a higher or lower value depending on the type of partition. The size is expanded by using the unallocated space. ■ You can delete a partition using Resize only if the Appliance is in a factory state (when it is not configured as a primary server or a media server). See "Resizing a partition" on page 77. See "Resize dialog" on page 79.	■ AdvancedDisk ■ Configuration ■ MSDP ■ Share (NetBackup Appliance Shell Menu only) ■ MSDP Catalog ■ NetBackup Catalog

Table 3-10 Operations to manage the appliance storage partitions *(continued)*

Operation	Description	Partition
`Move`	Moves the selected partition from a source disk to the destination disk. See "Moving a partition" on page 81.	■ AdvancedDisk ■ Configuration ■ MSDP ■ Share (NetBackup Appliance Shell Menu only) ■ MSDP Catalog **Note:** The NetBackup Catalog partition cannot be moved. **Note:** On a 53xx appliance, the MSDP Catalog partition exists on its own metadisk and can only be moved between metadisks (if applicable).

Resizing a partition

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

Starting with release 4.0, you can resize the VxUpdate repository upward from its minimum of 100 GB. The maximum size of the partition is dependent on the amount of all unallocated storage.

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

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

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

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

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

Review the following points before you resize a storage partition:

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

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

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

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

Note the following when expanding partitions:

- Make sure that the MSDP volume is larger than 10GB. Partitions smaller than 10GB or less than 1/100 of the average MSDP volume are not supported.
- If the available disk space is more than 10GB, a message informs you that the partition has been expanded.
- If the available disk space is less than 10GB, the process checks for the next disk in the storage array with more than 10GB of free space. A message informs you that the partition has been expanded.
- If no disks have more than 10GB of available space, a message informs you of the maximum available space and allows you to expand the partition to the smaller size.

The following procedure describes how to resize partitions.

To resize a storage partition

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

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

See “Resize dialog” on page 79.

6 The progress details are displayed when you resize a partition.

Click **OK** once the operation is complete. The partition details page is automatically refreshed.

See “Troubleshooting resize-related issues” on page 80.

See “About storage configuration” on page 60.

Resize dialog

Review the following points before you resize a storage partition:

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

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

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

Parameter	Description
Disk Pool Name	The Disk Pool Name appears only if you create AdvancedDisk or MSDP partition (Current Size is 0). You can assign a different disk pool name, other than the default. The disk pool name can contain any letters, numbers, or special characters. The name can include up to 256 characters. **Note:** The name should not start with the minus (-) character and spaces should not be used anywhere in the name.
New Size	Enter a value in the text box and select the appropriate unit. You can also drag the slider to the new size. (in GB, TB, or PB). You can also click on the bar up to the new size. Only an absolute value is supported if the unit is GB. Absolute and decimal values are supported if the units are TB or PB. The maximum value on the slider displays the partition size that you can scale up to. For AdvancedDisk and MSDP partitions, the maximum value is the sum of Current Size and Unallocated Size. For other partitions like Configuration and NetBackup Catalog, the maximum value on the slider is the lower value when you compare the following values: ■ Sum of Current Size and Unallocated Size ■ Maximum supported size of the partition For example, consider a NetBackup Catalog partition with a current size of 300 GB and an unallocated size of 6 GB. The maximum supported size of the partition is displayed as the sum of those two sizes; 306 GB. The catalog size is critical for NetBackup job schedules and primary server performance. Large catalog sizes can cause performance issues if the system architecture cannot meet the demands that the application requires.

Troubleshooting resize-related issues

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

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

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

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

See "Resizing a partition" on page 77.

Moving a partition

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

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

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

On a 53xx appliance, the MSDP Catalog partition must always be present on the Metadisk and can only be moved between Metadisks (wherever applicable).

To move a partition

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

   See "Move dialog" on page 81.
5. Click **Move** to move the partition.

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

   ---
6. The Move dialog displays the progress details and status of the move operation.

   Click **OK** once the operation is complete. The partition details page is automatically refreshed.

See "About storage configuration" on page 60.

Move dialog

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

Parameter	Description	Example
Source Disk	Displays the name of disk that currently holds the selected partition.	76YTGD2BA7CBACB4F416D631CE (Base)
Partition Size	Displays the selected partition's size on the source disk.	300 GB
Target Disk	Click the drop-down list and select the target disk to which you want to move the partition. **Note:** The Target disk must be different from the Source disk.	9DB0FD2BA7CBACB4F416D631CE (Expansion)
Unallocated Size	Displays the unallocated size on the target device.	100 GB
Size	Type the storage size in GB, TB, or PB that you want to move from the current disk to the new disk. **Note:** It is an optional field. If the size is not specified, the appliance moves the entire partition. **Note:** The size to be moved cannot be greater than the Unallocated Size on the target disk.	35 GB

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

If all or a part of your Media Server Deduplication Pool (MSDP) partition resides on the appliance base unit (base disk), it is recommended that you move the MSDP partition to an expansion disk. This recommendation applies to the 5240 appliance and is needed for optimum performance. For a 5250 appliance with attached external storage shelves, there is no requirement to exclude the appliance base unit (base disk) from the MSDP storage pool.

If high performance of the MSDP catalog is required, the MSDP storage pool should not include the appliance base unit (base disk) when external storage shelves are attached.

The following procedures explain how to move the MSDP partition from a base disk to an expansion disk. The base disk resides on the appliance base unit. The expansion disk resides on a storage shelf that is attached to the appliance.

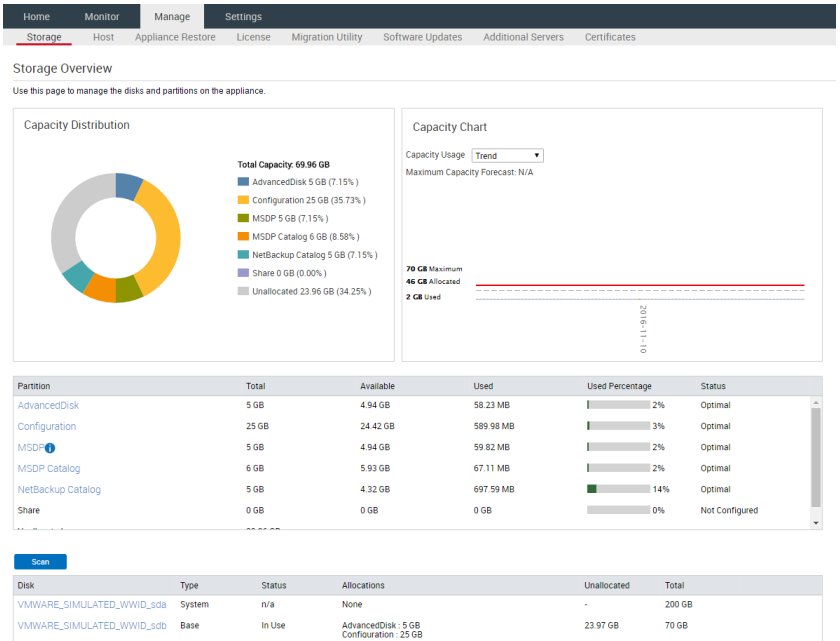
Consider the following scenarios:

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

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

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

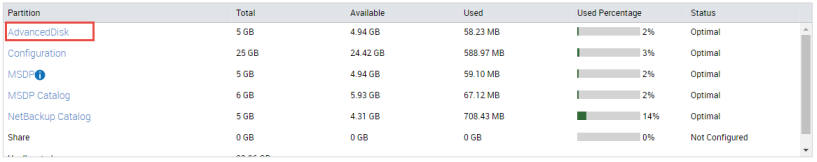
1. Log on to the NetBackup Appliance Web Console.
2. Click **Manage > Storage** and go to **Disks** section. Check the partitions that are on the Base disk. Suppose that you have MSDP, MSDP Catalog, AdvancedDisk, NetBackup Catalog, and Configuration partitions on the base disk.



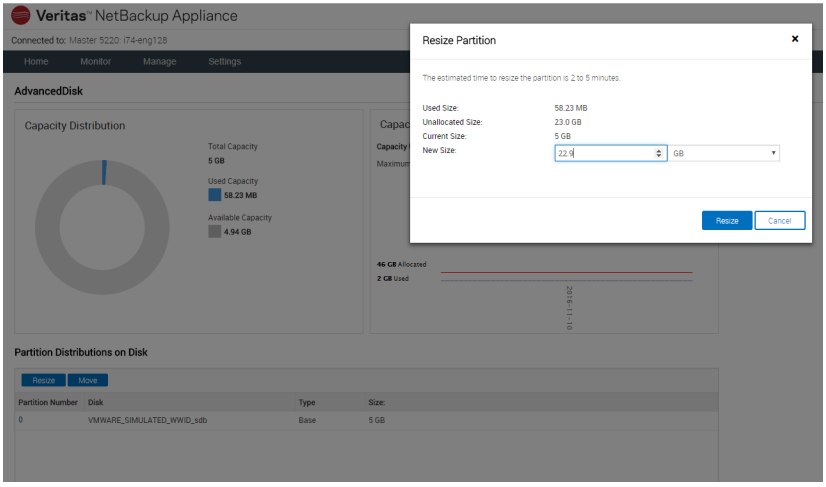
Note: If you have added storage shelves, click the **Scan** button to scan the new storage to create RAID volumes and add the new shelf to the unallocated storage.

3 Ensure that the base disk is fully allocated by resizing the non-MSDP partitions (like AdvancedDisk). To ensure that the base disk is full, resize the AdvancedDisk partition to a value that is just below the maximum value.

- In the **Partition** section, click **AdvancedDisk** partition to open the partition details page.



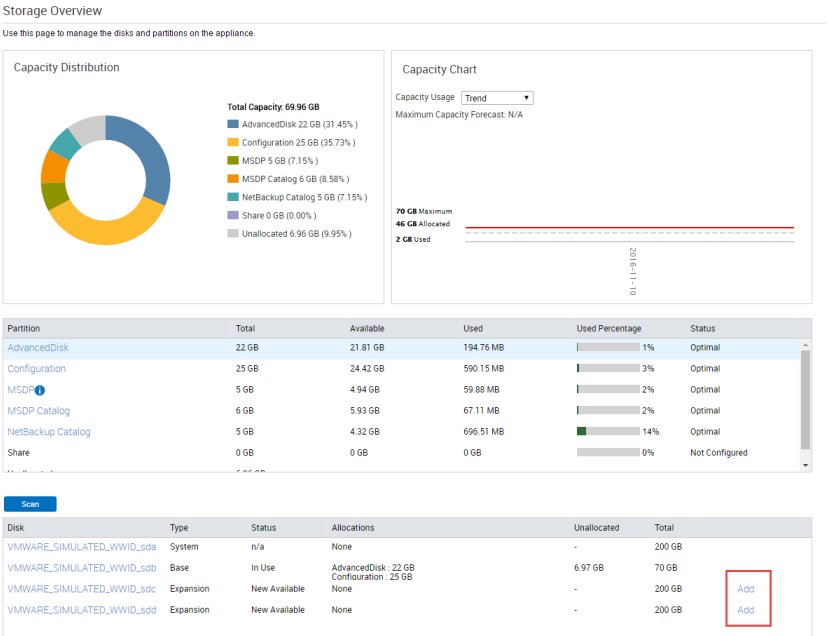
- On the partition details page, click **Resize** in the **Partition Distributions on Disk** section. Enter a size in the **New Size** field that is slightly below the maximum value.



Click **Resize** to resize. In this example, the AdvancedDisk partition is being resized to 22.9 GB. The maximum value that it can be resized to is 23 GB.

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

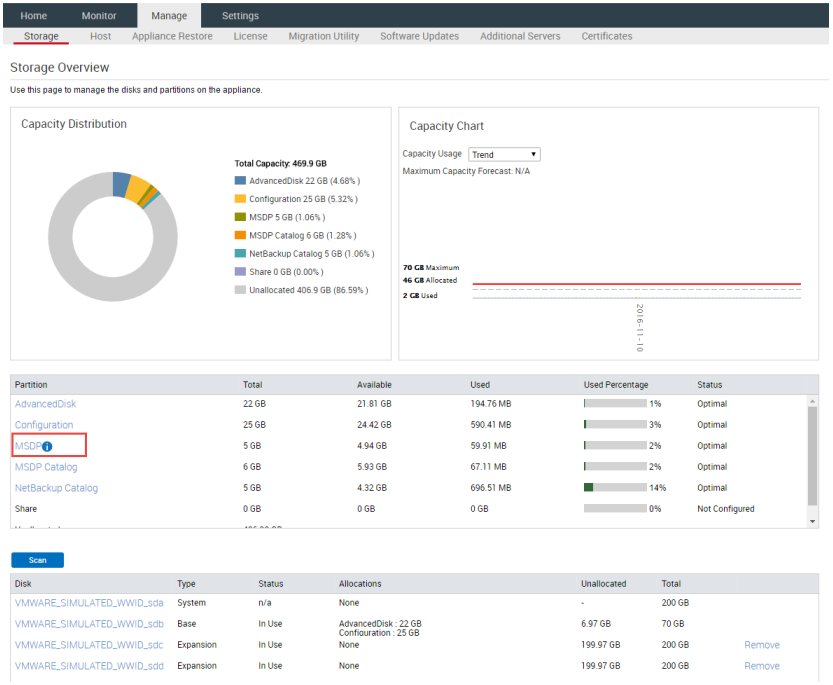
4 In the **Disks** section, click the **Add** link. Click **Yes** to confirm the addition and **OK** when it finishes. Repeat this process for the second expansion unit.



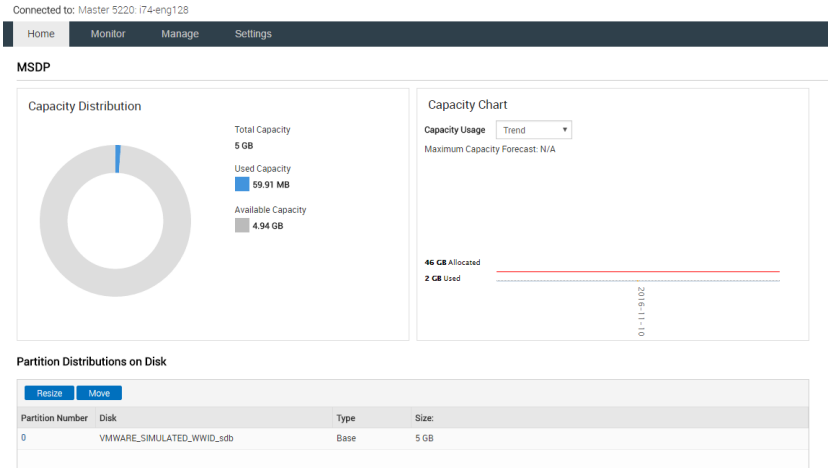
Note that the Unallocated space increases.

5 Check the space occupied by MSDP partition and how the MSDP partition is distributed across disks..

In the **Partition** section, click the **MSDP** link to open the MSDP partition detail page.



On MSDP partition detail page, check the **Partition Distributions on Disk** section.

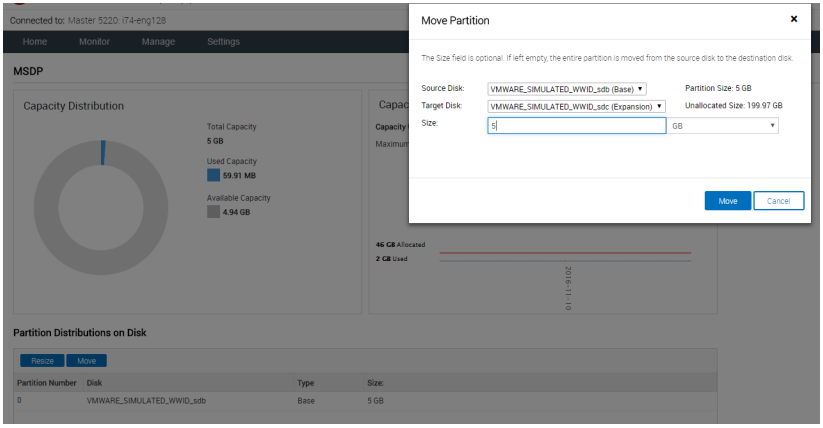


In this example, all of the MSDP partition resides on the base disk and occupies 5 GB.

Note that the expansion disk must have at least 5 GB of unallocated space when you move the MSDP partition to the expansion disk at a later point.

6 Click **Move** in the **Partition Distributions on Disk** section.

7 The **Move Partition** window is displayed. Select the target disk from the drop-down list to which you want to move the partition.



In this example, all of the MSDP partition that resides on the base disk is moved to one expansion disk.

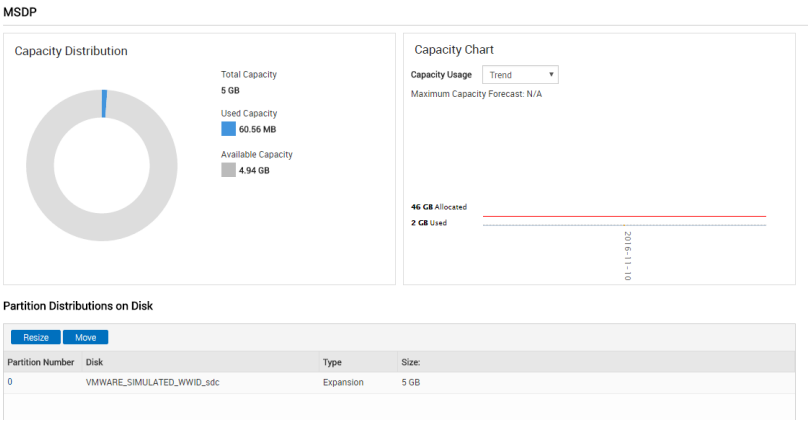
8 Click **Move** to move the partition.

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

---

9 Dialogs in the **Move Partition** displays the progress details and status of the move operation. Click **OK** once the operation is complete. The MSDP detail page is automatically refreshed.

10 On the MSDP detail page, check the **Partition Distributions on Disk** section. The MSDP partition resides on the expansion disk.

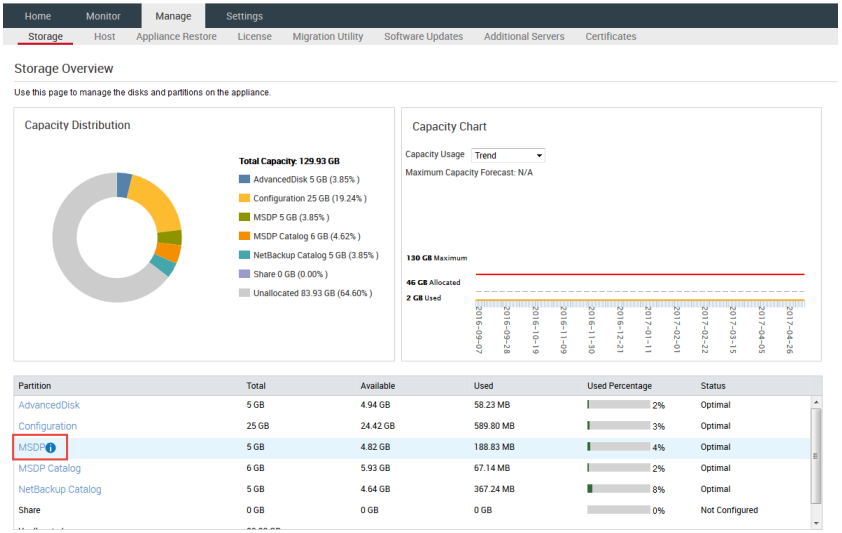


The following procedure explains how to move the MSDP partition from a base disk to an expansion disk when the expansion disk has partitions configured on it.

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

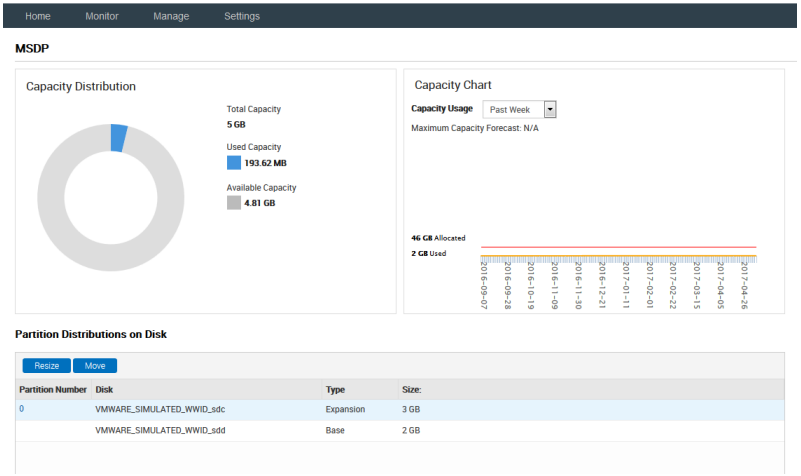
1. Log on to the NetBackup Appliance Web Console.
2. Click **Manage > Storage** .

   In the **Partition** area, click **MSDP** to go to the MSDP detail page.



3 On the MSDP partition detail page, check the **Partition Distributions on Disk** section.

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

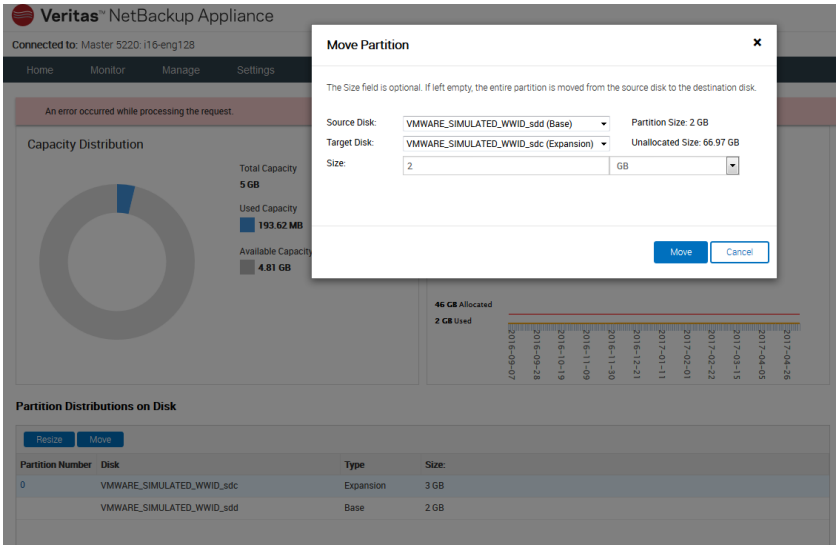


If the **type** is Expansion for all the disks, the MSDP partition doesn't exist on the base disk. In this case, you do not need to move the MSDP partition. You can ignore the rest of the procedure.

4 Click **Move** in the **Partition Distributions on Disk** section.

5 The **Move Partition** window is displayed. Select the target disk from the drop-down list to which you want to move the partition.

The target disk must be an expansion disk.



6 Click **Move** to move the partition.

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

7 After the operation completes, click **OK** to close the **Move Partition** window.

Scanning storage devices from the NetBackup Appliance Web Console

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

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

To scan storage devices from the NetBackup Appliance Web Console

1. Log on to the NetBackup Appliance Web Console.
2. Click **Manage > Storage > Disks**.
3. Click **Scan**.
4. You are prompted for confirmation. Click **Yes** to confirm. The scan starts.

   Note: If you are scanning the 53xx appliance for the first time, disk initialization may take some time. The disk initialization happens in the background and may take up to 56 hours depending on the system load.

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

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

   - Type = Expansion
   - Status = New Available

   For 53xx appliances, 6 Data disks and 1 Meta disk are displayed for a Primary Storage Shelf or an Expansion Storage Shelf. For a 53xx appliance that has a Primary Storage Shelf and an Expansion Storage Shelf, 12 Data disks and 2 Metadisks appear in the **Disks** section. The status for these disks is New Available.

   You can now add this disk to the Unallocated space.

   See "Adding the storage space from a newly available disk" on page 92.

Adding the storage space from a newly available disk

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

If you want to attach a Storage Shelf or an expansion system to an appliance, see the *NetBackup Appliance Hardware Installation Guide* for the appropriate platform.

Once these Storage Shelves are properly connected to the Appliance, you must scan for the newly available disks from the **Disks** section. The new disks have the **New Available** status. Once the newly available disks are displayed, these disks must be added so the additional space can be used.

To add the storage space from a newly available disk

1. Log on to the NetBackup Appliance Web Console.
2. Click **Manage > Storage** and go to the **Disks** section
3. The **Disks** section displays all the disks. Only disks that have the **Status** as **New Available** can be added. The **Add** link is displayed next to such disks.

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

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

   A dialog box displays the following message:

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

   Click **Yes**.

5. The system displays the following message:

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

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

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

Removing an existing storage disk

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

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

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

To remove an existing disk

1. Log on to the NetBackup Appliance Web Console.
2. Go to **Manage > Storage > Disks**.
3. The **Status** column in the **Disks** table displays the **Remove** link. It appears for disks with status **In Use** that do not contain any partitions. It also appears for disks with status **Foreign**.

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

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

   A dialog box displays the following message:

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

   Click **Yes** to continue.

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

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

   Click **Yes** to continue.

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

5. The system displays the following message:

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

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

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

See “About storage configuration” on page 60.

Monitoring the progress of storage manipulation tasks

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

To monitor storage tasks

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

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

```
Storage > Monitor


>>>>> Press 'CTRL + C' to quit. <<<<<

Resizing the AdvancedDisk storage partition...

The estimated time to resize the partition is 2 to 5 minutes.
Stopping NetBackup processes... (2 mins approx)
```

See “About storage configuration” on page 60.

Scanning storage devices using the NetBackup Appliance Shell Menu

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

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

To scan the storage devices

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

   ```
   Main > Manage > Storage
   ```

   The appliance displays all the sub-tasks in the storage menu.
3. Enter the `Scan` command to scan the storage devices.

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

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

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

See "About storage configuration" on page 60.

About Copilot functionality and Share management

Copilot integrates with native Oracle tools and processes to give database backup administrators more control, visibility, and the ability to recover their database backups. Backup administrators can then manage policies, move the data to different storage types, and create off-site backup copies of the database backups.

Additionally, Copilot features NetBackup Accelerator technology to boost Oracle backup and restore performance. NetBackup Accelerator integrates with Oracle's incremental merge capabilities to eliminate the need for full backups and allow new full database images to be synthesized on backup storage post-process.

Copilot lets you create shares on the appliance for Oracle backup and recovery and create further protection policies in NetBackup for advanced data protection features like long-term retention, replication, and NetBackup Oracle Accelerator technology. Copilot is exclusive to the appliance but requires additional configuration steps within NetBackup software.

Note: The NFS/CIFS shares used for Copilot that are created using the Appliance UI (CLISH/GUI) are not available in high availability(HA) configurations. You can use the universal share created using the NetBackup UI for Copilot.

Two types of Shares are available to create:

- Standard Share
- Optimized Share

Copilot configuration overview

To configure Copilot functionality, the following steps must be completed:

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

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

Share management

Shares can be created, modified, viewed, and deleted through the use of the shell menu or web console. Use the following topics as a guide to managing your Shares.

- See “Creating a Share” on page 98.
- See “Editing a Share” on page 101.
- See “Deleting a Share” on page 103.
- See “Moving a Share” on page 104.
-
- See “Manage > Storage > Shares” on page 72.
- See “Viewing Share information from the NetBackup Appliance Shell Menu” on page 107.

Optimized Share Reserve management

The Optimized Share Reserve can be created and deleted through the use of the shell menu or web console. Use the following topics as a guide to managing the Optimized Share Reserve.

- See “Creating the Optimized Share Reserve” on page 105.
- See “Deleting the Optimized Share Reserve” on page 106.

See “About Optimized Shares and the Optimized Share Reserve” on page 98.

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

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

About Optimized Shares and the Optimized Share Reserve

Optimized Shares work with all database sizes, but are enhanced to protect larger databases by leveraging additional storage capacity and a disk layout that supports larger database workloads. If you have the required storage available, create an optimized share for each Oracle database you want to back up. If you do not meet the storage requirements, consider adding a full capacity storage shelf to your 5340 appliance configuration.

Optimized Share and Optimized Share Reserve attributes:

- Optimized Shares can only reside in the Optimized Share Reserve, which is space pre-allocated specifically for Optimized Shares.
- The 5340 appliance hardware configuration must include a full capacity storage shelf.
- AdvancedDisk and MSDP partitions must reside on a different shelf. They cannot coexist on the dedicated shelf with the Optimized Share Reserve.

Optimized Share configuration overview

Veritas recommends the following order of operation to create Optimized Shares:

- Create the optimized share reserve during initial configuration of the appliance or after adding a new Expansion Storage Shelf.
- Create the optimized share.

Creating a Share

The following procedures explain how to create a Standard Share or an Optimized Share from the web console or shell menu.

Before you create a share, note the following:

- Standard and Optimized shares are not supported for use in high availability (HA) configuration setups.
- Starting with NetBackup Appliance release 5.1.1, the Copilot feature supports clients with IPv6 addresses to access Standard and Optimized shares. All IPv6 addresses must resolve to a valid hostname. If you enter a hostname format, the hostname must resolve to an IP address (IPv4 or IPv6) that is pingable. If the hostname can resolve to both IPv4 and IPv6 addresses, the IPv4 address has the priority.

Note:

- Creating a Standard or Optimized Share from the NetBackup Appliance Web Console
- Creating a Standard or Optimized Share from the NetBackup Appliance Shell Menu

Creating a Standard or Optimized Share from the NetBackup Appliance Web Console

The following procedure explains how to create a Standard or Optimized Share from the NetBackup Appliance Web Console.

To create a new Share from the web console

1. Navigate to **Manage > Storage > Shares**
2. Click **Create** on the main Shares page.
3. Choose the type of share to create, either **Standard** or **Optimized**.

   Note: If you have not created the Optimized Share Reserve, you are prompted to create it during the first Optimized Share creation process. Select the size of the Optimized Share Reserve, then click **Create Optimized Share Reserve**. When creation completes, you can continue with the next step.

4. Enter a name for the Share, for example `share_1`.
5. Enter a short description for the Share, for example `Test for share_1`.
6. Enter the Share size, for example `5GB`.
7. Click **Next**.
8. Click **Add Client**, then enter the client name into the blue box.

   Note: Client names can be entered using the short name, the FQDN, or the IP format.

9. Click the arrow next to the NFS options to make modifications to the NFS options for each client.

   See "NFS export options" on page 110.

10. Click the **checkmark** to confirm that the NFS options you entered for each client.

11 Click **Next**, then review the summary to confirm that the Share details are correct.

12 Click **Create Share** to create the Share. A success message is shown when the Share is created.

13 Click **Close** to return to the main **Shares** page.

Creating a Standard or Optimized Share from the NetBackup Appliance Shell Menu

The following procedure explains how to create a Standard or Optimized Share from the NetBackup Appliance Shell Menu.

To create a new Share from the shell menu

1 Open an SSH session to log on to the appliance as an administrator.

2 Enter the create command specific to Share you want to create:

- `Main_Menu > Manage > Storage > Create Share Standard` creates a Standard Share.
- `Main_Menu > Manage > Storage > Create Share Optimized` creates an Optimized Share.

The command guides you through the process of configuring a new Share.

3 Enter the Share name, for example `share_1`.

4 Enter a short description for the Share, for example `Test for share_1`.

5 Enter the allocated capacity for the Share, for example `5GB`.

6 Enter a comma-separated list of Oracle server clients that can access the Share, for example `10.100.0.2, 10.100.0.3`.

Note: Client names can be entered using the short name, the FQDN, or the IP format.

---

7 Enter the NFS export options for each of the Oracle clients. You are prompted to enter options for each client you added in the previous step.

See "NFS export options" on page 110.

8 Once you have entered the NFS export options, a summary is displayed.

9 Enter `yes` to create the Share. A series of messages are displayed as the Share is created.

See "About Copilot functionality and Share management" on page 96.

See "About Optimized Shares and the Optimized Share Reserve" on page 98.

Refer to the *NetBackup™ Copilot™ for Oracle Configuration Guide* for more information on configuring Oracle database backups.

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

Editing a Share

The following procedures explain how to edit a Share from the web console or shell menu. You can edit the description, size, clients, and NFS options of the clients.

- Editing a Share from the NetBackup Appliance Web Console
- Editing a Share from the NetBackup Appliance Shell Menu
- Resizing a Share from the NetBackup Appliance Shell Menu

Editing a Share from the NetBackup Appliance Web Console

The following procedure explains how to edit a Share from the NetBackup Appliance Web Console.

To edit a share from the web console

1. Navigate to **Manage > Storage > Shares**.
2. Click on the Share you want to edit to open the Share details pane, then click **Edit**.
3. Edit the description or the size of the Share, then click **Next**.
4. You can edit the following client attributes:
   - Click **Add Client** to add new clients.
   - Click the pencil icon to change the NFS options.
   - Click the x icon to remove clients.
5. Click **Next** when finished with client edits.
6. Click **Save Changes** to save the edits you made.
7. Click Close to return to the main **Shares** page.

Editing a Share from the NetBackup Appliance Shell Menu

The following procedures explain how to edit a Share from the NetBackup Appliance Shell Menu.

To edit a Share description from the shell menu

1. Open an SSH session to log on to the appliance as an administrator.
2. Enter `Main_Menu > Manage > Storage > Edit Share Description <ShareName>`.
3. Enter a new Share description, then press Enter to view a summary of the edit.
4. Enter `yes` to complete the edit process.

The following procedure explains how to add a client to a Share from the shell menu.

To add a client to a Share from the shell menu

1. Open an SSH session to log on to the appliance as an administrator.
2. Enter `Main_Menu > Manage > Storage > Edit Share Clients Add <ShareName>`.
3. Enter the clients you want to add, then press Enter.
4. Enter the NFS export options for each client. Press Enter to move to the next client. When you are finished, the summary is displayed.
5. Enter `yes` to complete the edit process.

The following procedure explains how to update the clients of a Share from the shell menu.

To update the clients of a Share from the shell menu

1. Open an SSH session to log on to the appliance as an administrator.
2. Enter `Main_Menu > Manage > Storage > Edit Share Clients Update <ShareName>` .
3. Enter the clients you want to update, then press Enter.
4. Enter the NFS export options for each updated client. Press Enter to move to the next client. When you are finished the summary is displayed.
5. Enter `yes` to complete the edit process.

The following procedure explains how to delete clients from a Share from the shell menu.

To delete clients from a Share from the shell menu

1. Open an SSH session to log on to the appliance as an administrator.
2. Enter `Main_Menu > Manage > Storage > Edit Share Clients Delete <ShareName>`.

3 Enter the clients you want to delete, then press Enter to delete the clients.

4 Enter `yes` to complete the edit process.

Resizing a Share from the NetBackup Appliance Shell Menu

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

To resize a Share from the shell menu

1 Open an SSH session to log on to the appliance as an administrator.

2 Enter `Main_Menu > Manage > Storage > Resize Share [Size] [Unit] <ShareName>` then press Enter.

Note: The Share is resized to the new size that you enter. It is not added or subtracted from the current size.

3 Type `yes`, then press Enter to complete the resize operation.

See "About Copilot functionality and Share management" on page 96.

Deleting a Share

The following procedures explain how to delete a Share from the web console or shell menu.

- Deleting a Share from the NetBackup Appliance Web Console
- Deleting a Share from the NetBackup Appliance Shell Menu

Before you delete any share, you must first expire all data images on the share. For details, see the topic "Expiring backup images" in the *NetBackup Administrator's Guide*.

Deleting a Share from the NetBackup Appliance Web Console

The following procedure explains how to delete a Share from the NetBackup Appliance Web Console.

To delete a Share using the web console

1 Navigate to the share as follows:

- For Standard Shares and Optimized Shares: **Manage > Storage > Shares**

2 Click **Delete**, then select the Share or Shares you want to delete.

3 Click **Delete** to delete the selected Share or Shares, then click **Delete** again at the confirmation screen.

4 Click **Close** when the Share is deleted to return to the main Shares page.

Deleting a Share from the NetBackup Appliance Shell Menu

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

To delete a Share using the shell menu

1 Open an SSH session to log on to the appliance as an administrator.

2 Enter `Main_Menu > Manage > Storage > Delete Share <ShareName>`.

3 Enter `yes` to delete the Share.

See "About Copilot functionality and Share management" on page 96.

Moving a Share

The following procedures explain how to move a Share from the web console or shell menu.

Note: Optimized Shares cannot be moved.

- Moving a Share from the NetBackup Appliance Web Console
- Moving a Share from the NetBackup Appliance Shell Menu

Moving a Share from the NetBackup Appliance Web Console

The following procedure explains how to move a Share from the NetBackup Appliance Web Console.

To move a Share using the web console:

1 Navigate to **Manage > Storage > Shares**.

2 Select the source disk from the drop-down menu. A list of shares residing on the disk are shown.

3 Select the target disk from the drop-down menu.

4 Enter the size to be moved.

5 Click **Move** to move the Shares, then click **Yes** to confirm the move.

6 Click **Close** to return to the main Shares page.

Moving a Share from the NetBackup Appliance Shell Menu

The following procedure explains how to move a Share from the NetBackup Appliance Shell Menu.

To move a Share using the shell menu:

1. Open an SSH session to log on to the appliance as an administrator.
2. Enter `Main_Menu > Manage > Storage > Move Share <Share_Name> <SourceDiskID> <TargetDiskID> [Size] [Unit]`
3. Enter `yes` to move the Share.

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

Creating the Optimized Share Reserve

The following procedures explain how to create the Optimized Share Reserve from the web console or shell menu.

Note: All storage space on the Expansion Storage Shelf must be dedicated to the Optimized Share Reserve.

- Creating the Optimized Share Reserve from the NetBackup Appliance Web Console
- Creating the Optimized Share Reserve from the NetBackup Appliance Shell Menu

Creating the Optimized Share Reserve from the NetBackup Appliance Web Console

The following procedure explains how to create the Optimized Share Reserve from the NetBackup Appliance Web Console.

To create the Optimized Share Reserve from the web console

1. Navigate to **Manage > Storage > Shares**.
2. Click **Create Optimized Share Reserve**.
3. Choose the size of the Optimized Share Reserve.
4. Click **Create Optimized Share Reserve**.
5. Click **Close** to return to the main Shares page.

Creating the Optimized Share Reserve from the NetBackup Appliance Shell Menu

The following procedure explains how to create the Optimized Share Reserve from the NetBackup Appliance Shell Menu.

To create the Optimized Share Reserve from the shell menu

1. Open an SSH session to log on to the appliance as an administrator.
2. Enter `Main_Menu > Manage > Storage > Create OptimizedShareReserve`.
3. Enter `yes` to create the Optimized Share Reserve. A series of messages are displayed as the reserve is created.

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

See "About Optimized Shares and the Optimized Share Reserve" on page 98.

Deleting the Optimized Share Reserve

The following procedures explain how to delete the Optimized Share Reserve from the web console or shell menu.

Note: All Optimized Shares must be deleted before you can delete the Optimized Share Reserve.

- Deleting the Optimized Share Reserve from the NetBackup Appliance Web Console
- Deleting the Optimized Share Reserve from the NetBackup Appliance Shell Menu

Deleting the Optimized Share Reserve from the NetBackup Appliance Web Console

The following procedure explains how to delete the Optimized Share Reserve from the NetBackup Appliance Web Console.

To delete the Optimized Share Reserve from the web console

1. Navigate to **Manage > Storage > Shares**.
2. Click on the Optimized Share Reserve summary. A window opens showing the summary.
3. Click **Delete Optimized Share Reserve**.

Deleting the Optimized Share Reserve from the NetBackup Appliance Shell Menu

The following procedure explains how to delete the Optimized Share Reserve from the NetBackup Appliance Shell Menu.

To delete the Optimized Share Reserve from the shell menu

1. Open an SSH session to log on to the appliance as an administrator.
2. Enter `Main_Menu > Manage > Storage > Delete OptimizedShareReserve`.
3. Enter `yes` to delete the Optimized Share Reserve.

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

See "About Optimized Shares and the Optimized Share Reserve" on page 98.

Viewing Share information from the NetBackup Appliance Shell Menu

The following procedure explains how to view Share information using the shell menu.

To view Share partition information using the shell menu:

1 Open an SSH session to log on to the appliance as an administrator.

2 Enter `Main_Menu > Manage > Storage > Show Partition All Share`.

The following is an example output displaying Share information:

```
-------------------------
Optimized Share Reserve
-------------------------
Total:        114.60 TB
Allocated:      5.19 GB
Unallocated:  114.59 TB

-------------------------------------------------------------------------
Partition       | Total      | Available  | Used       | %Used | Status
-------------------------------------------------------------------------
Optimized Share | 5 GB       | 4.94 GB    | 58.23 MB   | 2     | Optimal
Standard Share  | 5 GB       | 4.94 GB    | 58.23 MB   | 2     | Optimal

Optimized Share
-----------------------------------------------------------------
Partition  | Total      | Available  | Used       | %Used | Status
-----------------------------------------------------------------
opt_share1 |       5 GB |    4.94 GB |   58.23 MB |     2 | Mounted

Standard Share
-----------------------------------------------------------------
Partition  | Total      | Available  | Used       | %Used | Status
-----------------------------------------------------------------
std_share1 |       5 GB |    4.94 GB |   58.23 MB |     2 | Mounted

Share - opt_share1
---------------------------------------
Type - Optimized
---------------------------------------
Description:
  None
---------------------------------------
Clients   | Options
---------------------------------------
localhost | no_root_squash, rw, secure
---------------------------------------

Share - std_share1
---------------------------------------
```

```
Type - Standard
----------------------------------------
Description:
  None
----------------------------------------
Clients   | Options
----------------------------------------
127.0.0.1 | no_root_squash, rw, secure
----------------------------------------

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

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

See "About viewing storage space information using the `Show` command " on page 111.

NFS export options

The following table describes the export options available for Share creation or modification.

Option	Description
`ro`	Allows only read requests on the Share.
`rw`	Allows both read requests and write requests on the Share.
`no_root_squash`	Disables all root squashing. Allows root account on client to access export share on server as the root account.
`root_squash`	Maps requests from UID and GID 0 to the anonymous UID and GID.
`all_squash`	Maps all UIDs and GIDs to the anonymous user account. By default, the NFS server chooses a UID and GID of 65534 for squashed access. These values can be overridden by using the `anonuid` and `anongid` options.
`anonuid`	Sets the `uid` of the anonymous user account. This option forces all anonymous connections to a predefined UID on a server.

Option	Description
`anongid`	Sets the `gid` of the anonymous account. This option forces all anonymous connections to a predefined GID on a server.
`secure`	Requires that requests originate from an Internet port less than `IPPORT_RESERVED (1024).`
`insecure`	Disables the requirement that requests originate from an Internet port less than `IPPORT_RESERVED (1024).`

About viewing storage space information using the `Show` command

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

The *<Type>* parameter is required when using the `Show` command.

The following `Show <Type>` commands are described:

- `Show ALL` - to view disk, partition, and distribution information together.
  See "Viewing all storage information" on page 113.
- `Show Disk` - to view total capacity, unallocated storage capacity, and current status of a disk.
  See "Viewing disk information" on page 116.
- `Show Partition [All/Configuration/Usage]` - to view total, available, and used storage capacity of a partition.
  See "Viewing partition information" on page 119.
- `Show Distribution` - to view the distribution of partitions on a disk.
  See "Viewing the partition distribution on disks" on page 120.

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

SCSI(0:1) (Base)
------------------------------
AdvancedDisk       :     64 GB
- 0                :     64 GB
```

```
Configuration      :     50 GB
- 0                :     50 GB
MSDP               :   1.94 TB
- 0                :   1.94 TB
MSDP Catalog       :     20 GB
- 0                :     20 GB
NetBackup Catalog  :     30 GB
- 0                :     30 GB
```

Table 3-11 Partition type status

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

Table 3-12 describes the various status of a particular partition.

Table 3-12 Partition name status

Status	Description
Mounted	The partition is currently mounted.
Not Mounted	The partition is not currently mounted. If the partition is not mounted, the status can either be Degraded or Not Accessible. See Table 3-11 for more information.
I/O Error	There is an I/O error with the partition. If the partition has an I/O error, the status can either be Degraded or Not Accessible. See Table 3-11 for more information.

Note: The Available and Used Size values displayed for the MSDP partition on the **Manage > Storage > Partitions** page or by using the **Manage > Storage > Show** command on the NetBackup Appliance Shell Menu may not be the full space available or used by the MSDP partition. This is because space is reserved by the file system and also by MSDP. The file system reserves space for it's own use. In addition, MSDP reserves 4 percent of the storage space for the deduplication database and transaction logs.

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

See "About storage configuration" on page 60.

Viewing all storage information

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

To view all storage information

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

   ```
   Main > Manage > Storage
   ```

   The appliance displays all the sub-tasks in the storage menu.
3. Enter the `Show All` command to view device information.

For a 53xx platform, the appliance displays the storage information as shown in the following example:

```
- [Info] Performing sanity check on disks and partitions... (5 mins approx)
------------------------------------------------------------------------
Disk ID                    | Type   | Total      | Unallocated | Status
------------------------------------------------------------------------
5E000000000000000000000000 | System |  930.39 GB |        -    | n/a
7A30D550001B22423721D79081 | Base   |   13.64 TB |    10.84 TB | In Use

7A30D550001B22423721D79081 (Base)
---------------------------------
AdvancedDisk       :    500 GB
- 0               :    500 GB
Configuration      :     25 GB
- 0               :     25 GB
```

```
MSDP                :      1 TB
- 0                 :      1 TB
MSDP Catalog        :     43 GB
- 0                 :     43 GB
NetBackup Catalog   :    250 GB
- 0                 :    250 GB
Share               :      1 TB
- s1                :      1 TB

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

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

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

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

MSDP Catalog
---------------------------------------------------------------------
Partition | Total      | Available  | Used       | %Used | Status
---------------------------------------------------------------------
0         |      43 GB |   42.59 GB |  414.99 MB |     1 | Mounted
```

```
NetBackup Catalog
-----------------------------------------------------------------------
Partition | Total      | Available  | Used       | %Used | Status
-----------------------------------------------------------------------
0         |     250 GB |  247.62 GB |    2.38 GB |     1 | Mounted

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

AdvancedDisk
-----------------------------------
Disk Pool (DP)  | Storage Unit (STU)
-----------------------------------
dp_adv_nbapp2br | stu_adv_nbapp2br

MSDP
-------------------------------------
Disk Pool (DP)   | Storage Unit (STU)
-------------------------------------
dp_disk_nbapp2br | stu_disk_nbapp2br

Share - s1
-------------------------------------------
Description:
  None
-------------------------------------------
Clients       | Options
-------------------------------------------
appesx30-vm13 | no_root_squash, rw, secure
-------------------------------------------


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

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

Viewing disk information

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

To view disk information

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

   ```
   Main > Manage > Storage
   ```

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

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

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

```
Storage> Show Disk
- [Info] Performing sanity check on disks and partitions..(5 mins approx)
------------------------------------------------------------------------
Disk ID                   |  Type    |  Total   |Unallocated|Status
------------------------------------------------------------------------
5E00000000000000000000000|System   |930.39 TB|  -        | n/a
50001FD36800000790537BB0FA|Base     |  2.24 TB|  300 GB   | In Use
50001FEE6C00000A36537BB0CB|Expansion|4.5421 TB|  840.92 GB| In Use

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

For a 53xx platform, the appliance displays the disk information as shown in the following example:

```
Storage> Show Disk
- [Info] Performing sanity check on disks and partitions..(5 mins approx)
-------------------------------------------------------------------------------
Disk ID                   |Type      | Total    |Unallocated| Status
-------------------------------------------------------------------------------
5E00000000000000000000000|System    |  2.73 TB |   -       | n/a
5E00000000001000000000000|System    |  2.73 TB |   -       | n/a
50001FD36800000796537BB10F|Meta      |  5.46 TB | 5.46 TB   | In Use
50001FEE6C00000A38537BB0D5|Meta      |  5.46 TB | 5.37 TB   | In Use
50001FD3680000078A537BB0DC|Data      | 19.10 TB |19.10 TB   | In Use
50001FD3680000078C537BB0E4|Data      | 19.10 TB |19.10 TB   | In Use
50001FD3680000078E537BB0EC|Data      | 19.10 TB | 0 GB      | In Use
50001FD36800000790537BB0FA|Data      | 19.10 TB | 7.30 TB   | In Use
50001FD36800000792537BB102|Data      | 19.10 TB |19.08 TB   | In Use
50001FD36800000794537BB10B|Data      | 19.10 TB | 0 GB      | In Use
50001FEE6C00000A32537BB0B4|Data      | 19.10 TB |19.10 TB   | In Use
50001FEE6C00000A34537BB0C3|Data      | 19.10 TB |19.10 TB   | In Use
50001FEE6C00000A36537BB0CB|Data      | 19.10 TB |18.20 TB   | In Use
50001FEE6C00000A3A537BB0D8|Data      | 19.10 TB | 0 GB      | In Use
50001FEE6C00000A3C537BB0E1|Data      | 19.10 TB |19.10 TB   | In Use
50001FEE6C00000A3E537BB0EA|Data      | 19.10 TB |19.10 TB   | In Use


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

Table 3-13 lists the disk types that can appear depending on your Appliance platform.

Table 3-13 Disk Type

Type	Description	Supported Platforms
System	This category tells you the storage that is occupied by the Appliance operating system, logs etc.	52xx 53xx
Base	This category tells you the storage that is available with the Appliance base unit.	52xx
Expansion	A storage shelf that is connected to a 52xx appliance appears as a single expansion disk.	52xx
Data	All partitions, except MSDP Catalog, exist on the 53xx Data disk. Examples of partitions that exist on the data disks are MSDP, AdvancedDisk, Configuration etc. There can be six data disks for a Primary Storage Shelf and six for an Expansion Storage Shelf.	53xx
Meta	The MSDP Catalog partition exists only on the Meta disk. There can be one Meta disk for a Primary Storage Shelf and one for an Expansion Storage Shelf.	53xx
Unknown	This category appears when appliance cannot determine the disk type like when the disk is not accessible.	Not Applicable

Viewing partition information

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

- `All` *`PartitionType`*
- `Configuration` *`PartitionType`*
- `Usage` *`PartitionType`*

Replace *`PartitionType`* with `AdvancedDisk`, `All`, `MSDP`, or `Share`.

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

To view partition configuration

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

   ```
   Main > Manage > Storage
   ```

   The appliance displays all the sub-tasks in the storage menu.
3. Enter the `Show Partition Configuration Share` command to view the partition information for a share.
4. For 52xx platforms, the appliance displays the partition information as shown in the following example:

   ```
   Share - sh3
   ----------------------------------------
   Type - Standard
   ----------------------------------------
   Description:
     None
   ----------------------------------------
   Clients   | Options
   ----------------------------------------
   localhost | no_root_squash, rw, secure
   ----------------------------------------
   ```

Viewing the partition distribution on disks

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

To view the partition distribution on a disk

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

   ```
   Main > Manage > Storage
   ```

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

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

The following example displays the initiated procedure when you run the `Show [Distribution]` command on a 53xx appliance:

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

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

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

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

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

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

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

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

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

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

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

About storage email alerts

A software administrator can add his email account by running the Settings > Alerts > Email Software Add [Email Addresses] command to receive software alerts. If you have configured your email address to receive software alerts for a specific appliance, you will receive Appliance alerts like storage alerts, hardware monitoring alerts, and so on.

The storage alerts are generated in the following scenarios:

- When a Resize or Move operation is performed on the appliance. Once the Resize or Move operation is complete, an alert is sent to the email address specifying the operation and result. An alerts is sent if the resize or move operations succeed or fail.
- When Storage sanity check fails on the appliance. Storage sanity check runs daily and also runs as a part of storage manipulation operations. Storage sanity check helps to fix some of the storage issues or reports them.

A sample alert content is provided. This alert is generated when the AdvancedDisk partition was resized to 1 TB on host nb-appliance:

```
Alerts from NetBackup Appliance

  Host name:  nb-appliance
  Operation:  Resize AdvancedDisk 1 TB
  Status:     Succeeded

- NetBackup Appliance Alerts
```

The following sample alert is generated when the storage sanity check failed:

```
Alerts from NetBackup Appliance

  Host name:  nb-appliance
```

```
  Operation:  Storage sanity check
  Status:     Failed
  Reason:     Failed to mount the 'AdvancedDisk' partition '0'. A full file
  system check (fsck) needs to be performed on this partition.

- NetBackup Appliance Alerts
```

About appliance supported tape devices

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

Tape library	The NetBackup appliance supports backup to the tape libraries that are of NetBackup type TLD (tape library DLT). DLT is an acronym for digital linear tape. For the TLD types that NetBackup supports, see the Hardware Compatibility List at the following URL: https://www.veritas.com/support/en_US/article.100040093
Tape drives	The NetBackup appliance supports writing to the tape devices that are capable of SCSI T10 encryption to ensure that the tape media that is moved off-site is secure. Tape encryption requires configuration of the NetBackup Key Management Service (KMS) feature. To know more about KMS support and the list of the tape drives supported with KMS, see the Hardware Compatibility List at the following URL: https://www.veritas.com/support/en_US/article.100040093
Tape usage	Tapes with the barcode prefix of CLN are treated as cleaning tapes. Tapes with any other barcode prefix are treated as normal tapes.
NetBackup ACS libraries	Starting with appliance version 2.5, NetBackup appliances support the NetBackup type ACS libraries and the configuration of NetBackup ACS robotics on the NetBackup appliance. Appliance administrators can change the ACS entries in the `vm.conf` file on the local appliance. For complete details about the ACS commands that can be used to modify the `vm.conf` file, see the *NetBackup Appliance Command Reference Guide*.

See “Adding external robots to the NetBackup appliance” on page 124.

Adding external robots to the NetBackup appliance

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

Use the following procedure to add robots to the appliance.

To add an external robot to the appliance

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

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

See "About appliance supported tape devices" on page 124.

About configuring Host parameters for your appliance

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

- Specify Data Buffer parameters
  See "Configuring data buffer parameters" on page 127.
- Specify Lifecycle parameters
  See "Configuring lifecycle parameters" on page 131.
- Specify Deduplication parameters
  See "Configuring deduplication parameters" on page 134.
- Enable or disable BMR as a server recovery option
  See "About BMR integration" on page 134.

Manage > Host > Data Buffer options

You can configure the parameters for the data buffer shared with NetBackup using the **Manage > Host > Data Buffer** tab in the appliance NetBackup Appliance Web

Console. The **Data Buffer Parameters** tab enables you to enter the count and size of the following data buffer storage:

- Data buffer tapes
- Data buffer on disks
- Data buffer using Fibre Transport
- Data buffer restore
- Data buffer for NDMP (Network Data Management Protocol)
- Data buffer for multiple copies

The following data buffer parameters can be updated using the appliance NetBackup Appliance Web Console:

Table 3-14 Data Buffer parameters

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

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

Configuring data buffer parameters

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

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

To configure data buffer parameters

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

   The system displays the **Data Buffer** tab with the default NetBackup data buffer parameters.
3. Enter the data buffer parameters in the provided fields. A description of the data buffer parameters is available.

   See "Manage > Host > Data Buffer options" on page 125.
4. Click **Save**, to save the updated parameters.

Manage > Host > Lifecycle options

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

Table 3-15 describes the lifecycle parameters that are displayed.

Table 3-15 Lifecycle parameters

Parameter	Description
Cleanup session interval	Enter the time interval after which the deleted life cycle policies should be cleaned up. The default value is 24 hours. Select the unit to measure the time from the drop-down list. You can select from the following options: ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)
Duplication group criteria	Enter the duplication group criteria that is used to define how batches are created. The default value is 1.
Image extended retry period	Enter the interval period till NetBackup waits before an image copy is added to the next duplication job. The default value is 2 hours. Select the unit to measure the time from the drop-down list. You can select from the following options: ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)

Table 3-15 Lifecycle parameters *(continued)*

Parameter	Description
Job submission interval	Set the frequency of job submission for all operations. The default value is 5 minutes. By default, all jobs are processed before more jobs are submitted. Increase this interval to allow NetBackup to submit more jobs before all jobs are processed. Select the unit to measure the time from the drop-down list. You can select from the following options: ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)
Max size per duplication job	Enter the maximum size up to which the batch of images is allowed to grow. The default value is 100 GB. Select the unit to measure the size from the drop-down list. You can select from the following options: ■ Byte(s) ■ KB ■ MB ■ GB ■ TB ■ PB
Force interval for small jobs	Enter the time to determine how old any image in a group can become before the batch is submitted as a duplication job. The default value is 30 minutes. Select the unit to measure the time from the drop-down list. You can select from the following options: ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)

Table 3-15 Lifecycle parameters *(continued)*

Parameter	Description
Min size per duplication job	Enter the minimum size up to which the batch of images should reach before a duplication job is run for the entire batch. The default value is 8 GB. Select the unit to measure the size from the drop-down list. You can select from the following options: ■ Byte(s) ■ KB ■ MB ■ GB ■ TB ■ PB
Replica metadata cleanup timer	Enter the number of days after which the Import Manager stops trying to import the image. The default value is 0 hours. Select the unit to measure the time from the drop-down list. You can select from the following options: ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)
Tape resource multiplier	Enter the multiplier for the number of concurrently active duplication jobs that can access a single storage unit. The default value is 2.
Version cleanup delay	Enter the number of hours to determine how much time must pass since an inactive version was the active version. The default value is 14 days. Select the unit to measure the time from the drop-down list. You can select from the following options: ■ Hour(s) ■ Second(s) ■ Minute(s) ■ Day(s) ■ Week(s) ■ Month(s) ■ Year(s)

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

Configuring lifecycle parameters

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

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

To configure lifecycle parameters

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

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

   See "Manage > Host > Lifecycle options" on page 127.
3. Click **Save** to save the updated parameters.

About configuring deduplication solutions

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

Table 3-16 Deduplication solutions and appliance matrix

NetBackup Appliance Series	Deduplication solution applicable	
	Primary Server	**Media server**
NetBackup Appliance 52xx series	Media Server Deduplication Option (MSDP)	Media Server Deduplication Option (MSDP)
NetBackup Appliance 53xx series	Not Applicable	Media Server Deduplication Option (MSDP)

Adding the deduplication solution to a 52xx media appliance

You can configure the deduplication solution for your NetBackup Appliance 52xx series media appliance using the following two pages:

- **Intial Configuration** - You can select the deduplication solution at the time of initial configuration of your appliance.
- **Manage > Storage > Resize** - If you have not configured a deduplication solution at the time of initial configuration you can configure it using the **Resize** option from the **Manage > Storage** menu.
  See "Resizing a partition" on page 77.

Manage > Host > Deduplication

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

Manage > Host > Deduplication describes the deduplication parameters that are displayed on the **Deduplication Settings** tab.

Table 3-17 Deduplication parameters

Fields	Description
Log verbosity level	Select the amount of information to be written to the log file. You can select from the values 0 to 10, with 10 being the maximum information that can be logged. **Note:** Change this value only when directed to do so by a Veritas representative.
Debug log file maximum size	Enter the maximum size of the log file in megabytes.
NICs for backup and restore	Enter the IP address or range of addresses of the local network Interface Card (NIC) for maintaining backups and restores.

Table 3-17 Deduplication parameters *(continued)*

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

Configuring deduplication parameters

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

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

To configure deduplication parameters

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

   The system displays the **Deduplication** tab with the default deduplication parameters.
3. Enter the MSDP parameters. For more information about these parameters.

   See "Manage > Host > Deduplication" on page 132.
4. Click **Save**, to save the updated parameters.

About BMR integration

Bare Metal Restore (BMR) is the Server Recovery option of NetBackup. BMR automates and streamlines the server recovery process, making it unnecessary to manually reinstall Operating Systems or configure hardware. With simple commands, complete server restores can be accomplished in a fraction of the time without extensive training or tedious administration.

BMR allows the recovery of:

- Windows systems to completely different hardware (Dissimilar System Recovery or DSR)
- UNIX/Linux systems to disks of varying geometry (Dissimilar Disk Recovery or DDR)

See the *BMR Administrator's Guide* for more information.

Note: A NetBackup appliance cannot be used as a BMR boot server. This convention is unlike NetBackup, where you can use any primary server, media server, or client as a BMR boot server. Your boot server can be any non-appliance NetBackup platform with the same operating system as the hosts that are to be recovered.

See "Enabling BMR from the NetBackup Appliance Web Console" on page 135.

Manage > Host > Advanced options

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

The following option appears on Manage > Host > Advanced:

Enable BMR on this Appliance

You can enable BMR by using this option.

See "Enabling BMR from the NetBackup Appliance Web Console" on page 135.

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

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

Enabling BMR from the NetBackup Appliance Web Console

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

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

To enable BMR from the NetBackup Appliance Web Console

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

Manage > Host > IPMI options

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

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

See "Resetting the IPMI" on page 136.

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

Resetting the IPMI

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

To reset the IPMI

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

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

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

Manage > Appliance Restore

Appliance Restore implies that you want to restore the appliance to a specific state.

That state can be a state that is determined through the use of checkpoints. You can create a checkpoint, rollback the appliance to a checkpoint that you choose.

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

- **Create Appliance Checkpoint**
  Click this icon to create a user-directed checkpoint on your appliance.

- **Appliance Rollback**
  Click this icon to roll back the appliance to a checkpoint that you select.

The following list describes the different types of checkpoints:

- A pre-upgrade checkpoint is created before you install a software upgrade. You can use this type of checkpoint as a rollback checkpoint in case a software upgrade fails.
- A user-directed checkpoint is a checkpoint that you create at any point in time using the application user interface or the appliance shell menu. If an existing user-directed checkpoint already exists it is replaced by any new checkpoint that you create.

See “About creating an appliance checkpoint” on page 137.

See “Creating an appliance checkpoint” on page 140.

See “About appliance rollback ” on page 146.

See “About NetBackup appliance factory reset” on page 156.

About creating an appliance checkpoint

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

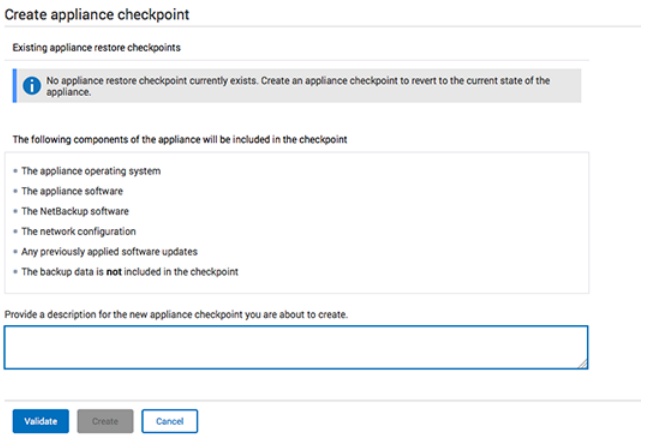


Table 3-18 contains the following fields and functions that you use to create a checkpoint.

Table 3-18 Create Appliance Checkpoint page

Field	Description
Existing appliance restore checkpoints	This field shows all of the current checkpoints that exist. If no checkpoints exist, the following message appears in the field. **No appliance restore checkpoint currently exists. Create an appliance checkpoint to revert to the current state of the appliance.** The following describes each of the checkpoint types. ■ Pre-upgrade checkpoint This checkpoint is created before a software upgrade is performed. ■ Post-upgrade checkpoint This checkpoint is created after you have upgraded your appliance to a newer software version. You may use this checkpoint if you have a need to roll back your appliance to correct a failure. ■ User-directed checkpoint You are responsible for creating this checkpoint. You can create a checkpoint at any time. Only one user-directed checkpoint can exist at any given time. If a user-directed checkpoint already exists and you create a new checkpoint, the new checkpoint overwrites the existing checkpoint. However, before you can create the new checkpoint, a message appears in the **Existing appliance restore checkpoints** field and informs you that if you create a new user-directed checkpoint, the new checkpoint overwrites any existing checkpoint. ■ You can also monitor the status of the checkpoint creation process from this field.
The following components of the appliance will be included in the checkpoint:	This field lists all of the components that are included in the checkpoint. The following list describes these 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 primary server appliance is not included. ■ The backup data is not included.

Table 3-18 Create Appliance Checkpoint page *(continued)*

Field	Description
Create appliance checkpoint	This field is optional. It enables you to provide a label or description for the checkpoint. What you enter in this field helps you identify the new checkpoint.
Action buttons on this page	**Validate** ■ When you click the **Validate** button you initiate a validation process that ensures the server is running and in a state to create a new checkpoint. ■ A message appears after the validation is run that informs you whether the validation was successful or not. ■ If the validation process is successful the following occurs: ■ The **Create** button becomes active. ■ The following message appears: **Checkpoint validation is complete. Click *Create* to create the new checkpoint.** ■ If the validation process is not successful the following occurs: ■ The following message appears: **Checkpoint validation was unsuccessful. The checkpoint cannot be created. Click *here* for more information.** ■ You can click a link within the message to view more information about the error details. **Create** ■ The **Create** button becomes active after the checkpoint validation completes successfully. Click **Create** to begin the checkpoint process. ■ When you create this checkpoint, it replaces any current user-directed checkpoint if one exists. **Cancel** This button cancels the create appliance checkpoint process.

See “Creating an appliance checkpoint” on page 140.

See “Checkpoint creation status” on page 143.

See “Creating an appliance checkpoint from the appliance shell menu” on page 144.

See “ Manage > Appliance Restore” on page 136.

Creating an appliance checkpoint

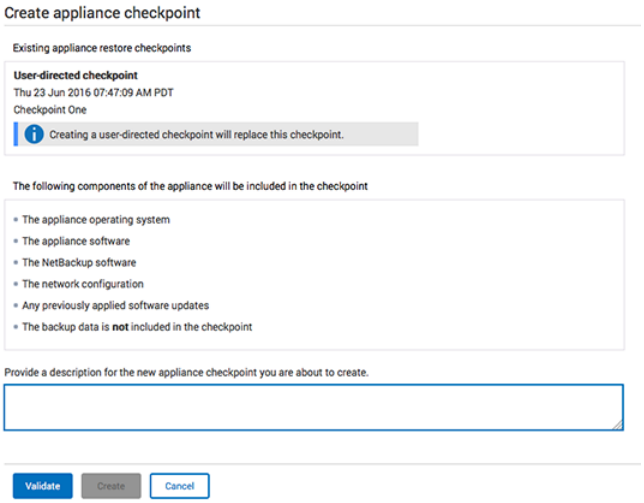
You begin the process of creating a user-directed checkpoint from the **Create Appliance Checkpoint** page on the NetBackup Appliance Web Console. The first two fields on this page do not require any input from you. The first field is the **Existing appliance restore checkpoints** field. That field displays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

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

To create a new checkpoint from the NetBackup Appliance Web Console

1. Select **Manage** > **Appliance Restore**.
2. Click **Create Appliance Checkpoint**.

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



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

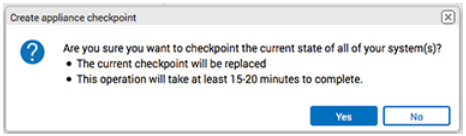
4 Click **Validate**.

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

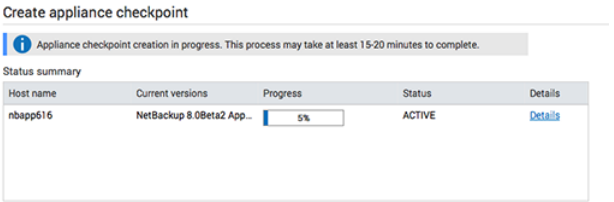
If the checkpoint validation was unsuccessful, a status message appears on the page letting you know that the checkpoint cannot be created. A link in the message is provided that you can select to view more information about the media server that is not operational. You should correct that issue and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

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

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



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

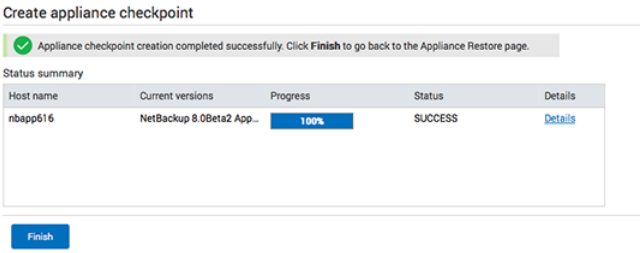


See “Checkpoint creation status” on page 143.

6 After the checkpoint creation completes the **Create appliance checkpoint** page displays a status summary that provides the following information:

- Host name is the IP address of the appliance or appliances that receive the checkpoint.
- Current NetBackup and appliance software versions installed
- Progress of the checkpoint creation.
- Status of the checkpoint.
- Details of the checkpoint

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



See "About creating an appliance checkpoint" on page 137.

See " Manage > Appliance Restore" on page 136.

Checkpoint creation status

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

Table 3-19 Checkpoint creation status

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

See "Creating an appliance checkpoint" on page 140.

See "About creating an appliance checkpoint" on page 137.

See " Manage > Appliance Restore" on page 136.

Creating an appliance checkpoint from the appliance shell menu

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

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

To create a new checkpoint from the appliance shell menu

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

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

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

   ```
   Creating an Appliance Checkpoint allows the user to easily
    rollback the entire system back to a point-in-time to undo any
    misconfiguration or system failure that might have occurred. An
   Appliance Checkpoint captures the following components:
           1) Appliance Operating System
           2) Appliance Software
           3) NetBackup Software
           4) Networking Configuration
           5) Any previously applied patches
           6) Backup data is not reverted

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

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

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

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

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

     Please wait...

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

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

See "Checkpoint creation status" on page 143.

See "About creating an appliance checkpoint" on page 137.

See " Manage > Appliance Restore" on page 136.

About rollback to a checkpoint

Rolling back to an appliance checkpoint restores the system to a previous point-in-time image. This process is referred to as a Rollback operation.

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

- Pre-upgrade checkpoint
  This checkpoint is created before a software upgrade is performed. If a software upgrade fails, this checkpoint is used automatically or manually to roll back the appliance to the pre-upgrade state.
- Post-upgrade checkpoint
  This checkpoint is created after you have upgraded your appliance to a newer version. You may use this checkpoint if you have a need to roll back your appliance to correct a failure.
- User-directed checkpoint
  A checkpoint that you created.

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

- Only valid checkpoints are displayed for you to select.

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

See “About appliance rollback ” on page 146.

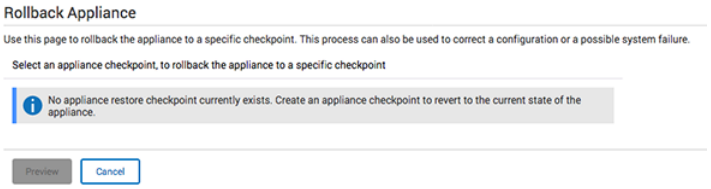
See “About appliance rollback validation” on page 148.

See “About checkpoint rollback status” on page 152.

About appliance rollback

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

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



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

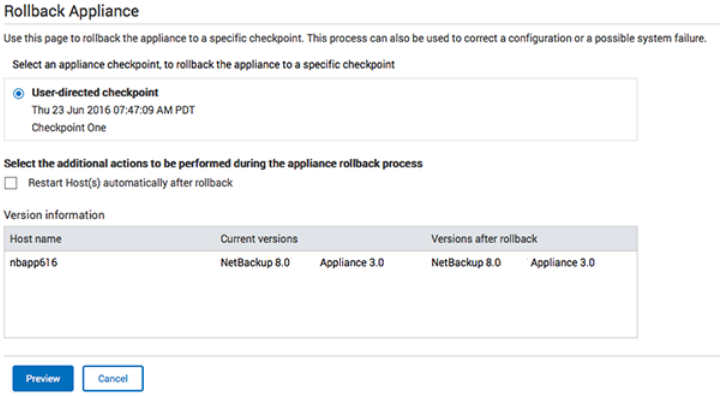


Table 3-20 contains the following fields and functions:

Table 3-20 Rollback Appliance page

Field	Description
Select an appliance checkpoint, to rollback the appliance to a specific checkpoint	This field shows the available checkpoints that you can use to revert your appliance. The available checkpoints can be: ■ Pre-upgrade checkpoint A checkpoint that is created before you perform a software upgrade. ■ Post-upgrade checkpoint A checkpoint that is created after you have upgraded your appliance to a newer software version. ■ User-directed checkpoint A checkpoint that you created.
Select the additional actions to be performed during the rollback process	You can elect to automatically restart the appliances after the rollback operation completes.

Table 3-20 Rollback Appliance page *(continued)*

Field	Description
Version information	If checkpoints exists, you see the table. If no checkpoints exist, this table is not shown. The table provides the following information: ■ **Host Name** The IP address of the primary or media server appliance. ■ **Current versions** The NetBackup and appliance software versions currently installed before the rollback operation begins. ■ **Versions after rollback** The NetBackup and appliance software versions that are installed after the rollback operation succeeds.
Action icons	The **Preview** icon provides you with the ability to preview the appliance(s) to ensure that a rollback operation can proceed. If an appliance is not up and running, a message appears that identifies the appliance, so that you can make any necessary adjustments. The **Preview** icon cancels the rollback operation.

See "About appliance rollback validation" on page 148.

See "About checkpoint rollback status" on page 152.

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 primary server appliance is not included.
- The backup data is not included.

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

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

See "About appliance rollback " on page 146.

See "About checkpoint rollback status" on page 152.

See "About appliance rollback " on page 146.

Rollback to an appliance checkpoint from the NetBackup Appliance Web Console

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

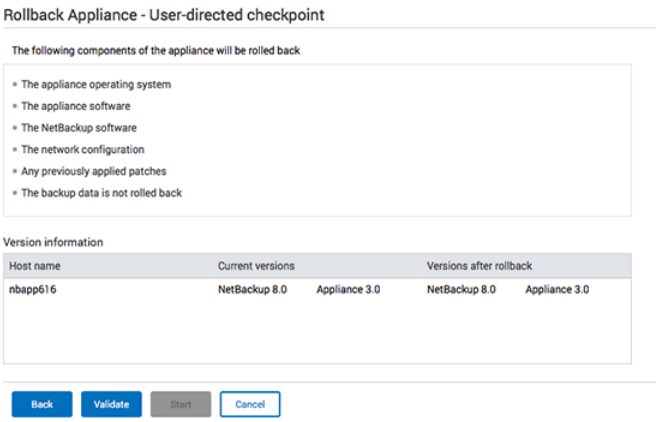
To roll back to an existing checkpoint from the NetBackup Appliance Web Console

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

   The list contains only those checkpoints that exist. At most, there can be three checkpoints. A pre-upgrade checkpoint, a post-upgrade checkpoint, and a user-directed checkpoint.
4. Determine if you want to restart the appliance automatically after the rollback operation completes. If you do, check the **Restart appliance automatically after rollback** check box.

5 Click **Preview**.

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

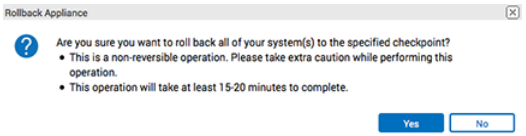


6 Click **Validate**.

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

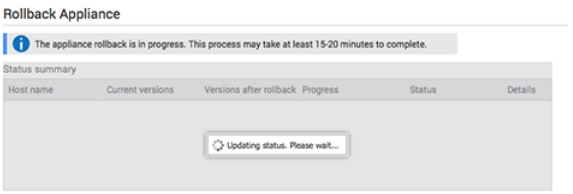
If the checkpoint validation was unsuccessful, you are not able to start the rollback operation. A link is provided that you can select to view more information about the cause of the issue. You can then, correct that issue, and click **Validate**. If the validation is successful, click **Start**.

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



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

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



9 After the rollback operation completes the compute appliance must be restarted:

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

See “Rollback to an appliance checkpoint from the appliance shell menu” on page 152.

See “ Manage > Appliance Restore” on page 136.

About checkpoint rollback status

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

Table 3-21 Checkpoint Rollback status

Field	Description
Host name	The IP address of the appliances that are about to be rolled back.
Current versions	The version NetBackup software that is currently installed on the appliance.
Verison after rollback	The version of appliance software that is installed on the appliance after the rollback is complete.
Progress	Displays the percentage of completion for each appliance.
State	Displays whether the checkpoint operation completed successfully or not. Possible status for this field: **Success**, **Failed**, **Completed**, **Timed-out**.
Details	This field contains a link labeled **Details**. Click this link to view more detailed information about the status of the appliance rollback operation.

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

See “About appliance rollback validation” on page 148.

See “About appliance rollback ” on page 146.

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!
```

See “Checkpoint creation status” on page 143.

See “About creating an appliance checkpoint” on page 137.

See “ Manage > Appliance Restore” on page 136.

About NetBackup appliance factory reset

The purpose of an appliance factory reset is to return your appliance to a clean, unconfigured, and factory state. By default, a factory reset discards all storage configuration and backup data. However, before you initiate the factory reset, you can elect to retain the storage configuration, network configuration and backup data if any currently exists. In addition, you can elect to restart the appliance after the reset completes.

If you run a factory reset of the appliance, note the following:

- A factory reset disables WAN optimization for all network interface bonds if you retain your network configuration.
  After the factory reset completes, you can then enable WAN optimization again for the network interface bonds.
- If you *do not* retain your network configuration, all network interface bonds are lost during the factory reset. After the reset completes, the appliance automatically enables WAN optimization for all network interface ports, including those that comprised the bonds.

Note: Starting with the NetBackup Appliance 5.0 release, if you perform a factory reset with storage preserved, you can reset the system to the current version only. If you perform a factory reset without storage preserved, you can reset the appliance to a different version. After the reset is completed, the original networking configuration will be lost, so you have to login using the IPMI to reconfigure the appliance.

Note: Starting with the NetBackup Appliance 5.0 release, during the re-image of a NetBackup 5240/5330/5340 Appliance from the USB drive/CDROM or in case of a factory reset or upgrade, a copy of the ISO being installed is saved in the newly added partition, /dev/mapper/system-iso.

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

See “ Manage > Appliance Restore” on page 136.

Factory reset best practices

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

- **Note:** Starting with the NetBackup Appliance 5.0 release, if you perform a factory reset with storage preserved, you can reset the system to the current version only. If you perform a factory reset without storage preserved, you can reset the appliance to a different version. After the reset is completed, the original networking configuration will be lost, so you have to login using the IPMI to reconfigure the appliance.

- During a factory reset, the data or storage may not be deleted. This situation happens if one or more partitions are in use or some processes continue to access the partition.
  The following is an example of an error message that is displayed when storage is in use:
  ```
  - [Error] Failed to unmount the 'Configuration' partition '0'
  because the partition is currently in use. Restarting the appliance
  and retrying the operation may help to resolve the issue. Contact
  Veritas Technical Support if the issue persists.
  ```
- Before performing 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.
- If you remove attached storage disks before performing a factory reset, you need to clear the preserved cache of the RAID controller.
  See "Discard RAID preserved cache after performing a factory reset" in the *NetBackup Appliance Troubleshooting Guide* for more information.
- If you remove a storage unit shelf during a factory reset, the factory reset operation can fail. Veritas recommends that you leave all storage unit shelves attached during a factory reset.
- Make sure to stop all running backup, duplication, or restore jobs before performing a Factory Reset. NetBackup storage objects, storage units, disk pools, and storage servers on the primary server that belong to the media server appliance are not cleaned up if a Factory Reset operation is performed while backup, duplication or restore jobs are still in progress.

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 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: Starting with the NetBackup Appliance 5.0 release, if you perform a factory reset with storage preserved, you can reset the system to the current version only. If you perform a factory reset without storage preserved, you can reset the appliance to a different version. After the reset is completed, the original networking configuration will be lost, so you have to login using the IPMI to reconfigure the appliance.

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

To begin a factory reset from the appliance shell menu

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

```
Appliance factory reset will reset the entire system to the
factory installed image. The appliance will have the following components
reset to the factory restored settings/image:
1) Appliance Operating System
2) Appliance Software
3) NetBackup Software
5) Networking configuration (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

- [Info] Performing a factory reset preserves all backup data on the storage
partitions of all connected storage expansion units.
```

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]

- [Info] Appliance will make the following version changes:

+-------------------------------------------------------------------------+
|  Appliance  |         Current Version       |        Reverted Version       |
|-------------+-------------------------------+-------------------------------|
|<hostname>   |NetBackup 10.3 Appliance 5.3   |NetBackup 10.0 Appliance 5.0   |
+-------------------------------------------------------------------------+
```

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

```
>> WARNING: An appliance factory reset cannot be reversed!
The reset process takes about 90 minutes. The appliance
will be restarted to start the reset process.
Do you want to continue? (yes/no) yes
```

The factory reset continues and info messages are shown.

5 You must use the remote management port to reconfigure the network settings and reconnect to the NetBackup Appliance Web Console. Perform the following steps:

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

See "About NetBackup appliance factory reset" on page 156.

Manage > Appliance License

You can review, add, and delete appliance license keys for your 5250 or 5350 appliance through the NetBackup Appliance Web Console using the **Manage > Appliance License** page. License keys are not required for 5240 and 5340 appliances.

Note: Starting with appliance release 5.3, you can no longer add or renew NetBackup licenses on the appliance. Instead, you must use the NetBackup Web UI for NetBackup license management. For details, see the following:

NetBackup Web UI Administration Guide

Veritas Entitlement Management System (VEMS) User's Guide:

https://www.veritas.com/content/support/en_US/article.100048764

Note: Starting with appliance release 5.1.1, license management is supported only on the primary server. On an appliance media server, the **License** tab in the web console provides no information or functionality.

Applied license keys	Describes the license type, license capacity, and the license expiration date.
License table	■ Describes the license details for the selected applied license. ■ **Add** Click to add a new appliance license. ■ **Delete** Click to remove an appliance license

To obtain the appropriate licenses for your environment, see the following article:

https://www.veritas.com/support/en_US/article.100048764

See "Managing license keys on the NetBackup appliance" on page 161.

Managing license keys on the NetBackup appliance

The following procedures describe how to view, add, and delete NetBackup 5250 and 5350 Appliance license keys through the NetBackup Appliance Web Console (web console) or the NetBackup Appliance Shell Menu (shell menu). License keys are not required for 5240 and 5340 appliances.

To obtain the appropriate licenses for your environment, refer to the following topic: "Generate and install an appliance license" See "Generate and install an appliance license" on page 163.

Note: Starting with appliance release 5.3, you can no longer add or renew NetBackup licenses on the appliance. Instead, you must use the NetBackup Web UI for NetBackup license management. For details, see the following:

NetBackup Web UI Administration Guide

Veritas Entitlement Management System (VEMS) User's Guide:

https://www.veritas.com/content/support/en_US/article.100048764

To add an appliance license key through the web console

1. Obtain the appropriate license as described in the topic "Generate and install an appliance license".
2. Log on to the NetBackup Appliance Web Console.

3 Click **Manage > Appliance License**. All installed license keys are displayed with their associated details.

4 To add a new appliance license key, click **Add**.

5 In the **Add new license file** dialog, click **Choose Files** to browse for the license that you want to add.

6 After selecting the license file, click **Apply**.

To delete an installed appliance license key through the web console

1 Log on to the NetBackup Appliance Web Console.

2 Click **Manage > Appliance License**. All installed license keys are displayed with their associated details.

3 Select the license key from the list, then click **Delete**.

4 When the **Delete License** dialog appears to ensure that you want to continue, click **Delete**.

5 When the confirmation message appears to show that the license was deleted, click **OK**.

To view, add, and delete license keys through the shell menu

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

- `Main_Menu > Manage > License > Appliance > List`
  A complete list of installed license keys appears.
- `Main_Menu > Manage > License > Appliance > ListInfo`
  The associated feature IDs and feature names appear.

2 To add license keys, do the following:

- Obtain the appropriate license as described in the topic "Generate and install an appliance license".
- Enter the following command:
  `Main_Menu > Manage > License > Appliance > Add <license_file_name>`
- Follow the prompts to upload the license file to this appliance if you have not done it yet. Then, enter **Yes** and press **Enter**.

3 To delete license keys, do the following:

- Enter the following command:
  `Main_Menu > Manage > License > Appliance > Remove <license_file_name>, then press` **`Enter.`**

Generate and install an appliance license

After you deploy a new 5250 or 5350 appliance with version 5.1.1 or later, or upgrade an existing 5250 or 5350 appliance to version 5.1.1 or later, you are required to install a valid appliance license on the appliance. Once you have completed either of these operations, you must access the Veritas Entitlement Management System (VEMS) website to generate the appropriate license for your appliance. See the following document:

https://www.veritas.com/support/en_US/article.100048764

An appliance license requires host ID validation and limits the use of the license to a specific appliance.

License keys are not required for 5240 and 5340 appliances.

Starting with appliance release 5.1.1, the following operations also require license compliance:

- Storage partition creation (Co-Pilot Shares, CDP Gateway partition, MSDP, AdvancedDisk).
- Storage resize (CDP Gateway partition, MSDP, AdvancedDisk).
- Online download of appliance upgrade packages from the NetBackup Appliance Web Console (web consol) or the NetBackup Appliance Shell Menu (shell menu).
- Installation of the upgrade package from the NetBackup Appliance Shell Menu.

Before you begin any of these tasks, review your existing licenses to determine if you need additional storage capacity or license renewal.

The following procedure describes how to generate the proper appliance license on the VEMS website and add it to the appliance. You must have the appliance hostname or the virtual hostname of the appliance high availability (HA) setup to generate the license with a host lock string.

To create an appliance license and install it on the appliance

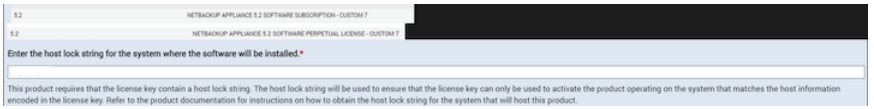
1. Log in to the shell menu and run one of the following commands to get the appliance hostname or virtual hostname for the HA setup:

   `Network > Hostname > Show`

   HA setups: `Manage > HighAvailability > Status`

2. Click on this link to access the Veritas Entitlement Management System (VEMS) User's Guide. Scroll down the page and click **Generating License Keys**.

3 For a NetBackup Appliance license, select a **Custom 7** license type and enter the hostname or virtual hostname in the field as shown in the following example:



4 After you have entered all of the other required information, click **Generate** to generate the license key.

5 To retrieve the generated license key, click the **License Keys Page** link. You can copy or email the license key.

6 Upload the license key to the general share on the appliance as follows:

```
Main > Settings > Share General Open
```

7 Add the license key to the appliance with the following command:

```
Manage > License > Appliance > Add license_key_filename
```

8 After the license key has been added successfully, close the general share as follows:

```
Main > Settings > Share General Close
```

About the Migration Utility

The Migration Utility lets you migrate backup images from source disk pool to destination disk pool. The original backup images remain on the source disk pool after the migration completes.

The backup images can be either full or all. A valid source disk pool is any recognized disk pool in the same domain. A valid target disk pool can be any Veritas NetBackup disk pool. You can create a migration task on any appliance within the same domain. However, Veritas recommends that you configure a migration task from a NetBackup appliance primary server.

With this feature, you can do the following:

- Copy all backup images or only full backup images from source storage disk pool to destination storage disk pool.
- Schedule a migration task and run it on multiple days.
- Backup image migration without affecting existing backup schedules.
- Update policies during the migration process so new backup images automatically go to the new storage.

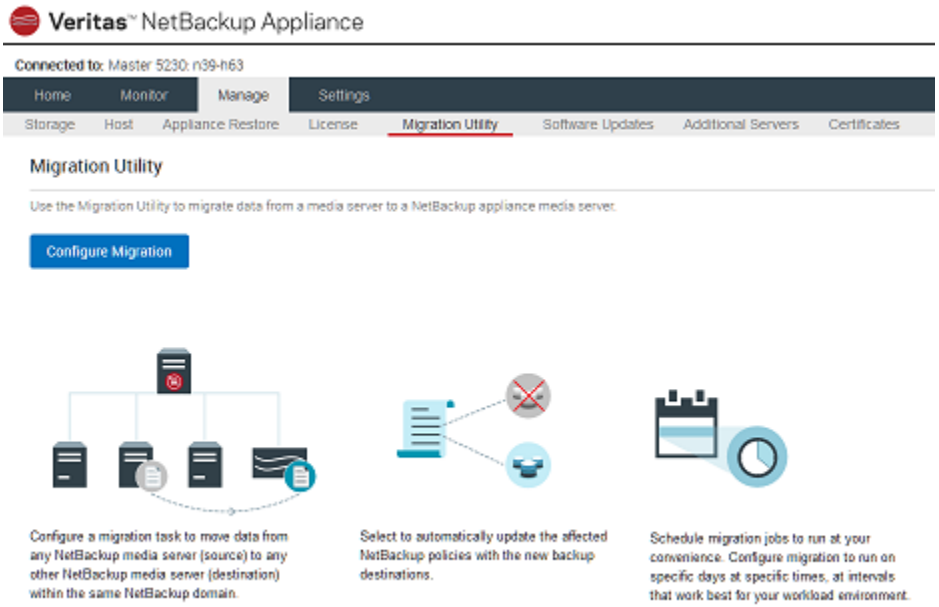
The Migration Utility feature is applicable with the following conditions:

- Images available for migration are the latest complete backup images for a specific policy-client pair.
- The image type has two options: **All backup images** and **Last full backup images**. Select **All backup images** to migrate full and incremental backup images. Select **Last full backup images** to migrate last full backup images.
- The latest complete backup only includes complete images and storage lifecycle complete images.
- The migration can be performed from an MSDP to another MSDP through the Fibre Channel.
- Before you start the migration utility, make sure that you have the logon credentials. Go to the **Media and Device Management > Credentials > Storage Servers > Media Servers** window in the NetBackup Administration Console. Check the boxes next to the media servers that are used for your migration task. You cannot perform a migration task unless these credentials have been selected. For more information, refer to the *NetBackup Administrator Guide*.

A four-step wizard enables you to schedule a migration task to migrate your backup images automatically. After you complete the migration task configuration, you are able to check details in the migration status table.

Click **Manage > Migration Utility**, the following page appears:

Figure 3-5 Migration Utility



The **Manage > Migration Utility** page enables you to configure and view the following:

- Migration utility wizard
  See "Manage > Migration Utility > Configure Migration" on page 166.
- Migration Status page
  See "Manage > Migration Utility > Migration Status" on page 171.
- Configuring a new migration task
  See "Configuring a new migration task" on page 173.
- Viewing the migration task status
  See "Viewing the migration task status" on page 176.
- Best practices for migration utility
  See "Best practices for migration utility" on page 177.

Manage > Migration Utility > Configure Migration

In the NetBackup Appliance Web Console, navigate to the **Manage > Migration Utility** page. A task-oriented wizard can help you schedule a migration task from the NetBackup Appliance Web Console.

Multiple migration tasks are not supported. The **Configure Migration** button is inactive when an existing migration task is queued or running.

Enter the migration configuration wizard by clicking the **Configure Migration** button.

To configure a migration task

1. Select source and destination
2. Specify selection criteria
3. Set up policy update
4. Schedule migration

About the migration task configuration steps: See "Configuring a new migration task" on page 173.

Table 3-22 lists the selections of **step 1: Select source and destination**.

Table 3-22 Selections of step 1: Select source and destination

	Selections	Description
Source	Source media server	Select a source media server where the original backup images reside.
	Source disk pool	Select a disk pool where the original backup images reside. The source disk pool is any recognized and connected disk pool in the source media server.
Destination	Destination media server	Select a destination media server for the migration.
	Destination disk pool	Select a destination disk pool where you want the migrated backup images to reside. The destination disk pool is any recognized Veritas provided disk pool in the destination media server.

Table 3-23 lists the selections of **step 2: Specify selection criteria**.

Table 3-23 Selections of step 2: Specify selection criteria

Selections	Description
Policy type	Click this checkbox to select the policy type from the list of policies displayed. You can search backup images based on the policy type selections. For example, if you select the policy type as **Standard**, all the policies that belong to this type are selected. You can use **Select All** and **Clear All** to select or remove the selections of all policies at the same time.
Policy name	Enter the policy name for the images to be migrated . If you do not know the policy name, do an advanced search as follows: ■ Use * as a placeholder to match one or more words in a policy name. For example, enter `policy*` to search the policy `policy1`, `policy12`, and `policy123`. ■ Use ? as a placeholder to match exactly one word in a policy name. For Example, enter policy? To search the policy name `policy1`, but not `policy12`.
Image Type	Select the image type that you want to migrate from the following: ■ **All backup images**: includes all full backup images and incremental images on the source disk pool. ■ **Last full backup images**: includes the last full backup image and all full backup images that are created in 2 hours before the last full backup image has been created.

The policy update is an optional step. You can skip this step if you do not want to automatically update polices. However, Veritas recommends that you set up policy update when you configure a migration task. You can update policies to save new backup images in the new Storage Units (STUs) or to apply new Storage Lifecycle Policies (SLPs) to new backup images without any additional steps.

Table 3-24 lists the selections of **step 3: Set up policy update**.

Table 3-24 Selections of step 3: Update policies

Selections	Description
Update policies during migration	Select the checkbox to enable policy updates during the migration.
Source storage	View the source media server and the source disk pool name.
Destination storage	View the destination media server and the destination disk pool name.
Storage Unites - Current Storage Unit	View the current available storage unit(s) (STUs).
Storage Units – New Storage Unit	Select a new STU from the drop-down list. Make sure that the new STU is ready for use.
Storage Lifecycle Policies – Current Storage Lifecycle Policy	View the current available storage lifecycle policies(SLPs). The SLP is a storage plan for a set of backups. An SLP contains instructions in the form of storage operations, to be applied to the data that is backed up by a backup policy.
Storage Lifecycle Policies – New Storage Lifecycle Policy	Select a new SLP from the drop-down list. Make sure that the new SLP has been created and is ready for use.

Table 3-25 lists the selections of **step 4: Schedule migration**.

Table 3-25 Selections of step 4: Schedule migration

Selections	Description
Start date	Click **Calendar** to select the appropriate date (in date, month, and year) for scheduling a start time for the migration task. The default value is the current date. The migration utility uses the appliance system date/time configurations.

Table 3-25 Selections of step 4: Schedule migration *(continued)*

Selections	Description
Migration window	Use migration window to complete the entire migration task through a small, defined processing window. You can specify the start and end time for a migration window. The limitation of migration window is from **1** minute to **23:59** hours. Specify the **Start time** and **End time** by following: ■ Enter a value in **HH:MM** format or click the arrows to increase or decrease the value ■ Click the button to select **AM** or **PM** for the value. You can check the migration window length in the **Duration of Migration window** field. Select the checkbox next to **Stop the current job when the end of the migration window is reached** to stop the backup migration immediately when the end is reached. The interrupted backup image is available for the next time that the migration window is open.
Run migration for	Specify how many times you want to run the migration task. Properly consider how to set this value according to the number of backup images that you want to migrate. **Note:** Go to the destination storage and make sure that all target backup images have been migrated completely when the migration task reaches the due date. If any scheduled backups are not migrated, set up a new migration task to continue migrating the remaining backup images.
Run on	Select one or more days that you want to run the migration task on per week. The options are from **Monday** to **Sunday**.

Manage > Migration Utility > Migration Status

After a migration task starts, you are able to view its status on the **Migration Utility** page. The most recent migration task appears on the top of the table. A migration task can contain one or more jobs. A migration job is created each time the migration window opens. In the **Migration Status** table, you can view details by doing the following:

- Click the arrow icon in the first column to expand a migration task record. The migration job details appear.
- Click **View** in the **Actions** column to view the migration task configuration.

Table 3-26 lists the elements of **Migration Status**.

Table 3-26 Migration Status

Elements	Description
Task ID	Displays the migration task ID number.
Progress	Displays migration task running progress. Expand a migration task to view migration job running progress.
Migration Window	Displays the elapsed time of completed migration window. The value is equal to the sum of the completed migration job windows. Expand a migration task record to view the migration window progress bar. The migration window progress bar displays in different colors, see the following: ■ **Gray**: remaining time ■ **Blue**: elapsed time ■ **Red**: exceeded time **Note:** The migration window may be exceeded if the checkbox **Stop the current job when the end of the migration window is reached.** is not selected.
Images Migrated	Displays the total number of backup images that have been migrated.
Data Transferred	Displays the size (MB) of data that have been transferred during migration.

Table 3-26 Migration Status *(continued)*

Elements	Description
Transfer Rate	Displays the data transfer rate (MBPS) of the migration task.
Policies Updated	Displays the total number of policies that have been updated during migration.
Status	Displays the status of the migration task. The available statuses are: ■ **RUNNING** - The migration task is querying policies and images, transferring images or updating policies. ■ **QUEUED** - The migration task is waiting for running. The migration task starts at the scheduled start date. ■ **CANCELED** - The migration task has been canceled. The backup images that have been migrated before you cancel the migration task exist both on source and destination storage. ■ **SUCCESS** - All of the backup images that meet the search criteria have been successfully migrated to the destination storage. ■ **FAILED** - The migration task failed to migrate all of the backup images to the destination storage. To check the detailed reasons, you can view logs from the **Job Detail** of the **Migration Status** table.

Table 3-26 Migration Status *(continued)*

Elements	Description
Actions	Do more actions by clicking the links as follows: ■ Click **View** to view migration task configurations in the **Migration Task Configuration Details** window. ■ Click **Remove** to remove a migration task record from the **Migration Status** table. A **QUEUED** or **RUNNING** migration task cannot be removed. ■ Click **Job Details** to view migration job logs after the migration job completes. ■ Click **Cancel** to cancel an active migration task. A completed task cannot be cancelled.

For more information about how to view the migration task status, refer to the following:

See "Viewing the migration task status" on page 176.

Configuring a new migration task

In the NetBackup Appliance Web Console, navigate to the **Manage > Migration Utility** page.

Configure a migration task and start the migration configuration wizard by clicking the **Configure Migration** button. Quit the configuration procedure at any time by clicking the **Cancel** button.

Note: Do not configure a migration task on the same appliance from a different web console. This may cause the migration task configuration to fail.

To Configure a migration task

1. Log on to the NetBackup Appliance Web Console.
2. Navigate to the **Manage > Migration Utility** page.
3. Click **Configure Migration** to enter the **Select source and destination** panel.
4. From the drop-down list, select the following:
   - **Source media server**

- **Source disk pool**
- **Destination media server**
- **Destination disk pool**

About the selections description: **To specify the selection criteria, do the following:**

See "Manage > Migration Utility > Configure Migration" on page 166.

5 Click **Next** to enter the **Specify selection criteria** panel.

6 In the **Policy type** field, select one or more policies that are used to search backup images that you want to migrate.

Click **Select All** to select all polices at one time.

Click **Clear All** to deselect all policies at one time.

For more information about backup policy, refer to the *NetBackup Admin Guide*.

7 In the **Policy name** text box, enter a policy name or use the * and ? characters to search for more policies at one time.

8 In the **Image type** field, select a image type that you want to migrate. The **All backup images** includes full and incremental backup images.

About the selections description: See "Manage > Migration Utility > Configure Migration" on page 166.

9 Click **Next** to enter the **Set up policy update** panel.

Veritas recommends that you enable the policy update when you configure a migration task. It lets you assign new destination Storage Units (STUs) or Storage Lifecycle Policies (SLPs) for NBU backup. If you select the **Update policies during migration**, the following occurs after the migration task completes successfully:

- The destination STU is updated to the policy. The new backups automatically go to the new STU.
- The new SLP automatically applies to the new backups.

Note: To complete the policy update configuration, at least one new STU or SLP must be selected.

---

10 Select the checkbox next to **Update policies during migration** to expand the policy conversion configuration.

11 Verify the following values:

- Source media server
- Source disk pool
- Destination media server
- Destination disk pool

12 In the **Storage Unites** area, the current STU(s) is displayed under the **Current Storage Unit** column. The current STU(s) can be one or more, depending on your source disk pool settings.

From the drop-down list under the **New Storage Unit** column, select a new STU(s).

13 In the **Storage Lifecycle Policies** area, the current SLP(s) is displayed under the **Current Storage Lifecycle Policy** column. The current SLP(s) can be one or more, depending on your source disk pool settings.

From the drop-down list under the **New Storage Lifecycle Policy** column, select a new SLP(s).

Note: SLP selection is not mandatory, however, it can help you automatically update the current SLP(s) to the new one after the migration completes.

About the selections description: See "Manage > Migration Utility > Configure Migration" on page 166.

14 Click **Next** to enter the **Schedule migration** panel.

15 In the **Start date** field, enter a date or click the calendar to select a date. The migration task is scheduled to start on that date.

Note: The date and time of migration task use the appliance system time settings. Note that the time of your web browser can be different from the appliance.

---

16 In the **Migration window** field, specify the **Start time** and **End time** to create a migration window. The migration window length decides how many backup images can be migrated in one job.

The running migration job does not stop when the migration window ends. If you intend to stop the running migration job immediately when the migration window ends, select the checkbox next to **Stop the current job when the end of the migration window is reached.** The image that is migrating will be available for the next search when the migration window is open.

The migration window makes the migration task migrating the backup images in phases. However this does add some complexity to the migration utility, because each of the backup images must be possible to fit in the migration window. Properly consider how to configure the migration window length according to your image size and network speed.

17 Specify a number in the **Run migration for** text box to indicate how many times that the migration window opens. If you have numerous backup images that you want to migrate, increase the migration task running times.

18 In the **Run on** field, select one or more days that the migration task runs on. The options are from **Monday** to **Sunday**.

About the selections description: See "Manage > Migration Utility > Configure Migration" on page 166.

19 Click **Start** to complete the migration task configuration.

The migration task is queued for running on scheduled date.

Viewing the migration task status

In the NetBackup Appliance Web Console, navigate to the **Manage > Migration Utility** page. The migration task status displays in the **Migration Status** table after you configure a migration task. The migration job detail is available when the migration job completed.

To view the migration task status

1 Log on to the NetBackup Appliance Web Console.

2 Navigate to **Manage > Migration Utility** page.

3 On the **Migration Status** page, under the **Actions** column, do the following:

- Click **View** to open the **Migration Task Configuration Details** window and view the migration task configuration.
- Click **Remove** to remove a migration task record that is marked as completed from the web console. A **QUEUED** or **RUNNING** migration task cannot be removed.

- Click **Cancel** to stop a **QUEUED** or **RUNNING** migration task.
- Click **Job Details** to view specific migration job logs.

If you want to see detailed reasons when a migration task fails, do the following:

1. Record the **Activity monitor job id** from the **Job Details** window.
2. Log on to the NetBackup Administrator Console.
3. Open the **Activity Monitor**.
4. Use the job Id to locate the specific job, and double click it.
5. The **Job Details xx** window appears. You can view job details in this window.

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

About the migration status table description: See "Manage > Migration Utility > Migration Status" on page 171.

Best practices for migration utility

This topic contains best practices information about migration utility operations.

- Use the appliance primary server to be the "Migration Utility Appliance." Because the migration utility requires access to the NetBackup domain information (for example, policy, storage, and catalog), using a primary server provides better performance in selection criteria searching.
- If you want to update policies with new SLPs during the migration, make sure the new storage lifecycle policy has been created and is available for the migration utility before the migration task starts.
- It is possible that some backup images cannot be migrated because the size of the backup images is too big to fit in the migration window. To solve this problem, you can check the image size, enlarge the migration window, and try again.
- For more guidelines on planning and configuring a migration task, see the following:
  - Log in to the NetBackup Java Console, and check the backup image size and the policy detail of the backup images that you want to migrate.
  - Create a test migration task with a small amount of data to migrate. This can help you roughly estimate the migration speed according to your system performance and workload.
  - Schedule a migration task based on the calculation results got from test run, and start the migration task.
  - Double check if all target backup images have been totally migrated to the destination storage after the migration task completes.

- If the **Update policies during migration** is enabled, you can check if the policies have been updated after the migration task succeeds. To check the updated policies, go to the NetBackup Administration Console. For more information, refer to the *NetBackup Administrator Guide*.

Software release updates for NetBackup Appliances

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

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

- VxOS (Linux-based) operating system
- NetBackup server
- NetBackup Appliance Web Console

NetBackup clients are not included with NetBackup appliance release updates. If you want to store clients on the appliance, a separate client package is available to download. The client package is available from the same location as the server release updates and includes the NetBackup Administration Console.

Note: Appliance upgrades are not supported from the NetBackup Appliance Web Console. Use an SSH session or the IPMI console to log in to the NetBackup Appliance Shell Menu to upgrade appliances. For upgrades from versions 3.1 and later, you may also use the **Appliance Management Console**.

Note: Client versions that are stored on the appliance do not have to match the NetBackup version that is currently installed on the appliance.

See “Installing a NetBackup appliance software update using the NetBackup Appliance Shell Menu” on page 180.

Manage > Software Updates

Use this page to browse for a software update that is available on the appliance or to upload packages to the appliance, such as hotfixes/patches, add-ons, and the

Appliance Upgrade Readiness Analyzer. You can also download the latest appliance software release from the Veritas Support website.

Note: Appliance upgrades are not supported from the NetBackup Appliance Web Console. Use an SSH session or the IPMI console to log in to the NetBackup Appliance Shell Menu to upgrade appliances. For upgrades from versions 3.1 and later, you may also use the **Appliance Management Console**.

The Software Updates page displays the following sections:

- **Downloaded Software Updates**
  - Shows the current software version that is installed on the appliance.
  - Shows the downloaded software updates (packages) that are available to install on the appliance.
- **Online Software Updates** - Shows the available software updates you can download and then install on the appliance.

The following table describes the fields and buttons in the **Downloaded Software Updates** section.

Table 3-27 Downloaded Software Updates

Field name	Description
Available Software Update	Shows the name and the version of the appliance software updates that are already downloaded and available to install.
Version	Shows the version of NetBackup Appliance software that is available for installation.
NetBackup Version	Shows the version of NetBackup software that is included with the appliance software update.
Size	Shows the size of the software update to help ensure that you have enough space on the appliance to accommodate the installation.
Details	Click to view additional information about the software update.
Upload	Click to upload packages to this appliance such as hotfixes/patches, add-ons, and the Appliance Upgrade Readiness Analyzer. Uploaded packages appear in the **Available Software Update** column.

Table 3-27 Downloaded Software Updates *(continued)*

Field name	Description
Delete	Click to remove any selected package in the **Available Software Update** column that is no longer needed.

The following table describes the fields and buttons in the **Online Software Updates** section. This table remains visible throughout the upgrade process.

Table 3-28 Online Software Updates

Field name	Description
Online Software Updates	Shows the version of the appliance software update that you can select to download to the appliance.
Version	Shows the version of NetBackup Appliance software that is available for installation.
Size	Shows the version of NetBackup software that is included with the appliance software update that you can select to download.
Download Progress	Shows the progress of the software download.
Download	After you have selected a software update version, click **Download** to start the download process. The table refreshes to show the status of the download. If you decide to cancel the download, click the red **X** next to the selected software update on the right side of the table.

Installing a NetBackup appliance software update using the NetBackup Appliance Shell Menu

Use the following procedure to start the appliance upgrade.

Note: Always perform upgrades with the admin user account. Do not use a non-admin user account to upgrade appliances.

Note: If you have enabled the STIG feature on an appliance and you need to upgrade it or install an EEB on it, do not plan such installations during the 4:00am - 4:30am time frame. By following this best practice, you can avoid interrupting the automatic update of the `AIDE` database and any monitored files, which can cause multiple alert messages from the appliance.

Note: Starting with appliance release 5.3, the STIG feature is enabled by default. Upgrades to version 5.3 enable STIG automatically, even if it was not enabled before the upgrade. The upgrade preflight check and the Appliance Upgrade Readiness Analyzer tool do not check for STIG password compliance. You are not prompted or required to change passwords before or during the upgrade.

To install a downloaded release update using the NetBackup Appliance Shell Menu

1. Check to make sure that the following required updates and pre-upgrade tasks have already been performed:
   - All required pre-upgrade updates have been completed. For a complete list of required updates prior to 5.3 upgrades, refer to the following article: https://www.veritas.com/content/support/en_US/article.100052181
   - The upgrade script stops and restarts the NetBackup services as needed during the upgrade. To avoid job interruptions during the upgrade, you may want to manually stop or suspend all jobs and pause all SLPs before the upgrade.
   - The `Support > Test Software` command has been run and it returned a **Pass** result.
2. Log in to the NetBackup Appliance Shell Menu from the IPMI console.

   Note: Veritas recommends that you log in using the shell menu from the IPMI console instead of an SSH session. The IPMI console is also known as the Veritas Remote Manager interface. For details about how to access and use the Veritas Remote Manager, refer to the following document: *NetBackup Appliance Hardware Installation Guide*.

3. Make sure that you have downloaded and have run the latest version of the Appliance Upgrade Readiness Analyzer tool. The analyzer tool must produce a `pass` result before you can continue to the next step.

4 To install the software release update, run the following command:

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

Where *patch_name* is the name of the release update to install. Make sure that this patch name is the one that you want to install.

5 Monitor the preflight check and watch for any failure and warning messages.

- If no **Check failed** messages appear, you are prompted to continue to the next step to start the upgrade.
- If any **Check failed** messages appear, the upgrade is not allowed. You must resolve the reported failures, then launch the upgrade script again so that the preflight check can verify that the failures have been resolved.
- If any **Check failed** messages indicate that a RHEL version third-party plug-in was not found, you must obtain the plug-in from the appropriate vendor.
- If any warning messages appear, Veritas recommends that you read the message and try to resolve the issue before you continue the upgrade. A warning message does not prevent the upgrade from proceeding.

6 Starting with release 5.0, a Call Home settings test is performed. If Call Home is disabled, a prompt appears for you to enable the feature to ensure the Call Home test is performed. You can also enable a proxy server if the test fails. The following warning message is displayed:

Warning: The appliance is not able to connect to the Veritas Call Home server to upload hardware and software telemetry. Providing the Call Home information to Veritas allows for an improved support experience and recommendations through the NetInsights Console. It is recommended that you enable Call Home and ensure the system can reach the Veritas Call Home server through correct name resolution or proxy server setting.

You can ignore this warning and continue to the next step.

7 After all preflight check items have passed, and before the upgrade begins, you must first select how the upgrade process should respond if any errors occur during the upgrade. The following prompt appears:

```
If an error occurs during the upgrade, do you want to

immediately enforce an automatic rollback? [yes, no]
```

Enter **yes** to immediately enforce an automatic rollback.

Enter **no** to pause the upgrade process and investigate the errors.

8 After all preflight check items have passed, you may need to trust the CA certificate and the host ID-based certificate to start the upgrade process.

To trust and deploy the CA certificates, do the following:

- Verify the CA certificate detail and enter **yes** to trust the CA certificate, as follows:

```
To continue with the upgrade, verify the following CA
certificate detail and enter "yes" to trust the CA certificate.
CA Certificate Details:
     Subject Name : /CN=nbatd/OU=root@abc.example.com/O=vx
       Start Date : Jul 14 12:59:18 2017 GMT
      Expiry Date : Jul 09 14:14:18 2037 GMT
 SHA1 Fingerprint : 31:E9:97:2E:50:11:51:7C:D6:25:7F:32:86:3D:
                    6B:D5:33:5C:11:E2

>> Do you want to trust the CA certificate? [yes, no](yes)
```

- If the security level of the primary server is **Very High**, you must manually enter an authorization token to deploy the host ID-based certificate on the appliance, as follows:

```
>> Enter token:
```

Note: If the appliance does not have a valid host-id certificate before the next upgrade to a later version, a reissue token is required for the next upgrade.

- If the security level of the primary server is **High** or **Medium**, the authentication token is not required. The host ID-based certificate is automatically deployed onto the appliance.

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

9 During the upgrade process, you can login using SSH and start the AIM window to check the upgrade status (except during the reboot process).

To check the upgrade status, you can:

- Login using an SSH session and start the AIM window to monitor the upgrade process. Enter the following command:
  Main_Menu > **Manage** > **Software** > **UpgradeStatus**.
- Login using the IPMI console and start the AIM window. Enter the following command:

Main_Menu > **Manage** > **Software** > **UpgradeStatus**.

- Monitor the upgrade process using the IPMI console. When all the updates have been installed successfully, a login prompt appears.

10 If problems are detected during the post-upgrade self-test, the **AIM** window shows the upgrade status as **Paused**. Other SSH sessions and email notifications also indicate this status.

To clear the **Paused** status, perform the following tasks:

- Press the **V** key to switch to the **Verbose** view to see the logs. If there are any Unique Message Identification (UMI) codes for the errors, search for them on the Veritas Support website to get more detailed information.
- Try to fix the problem that the **AIM** window reports.
  If you need to use the shell menu, log on to the NetBackup Appliance Shell Menu through an SSH session. When the **AIM** window appears, press the **S** key to close it.
- Go back to the **AIM** window on the IPMI console.
  If you tried fixing the problem, press the **A** key to attempt the self-test again. If you cannot fix the problem, contact Veritas Support or press the **R** key to roll back the appliance to the previous software version.

11 After the upgrade has completed, the **AIM** window shows a summary of the upgrade results.

After the disk pools are back online, the appliance runs a self-diagnostic test. Refer to the following file for the test results:

`/log/selftest_report_<appliance_serial>_<timedate>.txt`

If SMTP is configured, an email notification that contains the self-test result is sent.

12 For HA setups only:

After you have completed the upgrade on the first node, run the `Support > Test Software` command to verify the status of various appliance software components. If the test passes, log in to the other node and upgrade it in the same manner as the first node.

13 Complete this step only if your backup environment includes SAN client computers.

The Fibre Channel (FC) ports must be re-scanned to allow any SAN client computers to reconnect to the Fibre Transport (FT) devices. The re-scan must be done from the NetBackup CLI view on the appliance.

To re-scan the FC ports:

- Enter the following command to see a list of NetBackup user accounts:
  `Manage > NetBackupCLI > List`
- Log on to this appliance as one of the listed NetBackup users.
- Run the following command to rescan the FC ports:
  `nbftconfig -rescanallclients`
- If any SAN clients still do not work, run the following commands on each of those clients in the order as shown:
  On UNIX clients:
  `/usr/openv/netbackup/bin/bp.kill_all`
  `/usr/openv/netbackup/bin/bp.start_all`
  On Windows clients:
  `<install_path>\NetBackup\bin\bpdown`
  `<install_path>\NetBackup\bin\bpup`
- If any SAN clients still do not work, manually initiate a SCSI device refresh at the OS level. The refresh method depends on the operating system of the client. Once the refresh has completed, attempt the `nbftconfig -rescanallclients` command again.
- If any SAN clients still do not work, reboot those clients.

Note: If you have SLES 10 or SLES 11 SAN clients that still do not work, Veritas recommends upgrading the QLogic driver on those clients. For the affected SLES 10 clients, upgrade to version 8.04.00.06.10.3-K. For the affected SLES 11 clients, upgrade to version 8.04.00.06.11.1.

Note: Starting with NetBackup Appliance version 5.0, refer to the *NetBackup Appliance Security Guide* to run NetBackup commands as a NetBackupCLI user.

Appliance servers to upgrade

After you click **Install** to install a software update, the **Manage > Software Updates** page refreshes and displays the following tables:

- **Install Software Update**
  This table displays the servers that are to be upgraded with the software update that you selected to install.
- **Online Software Updates Available**

This table remains visible throughout the upgrade process. It shows the available software updates that are applicable to your appliance that you can download.

Table 3-29 Servers identified for the software update

Field name	Description
Server	The name of the server that is currently configured in your primary server environment. In a cluster configuration, multiple media servers are displayed.
Software Update Name	The name of the software update that you have selected for installation.
Software Update Version	The new version of the appliance software on the server after the software is updated successfully.

See "Manage > Software Updates" on page 178.

Installing NetBackup PSF add-ons using the NetBackup Appliance Shell Menu

The NetBackup appliance supports installing appliance Parallel Streaming Framework (PSF) add-ons. The add-ons help protect the **Hadoop** and **Nutanix Acropolis Hypervisor (AHV)** data on your NetBackup appliance.

To install the PSF add-ons using the NetBackup Appliance Shell Menu

1. Log in to the NetBackup Appliance Shell Menu.
2. Open an NFS or a CIFS share by using the following command:

   ```
   Main_Menu > Manage > Software > Share Open
   ```

   Copy the downloaded packages to the open share.
3. Close the NFS and the CIFS shares by using the following command:

   ```
   Main_Menu > Manage > Software > Share Close
   ```
4. Install the PSF add-ons by using the following command:

   ```
   Main_Menu > Manage > Software > Install Patch_name
   ```

   Where *Patch_name* is the name of the PSF add-ons to install.

   For example:

   - `NBAPP_addon_PSF_Hadoop_Plugin-8.1.0.0-xxxxxxxxx.x86_64.rpm`
   - `NBAPP_addon_PSF_Nutanix-AHV_Plugin-8.1.0.0-xxxxxxxxxx.x86_64.rpm`

5 Enter `yes` when you are asked the following question:

```
Do you want to proceed with the installation of this
add-on?(yes/no)yes
```

6 Read and agree the Veritas Software License Agreement that displays on your output screen.

7 To continue installing the add-ons, enter `y` when you see the following message:

```
Would you like to continue?[y,n](y)
```

See the *Veritas NetBackup for Hadoop Administrator's Guide* and the *Veritas NetBackup for Acropolis Hypervisor (AHV) Administrator's Guide* for more information on this feature.

About installing EEBs

Emergency engineering binaries (EEBs) are provided on an individual basis to meet specific needs for a specific customer. A hotfix/patch is an EEB that is available to all customers. If you have one or more EEBs that you want to install, you should store them locally so that you can upload them to the appliance using the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu (appliance shell menu). You must install EEBs using the shell menu must be installed using the appliance shell menu or the Appliance Management Server (AMS).

Starting with the 3.3.0.1 release, an installed EEB can be replaced with a newer revision of the same EEB without the need for a manual rollback of the currently installed revision.

A revision number in the EEB file name appears immediately after the software version number, as follows:

```
NBAPP_EEB_ET1234567-3.2-1.x86_64.rpm
```

In this example, `-1` indicates revision one, or the first issued revision of the EEB. When the same EEB is revised or updated, the revision number is changed to `-2`.

The following describes how the installation process works when you install a new revision of the same EEB:

1. You install `NBAPP_EEB_ET1234567-3.2-1.x86_64.rpm`.
2. A few months later, you obtain and install the revised EEB: `NBAPP_EEB_ET1234567-3.2-2.x86_64.rpm`.
3. When the installation starts, the revised EEB script first checks and finds the earlier EEB revision, and performs a rollback automatically.

4. After the rollback of the earlier revision has completed, the new revision is installed.

Note: You cannot replace an existing EEB with an earlier or older revision of the EEB.

See "Installing an EEB" on page 188.

Installing an EEB

An emergency engineering binary, also known as an EEB or a hotfix/patch, is installed the same way as a software update by using the appliance shell menu. Starting with release 3.2, you can install EEBs from the Appliance Management Server (AMS). For details, see the *Veritas Appliance Management Guide*.

Note: Starting with release 4.0, you can upload EEB packages to the appliance using the NetBackup Appliance Web Console. However, the web console does not support EEB installation.

You should perform this procedure from a computer that is connected to the appliance as well as to the Internet.

To install an appliance emergency engineering binary using the NetBackup Appliance Shell Menu

1 Upload the EEB package as follows:

- NetBackup Appliance Web Console
  Log in to the web console and go to the Manage > Software Updates page. Click the Upload option and follow the prompts to locate and upload the package.
- NetBackup Appliance Shell Menu
  - Open an SSH session and log on to the appliance as an administrator.
  - Enter the following command to open the NFS and the CIFS shares:
    `Main_Menu > Manage > Software > Share Open`
  - Map or mount the appliance share directory as follows:
    Windows CIFS share: `\\<appliance-name>\incoming_patches`
    UNIX NFS share: `<appliance-name>:/inst/patch/incoming`
    Note that on Windows systems, you are prompted to provide the user name, `admin`, and its corresponding password.

2 Copy the EEB from your local computer to the mapped directory.

3. Unmap or unmount the directory after you have successfully downloaded the EEB.
4. From the appliance, enter the following command to close the NFS and the CIFS shares:

   `Main_Menu > Manage > Software > Share Close`

   Once the EEB is downloaded on to the share directory that you defined, it is moved to the proper location. You are not notified that this move has occurred.

   If you run the `List EEBs` command before you run the `Share Close` command, the update is still moved from the share directory location to its proper location. Make sure that you have run the `Share Close` command to ensure that you close the NFS and the CIFS shares.
5. Enter the following command to list the EEBs that are available for downloading

   `Main_Menu > Manage > Software > List Downloaded`
6. Enter the following command to install the release update.

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

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

   Before you proceed with the installation of the EEB, ensure that there are no jobs running on the appliance.

About installing NetBackup Administration Console and client software

You can use two different methods to install the NetBackup client software on the clients that you want to back up. You can install NetBackup client software on clients as follows:

- Use CIFS and NFS shares and run scripts to install the software silently. Depending on the operating system, you run the `quickinstall.exe` script or the `unix-client-install` script. This is a silent install. The scripts do not prompt you for any user-related questions. They automatically update the NetBackup configuration on the client with the appliance server name as the Primary server.
- Select a link on the appliance login page to download the packages and install the software.

On the appliance login page, you can click on the **Software** link to download a package that contains the NetBackup Administration Console and the NetBackup client software.

You can also elect to download and install the NetBackup Administration Console. To download and install the client software, you perform the following functions:

- Choose the client type that you want to install.
- Select the software package to download.
- Unzip or untar the package.
- Run the install (UNIX) or setup.exe (Windows) script.
- Update the NetBackup configuration on client with the Primary Server information (for example, `bp.conf` on UNIX systems).

See "Installing NetBackup client software through an NFS share" on page 190.

See "Downloading NetBackup client packages to a client from a NetBackup appliance" on page 193.

Installing NetBackup client software through an NFS share

After all appliance configuration has been completed, you can open an NFS share to install NetBackup client software on the UNIX clients that you plan to use with your configured appliance.

Before the installation, make sure that you have downloaded the NetBackup client software package to the appliance and verified that it exists in the following NFS share: `<appliance-name>:/inst/client`

NetBackup UNIX client software installation through an NFS share

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

1. Log on to the primary appliance from the NetBackup Appliance Shell Menu with your administrator credentials.
2. Add the client host names to the additional servers list of the primary server appliance using the following command:

   ```
   Main_Menu > Settings > NetBackup AdditionalServers Add
   ```

3. Open the NFS share using the following command:

   ```
   Main_Menu > Settings > Share ClientInstall Open
   ```

4. On the UNIX client host where you want to install the NetBackup client software, log on as root.
5. Mount the following NFS share:

   `<appliance_name>:/inst/client`
6. On the client, browse the files within the NFS share directory. The following files or directories appear:
   - `NetBackup_8.x_CLIENTS2` and/or `NetBackup_8.x_CLIENTS1`
   - `.packages`
   - `clientconfig`
   - `quickinstall.exe`
   - `PC_Clnt`
   - `docs`
   - `unix-client-install`
7. On the client, use a text editor to open the following file:

   `/inst/client/clientconfig/defaults.txt`
8. Add one or more media servers from this NetBackup domain to the `ADDITIONALSERVERS` entry. Use only the host name to specify a media server. Use a comma-separated list if you want to add multiple media servers.

   Example:

   ```
   PRIMARIESERVER=primary123.test.com
   ADDITIONALSERVERS=media1.test.com,media2.test.come,media3.test.com
   ```

   Note: Media servers that are used for backing up the client hosts are preferred. If you do not know the media servers in this NetBackup domain, run the `Main > Settings > NetBackup AdditionalServers Show|ShowAll` commands on the primary appliance. You can also check the media servers from the NetBackup Administration Console.

   Save the file and exit the editor.

9 Create the NetBackup answer file (`NBInstallAnswer.conf`) in the client `/tmp` directory.

Example:

```
CA_CERTIFICATE_FINGERPRINT=<fingureprint_value>
AUTHORIZATION_TOKEN=<token>
```

More information about the answer file and its contents is available in the *NetBackup Installation Guide*

10 Populate `NBInstallAnswer.conf` with the following information:

```
CA_CERTIFICATE_FINGERPRINT=<fingureprint_value>
```

Example (the fingerprint value is wrapped for readability):

```
CA_CERTIFICATE_FINGERPRINT=30:A5:9A:D1:18:F0:01:E4:21:E8:0D:A0:
26:95:14:52:7C:7A:58:B1
```

Depending on the security configuration in your NetBackup environment, you may need to add the `AUTHORIZATION_TOKEN` option to the answer file.

Additional information about the NetBackup answer file is available:

See the *NetBackup Installation Guide*

Additional information about the CA certificate fingerprint and the authorization token is available:

See the *NetBackup Security and Encryption Guide*

11 Run the `unix-client-install` script.

This action installs the NetBackup client software.

12 Check the following file on the client. Make sure that the `bp.conf` file contains the media server names you added to the `defaults.txt` file in Step 8.

```
/usr/openv/netbackup/bp.conf
```

13 On the appliance, close the shared directory using the following command:

```
Main > Settings > Share ClientInstall Close
```

See "Downloading NetBackup client packages to a client from a NetBackup appliance" on page 193.

Downloading NetBackup client packages to a client from a NetBackup appliance

You can download NetBackup client software from a NetBackup appliance to any client that you want to back up. The NetBackup Appliance Web Console logon page provides a **Download Packages** section to download the client packages. If no packages are available on the logon page, you can download client and add-on packages from the Veritas Download Center.

Note: If you need to install or upgrade the Windows client add-on, log in to your Veritas Entitlement Management System (VEMS) account and download it.

The packages are listed by operating system type in a drop-down box as follows:

- All
- Windows
- Linux
- Solaris
- AIX
- HP
- BSD

In addition to the downloading instructions, this procedure also includes the steps to extract and install the downloaded files on to the client.

To download NetBackup client packages from a NetBackup appliance to a client

1. Log in to the client that you want to back up.
2. Open a browser window and enter the appliance URL.
3. In the middle of the landing page, in the section **Download Packages**, click on the drop-down box to see the list of packages.
4. Right-click the selected package and specify the location to download it onto the client.

   For example, on Linux or UNIX platforms, download the package to `/tmp`.

   Note: If the message **No packages found** appears after you make a selection, that client package is not currently installed on the appliance. Refer to the following topic to download client packages on to the appliance:

   ---

5 Untar the package.

6 Install the client software as follows:

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

7 After you have successfully installed the client software, add the appliance primary server name to the client as follows:

Windows systems

- After NetBackup has been installed on the client, open the Backup, Archive, and Restore interface:
  Start > All Programs > Veritas NetBackup > Backup, Archive, and Restore
- From the Backup, Archive, and Restore interface, select **File > Specify NetBackup Machines and Policy Type...**
- From the **Specify NetBackup Machines and Policy Type** dialog, enter the server name in the field **Server to use for backups and restores**. Then click **Edit Server List** and click **OK**.
- In the dialog box that appears, enter the fully qualified host name of the appliance primary server and click **OK**.
- Close the Backup, Archive, and Restore interface.
- Restart the NetBackup Client Services by opening a Windows Command prompt. Then, enter `services.msc` and press **Enter**.

UNIX systems

- On the client, navigate to the following location:
  `cd /usr/openv/netbackup`
- Enter `ls` to see the contents of the directory.
- Open the `bp.conf` file in a text editor.
- Enter the fully qualified host name of the appliance primary server.
- Save the changes and close the file.

See "Installing NetBackup client software through an NFS share" on page 190.

Manage > Additional Servers

From the **Manage > Additional Servers** page you can add or delete additional servers. This tab lets you add an entry to the NetBackup `bp.conf` file. The `bp.conf` file allows communication to occur between the appliance and the Windows NetBackup Administration Console, so you can manage your appliance through

that console. You must add the host name of a media server to the additional servers before configuring the media server.

See "Managing additional servers to the appliance" on page 195.

Managing additional servers to the appliance

The following procedures enable you to add or delete servers from the **Additional Servers** page on the NetBackup Appliance Web Console.

Use the following procedure to add additional servers to the appliance.

To add an additional server:

1. Log on to the NetBackup Appliance Web Console.
2. Click **Manage > Additonal Servers**.
3. Click the **Add** button.

   The **Add Additional Server** dialog box is displayed.
4. In the **Server Name** field, enter the name of the server that you want to add, and then click **OK**.

   Note: You can add multiple server name entries separated using a comma(,).

   The appliance displays the following message:

   ```
   Additional server(s) added successfully.
   ```
5. Click **Cancel** to exit the **Add Additional Server** dialog box.

Use the following procedure to delete servers from the appliance.

To delete an additional server

1. Log on to the NetBackup Appliance Web Console.
2. Click **Manage > Additional Servers**.

   The **Additional Servers** page displays a list of all the additional servers added to your appliance.
3. Select the check box against the server that you want to delete, and then click the **Delete** button.
4. The following warning is displayed:

   ```
   Are you sure you want to proceed?
   ```

5 Click **Yes** to delete the selected server. The following message is displayed:

```
Additional server(s) deleted successfully.
```

6 To delete all the servers from the appliance, select the **Server Name** check box, and click **Delete**.

See "Manage > Additional Servers" on page 194.

Manage > File Manager

Use this tab to manage all uploaded files on the appliance. You can upload certificate files and other similar files.

Note: To upload packages such as hotfixes/patches, add-ons, and the Appliance Upgrade Readiness Analyzer, go to the **Manage > Software Updates** page.

The following table describes the functions and the information fields that appear on this page:

Table 3-30 File Manager

Function/Field	Description
Upload	Click to open a dialog box where you can find and select files to upload.
Delete	Click to remove any selected file that currently resides in the `/inst/share` directory on the appliance.
File name	Shows the names of the files that currently reside in the `/inst/share` directory on the appliance.
File size	Shows the size of the files that currently reside in the `/inst/share` directory on the appliance.

Manage > High Availability

The **Manage > High Availability** menu enables you to manage your high availability (HA) configuration:

- Check the status. The menu includes status information for the nodes in an HA configuration and the services that are running on those nodes.

See "Monitoring a high availability configuration from the NetBackup Appliance Web Console" on page 197.

For more information about the NetBackup 53xx HA configuration, refer to *NetBackup 53xx Appliance High Availability Reference Guide*.

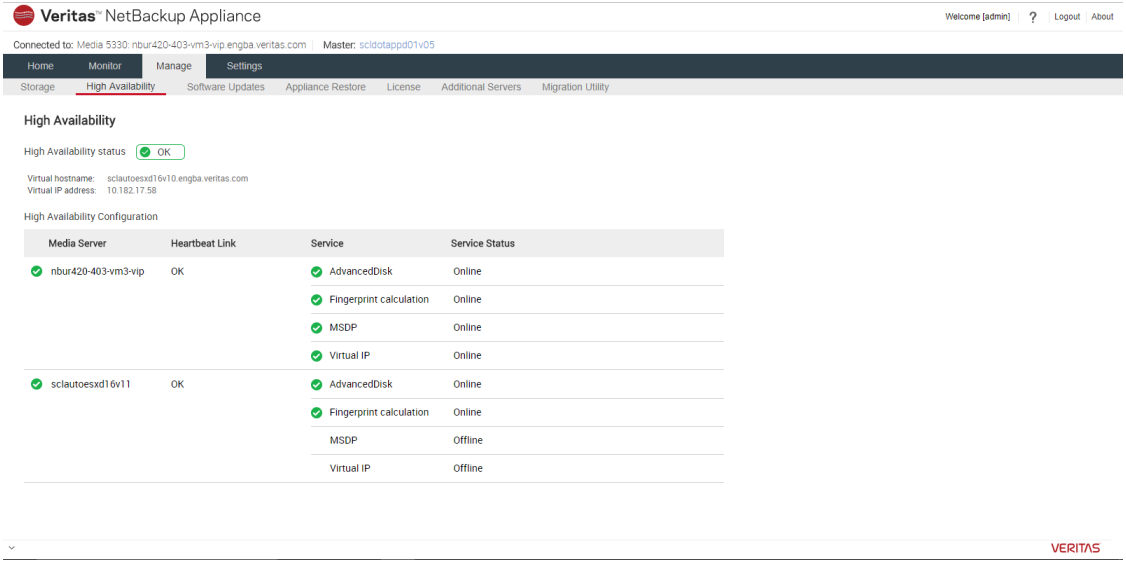
Monitoring a high availability configuration from the NetBackup Appliance Web Console

In a NetBackup 53xx high availability (HA) configuration, you can check the status of the configuration from the NetBackup Appliance Web Console.

To check the status of the HA configuration

1. On the configured node, log on to the NetBackup Appliance Web Console as `admin`.
2. On the **Welcome to Vertias NetBackup Appliance Web Console** page, click **Manage** > **High Availability**.
3. On **High Availability** page, you can see the status of the HA configuration and the status of the related services.

The following is an example of the status information for a complete HA configuration:



If you want to check the hardware status of the HA configuration, navigate to the **Monitor** > **Hardware** page.

See “Monitor > Hardware options” on page 36.

Chapter 4

Managing NetBackup appliance using the NetBackup Appliance Shell Menu

This chapter includes the following topics:

Expanding the bandwidth on the NetBackup appliance

The appliance has the capability to provide link aggregation. Link aggregation increases the bandwidth and availability of the communications channel between the appliance and other devices.

Link aggregation is enabled by default when you perform the initial network configuration from the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu.

You can use the NetBackup Appliance Shell Menu to enable or disable link aggregation, as well as view the status of the link aggregation.

Use the following commands to enable, disable, and view the status of link aggregation:

- To enable the network link aggregation:
  Main_Menu > **Network** > **LinkAggregation Enable**
- To disable the network link aggregation:
  Main_Menu > **Network** > **LinkAggregation Disable**
- To show the status of the network link aggregation:
  Main_Menu > **Network** > **LinkAggregation Status**

About configuring the maximum transmission unit size

The MTU property controls the maximum transmission unit size for an Ethernet frame. The standard maximum transmission unit size for Ethernet is 1500 bytes (without headers). In supported environments, the MTU property can be set to larger values in excess of 9,000 bytes. Setting a larger frame size on an interface is commonly referred to as using jumbo frames. Jumbo frames help reduce fragmentation as data is sent over the network and in some cases, can also provide better throughput and reduced CPU usage. To take advantage of jumbo frames, the Ethernet cards, drivers, and switching must all support jumbo frames. Additionally, each server interface that is used to transfer data to the appliance must be configured for jumbo frames.

If you configure the MTU property of an interface to values larger than 1500 bytes, it is recommended that all systems that are connected to the appliance on the specific interface have the same maximum transmission unit size. Such systems include, but are not limited to, NetBackup clients and remote desktops. Also verify the network hardware, the OS, and the driver support on all systems before you configure the MTU property.

You can configure the MTU property for an interface by using the `SetProperty` command in the NetBackup Appliance Shell Menu.

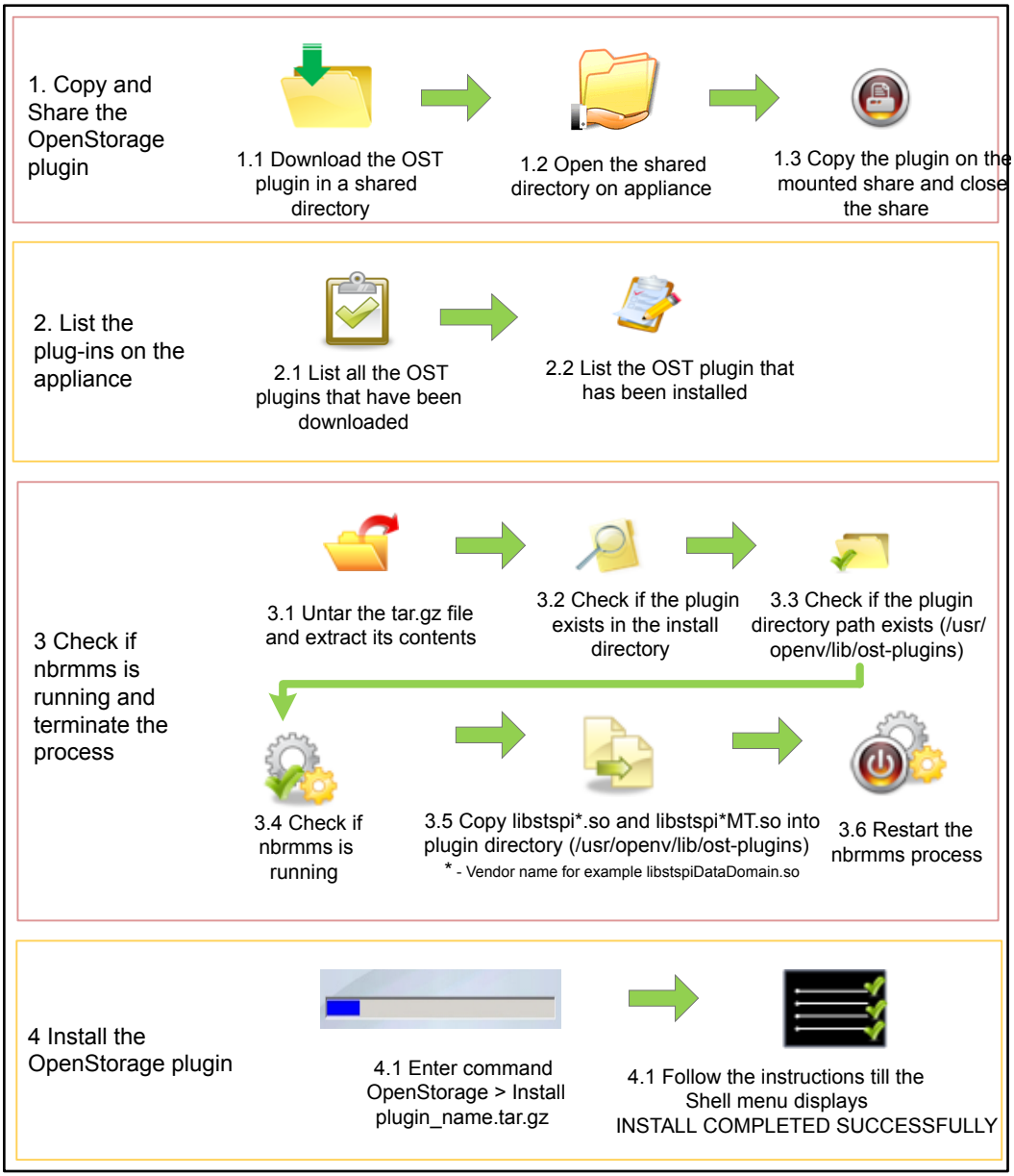
See the `SetProperty` command in the *NetBackup Appliance Command Reference Guide*.

About OpenStorage plugin installation

You can install and open an OpenStorage (OST) plugin on the NetBackup appliance using the NetBackup Appliance Shell Menu. The OST plugins enable you to install multiple plugins to communicate with their corresponding storage systems.

The following diagram illustrates the process to install the OpenStorage plugin.

Figure 4-1 OpenStorage plugin installation process



See "Installing the OpenStorage plugin" on page 203.

See "Uninstalling the OpenStorage plugin" on page 204.

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

Installing the OpenStorage plugin

The following procedure describes how to install the OpenStorage (OST) plugin through the NetBackup Appliance Shell Menu.

To install the OpenStorage plugin

1. Log on to the NetBackup Appliance Shell Menu.
2. Download the latest version of the OST plugin from the required vendor's support Website.
3. Open the shared directory. To open the shared directory on the appliance choose from the following commands:

   - `Main Menu > Manage > OpenStorage > Share Open`

   The appliance displays the following message:

   ```
   The CIFS share \\nbapphostname\general_share
   and the NFS share nbapphostname:/inst/share
   have been opened on this appliance.
   ```

4. Copy the OST plugin using CIFS or NFS share.
5. Close the shared directory. To close the shared directory use the following command:

   - `MainMenu > Manage > OpenStorage > Share Close`

6. After the plugin is downloaded on the appliance, you can use the list commands to view the plugin details. To view the details of the downloaded plugins choose from the following commands:

   - `OpenStorage > List Available`
     Displays a list of all the downloaded plugins and not yet applied.
   - `OpenStorage > List Installed`
     Displays a detailed list of all the installed plugins on the appliance.

7. Install the downloaded plugin. To install the downloaded plugin, choose from the following commands based on the appliance you use:

   - `OpenStorage > Install` *`plugin_name`* to install the OST plugin on media and primary appliances.

   The appliance initiates the installation process.

See "About OpenStorage plugin installation" on page 201.

See "Uninstalling the OpenStorage plugin" on page 204.

Uninstalling the OpenStorage plugin

The following procedure describes how to uninstall the OpenStorage (OST) plugin through the appliance shell menu.

To uninstall a OpenStorage plugin

1 To uninstall the OST plugin use the following command:

```
OpenStorage > Uninstall plugin_name

Uninstalls the OST plugin on media and primary appliances.
```

The appliance initiates the process to uninstall the OST plugin as displayed using the following example:

```
- [Info] Checking for the installed OpenStorage plugin ...
>> The plugin package plugin_name.tar.gz is currently installed
on the system. Do you want to continue uninstalling it? (yes/no)
```

2 Type `yes` to continue and uninstall the plugin.

The appliance displays the following message:

```
There might be some existing backups on the storage server.

Are you sure you want to continue uninstalling the plugin? (yes/no)
```

3 Type `yes` to continue and uninstall the plugin.

The appliance continues the uninstall process and displays the following:

```
- Uninstalling the plugin plugin_name.tar.gz    ok

- Successfully uninstalled the plugin plugin_name.tar.gz
```

See "About OpenStorage plugin installation" on page 201.

See "Installing the OpenStorage plugin" on page 203.

About mounting a remote NFS

You can use the NetBackup Appliance Shell Menu to mount a remote Network File System (NFS) onto the appliance server through the `Manage > MountPoints` menu.

To work with the NFS drive, you can use the following commands in the NetBackup Appliance Shell Menu.

Table 4-1 Commands to work with NFS drive

Command	Descriptions
`Mount`	Use the `Mount` command to mount an NFS drive.
`List`	Use the `List` command to list all the existing mount points on your appliance.
`Unmount`	Use the `Unmount` command to un-mount a previously mounted NFS drive.

See "Mounting a remote NFS drive" on page 205.

See "Unmounting an NFS drive" on page 207.

In certain circumstances, you may find that a NetBackup appliance NFS share is not accessible. If this issue occurs, use the NetBackup Appliance Shell Menu to restart the NFS server. Use the following command:

```
Support > Service Restart nfs-server
```

Once you have restarted the server, try again to access the NFS share.

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

Mounting a remote NFS drive

This procedure describes how to mount your remote NFS drive.

To mount a remote NFS drive

1. Log on to the NetBackup Appliance Shell Menu using your administrator's credentials.
2. Type the `Main > Manage> MountPoints` command.

   The appliance lists all the commands under in the `MountPoints` menu.

3 To mount your remote NFS drive, type the following command:

```
Mount RemotePath MountPoint [FileSystemType] [options]
```

This command includes the following parameters:

	RemotePath	***MountPoint***	**[FileSystemType]**	**[Options]**
Description	Provide the address of a device or a directory to be mounted on to your appliance.	Provide the name of the local mount point. This appears as a subdirectory where the NFS drive is mounted. After the command runs successfully, this subdirectory is created under /mnt/remote. **Note:** An error may be displayed if the full directory path (example: '/tmp/garry') is specified instead of just a mount point name (example: garry).	Specify the type of the device to be mounted.	Specify any additional options to be passed to the appliance along with the `Mount` command.
Format	`HOST:DIRECTORY` **Note:** A short hostname is also supported. Ensure that the short hostname can be resolved.	A subdirectory name under /mnt/remote. The subdirectory may or may not exist and is created under /mnt/remote by default.		You can only use options specific for mounting the NFS drive.
Parameter type	Mandatory	Mandatory	Optional	Optional
Example	`appesx5.ros.veritas.com:/build1`	`garry`	`NFSv3` or any other supported type by the underlying `Mount` command.	`ro` is used to mount the device as read only.

4 The appliance mounts your remote NFS drive.

Note: If you mount a remote share and then restart the appliance, the mount is re-established when the appliance starts. The mount points are persistent across all the restart operations and there is no exception to this rule.

To list and view the mounted devices

1. Log in to the NetBackup Appliance Shell Menu using your administrator credentials.
2. Type the `Main > Manage > MountPoints` command.

   The appliance lists all the commands under the `MountPoints` menu.
3. To view the list of mounted devices use the following command:

   `List [Type]`

   When you specify the value for the `[Type]` parameter as [All], the appliance displays all the available mount points along with the NFS drives. If this parameter is not provided, this command lists all the NFS mount points.

Note: In certain circumstances, you may find that a NetBackup appliance NFS share is not accessible. If this issue occurs, use the NetBackup Appliance Shell Menu to restart the NFS server.

Use the followin gcommand: Support > Service Restart nfs-server

Once you have restarted the server, try to access the NFS share again.

See "About mounting a remote NFS" on page 204.

Unmounting an NFS drive

This procedure describes how to unmount an NFS drive.

To unmount an NFS drive

1. Log on to the NetBackup Appliance Shell Menu using your administrator credentials.
2. Type the `Main > Manage > MountPoints` command.

   The appliance lists all the commands under the `MountPoints` menu.
3. To unmount a drive, use the following command:

   `Unmount` *`MountPoint`* `[force].`

   The following options are used to identify the NFS drive to be unmounted.

	MountPoint	**[force]**
Description	Provide the name of the directory that is to be un-mounted. **Note:** An error is displayed in case of the following situations: ■ If the directory name is incorrect. ■ If the directory with the given name does not exist.	Specify this parameter to unmount the NFS forcibly.
Format	The directory name must start with `/` and must have the correct directory name. **Note:** If the specified directory is a valid mount directory, it is unmounted.	
Parameter type	Mandatory	Optional
Example	`/mymounts/mount1`	

4 If the directory name is specified correctly the following process takes place:

- The NFS is unmounted successfully.
- The directory is removed from the file system.
- In case the directory is on a nested path, only that directory is removed.

See "Mounting a remote NFS drive" on page 205.

About running NetBackup commands from the appliance

The NetBackup command-line shell feature enables NetBackup administrators to execute NetBackup commands with superuser privileges. These privileges enable NetBackup administrators to execute the commands that support full NetBackup logging as well as develop and use scripts and automation.

NetBackup appliance administrators can provide access for multiple NetBackup administrators and audit the activity of these administrators. In addition, NetBackup appliance administrators can manage the NetBackup administrator accounts from the `Main > Manage > NetBackupCLI` view within the NetBackup Appliance Shell Menu. From the `NetBackupCLI` view, a NetBackup appliance administrator can

create, delete, and list NetBackup administrator accounts as well as manage their user account passwords.

See "About NetBackup administrator capabilities" on page 209.

See "Creating NetBackup administrator user accounts" on page 215.

See "Managing NetBackup administrator user account passwords" on page 216.

See "Auditing NetBackup administrator accounts" on page 217.

See "Deleting NetBackup administrator user accounts" on page 218.

See "Viewing NetBackup administrator user accounts" on page 219.

About NetBackup administrator capabilities

NetBackup administrators have superuser privileges and share a common home directory within a restricted shell. From this restricted shell, the NetBackup administrators can do the following:

- Use a base command name, an absolute or a relative path, or a shell script as a way to execute NetBackup commands.
- Have full NetBackup logging capabilities.

The following list shows the NetBackup commands that a NetBackup administrator can run with superuser privileges and the directories that contain the NetBackup commands.

- `/usr/openv/netbackup/bin/*`
- `/usr/openv/netbackup/bin/admincmd/*`
- `/usr/openv/netbackup/bin/goodies/*`
- `/usr/openv/volmgr/bin/*`
- `/usr/openv/volmgr/bin/goodies/*`
- `/usr/openv/pdde/pdag/bin/mtstrmd`
- `/usr/openv/pdde/pdag/bin/pdcfg`
- `/usr/openv/pdde/pdag/bin/pdusercfg`
- `/usr/openv/pdde/pdconfigure/pdde`
- `/usr/openv/pdde/pdcr/bin/*`

Note: Because there are NetBackup commands on a NetBackup appliance, it is possible that some of the command arguments are not supported.

The following list shows the commands and scripts that you cannot run from the directories:

- Library files - The files that end with the `.so` or `.so64` extensions.
- Notify scripts - Scripts that contain `notify` string within the file name.
- File list files - The files that end with the `.filelist` extension.

See "About running NetBackup commands from the appliance" on page 208.

See "Running NetBackup commands from the NetBackup appliance" on page 210.

See "Creating NetBackup administrator user accounts" on page 215.

See "Deleting NetBackup administrator user accounts" on page 218.

See "Viewing NetBackup administrator user accounts" on page 219.

Running NetBackup commands from the NetBackup appliance

NetBackup administrators can use multiple methods to execute NetBackup commands from the restricted NetBackup appliance shell. NetBackup administrators can use a base command name, an absolute or a relative path, or execute commands from shell scripts.

The following are examples of how a NetBackup administrator can run NetBackup commands from the restricted NetBackup appliance shell:

- Using a base command name. For example,
  - `# bpps`
  - `# nbemmcmd -listhosts`
- Using an absolute or a relative path. You must specify `sudo` before the command in this case. For example,
  - `# sudo /usr/openv/netbackup/bin/bpps`
  - `# sudo /usr/openv/netbackup/bin/admincmd/nbemmcmd -listhosts`
- Execute from shell scripts. You must specify `sudo` before you use a command. That applies to a base command name, an absolute path, or a relative path.

See "Creating a NetBackup touch file from the NetBackup appliance" on page 211.

See "About NetBackup operating system commands" on page 213.

See "Best practices for running NetBackup commands from the NetBackup appliance" on page 213.

See "Known limitations of running NetBackup commands from the NetBackup appliance" on page 214.

Creating a NetBackup touch file from the NetBackup appliance

A NetBackup administrator can use the `cp-nbu-config` command to create and edit a NetBackup touch configuration file in any of the following directories:

- `/usr/openv/netbackup`
- `/usr/openv/netbackup/bin`
- `/usr/openv/netbackup/bin/snapcfg`
- `/usr/openv/netbackup/db/config`
- `/usr/openv/netbackup/db/event`
- `/usr/openv/netbackup/db/images`
- `/usr/openv/netbackup/db/media`
- `/usr/openv/netbackup/ext/db_ext`
- `/usr/openv/netbackup/ext/db_ext/db2`
- `/usr/openv/lib/ost-plugins`
- `/usr/openv/volmgr`
- `/usr/openv/volmgr/database`
- `/usr/openv/var`

For example, to create a touch file called `DEFERRED_IMAGE_LIMIT` in the `/usr/openv/netbackup/db/config` directory, use the following steps:

- Create a file with that name in the NetBackup administrator home directory or a subdirectory.
- Use the `cp-nbu-config` *`configuration-file target-directory`* command to add the desired content to the touch file. For example:

  ```
  cp-nbu-config DEFERRED_IMAGE_LIMIT /usr/openv/netbackup/db/config
  ```

See "Running NetBackup commands from the NetBackup appliance" on page 210.

See "About NetBackup operating system commands" on page 213.

See "Best practices for running NetBackup commands from the NetBackup appliance" on page 213.

See "Known limitations of running NetBackup commands from the NetBackup appliance" on page 214.

Loading the NetBackup notify scripts

The `cp-nbu-notify` utility is similar to `cp-nbu-config` utility that is added to the NetBackup appliance to modify the NetBackup notify scripts, like the `start` and `exit` notification scripts to be run after each job.

The NetBackup CLI users can modify the notify scripts from the following script locations:

- `/usr/openv/netbackup/bin`
- `/usr/openv/volmgr/bin`

Note: The `cp-nbu-notify` assumes that the notify script pre-exists either in the actual location as a sample file or its goodies directory as a template. If a sample or template notify script does not exist in these directories, then the script that you may try to load is not considered valid.

To install or edit the notify scripts:

1. Login to the appliance as a NetBackupCLI user and then create the notify script in the home directory.
2. Enter `cp-nbu-notify` command to install the script:

   `cp-nbu-notify <notify-script>`

   The appliance displays the following messages:

   ```
   NetBackup Appliance admin must review and
   approve this operation.
   Enter admin password:
   ```

3. When the command prompts for admin password, enter the Appliance admin password (not the NetBackupCLI password). The password is needed for security purpose to make sure that the notify script is approved by the Appliance admin.

   When the password is successfully verified the notify script is automatically loaded in the right location.

   Note: The source notify script must exist in the home directory or its subdirectory.

Caution: You can only copy the notify scripts. Not any other scripts in the NetBackup install path. Execution of any external script through the notify script can lead to a security issue.

About NetBackup operating system commands

The following rules apply to the operating system commands:

- The following commands are available:
  `awk, bash, cat, clear, cut, grep, head, ls, rm, sudo, uname, vi`
- The commands that are useful for scripting :
  `date, mkdir, rmdir, touch, whoami, hostname,` and so forth
- A NetBackup administrator can use the `passwd` command to change their password.
- To perform a host name lookup you must use the `host` command. The `nslookup` command is not supported.

See "Running NetBackup commands from the NetBackup appliance" on page 210.

See "Creating a NetBackup touch file from the NetBackup appliance" on page 211.

See "Best practices for running NetBackup commands from the NetBackup appliance" on page 213.

See "Known limitations of running NetBackup commands from the NetBackup appliance" on page 214.

Best practices for running NetBackup commands from the NetBackup appliance

The following list provides examples of how you, a NetBackup administrator, can configure an appliance so you can run NetBackup commands from the restricted shell.

- You can only create files and directories in user home directory and the subdirectories.
- An auto-generated alias file is created in the user home directory that contains a `sudo` alias for all the NetBackup commands. Thus, when you use a base command name you do not need to specify `sudo` when you run the command.
- The alias file is not honored when you run a command in a script. You must specify `sudo` before you can use the command.
- You can create a file that contains variables for all NetBackup commands with `sudo` prefix. The variable can be used in the automation scripts to avoid use of

`sudo` for every NetBackup command invocation. The variable file can be sourced in the scripts. For example:

- The following command enables you to use the variable `${bpps}`.
  `bpps="sudo /usr/openv/netbackup/bin/bpps"`
- The following command enables you to use the variable `${nbemmcmd}`.
  `nbemmcmd="sudo /usr/openv/netbackup/bin/admincmd/nbemmcmd"`

- A `cdnbu` alias is available for you to use to change directory to a NetBackup install path. That alias takes you to the `/usr/openv/` directory.

See "Running NetBackup commands from the NetBackup appliance" on page 210.

See "About NetBackup operating system commands" on page 213.

See "Known limitations of running NetBackup commands from the NetBackup appliance" on page 214.

Known limitations of running NetBackup commands from the NetBackup appliance

The following list identifies the known limitations that a NetBackup administrator should understand before they use this feature:

- You cannot edit the `bp.conf` file directly using an editor. To edit the `bp.conf` file you must use the `bpsetconfig` command to set an attribute within the file.
- You cannot modify or create NetBackup notify scripts.
- The `nslookup` command is not supported.
- You cannot use the `man` command. To see the usage of a command, use the `help` option that is provided with the command.
- The operating system commands that are used to perform appliance management are not supported.

See "Running NetBackup commands from the NetBackup appliance" on page 210.

See "Creating a NetBackup touch file from the NetBackup appliance" on page 211.

See "About NetBackup operating system commands" on page 213.

See "Best practices for running NetBackup commands from the NetBackup appliance" on page 213.

Creating NetBackup administrator user accounts

NetBackup appliance administrators can use the following procedure to create new NetBackup administrator user accounts. These user accounts have permissions to log on to the appliance and run NetBackup commands with superuser privileges.

To create a NetBackup administrator user account

1. Open an SSH session on the appliance.
2. Log on as **admin**.
3. Enter the following command to create a NetBackup administrator user account:

   ```
   Main > Manage > NetBackupCLI > Create UserName
   ```

   Where *UserName* is the name that you designate for the new user. In addition, you can only create one user account at a time.
4. You must then enter a new password for the new user account.

   Veritas recommends that the new password is a mix of upper and lowercase letters, digits, and other characters to increase the strength of the password. In addition, you are asked to enter the password a second time for validation purposes.

   After the new user account is created, a confirmation message appears stating the new user account was created successfully.

See the *NetBackup Appliance Command Reference Guide* for additional information about this command and its use.

See “About running NetBackup commands from the appliance” on page 208.

See “About NetBackup administrator capabilities” on page 209.

See “Viewing NetBackup administrator user accounts” on page 219.

See “Managing NetBackup administrator user account passwords” on page 216.

See “Auditing NetBackup administrator accounts” on page 217.

See “Deleting NetBackup administrator user accounts” on page 218.

Logging on as a NetBackup administrator

After a NetBackup administrator account has been created for you, you can log onto the appliance using the new account credentials.

Logging onto an appliance as a NetBackup administrator

1. Open an SSH session on the appliance.
2. Enter the user name and password that was created for your NetBackup administrator account to log on to the appliance.

   The following welcome message appears after you have successfully logged into the appliance as a NetBackup administrator.

   ```
   Welcome NetBackup CLI Administrator to the NetBackup Appliance
   ```

3. To leave the session, type `exit` and press **Return**.

See "About NetBackup administrator capabilities" on page 209.

See "Managing NetBackup administrator user account passwords" on page 216.

See "Creating NetBackup administrator user accounts" on page 215.

See "Auditing NetBackup administrator accounts" on page 217.

See "Deleting NetBackup administrator user accounts" on page 218.

See "Viewing NetBackup administrator user accounts" on page 219.

Managing NetBackup administrator user account passwords

After the NetBackup appliance administrator has created a NetBackup administrator account, the appliance administrator can manage the password of that account through the NetBackup Appliance Shell Menu.

Table 4-2 describes the functions that you can perform as you manage your account passwords.

Table 4-2 Managing NetBackup administrator user account passwords

Function	Command
The NetBackup appliance administrator can specify a maximum number of days that a password is valid for a user or users.	`Main > Settings > Security > Authentication > LocalUser > PasswordExpiry Age` *`UserName Days`* You use the *`Days`* variable to set the number of days the password is valid. In addition, you use the *`UserName`* variable to specify the user or users. Enter `All` to apply this setting to all users. You can also enter `Default` to apply this setting to all new users accounts that were created later.

Table 4-2 Managing NetBackup administrator user account passwords *(continued)*

Function	Command
The NetBackup appliance administrator can force a password to expire immediately for one or more users.	`Main > Settings > Security > Authentication > LocalUser > PasswordExpiry Now` *`UserName`* You use the *`UserName`* variable to specify the user or users. Enter `All` to expire the password for all users.
The NetBackup appliance administrator can view the password expiry information.	`Main > Settings > Security > Authentication > LocalUser > PasswordExpiry Show` *`UserName`* You use the *`UserName`* variable to specify the user or users. Enter `All` to expire the password for all users. You can also enter `Default` to view the default settings.
The NetBackup appliance administrator can configure a warning period in which you receive a warning before the password expires. You can also configure one or more users to receive the warning.	`Main > Settings > Security > Authentication > LocalUser > PasswordExpiry Warn` *`UserName Days`* You use the *`Days`* variable to set the number of days or warning before the password expires. In addition, you use the *`UserName`* variable to specify the user or users who receive the warning. Enter `All` to apply the setting to all users. You can also enter `Default` to specify the default settings.

See "About running NetBackup commands from the appliance" on page 208.

See "About NetBackup administrator capabilities" on page 209.

See "Logging on as a NetBackup administrator" on page 215.

See "Auditing NetBackup administrator accounts" on page 217.

See "Deleting NetBackup administrator user accounts" on page 218.

See "Viewing NetBackup administrator user accounts" on page 219.

See "Creating NetBackup administrator user accounts" on page 215.

Auditing NetBackup administrator accounts

NetBackup appliance administrators can monitor the activity of each NetBackup administrator account. That means a NetBackup appliance administrator can monitor the NetBackup commands that a NetBackup administrator executes. To audit that activity from the NetBackup Appliance Shell Menu, the NetBackup appliance administrator can run the following command.

```
Main > Support > Logs > Browse > cd OS > less messages.
```

If you run that command, an output similar to the following is shown. The following example shows the NetBackup administrator, `nbadmin`, executed a `bpps` command on an appliance named, `nbappliance`.

```
Aug 24 23:10:28 nbappliance sudo:   nbadmin : TTY=pts/1 ;
PWD=/home/nbusers ; USER=root ; COMMAND=/usr/openv/netbackup/bin/bpps
```

See "Creating NetBackup administrator user accounts" on page 215.

See "Managing NetBackup administrator user account passwords" on page 216.

See "Deleting NetBackup administrator user accounts" on page 218.

See "Viewing NetBackup administrator user accounts" on page 219.

Deleting NetBackup administrator user accounts

NetBackup appliance administrators can use the following procedure to delete NetBackup administrator user accounts.

To delete a NetBackup administrator user account

1. Open an SSH session on the appliance.
2. Log on as **admin**.
3. Enter the following command to delete a user account:

   ```
   Main > Manage > NetBackupCLI > Delete UserName
   ```

   Where *UserName* is the name of an existing user account. In addition, you can only delete one user account at a time.

   After the user account is deleted, a confirmation message appears that states the user account was deleted successfully.

See the *NetBackup Appliance Command Reference Guide* for additional information about this command and its use.

See "About running NetBackup commands from the appliance" on page 208.

See "About NetBackup administrator capabilities" on page 209.

See "Viewing NetBackup administrator user accounts" on page 219.

See "Creating NetBackup administrator user accounts" on page 215.

See "Managing NetBackup administrator user account passwords" on page 216.

See "Auditing NetBackup administrator accounts" on page 217.

Viewing NetBackup administrator user accounts

NetBackup appliance administrators can use the following procedure to view a list of NetBackup administrator user accounts.

To view the current list of NetBackup administrator user accounts

1. Open an SSH session on the appliance.
2. Log on as **admin**.
3. Enter the following command to view the existing user accounts:

   ```
   Main > Manage > NetBackupCLI > List
   ```

   All of the existing user account names appear.

See the *NetBackup Appliance Command Reference Guide* for additional information about this command and its use.

See "About running NetBackup commands from the appliance" on page 208.

See "About NetBackup administrator capabilities" on page 209.

See "Creating NetBackup administrator user accounts" on page 215.

See "Managing NetBackup administrator user account passwords" on page 216.

See "Auditing NetBackup administrator accounts" on page 217.

See "Deleting NetBackup administrator user accounts" on page 218.

About Auto Image Replication between appliances

Auto Image Replication is the ability to replicate backups that are generated in one NetBackup domain to storage in other NetBackup domains, often across various geographical sites.

You can perform Auto Image Replication between appliances in the following manner:

- Auto Image Replication between NetBackup appliances
  More information on how to perform Auto Image Replication between NetBackup appliances is available.
  See "About Auto Image Replication between NetBackup appliances" on page 220.
- Auto Image Replication between NetBackup appliances and deduplication appliances
  More information on how to perform Auto Image Replication between a NetBackup appliance and a deduplication appliance is available.
  See "About Auto Image Replication between NetBackup appliances and deduplication appliances" on page 222.

About Auto Image Replication between NetBackup appliances

The backups that are generated in one NetBackup domain can be replicated to storage in one or more NetBackup domains. This process is referred to as Auto Image Replication. You can configure Auto Image Replication between two NetBackup appliances.

To configure Auto Image Replication between two NetBackup appliances, you need to perform the following tasks:

Step No.	Task	Reference
1.	Establish trust between the two primary servers	
2.	Review the prerequisites for Auto Image Replication	See "Prerequisites for Auto Image Replication" on page 220.
3.	Configure the replication target	See "Configuring a replication target" on page 220.
4.	Configure storage lifecycle policy on source and target domains	See the section titled 'Creating a storage lifecycle policy' in the *NetBackup Administrator's Guide, Volume I*.

Prerequisites for Auto Image Replication

The following prerequisites must be followed before you set up replication configuration between NetBackup appliances:

- The target storage server type must be the same that is configured in the target primary server domain.
- The target storage server name must be the same that is configured in the target primary server domain.

Configuring a replication target

Use the following procedure to configure a replication target in the source domain.

To configure a replication target

1. In the NetBackup Administration Console in the source NetBackup domain, expand **Media and Device Management > Credentials > Storage Server**.
2. Select the source storage server.
3. On the **Edit** menu, select **Change**.

4 In the **Change Storage Server** dialog box, select the **Replication** tab.

5 Select a trusted primary server and a replication target.

In the **Target Primary Server** drop-down list, select the primary server of the domain to which you want to replicate data. All trusted primary servers are in the drop-down list.

6 In the **Storage Server Type** drop-down list, select the type of target storage server. All available target types are in the drop-down list.

The target storage server type must be the same that is configured in the target primary server domain.

7 In the **Storage Server Name** field, enter the shortname of the target storage server.

You must enter the target storage server name that is configured in the target primary server domain.

8 In the **Deduplication Server Name** field, enter the name of the deduplication server.

Note: The **Deduplication Server Name** and **User Name** fields may be pre-populated in some scenarios.

---

9 Enter the User name and Password for the target appliance's deduplication storage server.

Password: *appliance dedupe password*

Use the following procedure to determine the appliance deduplication password:

See "Determining the appliance deduplication password" on page 222.

10 Click **Add**. You can now see the new replication target in the **Replication Targets** section at the top.

Click **OK**.

11 You must refresh the disk pool after setting up a replication target. In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management Devices > Disk Pools**. In the right pane, select the disk pool you want to update. In the **Change Disk Pool** dialog box, click **Refresh** to configure the replication settings for the disk pool.

Once you have configured a replication target, you can configure storage lifecycle policies on source and target domains. For more information about configuring storage lifecycle policies, refer to the section named 'Creating a storage lifecycle policy' in *NetBackup Administrator's Guide, Volume I for UNIX, Windows, and Linux*.

Determining the appliance deduplication password

The following credentials are required to configure Auto Image Replication between appliances.

- **username:** `user_name`
- **password:** *appliance dedupe password*

To determine the appliance deduplication password

1. Log on to the target appliance and enter into the appliance shell menu.
2. From the Main_Menu prompt, enter the following:

   `Appliance` > `ShowDedupPassword`

   This command shows the password for the deduplication solution that is configured on the appliance. The deduplication password appears on the screen.

Note: If you changed the deduplication password, the appliance shell menu does not display the new password. The `ShowDedupPassword` option only displays the original password that was created during the installation process.

Note: If your configuration has an appliance primary server and one or more appliance media servers, the deduplication password is the same for all servers. In this case, use the appliance primary server's shell menu to retrieve the deduplication password.

For more information about Auto Image Replication, refer to the *NetBackup™ Administrator's Guide, Volume I*.

About Auto Image Replication between NetBackup appliances and deduplication appliances

The backups that are generated in NetBackup appliances can be replicated to the storage pools in one or more deduplication appliances. You can configure Auto Image Replication from a NetBackup appliance on one domain to a deduplication appliance on another domain.

To configure Auto Image Replication from a NetBackup appliance to a deduplication appliance, you are required to enter the user name and password for the target deduplication appliance.

The following credentials are required to configure Auto Image Replication from a NetBackup appliance to a deduplication appliance:

- **username:** root
- **password:** *P@ssw0rd* or a custom password that you have configured for the SPA (Storage Pool Authority)

For more information about Auto Image Replication, refer to the *NetBackup™ Administrator's Guide, Volume I for UNIX, Windows and Linux*.

About forwarding logs to an external server

This feature can forward NetBackup appliance system logs (syslogs) to an external log management server.

The following types of log severs are supported:

- Splunk

NetBackup appliance uses the Rsyslog client to forward logs. In addition to Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance. Refer to the log management server documentation to verify Rsyslog client support.

You can view, enable, and disable log forwarding from the NetBackup Appliance Shell Menu.

See "Uploading certificates for TLS" on page 223.

See "Enabling log forwarding" on page 224.

See "Changing the log forwarding interval" on page 225.

See "Viewing the log forwarding configuration" on page 226.

See "Disabling log forwarding " on page 226.

Uploading certificates for TLS

Use TLS to secure the log transmissions from the appliance to the log server. TLS is optional for log forwarding. However, Veritas recommends that you enable TLS for security purposes.

NetBackup appliance currently only supports the following:

- TLS Anonymous Authentication for log forwarding.
- X.509 file format for certificate files.

Before you enable TLS, you must first do the following:

- Deploy the configured certificate and private key files from the Certificate Authority (CA) server onto your log server.

- Upload valid certificates to opened NFS and CIFS shares on the appliance. For log forwarding security information, see the *NetBackup Appliance Security Guide*.

Note: You can also upload certificate files from the **Manage > File Manager** menu in the appliance web console.

To upload the certificate

1. Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
2. To open NFS and CIFS shares on the appliance, enter the following command:

   `Share General Open`
3. On the server where the certificates reside, mount an NFS or a CIFS share to the appliance as follows:

   NFS: `<appliance.name>:/inst/share`

   CIFS: `\\<appliance.name>\general_share`
4. Upload two certificates and one private key file. The certificate file names are as follows:
   - `ca-server.pem`
   - `nba-rsyslog.pem`
   - `nba-rsyslog.key`
5. To close the shares on the appliance, enter the following command:

   `Share General Close`

See "About forwarding logs to an external server" on page 223.

See "Enabling log forwarding" on page 224.

See "Changing the log forwarding interval" on page 225.

See "Viewing the log forwarding configuration" on page 226.

See "Disabling log forwarding " on page 226.

Enabling log forwarding

This procedure describes how to enable the log forwarding feature.

To enable log forwarding

1. Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
2. To enable log forwarding, enter the following command:

   `Enable`

   Specify the following:

   - **Server name or IP address**: Enter the name or the IP address of the external log management server.
   - **Server port**: Enter the port number of the external log management server.
   - **Protocol**: Select either **UDP** or **TCP**. **TCP** is the default.
   - **Forward logs**: Select which types of logs to forward (OS, Appliance, AutoSupportClient, Infoscale). You can enter multiple log types with a comma-separated list.
   - **TLS**: Select either **Yes** or **No**. **Yes** is the default.

   Note: Enabling TLS requires that you upload two certificates and one private key to the appliance.

   See "Uploading certificates for TLS" on page 223.

3. Verify the configuration summary, and type `yes` to complete the configuration.

See "About forwarding logs to an external server" on page 223.

See "Uploading certificates for TLS" on page 223.

See "Changing the log forwarding interval" on page 225.

See "Viewing the log forwarding configuration" on page 226.

See "Disabling log forwarding " on page 226.

Changing the log forwarding interval

This procedure describes how to change the log forwarding interval.

To change the current log forwarding interval

1. Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
2. To change the log forwarding interval, enter the following command:

   `Interval`

3 Enter the new log forwarding interval, then press **Enter**.

4 Verify the interval summary, and type `yes` to complete the change.

See "About forwarding logs to an external server" on page 223.

See "Uploading certificates for TLS" on page 223.

See "Enabling log forwarding" on page 224.

See "Viewing the log forwarding configuration" on page 226.

See "Disabling log forwarding " on page 226.

Viewing the log forwarding configuration

This procedure describes how to view the current log forwarding configuration.

To view the current log forwarding configuration

1 Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.

2 To view the current configuration, enter the following command:

```
Show
```

See "About forwarding logs to an external server" on page 223.

See "Uploading certificates for TLS" on page 223.

See "Enabling log forwarding" on page 224.

See "Changing the log forwarding interval" on page 225.

See "Disabling log forwarding " on page 226.

Disabling log forwarding

This procedure describes how to disable the log forwarding feature and remove the current configuration.

To disable log forwarding

1 Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.

2 To disable log forwarding, enter the following command:

```
Disable
```

3 Enter `yes` to disable log forwarding.

See "About forwarding logs to an external server" on page 223.

See “Uploading certificates for TLS” on page 223.

See “Enabling log forwarding” on page 224.

See “Changing the log forwarding interval” on page 225.

See “Viewing the log forwarding configuration” on page 226.

About high availability configuration

This section describes how to manage the high availability (HA) configuration from the NetBackup Appliance Shell Menu. You can use the NetBackup Appliance Shell Menu to perform the following HA operations:

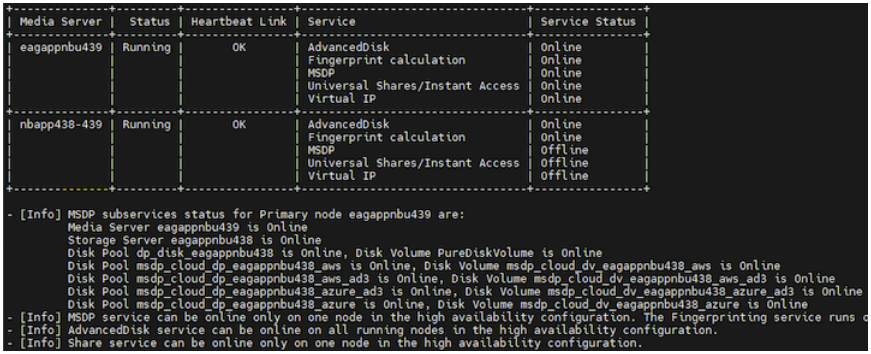
- Checking the status
  See “Checking the status” on page 227.
- Getting the asset tag
  See “Getting the asset tag” on page 228.
- Switching the services over
  See “Switching the services over” on page 228.
- Removing a node from the HA configuration
  See “Removing a node” on page 229.

For more information about the HA configuration, refer to the *NetBackup 53xx Appliance High Availability Reference Guide*.

Checking the status

This operation displays the status of the high availability (HA) configuration and the status of the relevant services that are running on the two nodes.

The following is an example of the information that is displayed when you run the `Main > Manage > HighAvailability > Status` command:



Getting the asset tag

In a high availability (HA) configuration, the asset tag works as the identity. Once the HA configuration is complete, an asset tag is automatically attached to each firmware of the two nodes and the shared Primary Storage Shelf. To ensure that the changes take effect, Veritas recommends that you restart the two nodes.

The values on the three components are identical. If the values vary, restart the node or nodes with the different value from the shared Primary Storage Shelf.

To get the asset tag of an HA configuration, perform the following procedures:

1. On either node of the HA configuration, log on to the NetBackup Appliance Shell Menu as **admin**.
2. Navigate to the `HighAvailability` view:

   ```
   Main > Manage > HighAvailability
   ```

3. Get the asset tag with the following command:

   ```
   GetAssetTag
   ```

Switching the services over

This operation switches the services from one node to the target node in a high availability (HA) configuration for a planned upgrade or maintenance. Because you need to perform the upgrade or maintenance operations on the node where the MSDP service is not running.

For example, two nodes, node A and node B, are set in the HA configuration, and the MSDP service is running on the node A. If you want to shut down the node A for maintenance, do the following:

1. On the node A, log on to the NetBackup Appliance Shell Menu as `admin` with the physical hostname or IP address.

2. Naviage to the `HighAvailability` view:

   `Main > Manage > HighAvailability`

3. Switch the HA services from the node A to the node B with the following command:

   `Switchover` *`hostname of node B`*

   Note: Alternatively, you can also log on to the NetBackup Appliance Shell Menu on the node B, perform the `HighAvailability > Switchover` *`hostname of node B`*.

4. After the switchover is complete, shut down the node A for the upgrade or maintenance purpose.

Removing a node

This operation removes a node from a high availability (HA) configuration for maintenance, replacement, or repurposing.

Note: You can only revert the partner node to be the non-HA node by performing the `RemoveNode` operation. Other operations, such as factory reset, or rolling back to a non-ha checkpoint, may cause the malfunction of the HA configuration.

If the node to be removed is where the MSDP service is running, you need to run the `HighAvailability > Switchover` command to switch the MSDP service and other HA services over to the partner node. Then log on to the node and run the `RemoveNode` command.

To identify the node where the MSDP service is running, run the `HighAvailability > Status`command.

Warning: In case the HA configuration has only one node, make sure that all NetBackup operations are not running before you remove the node. Otherwise, all NetBackup jobs associated with the MSDP service fail as a result of this removal operation.

For example, two nodes, node A and node B, are set in an HA configuration. The MSDP service is running on the node A. If you want to remove the node A from the HA configuration, perform the following procedures:

1. On the node A, log on to the NetBackup Appliance Shell Menu as `admin` with the physical hostname or physical IP address.
2. Naviage to the `HighAvailability` view:

   ```
   Main > Manage > HighAvailability
   ```

3. Switch the HA services from the node A to the node B with the following command:

   ```
   HighAvailability > Switchover hostname of node B
   ```

   Note: Alternatively, you can also log on to the NetBackup Appliance Shell Menu on the node B, run the `HighAvailability > Switchover hostname of node B` command.

4. On the node B, log on to the NetBackup Appliance Shell Menu as `admin`.
5. Naviage to the `HighAvailability` view:

   ```
   Main > Manage > HighAvailability
   ```

6. Remove the node A with the following command:

   ```
   HighAvailability > RemoveNode hostname of node A
   ```

After the node removal succeeds, Veritas recommends that you perform the following procedures on the removed node:

- Disconnect the Ethernet cables from the removed node.
- Disconnect the FC cables from the removed node.
- Perform the factory reset on the removed node.

Chapter 5

Understanding the NetBackup appliance settings

This chapter includes the following topics:

About modifying the appliance settings

After you have successfully configured your appliance you can use the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu to change various settings for your appliance. You can use the **Settings** tab in the NetBackup Appliance Web Console to view and configure the following settings.

Table 5-1 describes the settings that are available from **Settings > Notification** menu:

Table 5-1 Settings > Notification

Sub Menu	Lets you...	Topic
Alert configuration	Configure the SNMP, SMTP, and Call Home settings.	See "Settings > Notifications > Alert Configuration " on page 234.
Login Banner	Create a customized text banner that appears when you access the appliance.	See "Settings > Notifications > Login Banner" on page 248.

Note: The MyAppliance portal is no longer supported with the release of the Veritas NetInsights Console and will be decommissioned. Appliance registration should be done by signing in to the NetInsights portal (https://netInsights.veritas.com) with your Veritas Account Manager credentials. For more information, see the *Veritas Appliance AutoSupport Reference Guide* and the *Veritas NetInsights Console User Guide*.

Table 5-2 describes the settings that are available from **Settings > Network** menu:

Table 5-2 Settings > Network

Sub Menu	Lets you...	Topic
Network	View and change network configuration settings.	See "Settings > Network > Network Settings" on page 253.
Host	Configure the host name, for either DNS or non-DNS systems	See "Settings > Network > Host" on page 271. See "Changing DNS and Host Name Resolution (non-DNS) configuration settings" on page 272.
Fibre Transport	Configure fibre transport settings for your appliance.	See "Settings > Network > Fibre Transport" on page 266.

Table 5-3 describes the settings that are available from the **Settings > Date and Time** menu:

Table 5-3 Settings > Date and Time

Sub Menu	Lets you...	Topic
Date and Time Configuration	Change the date and time on your appliance.	See "Settings > Date and Time " on page 274.

Table 5-4 describes the settings that are available from **Settings > Authentication** menu:

Table 5-4 Setting > Authentication

Sub Menu	Lets you...	Topic
Authentication	Manage the following three types of user authentication: ■ LDAP ■ Active Directory	See "Settings > Authentication " on page 283.
User Management	Add new local users and create user groups for accessing your appliance.	See "Settings > Authentication > User Management" on page 297.

Table 5-5 describes the settings that are available from the **Settings > Password** menu:

Table 5-5 Settings > Password

Sub Menu	Lets you...	Topic
Password	Change the admin password for your appliance.	See "Settings > Password Management" on page 302.

Settings > Notifications

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

- **Alert Configuration** - enables you to provide the SMTP, SNMP, and Call Home settings.
  See "Settings > Notifications > Alert Configuration " on page 234.
- **Login Banner** - enables you to create a text banner for your appliance that appears before a user logs on through one of the appliance interfaces.
  See "Settings > Notifications > Login Banner" on page 248.

Settings > Notifications > Alert Configuration

The **Settings > Notifications > Alert Configuration** page on the NetBackup Appliance Web Console provides you with one location from where you can enable SNMP, SMTP, and Call Home alert notifications. The page is divided into three sections. Each section is dedicated to provide details for **SNMP**, **SMTP**, and **Call Home** alert notifications.

Under **Alert Configuration** is the **Notification Interval** field. You must enter the time interval in minutes between two subsequent notifications for the SNMP and the SMTP configurations. The time interval should be in multiples of 15 and it should not be zero.

Configuring SNMP

Table 5-6 lists the fields from the **SNMP** (Simple Network Management Protocol) section of the NetBackup Appliance Web Console.

Table 5-6 SNMP Server Configuration settings

Fields	Description
Notification Interval	Enter the interval for the server to upload alerts to the Veritas Call Home server. Entries must be in increments of 15 minutes.
SNMP Server Configuration	Select one of the following options: ■ **SNMP V2** ■ **SNMP V3** ■ **None** (default)
SNMP Server	Enter the SNMP Server host name. You can enter a host name or an IP address to define this computer. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed. Notification of the alerts or traps that are generated in the appliance are sent to this SNMP manager. **Note:** The NetBackup appliance supports all the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified for version 2.6. See “About IPv4-IPv6-based network support” on page 273.
SNMP Port	Enter the SNMP Server port number. The default port is 162. **Note:** Your firewall must allow access from the appliance to the SNMP server through this port.

Table 5-6 SNMP Server Configuration settings *(continued)*

Fields	Description
SNMP Community	This field is required for SNMP V2 and is optional for SNMP V3. Enter the community to which the alerts or traps are sent. For example, Backup Reporting Department. You can enter a value that you configured on your SNMP server. For example, your company name. If you do not expect to disclose your company name, Veritas provides the system-defined values including: `admin_group`, `public`, and `private`. The default is `public`.
SNMP Username (SNMP V3 only)	Enter an SNMP user name as follows: ■ Enter up to 32 characters maximum. ■ May include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore. ■ Spaces, commas, and special characters are not allowed.
Authentication Protocol (SNMP V3 only)	Configure as follows to set the security level: ■ **None** (default) Sets the security level to no authentication and no privileges (authentication is disabled). Password and encryption fields are greyed out and not required. ■ **SHA256** or **SHA512** Sets the security level for authentication. An SNMP password is required.
SNMP Password/**Confirm SNMP Password** (SNMP V3 only)	Enter a password for the SNMP user as follows: ■ Must have 8 or more characters. ■ May include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore. ■ Spaces, commas, and special characters are not allowed. Enter the same password in the **Confirm SNMP Password** field.

Table 5-6 SNMP Server Configuration settings *(continued)*

Fields	Description
Encryption Protocol (SNMP V3 only)	Configure as follows to set the encryption policy: ■ **None** (default) Encryption policy is not used or enforced. Passphrase fields are greyed out and not required. ■ **AES128 AES192 AES256 AES512** Select one of these options to enforce the associated encryption policy. An **Encryption Passphrase** is required.
Encryption Passphrase/**Confirm Encryption Passphrase** (SNMP V3 only)	If you set the **Encryption Protocol** to use an encryption policy, enter a passphrase for the SNMP user as follows: ■ Must have 8 or more characters. ■ May include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore. ■ Spaces, commas, and special characters are not allowed. Enter the same passphrase in the **Confirm Encryption Passphrase** field.

The following describes summaries of the required fields for specific SNMP configuration scenarios:

- **SNMP V2**
  SNMP Server
  SNMP Port
  SNMP Community
  All other fields are not required.
- **SNMP V3** - no authentication/no privileges
  SNMP Server
  SNMP Port
  SNMP Community (optional)
  Authentication Protocol - None
  All other fields are not required.
- **SNMP V3** - authentication/no privileges
  SNMP Server
  SNMP Port
  SNMP Community (optional)
  Authentication Protocol (SHA256, SHA512)
  SNMP Password/Confirm SNMP Password

All other fields are not required.

- **SNMP v3** - authentication/privileges
  SNMP Server
  SNMP Port
  SNMP Community (optional)
  Authentication Protocol (SHA256, SHA512)
  SNMP Password/Confirm SNMP Password
  Encryption Protocol (AES128, AES192, AES256, AES512)
  Encryption Passphrase/Confirm Encryption Passphrase

The SNMP MIB file serves as a data dictionary that is used to assemble and interpret SNMP messages. If you configure SNMP, you must import the MIB file into the monitoring software so that the software can interpret the SNMP traps. You can view the details of the MIB file from the SNMP Server Configuration pane. To view details about the SNMP MIB file, click **View SNMP MIB file**. An SNMP MIB file opens.

You can also use the following command in the appliance shell menu to configure the SNMP server:

```
Main_Menu > Settings > Alerts > SNMP Set Server [Community] [Port]
```

For example: `Main_Menu > Settings > Alerts > SNMP Set Server 1.1.1.1`

For information on how to send a test SNMP trap after configuration, see the following technical article on the Veritas Support website:

https://www.veritas.com/content/support/en_US/article.100009877

Configuring SMTP

The SMTP mail server protocol is used for outgoing email. You can configure SMTP from the NetBackup Appliance Web Console (**Settings > Alert Configuration > SMTP Server Configuration**).

You can also use the following command in the appliance shell menu to configure the SMTP server and add a new email account:

`Main_Menu > Settings > Alerts > Email SMTP Add` *`Server`* `[Account] [Password]`, where *`Server`* is the host name of the target SMTP server that is used to send emails. `[Account]` and `[Password]` are optional parameters to identify the name of the account and the account password if authentication is required.

For more information, see the related documentation of your appliance.

Starting with release 3.1.2, you can configure the SMTP port and set encryption.

You can use the following commands in the appliance shell menu to configure encrypted communication with the SMTP server:

- `Main_Menu > Settings > Alerts > Email SMTP ConfigurePort [25] [465] [587] [custom]`
- `Main_Menu > Settings > Alerts > Email SMTP Encryption [Disable] [Enable]`

You can use the following command to view the SMTP port number and encryption configuration details.

```
Main_Menu > Settings > Alerts > Email Show
```

Table 5-7 lists the fields from the **SMTP** section of the NetBackup Appliance Web Console.

Table 5-7 SMTP server configuration settings

Fields	Description
SMTP Server	Enter the SMTP (Simple Mail Transfer Protocol) Server host name. Notifications of the alerts that are generated in Appliance are sent using this SMTP server. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed. See "About IPv4-IPv6-based network support" on page 273.
SMTP port	You can select one of the following options: ■ Port 25 to use Plain Text ■ Port 465 to use the SMTPS protocol ■ Port 587 to use the STARTTLS protocol ■ Custom port within the range of 1 to 65,535 The default SMTP port number is 25. Encryption is disabled by default.
Encryption	Select **Enable Encryption** to use a secure connection.

Software Administrator Email	Enter the email ID of the software administrator, to receive software alerts that are specific to the Veritas NetBackup Appliance software. The email ID that you designate receives alerts for the following software conditions:
	
	■ Host information such as:
	  ■ Disk information.
	  ■ Overall backup status.
	  ■ Results of last seven backups for each client.
	■ An email of your catalog backup disaster recovery file.
	■ A patch installation success report.

Table 5-7 SMTP server configuration settings *(continued)*

Fields	Description
Hardware Administrator Email	Enter the email ID of the hardware administrator, to receive hardware alerts that are specific to the Veritas NetBackup Appliance hardware. For example, enter hardwareadmin@usergroup.com.
Email Test	A test email is sent to the email address that was configured above. If the test email is not received, follow the error prompts to view the network connections, SMTP settings, and email settings. You can contact your system administrator for more assistance.
Sender Email	Enter the email ID to receive any replies to the alerts or the reports that the appliance sends.
SMTP Account	Enter the user name to access the SMTP account.
Password	Enter the password for the above mentioned SMTP user account.

All email notifications that get generated by the appliance use the same SMTP settings. These emails include hardware monitoring notifications and NetBackup job notifications. The configuration settings are located under **Settings > Notification > Alert Configuration** in the NetBackup Appliance Web Console or `Main_Menu > Settings > Alerts` in the NetBackup Appliance Shell Menu. These settings override any previous SMTP setup you may have previously used to send NetBackup job notifications.

Configuring Call Home

Table 5-8 lists the fields from the **Call Home Configuration** section.

Table 5-8 Call Home Configuration settings

Fields	Description
Enable Call Home	Select this check box to enable Call Home alert configuration.
Enable AutoUpdate for Upgrade Readiness Check	Select this check box to enable automatic updates for the Appliance Upgrade Readiness Analyzer tool (analyzer tool) on the appliance. Enabling this feature lets you keep pre-upgrade checks up to date and receive accurate upgrade readiness status recommendations through System Health Insights on the NetInsights Console. You can download the latest version of the analyzer tool from the Veritas Download Center. Veritas recommends that you enable AutoUpdate.
Enable Proxy Server	Select this check box to enable proxy.

Table 5-8 Call Home Configuration settings *(continued)*

Fields	Description
Enable Proxy Tunneling	Select this check box if your proxy server supports SSL tunneling.
Proxy Server	Enter the name of the proxy server.
Proxy Port	Enter the port number of the proxy server.
Proxy CA certificates	If your proxy server uses HTTPS, upload the CA certificate to use to validate the server certificate.
Proxy Username	Enter the user name to log into the proxy server.
Proxy Password	Enter the password for the user name to log into the proxy server.

When Call Home is enabled, you can test if Call Home functions correctly by clicking the **Test Call Home** option that is available below the Call Home configuration settings.

Note: The **Test Call Home** option is active on the NetBackup Appliance Web Console only when Call Home is enabled.

Starting with the 5.0 release, when you enable Call Home and click **Save**, a Call Home test is performed automatically.

The following describes the supported proxy servers:

- Squid
- Apache
- TMG

NTLM is the supported authentication method for Call Home proxy settings.

Configuring alert settings

This section provides the procedure to configure the SNMP, SMTP, and Call Home server settings using the **Settings > Notification > Alert Configuration** page.

To configure the SNMP, SMTP, and Call Home server settings

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Notification > Alert Configuration**.

   The system displays the **Alert Configuration** page.

   The **Alert Configuration** page is divided into three sections to enable and provide details for **SNMP**, **SMTP**, and **Call Home**.
3. In the **Notification Interval** field, enter the time interval in 15-minute increments between two subsequent notifications for **SNMP**, **SMTP**, and **Call Home** alert configurations.
4. Enter the SNMP settings in the provided fields.
5. Enter the SMTP settings in the provided fields.

   The appliance uses the global server settings to send email notifications to the SMTP server that you specify.
6. Enter the Call Home settings in the provided fields.
7. Click **Save**, to save the SNMP, SMTP, and Call Home settings.

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It uses either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) for transport, depending on configuration. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is based on the manager model and agent model. This model consists of a manager, an agent, a database of management information, managed objects, and the network protocol.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical devices being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

NetBackup Appliance versions 3.1 and later support SNMP V2.

NetBackup Appliance versions 4.0 and later support SNMP V2 and SNMP V3.

About the Management Information Base (MIB)

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) that is associated with it. Each OID consists of the numbers that are separated by decimal points (for example, 1.3.6.1.4.1.48328.1).

These OIDs form a tree. A MIB associates each OID with a readable label and various other parameters that are related to the object. The MIB then serves as a data dictionary that is used to assemble and interpret SNMP messages. This information is saved as a MIB file.

You can view the details of the SNMP MIB file from the **Settings > Notifications > Alert Configuration** page of the web console. To configure the appliance SNMP manager to receive hardware monitoring related traps, click **View SNMP MIB file** in the **SNMP Server Configuration** page.

You can also view the SNMP MIB file with the `Settings > Alerts > SNMP ShowMIB` command in the Shell Menu of your appliance.

About Call Home

Your appliance can connect with a Veritas AutoSupport server and upload hardware and software information. Veritas support uses this information to resolve any issues that you might report. The appliance uses the HTTPS protocol and uses port 443 to connect to the Veritas AutoSupport server. This feature of the appliance is referred to as Call Home. It is enabled by default.

AutoSupport uses the data that Call Home gathers to provide proactive monitoring for the appliance. If Call Home is enabled, the appliance uploads information or data to the Veritas AutoSupport server at a default interval of 24 hours.

If you determine that you have a problem with your appliance, you might want to contact Veritas support. The Technical Support engineer uses the serial number of your appliance and assesses the status from the Call Home data.

To obtain the serial number of your appliance from the NetBackup Appliance Web Console, go to the **Monitor > Hardware > Health details** page. To determine the serial number of your appliance using the shell menu, go to the `Monitor > Hardware` commands. For more information about the `Monitor > Hardware` commands, refer to the *NetBackup Appliance Command Reference Guide*.

Use the **Settings > Notification** page to configure Call Home from the NetBackup Appliance Web Console. Click **Alert Configuration** and enter the details in the **Call Home Configuration** pane.

Table 5-9 describes how a failure is reported when the feature is enabled or disabled.

Table 5-9 What happens when Call Home is enabled or disabled

Monitoring status	Failure routine
Call Home enabled	When a failure occurs, the following sequence of alerts occur: ■ The appliance uploads all the monitored hardware and software information to a Veritas AutoSupport server. The list following the table contains all the relevant information. ■ The appliance generates 3 kinds of email alerts to the configured email address. ■ An error message by email to notify you of the failure once an error is detected. ■ A resolved message by email to inform you of any failure once an error is resolved. ■ A 24-hour summary by email to summarize all of the currently unresolved errors in the recent 24 hours. ■ The appliance also generates an SNMP trap.
Call Home disabled	No data is sent to the Veritas AutoSupport server. Your system does not report errors to Veritas to enable faster problem resolution.

The following list contains all the information that is monitored and sent to Veritas AutoSupport server for analysis.

- CPU
- Disk
- Fan
- Power supply
- RAID group
- Temperatures
- Adapter
- PCI
- Fibre Channel HBA
- Network card
- Partition information
- MSDP statistics
- Storage connections
- Storage status

- 52xx Storage Shelf - Status of disk, fan, power supply, and temperature
- 53xx Primary Storage Shelf - Status of disk, fan, power supply, temperature, battery backup unit (BBU), controller, volume, and volume group
- 53xx Expansion Storage Shelf - Status of disk, fan, power supply, and temperature
- NetBackup appliance software version
- NetBackup version
- Appliance model
- Appliance configuration
- Firmware versions
- Appliance, storage, and hardware component serial numbers
  See "Hardware components that are monitored" on page 39.
- Upgrade readiness status - upgrade readiness check results, downloaded upgrade package versions, appliance upgrade readiness analyzer package versions, AutoUpdate configuration for upgrade readiness check

See "Settings > Notifications > Alert Configuration " on page 234.

See "About AutoSupport " on page 252.

See "Monitor > Hardware options" on page 36.

Enabling and disabling Call Home from the appliance shell menu

You can enable or disable Call Home from the appliance shell menu. Call Home is enabled by default.

Note: For Call Home to work properly, you need to register your appliance. To register your appliance, sign in to the System Health Insights portal (https://systemhealth.netinsights.veritas.com) with your Veritas Account Manager credentials. For more information, see the *System Health Insights User Guide*.

To enable or disable Call Home from the shell menu

1. Log on to the shell menu.
2. To enable Call Home, run the `Main > Settings > Alerts > CallHome Enable` command.
3. To disable Call Home, run the `Main > Settings > Alerts > CallHome Disable` command.

For more information on the NetBackup appliance `Main > Settings > Alerts > CallHome` commands, refer to the *NetBackup Appliance Commands Reference Guide*.

About AutoUpdate for Upgrade Readiness Check

Enabling this feature lets you keep pre-upgrade checks up to date and receive accurate upgrade readiness status recommendations through System Health Insights on the NetInsights Console. You can download the latest version of the analyzer tool from the Veritas Download Center. Veritas recommends that you enable AutoUpdate.

Note: To ensure that the upgrade readiness status data is collected every 24 hours, you must download the analyzer tool onto the appliance. The minimum supported analyzer tool version is 8.2.0-1. For more information, see the *NetBackup Appliance Upgrade Guide*.

You can enable the feature when you set the appliance role during the initial configuration, or after you have completed the initial configuration.

Enabling and disabling AutoUpdate for Upgrade Readiness Check

The following procedures describe how to enable and disable **AutoUpdate for Upgrade Readiness Check** in the NetBackup Appliance Web Console (web console) and the NetBackup Appliance Shell Menu (shell menu).

To enable or disable AutoUpdate for Upgrade Readiness Check in the web console

1. Log on to the web console and navigate to the **Settings > Notification > Alert Configuration** page.
2. To enable the feature, click the **Enable AutoUpdate for Upgrade Readiness Check** checkbox, then click **Save**.
3. To disable the feature, click the **Enable AutoUpdate for Upgrade Readiness Check** checkbox to remove the check mark, then click **Save**.

To enable or disable AutoUpdate for Upgrade Readiness Check in the shell menu

1. Log in to the shell menu.
2. To enable the feature, run the following command:

   `Manage > Software > UpgradeReadinessCheck > AutoUpdate Enable`

3. To disable the feature, run the following command:

   `Manage > Software > UpgradeReadinessCheck > AutoUpdate Disable`

Configuring a Call Home proxy server from the NetBackup Appliance Shell Menu

You can configure a proxy server for Call Home, if required. If the appliance environment has a proxy server between the environment and external Internet access, you must enable the proxy settings on the appliance. The proxy settings include both a proxy server and a port. The proxy server must accept https connections from the Veritas AutoSupport server. This option is disabled by default.

Note: Note: If you use the HTTPS protocol, you cannot upload DataCollect log files with the `Support > DataCollect Upload` command. To work around this issue, configure Call Home with the HTTP protocol before you upload the files.

To add a Call Home proxy server from the NetBackup Appliance Shell Menu

1. Log on to the NetBackup Appliance Shell Menu.
2. To enable proxy settings, run the `Main > Settings > Alerts > CallHome Proxy Enable` command.
3. To add a proxy server, run the `Main > Settings > Alerts > CallHome Proxy Add` command.
   - You are prompted to enter the name of the proxy server. The proxy server name is the TCP/IP address or the fully qualified domain name of the proxy server. By default, the HTTP protocol is used to communicate with the proxy server.

     Note: If you want to use the HTTPS protocol, enter **https://** before the proxy server name. To ensure successful communication with the proxy server, add the latest CA certificate used by the proxy server by running the `Settings > Security > Certificate > AddCACertificate` command.

- After you have entered a name for the proxy server, you are prompted to enter the port number for the proxy server.
- Further, you are required to answer the following:

  ```
  Do you want to set credentials for proxy server? (yes/no)
  ```

- On answering *yes*, you are prompted to enter a user name for the proxy server.
- After you have entered the user name, you are prompted to enter a password for the user. On entering the required information, the following message is displayed:

  ```
  Successfully set proxy server
  ```

4 To disable proxy settings, run the `Main > Settings > Alerts > CallHome Proxy Disable` command.

Further, you can also use the NetBackup Appliance Shell Menu to enable or disable proxy server tunneling for your appliance. To do so, run the `Main > Settings > CallHome Proxy EnableTunnel` and `Main > Settings > Alerts > CallHome Proxy DisableTunnel` commands. Proxy server tunneling lets you provide a secure path through an untrusted network.

Understanding the Call Home workflow

This section explains the mechanism that Call Home uses to upload data from your appliance to the Veritas AutoSupport server.

Call Home uses HTTPS (secure and encrypted protocol) with port number 443 for all communication with Veritas AutoSupport servers. For Call Home to work correctly, ensure that your appliance has Internet access either directly, or through a proxy server to reach the Veritas AutoSupport servers. AutoSupport, a mechanism that monitors the appliance proactively, uses the Call Home data to analyze and resolve any issues that the appliance may encounter.

The appliance initiates all communications. On the appliance, make sure that you enable the proxy and/or the firewall to outbound 443/TCP TLS socket connections to the following site:`https://api.appliance.veritas.com`

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

- Access a port to `https://api.appliance.veritas.com` every 24 hours.
- Perform a self-test operation to `https://api.appliance.veritas.com`

- If the appliance encounters an error state, all logs from past three days are gathered along with the current log.
- The logs are then uploaded to the Veritas AutoSupport server for further analysis and support. These error logs are also stored on the appliance. You can access these logs from `/log/upload/<date>` folder.
- If the error state persists three days later, the logs will be re-uploaded.

See "About Call Home" on page 242.

See "About AutoSupport " on page 252.

About the Product Improvement Program

The NetBackup appliance Product Improvement Program uses Call Home to capture installation deployment and product usage information. The information that Veritas receives becomes part of a continuous quality improvement program that helps understand how customers configure, deploy, and use the product. This information is then used to help Veritas identify improvements in product features, testing, technical support, and future requirements.

You can enable or disable the Product Improvement Program from the NetBackup Appliance Shell Menu.

This option is not available from the NetBackup Appliance Web Console.

The Product Improvement Program is enabled by default. However, if you have disabled Call Home, the Product Improvement Program is also disabled. You cannot enable the Product Improvement Program without Call Home.

To enable or disable the Product Improvement Program from the NetBackup Appliance Shell Menu

1. Log on to the NetBackup Appliance Shell Menu
2. To enable the Product Improvement Program, run the `Main > Settings > Alerts > CallHome NBInventory Enable` command.
3. To disable the Product Improvement Program, run the `Main > Settings > Alerts > CallHome NBInventory Disable` command.

For more information on the `Main > Settings > Alerts > CallHome` commands, refer to the *NetBackup Appliance Command Reference Guide*.

Settings > Notifications > Login Banner

The **Settings > Notifications > Login Banner** page lets you create a customized text banner that appears when you access the appliance. After you create and configure the login banner, it appears in both the NetBackup Appliance Shell Menu

and the NetBackup Appliance Web Console. You can use the login banner to communicate important information to users, such as a corporate security policy.

Use the **Display Login Banner** check box to turn on and turn off the login banner.

By default, the login banner appears when anyone tries to access an appliance-specific interface. You can choose to have the login banner appear in the NetBackup Console by selecting the **Apply changes in NetBackup** check box.

The login banner consists of the following two elements:

- **Login Banner Heading**
  - 250 characters maximum
  - Standard English alphabet
- **Login Banner Text**
  - Unlimited characters
  - Standard English alphabet

Before you click **Save**, make sure to click **Preview** to see how your changes appear in the NetBackup Appliance Web Console.

Note: None of the login banner settings on this page take effect until you click **Save**.

See "Creating the appliance login banner" on page 249.

See "Removing the appliance login banner" on page 251.

Creating the appliance login banner

The following procedures describe how to set the appliance login banner using the NetBackup Appliance Web Console.

To enable and create a new login banner using the NetBackup Appliance Web Console

1. Log onto the NetBackup Appliance Web Console.
2. Click **Settings > Notifications > Login Banner**.
3. Select the **Display Login Banner** check box.

Note: The **Login Banner Heading** and **Login Banner Text** fields are only activated if **Display Login Banner** is checked.

---

4. Enter the desired text in the **Login Banner Heading** and the **Login Banner Text** fields.
5. Click **Preview** to review your changes.
6. Select the **Apply changes in NetBackup** check box if you want the same login banner to appear in the NetBackup Administration Console.
7. Click **Save**.

   When the confirmation dialog window appears, click **Yes** to apply the changes, or click **No** to continue making changes.

Once the login banner is enabled, you can go back and make changes. New changes are only applied if you click **Save**.

The following procedures describe how to set the appliance login banner using the NetBackup Appliance Shell Menu.

To enable and create a new login banner using the NetBackup Appliance Shell Menu

1. Log onto the NetBackup Appliance Shell Menu.
2. Run the `Main > Settings > Notifications > LoginBanner Set` command.
3. Enter a banner heading, and then press **Enter**.
4. Enter the banner message text.

   Once you have entered the banner message, type **end** on a new line and press **Enter**.
5. A preview of the login banner appears with the following message:

   ```
   The existing login banner will be overwritten and the SSH daemon
   will be restarted. Do you want to proceed? [y, n]: (y)
   ```

   Type **y** and press **Enter** to set the login banner. Type **n** and press **Enter** to cancel any changes and exit the login banner configuration.
6. The following message appears:

   ```
   Do you want to use this banner for the NetBackup Administration
   Console as well? (Any existing Netbackup login banner will be
   overwritten.) [y, n]: (y)
   ```

   Type **y** and press **Enter** to set the login banner in the NetBackup Administration Console. Type **n** and press **Enter** to continue without changing the NetBackup login banner.

Once the login banner is enabled, you cannot make individual changes to it using the NetBackup Appliance Shell Menu. However, you can run the `LoginBanner Set`

command again and overwrite the existing banner with one that contains your desired changes. Alternatively, you can use the NetBackup Appliance Web Console to make individual changes.

For more information on the login banner commands, refer to the *NetBackup Appliance Command Reference Guide*.

Removing the appliance login banner

The following procedures describe how to remove the appliance login banner using the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu.

To remove the login banner using the NetBackup Appliance Web Console

1. Log onto the NetBackup Appliance Web Console.
2. Click **Settings > Notifications > Login Banner**.
3. Uncheck the **Display Login Banner** check box.
4. Select the **Apply changes in NetBackup** check box if you want to remove the login banner from the NetBackup Administration Console as well.
5. Click **Save**.

   When the confirmation dialog window appears, click **Yes** to remove the login banner, or click **No** to continue making changes.

To remove the login banner using the NetBackup Appliance Shell Menu

1. Log onto theNetBackup Appliance Shell Menu.
2. Run the `Main > Settings > Notifications > LoginBanner Remove` command.
3. When the following message appears, select the appropriate action:

   ```
   The existing login banner will be removed and the SSH daemon
   will be restarted. Do you want to proceed? [y, n]: (y)
   ```

   Type **y** and press **Enter** to remove the login banner. Type **n** and press **Enter** to cancel.
4. When the following message appears, select the appropriate action:

   ```
   Do you want to remove the login banner from the NetBackup
   Administration Console as well? [y, n]: (y)
   ```

   Type **y** and press **Enter** to remove the NetBackup login banner. Type **n** and press **Enter** to leave the banner set in the NetBackup Administration Console.

For more information on the login banner commands, refer to the *NetBackup Appliance Command Reference Guide*.

About AutoSupport

The AutoSupport feature lets you register the appliance and your contact details at the Veritas support website. Veritas support uses this information to resolve any issue that you report. The information allows Veritas support to minimize downtime and provide a more proactive approach to support.

The https://netInsights.veritas.com portal is the unified address where you register the appliance and edit registration details.

The support infrastructure is designed to allow Veritas support to help you in the following ways:

- Proactive monitoring lets Veritas support to automatically create cases, fix issues, and dispatch any appliance parts that might be at risk.
- The AutoSupport infrastructure within Veritas analyzes the Call Home data from appliance. This analysis provides proactive customer support for hardware failures, reducing the need for backup administrators to initiate support cases.
- With AutoSupport ability, Veritas support can begin to understand how customers configure and use their appliances, and where improvements would be most beneficial.
- Send and receive status and alert notifications for the appliance.
- Receive hardware and software status using Call Home.
- Provide more insight into the issues and identify any issues that might further occur as a result of the existing issue.
- View reports from the Call Home data to analyze patterns of hardware failure, and see usage trends. The appliance sends health data every 30 minutes.

Settings > Network

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

- **Network Settings** - enables you to configure network and routing settings for your appliance.
  See “Settings > Network > Network Settings” on page 253.
- **Host** - enables you to reconfigure your appliance's host settings.
  See “Settings > Network > Host” on page 271.
- **Fibre Transport** - enables you to reconfigure the Fibre Transport settings.
  See “Settings > Network > Fibre Transport” on page 266.

You can also configure the network settings using the `Main_Menu > Network` commands from the NetBackup Appliance Shell Menu. For more information refer to the *NetBackup Appliance Command Reference Guide*.

VLAN configuration for NetBackup Appliances

Starting with NetBackup Appliance version 2.6.0.3, you can configure VLANs in your existing network environments.

The concept of a Virtual Local Area Network (VLAN) is devised to logically partition a physical network for creating multiple distinct broadcast domains. These broadcast domains can be segmented on the basis of organization functions, teams within a function, or applications. Although the properties of VLANs are same as those of LANs, VLANs have pivotal advantages over the traditional LANs in the following ways:

- Allows the formation of virtual workgroups.
- Enhances network performance.
- Simplifies network administration.
- Provides better security.
- Reduces the overall costs of network management.

To configure VLAN for your appliance from the NetBackup Appliance Web Console, use the **Network** tab on the **Settings > Network** page.

To configure VLAN from the NetBackup Appliance Shell Menu, run the `Main_Menu> Network > VLAN` command.

See "Settings > Network > Network Settings" on page 253.

Settings > Network > Network Settings

The **Settings > Network** menu directs you to its default **Network Settings** page. The **Network Settings** page enables you to configure and update the network settings for your appliance. These network settings are applied at the time of initial configuration.

The **Network Settings** page is divided into two panes. The first pane contains the **Interface Properties** and **Routing Properties** tabs. The second pane contains **Network Configuration** pane.

The taskbar underneath the **Interface Properties** tab enables you to complete the following tasks:

Table 5-10 Taskbar elements under the Interface Properties tab

This function...	Lets you...
Filter by Network Interface	Filter the network interface by its name. If you enter the name of a physical interface in the field, the resultant displays information for the physical interface along with information of any bond that is created over the physical interface. For example, if *eth2* is a part of *bond1*, then the filter criteria for *eth2* displays information for *bond1* too.
Edit	Edit network interface properties. Use this button to edit MTU, remove an IP address, and assign an IP address on a selected network interface. **Note:** You must select a single network interface to edit its properties. If you select multiple interfaces, the **Edit** button is disabled. You can edit the following properties depending on the type of interface that is selected for editing: ■ **MTU** - Use to update the maximum transmission unit (MTU) size for the selected interface. **Note:** This field is available only for physical and bond interfaces. ■ **Description** - Use to update the description for the selected VLAN device. **Note:** This field is available only for VLAN devices. Further, the provision to add a description for the VLAN is available only through theNetBackup Appliance Web Console. ■ **Remove IP Interface** - Use to remove an IP address. ■ **Assign IP** - Use to update or assign an IP address. The **Assign IP** section lets you edit the following fields: ■ **IP Address [IPv4]** - Enter the IPv4 address. ■ **Netmask IP Address [IPv4]** - Enter netmask information for the IPv4 address. ■ **IP Address [IPv6]** - Enter the IPv6 address. ■ **Prefix size [IPv6]** - Enter the prefix size for the IPv6 address. ■ **Enable WAN optimization** Enables or disables WAN (wide area network) optimization for individual network interfaces and network interface bonds. See “About WAN Optimization” on page 257.

Table 5-10 Taskbar elements under the Interface Properties tab *(continued)*

This function...	Lets you...
Delete	Delete multiple virtual interfaces. For example, *bond1, bond2* or *vlan2, vlan3, vlan4*. **Note:** You cannot delete multiple network interfaces simultaneously. Further, you cannot delete a physical interface. In addition, you cannot delete an interface that is a part of a bond or that has a VLAN tagged to it.

The taskbar below the **Routing Properties** tab lets you delete routing information for a selected network interface using the **Delete** button.

The **Interface Properties** tab and the **Routing Properties** tab provide the following information:

Table 5-11 Interface Properties tab and Routing Properties tab information

Field names	Description
Interface Properties: Click this tab to view the existing network interface configuration settings for the appliance.	
Network Interface	Displays the NIC (network interface card) number. For example, eth1 or vlan1. **Note:** A private interface (eth0) can not be edited from the NetBackup Appliance Web Console. However, you can edit a private interface from the NetBackup Appliance Shell Menu.
Description	Displays information that is entered for a VLAN interface. For example, HR domain, Finance domain.
IP Address [IPv4 or IPv6]	Displays the IPv4 or the IPv6 address of the network connection.
Subnet Mask	Displays the subnet mask value that corresponds to the IP address.
Speed	Displays the current speed of the network connection. For example, 1Gb/s.
Cable State	Displays the status of the cable connection as Plugged or Unplugged.
Link State	Displays the status of network connection as Up or Down.
Link Aggregation	Displays whether a physical interface is a part of a bond. If the physical interface is a part of a bond, the field displays YES.

Table 5-11 Interface Properties tab and Routing Properties tab information *(continued)*

Field names	Description
Reserved	Displays if the network is reserved or not.
WAN optimization	Displays the WAN optimization status of each network interface. Status messages include Enabled or Disabled.
VLAN	Display whether a VLAN is tagged to a network interface. If a VLAN is tagged to a network interface the field displays YES.
Routing Properties: Click this tab to view the existing routing configuration settings for the appliance.	
Network Interface	Displays the NIC (network interface card) number. For example, eth1.
Destination IP	Displays the network IP address of a destination network.
Destination Subnet Mask	Displays the subnet value that corresponds to the IP address.
Gateway	Displays the address of the network point that acts as an entrance to another network.

In addition, the network interfaces that you find in the **Interface Properties** tab and the **Routing Properties** tab also provide links to access detailed network properties. Clicking a network interface opens a properties window for the selected network interface. The window provides information about the selected network interface.

The following table describes the type of network configurations that you can perform.

Table 5-12 Network Configuration pane options

Operation	Description
Create Bond	Provides the data entry fields to create a network bond. See “Creating a bond” on page 262.
Tag VLAN	Provides the data entry fields to tag a VLAN over a network interface. See “Tagging VLAN” on page 264.
Add Static Route	Provides the data entry fields to add network routing information. See “Adding static route” on page 265.

About WAN Optimization

The Wide Area Network (WAN) Optimization feature applies various techniques to improve outbound network traffic from your appliance.

This feature includes the following benefits:

- Improves NetBackup Auto Image Replication (AIR) performance.
  NetBackup AIR is a disaster recovery solution. Its purpose is to create off-site copies of mission critical backups to protect against site loss.
  For example, the backups that are generated in one NetBackup domain can be replicated to storage in other NetBackup domains. These other NetBackup domains may be located in diverse geographical locations. Because WAN optimization can improve wide area network data throughput to and from your appliance, more efficient backup data transfers and disaster recovery transfers occur.
- Benefits those appliances for which the traffic is sent across on slower networks. Such as networks with a latency greater than 20 milliseconds and packet loss rates greater than 0.01% (1 in 10,0000).
- Operates on individual TCP connections. Evaluates each outbound network connection to determine whether the performance can be improved.
- Improves the network performance with minimal dependency on the outbound network traffic.
- Improves the network performance of optimized duplications.
- Improves the network performance of restores to remote clients.
- Imposes no network overhead. WAN optimization is non-intrusive, as it does not impose any network overhead in situations where the overall network data transfers are high. In some scenarios, when the overall network data transfer is high, the connection speed may not be optimized despite this feature being enabled.

You can enable or disable WAN Optimization for individual network interfaces and network interface port bonds from **Settings > Network > Interface Properties** tab in the NetBackup Appliance Web Console. You can also use the NetBackup Appliance Shell Menu.

For more information about using WAN Optimization commands in the NetBackup Appliance Shell Menu, refer to *NetBackup™ Appliance Commands Reference Guide.*

Table 5-13 WAN Optimization operations

Operation	Description	NetBackup Appliance Shell Menu	NetBackup Appliance Web Console
Enable	The `Enable` command is used to enable the WAN optimization settings. The WAN optimization feature is enabled by default. See "How to enable WAN optimization for a network interface port or a network interface port bond" on page 259.	Yes	Yes
Disable	The `Disable` command is used to disable the WAN optimization settings. You can disable this setting using the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu. See "How to disable WAN optimization for a network interface port or a network bond" on page 260.	Yes	Yes
Status	The `Status` command is used to view WAN optimization reports. See "Viewing the WAN optimization status" on page 260.	Yes	Yes

See "Settings > Network > Fibre Transport" on page 266.

See "Settings > Network > Host" on page 271.

How to enable WAN optimization for a network interface port or a network interface port bond

Use the following procedure to enable WAN optimization for a network interface port or a network interface port bond.

To enable WAN optimization for a network interface port or a network interface port bond

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings** > **Network**.
3. On the Network Settings page, under the **Interface Properties** tab, select a network interface.
4. Click **Edit**.

   The **Edit Network Interface Properties** dialog box appears.
5. To enable WAN optimization, select **Enable WAN optimization**.
6. Click **Save**.

   The following message appears while the appliance enables WAN optimization for the selected network interface:

   ```
   Updating network configuration...
   ```

   After the appliance successfully enables WAN optimization, the following message appears under the **Network Settings** page name:

   ```
   WAN optimization for [selected eth port or bond] was enabled
   successfully.
   ```

   In addition, the status of the selected network interface changes to **Enabled** in the **WAN optimization** column of the **Interface Properties** tab.

Note: If you run a factory reset of the appliance, note the following:

A factory reset disables WAN optimization for all network interface port bonds when you retain your network configuration.

After the factory reset completes, you can then enable WAN optimization again for the network interface port bonds.

If you choose *not* to retain your network configuration, all network interface port bonds are lost during the factory reset. After the reset completes, the appliance automatically enables WAN optimization for all network interface ports, including those that comprised the bonds.

How to disable WAN optimization for a network interface port or a network bond

Use the following procedure to disable WAN optimization for a network interface port or a network bond.

To disable WAN optimization for a network interface port or a network bond

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings** > **Network**.
3. On the Network Settings page, under the **Interface Properties** tab, select a network interface.
4. Click **Edit**.

   The **Edit Network Interface Properties** dialog box appears.
5. To disable WAN optimization, deselect **Enable WAN optimization**.
6. Click **Save**.

   The following message appears while the appliance disables WAN optimization for the selected network interface:

   ```
   Updating network configuration...
   ```

   After the appliance successfully disables WAN optimization, the following message appears under the **Network Settings** page name:

   ```
   WAN optimization for [selected eth port or bond] was disabled
   successfully.
   ```

   In addition, the status of the selected network interface changes to **Disabled** in the **WAN optimization** column of the **Interface Properties** tab.

Viewing the WAN optimization status

The `Status` command displays the WAN optimization status of the network interface ports and the network interface port bonds.

- If WAN Optimization is disabled, the connection is not optimized.
- If the WAN Optimization status is changed (from disabled to enabled or vice versa), the status of existing connections is immediately updated.

To view the WAN optimization status

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

   ```
   Main_Menu > Network > WANOptimization
   ```

   All of the options for the WAN Optimization command appear.
3. To view the WAN optimization status, type the following command:

   ```
   status
   ```

   The appliance displays the WAN optimization status in a table that resembles the following example:

   ```
   Bond     Interface   State        IP address     WAN Optimization

   bond0    eth4        Plugged                     Disabled
            eth5        Plugged

            eth0        Unplugged    192.168.00.00  Enabled

            eth1        Plugged      10.200.00.00   Disabled

            eth2        Plugged                     Enabled

            eth3        Plugged                     Enabled
   ```

Network and VLAN configuration guidelines

To facilitate network configuration and administration, it is recommended that you follow certain guideline to configure or update your network settings.

Guidelines for creating a network interface bond (NIC bond)

- Ensure that the network interfaces that participate in bond formation have the same port speed (i.e. either 1GB or 100GB).
- At least one of the network interfaces that participates in bond formation must be plugged.
- Ensure that none of the network interfaces that are selected for creating the bond have any VLANs tagged to them.

- Verify that any of the selected network interfaces are not already part of another bond.

Note: When configuring multiple network interfaces as a NIC bond, use the NetBackup Appliance Shell Menu or the NetBackup Appliance Web Console to configure the bond. NIC bonds that are configured with tools other than the recommended appliance tools appear as *Disabled* when you run the WAN optimization `Status` command. They also appear as *Disabled* when you view them in the NetBackup Appliance Web Console.

Use either the NetBackup Appliance Shell Menu or the NetBackup Appliance Web Console to enable these NIC bonds.

Guidelines for tagging a VLAN

- Ensure that the selected interface or ethernet device is plugged.
- Verify that the selected interface is not a part of a bond.
- Starting with appliance release 3.2, the selected interface can have an IP address configured to it.

Creating a bond

Use the following procedure to create a bond between two or more network interfaces.

To create a bond

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Network** tab. The appliance displays the default **Network Settings** page.
3. Click **Create Bond**.
4. In the **Network Configuration** section, enter the network interface information that is required to create a bond using the following fields:

Field name	Description
Select Interface	Select the interface or the device name between which you want to create the bond. To bond multiple Network Interface Cards (NICs), consider the following guidelines: ■ The **Network Interface** drop-down list shows appliance Ethernet ports available for creating a bond. Select two or more interfaces to create a bond. To deselect an interface, click it again. ■ You can enter either an IPv4 address or an IPv6 address. Multiple or duplicate IP addresses are not excepted for a NIC or bond. ■ Only NICs of the same type and speed can be bonded. See "Network and VLAN configuration guidelines" on page 261. for additional guidelines on creating a bond.
Bond Mode	Select the bond mode to configure bonding. The eight available modes are: ■ balance-rr ■ active-backup ■ balance-xor ■ broadcast ■ 802.3ad ■ balance-tlb ■ balance-alb The default mode is balance-alb. Some bond modes require additional configuration on the switch or the router. You should take additional care when you select a bond mode. For more information about bond modes, see the following documentation: http://www.kernel.org/doc/Documentation/networking/bonding.txt
IP Address [IPv4 or IPv6]	Enter the IPv4 or the IPv6 address to be used for this appliance. Only global-scope and unique-local IPv6 addresses are allowed.
Subnet Mask	Enter the subnet mask value that corresponds to the IP address.

5 To add the network configuration details for creating the bond, click **Add**.

The new entries are configured on the appliance and are listed automatically in the read-only fields of the **Interface Properties** tab.

To create a bond using the NetBackup Appliance Shell Menu, run the `Main_Menu > Network > LinkAggregation Create` command. For detailed information on the `LinkAggregation Create` command, refer to the *NetBackup Appliance Command Reference Guide*.

See "Tagging VLAN" on page 264.

See "Adding static route" on page 265.

Tagging VLAN

Use the following procedure to tag VLAN into your existing network environment.

To tag VLAN

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Network** tab. The appliance displays the default **Network Settings** page.
3. In the **Network Configuration** section, expand the **Tag VLAN** option and enter the network information that is required to tag a VLAN using the following fields:

Field Name	Description
Select Interface	Select the network interface or the device name to which you want to tag the VLAN. See "Network and VLAN configuration guidelines" on page 261. for additional guidelines on tagging a VLAN.
Description	Enter a description for the VLAN. For example, Finance or Human Resource.
VLAN Id	Enter a numeric identifier for the VLAN. For example, 1 or 10.
IP Address [IPv4 or IPv6]	Enter the IPv4 or the IPv6 address to be used for this appliance.
Subnet Mask	Enter the subnet mask value that corresponds to the IP address.

4 Click **Add** to add the configuration information for tagging VLAN into to your existing network environment.

5 To enter information for tagging additional VLANs, click the **+** sign to add a row. To remove any of the rows, click the **-** sign that is adjacent to the **Subnet Mask** field.

The new entries are configured on the appliance and are listed automatically in the read-only fields of the **Interface Properties** tab.

To tag VLAN from the NetBackup Appliance Shell Menu, run the `Main_Menu > Network > VLAN Tag` command. For detailed information on the `VLAN Tag` command, refer to the *NetBackup Appliance Command Reference Guide*.

See "Creating a bond" on page 262.

See "Adding static route" on page 265.

Adding static route

Use the following procedure to add or update the network routing information for your appliance.

To add network routing information for your appliance

1 Log on to the NetBackup Appliance Web Console.

2 Click **Settings > Network > Network** tab. The appliance displays the **Network Settings** page.

3 In the **Network Configuration** section, expand the **Add Static Route** option and enter the network interface information that is required to add routing information using the following fields:

Field Name	Description
Destination IP	Enter the network IP address of a destination network. Enter the network IP address of a destination network. For the initial appliance configuration, this field contains a default value that cannot be changed. When you configure another destination IP, you must enter the appropriate address.
Destination Subnet Mask	Enter the subnet value that corresponds to the IP address. Enter the subnet value that corresponds to the IP address. For the initial appliance configuration, this field contains a default value that cannot be changed. When you configure another route, you must enter the appropriate value.
Gateway	Enter the address of the network point that acts as an entrance to another network.
Network Interface	The appliance can use multiple network interface cards (NICs). This column displays the network device name. for example, eth0 or bond0 or vlan1.

4 Click **Add** to add the network routing information for your appliance.

The new entries are configured on the appliance and are listed automatically in the read-only fields of the **Routing Properties** tab.

See "Creating a bond" on page 262.

See "Tagging VLAN" on page 264.

Settings > Network > Fibre Transport

The Fibre Transport (FT) options let you set up the appliance for FT use with SAN Clients or for optimized duplication and Auto Image Replication. By default, the FT options are disabled and the configuration of one option does not affect the other one.

The following describes the FT options:

Table 5-14 FT option descriptions

FT option	Description
Enable Fibre Transport target mode (FTMS and MSDP) on the media server	This option lets you enable Fibre Transport target mode as follows: ■ FTMS Target You must configure at least one SAN Client target port before you can enable FTMS Target mode. ■ MSDP Target See "Configuring Fibre Transport settings" on page 268.
Enable Fibre Transport for replication to other NetBackup Appliances	This option lets you enable Fibre Transport for optimized duplication and Auto Image Replication to other NetBackup appliances that are used as target hosts. By default, this option is disabled and the appliance cannot communicate with a target appliance over FC. **Note:** To use this option, you must enable FC communication on the associated target NetBackup appliance. If you plan to use a NetBackup 52xx or 53xx appliance as the target, see the following for configuration. See "Configuring Fibre Transport to other NetBackup appliances" on page 270.

For more information about SAN Client and Fibre Transport support on NetBackup appliance, see the *NetBackup Appliance Fibre Channel Guide*.

About the HBA port mode configuration table

The port mode configuration table shows the details of the HBA ports that can be used for Fibre Transport Deduplication.

Fibre Transport Deduplication is a feature that enables you to use an appliance as a target host for optimized duplication and Auto Image Replication.

Note: The HBA port mode configuration table shows all HBA ports except for those that are connected to external storage (Primary Storage Shelf) on NetBackup 53xx appliances.

You can configure an HBA port in the table to be in target mode or standard initiator mode.

Table 5-15 describes the HBA port mode configuration table.

Table 5-15 HBA port mode configuration

Column Name	Description
Slot	This column shows the slot number of the HBA card on this appliance.
Port	This column shows the port number of the HBA ports.
Link Status	This column shows whether the HBA port is connected to a fabric switch or another port. The link status on an HBA port can be the following: ■ **up** - connected ■ **down** - not connected
World Wide Name (WWN)	This column shows the port WWN. You can use the port WWN to identify a port on the appliance.
Port Mode	This column shows the configured port mode of an HBA port. The available options for HBA port mode are the following: ■ **Initiator** - Standard initiator mode ■ **Target** - Target mode for optimized duplication, Auto Image Replication, and NetBackup SAN Client You can click on the current port mode, and then change the port mode configuration. If you change the port mode, you can see the new port mode with a red earmark. You can click on the **Restore FactoryDefaults** option to restore the port configuration to the factory default state. See "Configuring Fibre Transport settings" on page 268.

Configuring Fibre Transport settings

This topic describes how to configure an appliance media server for the following Fibre Transport (FT) options:

- Configure Fibre Transport target mode (FTMS and MSDP) for NetBackup SAN client, optimized duplication, and Auto Image Replication over Fibre Channel (FC) to other NetBackup appliances.
- Configure any available HBA Fibre Channel (FC) ports for **Target** or **Initiator**

About Fibre Transport support for high availability (HA) setups

Fibre Transport Target Service (or FTMS) is supported for NetBackup Appliance HA setups. FTMS operates in the A/P (active/passive)mode only. Therefore, FTMS is available only on the node where MSDP is running (active node), while it is disabled on the partner node (passive node). Whenever you perform an HA switchover operation, the FTMS state changes on each node automatically as is appropriate to reverse the operation of the nodes. Perform the FTMS configuration only on the node where MSDP is running (active node). The configuration steps are the same as for a single appliance media server.

The following procedures describe how to configure FT settings from the appliance interfaces.

To configure Fibre Transport media server settings from the NetBackup Appliance Web Console

1. Log in to the NetBackup Appliance Web Console.
2. Click **Settings > Network**, then select **Fibre Transport**.
3. To enable the feature, click the check box for **Enable Fibre Transport target mode (FTMS and MSDP) on media server**
4. To keep the current port configuration, skip this step.

   To change the port modes on the appliance, do the following:

   - In the **Port Mode** column, click on the current port mode of a port.
   - From the drop-down menu, select **Initiator** or **Target** to configure the port mode. Repeat this for every port that you want to change.
   - To restore the customized port configuration to the factory default settings, click **Restore FactoryDefaults**.
5. After you have made all changes, click **Save** to apply the changed settings.

To configure Fibre Transport media server settings from the NetBackup Appliance Shell Menu

1. Log in to the NetBackup Appliance Shell Menu.
2. To enable Fibre Transport Deduplication and NetBackup SAN Client features, run the following commands:

   - To administer the use of Fibre Transport features on other appliances:

     ```
     Main > Settings > FibreTransport Initiator
     ```
   - To administer Fibre Transport features on this appliance:

     ```
     Main > Settings > FibreTransport Target
     ```

3 To configure the port modes, go to the `Main > Manage > FibreChannel` view and run the following commands:

- For FTMS and MSDP target:

  `Configure Target` *`HBAportid`*

  Where *HBAportid* is HBA card slot number 1 - 8 and HBA port number 1 - 2. For example, to set port 2 on the HBA card in slot 5 for Target, enter the following: `Configure Target 5:2`

- For Initiator:

  `Configure Initiator` *`HBAportid`*

  Where *HBAportid* is HBA slot number 1 - 8 and HBA port number 1 - 2. For example, to set port 1 on the HBA card in slot 5 for initiator, enter the following: `Configure Initiator 5:1`

4 To verify that all changed settings are correct, run the following command:

`Main > Manage > FibreChannel > Show`

Configuring Fibre Transport to other NetBackup appliances

Use the following procedure to configure Fibre Transport (FT) to other NetBackup appliances.

Note: If you plan to enable or change the **Enable Fibre Transport for replication to other NetBackup Appliances** feature, it is recommended that you first suspend or cancel all jobs before you enable or change the feature.

To configure Fibre Transport to other NetBackup appliances from the NetBackup Appliance Web Console

1 Log on to the NetBackup Appliance Web Console.

2 Click **Settings > Network**, then select **Fibre Transport**.

3 To enable the feature, click **Enable Fibre Transport for replication to other NetBackup Appliances**, then click **Save**.

When the message appears to inform you of the required appliance version, click **OK** to continue or click **Cancel** to exit without making changes.

Note: You must also enable FC communication on the associated NetBackup appliance.

On a target NetBackup 52xx or 53xx, you must enable that appliance as a replication target to use it as the storage destination.

---

4 To disable the **Fibre Transport to other NetBackup Appliances** option, deselect the check box to clear the check mark. Then, click **Save**.

To configure Fibre Transport to other NetBackup appliances from the NetBackup Appliance Shell Menu (5350 model with software versions 4.0 and later, all other supported models with software versions 4.1 and later)

1 Log on to the appliance shell menu.

2 To enable the feature, run the following command:

```
Main > Settings > FibreTransport Initiator Enable
```

3 To disable the feature, run the following command:

```
Main > Settings > FibreTransport Initiator Disable
```

4 To check the current settings, run the following command:

```
Main > Settings > FibreTransport Initiator Show
```

See "Settings > Network > Fibre Transport" on page 266.

Settings > Network > Host

The **Settings > Network > Host** tab enables you to configure the DNS configuration settings for DNS systems and the Host Name Resolution settings for non-DNS systems.

The **Settings > Network > Host** tab displays the **Host name** of your appliance.

Note: The host name can only be set during an initial configuration session. After the initial configuration has completed successfully, you can re-enter initial configuration by performing a factory reset on the appliance.

See "About NetBackup appliance factory reset" on page 156.

The **Settings > Network > Host** tab displays the **Host name** of your appliance and the remaining tab is divided into the following two sections:

The remaining part of the **Settings > Network > Host** tab is divided into the following two sections:

- **Domain Name System** displays the fields for entering DNS configuration details.
- **Host Name Resolution** displays the fields for configuring systems that use the host name (non-DNS) details.

Changing DNS and Host Name Resolution (non-DNS) configuration settings

Use the following procedure to change or add the DNS and Host Name Resolution (non-DNS) configuration settings.

To change the DNS configuration settings

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Network > Host** tab.
3. Enter the appropriate information in the **DNS** data entry fields as follows:

Fields	Description
DNS IP Address(es)	Enter the IP address of the DNS server. To enter multiple DNS server names, use a comma character as the delimiter between each name. 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 273.
Domain Name Suffix	Enter the suffix name of the DNS server.
Search Domain(s)	You can enter one or more DNS search domain names to search when an unqualified host name is given. To enter multiple search domain names, use a comma character as the delimiter between each name.

4. Click **Save**.

To change the Host Name Resolution (non-DNS) configuration settings

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

3 Enter the **Host Name Resolution** configuration information using the following fields:

Fields	Description
IP Address	Enter the IP address of the appliance. The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed. See "About IPv4-IPv6-based network support" on page 273.
Fully qualified host name	Enter the Fully Qualified Host Name (FQHN) of the appliance.
Short host name	Enter the short name of the appliance. After you enter all of the necessary information in these fields, you must click **Add**.

4 Click **Save**.

About IPv4-IPv6-based network support

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:

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

For example, to add an appliance media server to the primary server, enter the IPv6 address of the appliance media server as follows:

Example:

```
Main > Network > Hosts add 9ffe::45 v45 v45
Main > Settings > NetBackup AdditionalServers Add v45
```

You do not need to provide the IPv4 address of the appliance media server.

- A pure IPv6 client is supported in the same way as in NetBackup.
- You can 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.
- The `Main_Menu > Network > Hosts` command supports multiple IPv6 addresses to be assigned to the same host name having one network interface card (NIC). However, only one IPv4 address can be assigned to a specific host name having one NIC using this command.
- You can add an IPv6 address of a network interface without specifying a gateway address.
  For more details, see the *NetBackup Appliance Command Reference Guide*.

Settings > Date and Time

On the **Settings > Date and Time** page, you can change the date, the time, and the time zone parameters that are added at the time of initial configuration.

Use the following procedure to change the date and time settings post-configuration.

To change the date, the time, and the time zone configuration

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Date and Time**.
3. Enter the appropriate information in the fields:

Select Time Zone	To assign a time zone to the appliance, click on the **Time zone** drop-down box and select the appropriate region, country, and time zone. **Note:** The Coordinated Universal Time (UTC) option does not appear in the drop-down list. To set the time zone for UTC, you must manually type **UTC** into the data entry field.

Set Date and Time

You can select any one of the following options to set the date and the time for the appliance.

- **Use NTP server date and time settings** - Use this option to synchronize the appliance with an NTP server. In the **Server IP or Host name** field, specify the IP address or the host name of the NTP server
- **Specify date and time** - Use this option to manually specify the date and time. In the **Date** field, click the calendar to select the appropriate date (in month, date, and year or the mm/dd/yyyy format). In the **Time** field, enter the time in hh:mm:ss format.

4 Click **Save**.

You can also configure the Date and Time settings using the `Main > Network > Date` commands under the NetBackup Appliance Shell Menu. For more information on the `Date` command refer to the *NetBackup Appliance Command Reference Guide*.

Settings > Authentication

The NetBackup appliance provides you authentication and authorization functions to help provide controlled user access to various administration interfaces. You can manage users both by GUI and NetBackup CLI.

- The **Authentication** feature lets you configure the appliance to authenticate various types of users so that they can access and manage the appliance.
- The **Authorization** feature lets you grant various types of users and user groups with specific access privileges on the NetBackup appliance. See "Settings > Authentication > User Management" on page 297.

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

About configuring user authentication

Table 5-16 describes the options that are provided in the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu for configuring the appliance to authenticate various types of users and grant them access privileges.

Table 5-16 User authentication management

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Local (native user)	Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add local users. See "About authorizing NetBackup appliance users" on page 280.	The following commands and options are available under `Settings > Security > Authentication > LocalUser`: ■ `Clean` - Delete all of the local users. ■ `List` - List all of the local users that have been added to the appliance. ■ `Password` - Change the password of a local user. ■ `Users` - Add or remove one or more local users.

Table 5-16 User authentication management *(continued)*

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
LDAP	You can perform the following LDAP configuration tasks under **Settings > Authentication > LDAP**: ■ Add a new LDAP configuration. ■ Import a saved LDAP configuration from an XML file. ■ Add, edit, and delete configuration parameters for the LDAP server. ■ Identify and attach the SSL certificate for the LDAP server. ■ Add, edit, and delete attribute mappings for the LDAP server. ■ Export the current LDAP configuration (including users) as an XML file. This file can be imported to configure LDAP on other appliances. ■ Disable and re-enable the LDAP configuration. ■ Unconfigure the LDAP server. Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add LDAP users and user groups. See "About authorizing NetBackup appliance users" on page 280.	The following commands and options are available under `Settings > Security > Authentication > LDAP`: ■ `Attribute` - Add or delete LDAP configuration attributes. ■ `Certificate` - Set, view, or disable the SSL certificate. ■ `ConfigParam` - Set, view, and disable the LDAP configuration parameters. ■ `Configure` - Configure the appliance to allow LDAP users to register and authenticate with the appliance. * ■ `Disable` - Disable LDAP user authentication on the appliance. ■ `Enable` - Enable LDAP user authentication on the appliance. ■ `Export` - Export the existing LDAP configuration as an XML file. ■ `Groups` - Add or remove one or more LDAP user groups. Only the user groups that already exist on the LDAP server can be added to the appliance. ■ `Import` - Import the LDAP configuration from an XML file. ■ `List` - List all of the LDAP users and user groups that have been added to the appliance. ■ `Map` - Add, delete, or show NSS map attributes or object classes. ■ `Show` - View the LDAP configuration details. ■ `Status` - View the status of LDAP authentication on the appliance. ■ `Unconfigure` - Delete the LDAP configuration. ■ `Users` - Add or remove one or more LDAP users. Only the users groups that already exist on the LDAP server can be added to the appliance.

Table 5-16 User authentication management *(continued)*

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Active Directory	You can perform the following AD configuration tasks under **Settings > Authentication > Active Directory**: ■ Configure a new Active Directory configuration. ■ Unconfigure an existing Active Directory configuration. Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add Active Directory users and user groups. See "About authorizing NetBackup appliance users" on page 280.	The following commands and options are available under `Settings > Security > Authentication > ActiveDirectory`: ■ `Configure` - Configure the appliance to allow AD users to register and authenticate with the appliance. ■ `Groups` - Add or remove one or more AD user groups. Only the user groups that already exist on the AD server can be added to the appliance. ■ `List` - List all of the AD users and user groups that have been added to the appliance. ■ `Status` - View the status of AD authentication on the appliance. ■ `Unconfigure` - Delete the AD configuration. ■ `Users` - Add or remove one or more AD users. Only the users that already exist on the AD server can be added to the appliance.
Smart Card Authentication	NA	Enable authentication with smart cards as follows: ■ Configure remote authentication with OpenLDAP or ActiveDirectory under `Settings > Security > Authentication > LDAP` ■ Add CA certificate under `Settings > Security > Certificate AddCACertificate`. ■ Configure DNS to resolve the OCSP URI under `Network > DNS Add Nameserver`. ■ Configure and enable smart card authentication under `Settings > Security > Authentication > SmartCard`. You can also enable authentication for smart cards by logging in to the appliance as a NetBackupCLI user and running the following command: `vssat addldapdomain`

Table 5-16 User authentication management *(continued)*

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Single sign-on (SSO) authentication	NA	Enable SSO authentication for web console users as follows: ■ Configure remote authentication with ActiveDirectory under `Settings > Security > Authentication > ActiveDirectory`. ■ Authorize SSO users and user groups under `Settings > Security > Authorization`. ■ Configure the identity provider (IDP) for SSO under `Settings > Security > Authentication > SingleSignOn`. To configure SSO, click this link to obtain the following documents: *NetBackup Appliance Security Guide* *NetBackup Appliance Commands Reference Guide*
Multifactor authentication	NA	The following commands and options are available under `Settings > Security > Authentication > MFA`: ■ `Configure` - Configure multifactor authentication for the current user. ■ `Enforce` - Enforce multifactor authentication for all appliance users. ■ `Reset` - Reset the multifactor authentication configuration for a user that is unable to log in. ■ `Show GlobalEnforcement` - Check if multifactor authentication is enforced for all users. ■ `Show Key` - Show the key and the QR code for the current user. ■ `Unconfigure` - Unconfigure multifactor authentication for the current user. If multifactor authentication is enforced, users can unconfigure it only within the grace period.

Generic user authentication guidelines

Use the following guidelines for authenticating users on the appliance:

- Only one remote user type (LDAP, or Active Directory/AD can be configured for authentication on an appliance. For example, if you currently authenticate LDAP users on an appliance, you must remove the LDAP configuration on it before changing to AD user authentication.
- The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.
- You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from the NetBackup Appliance Shell Menu.
- You cannot add a new user or a user group to an appliance with the same user name, user ID, or group ID as an existing appliance user.
- Do not use group names or user names that are already used for appliance local users or NetBackupCLI users. Additionally, do not use the appliance default names **admin** or **maintenance** for LDAP or AD users.
- The appliance does not handle ID mapping for LDAP configuration. Veritas recommends that you reserve a user ID and group ID range of 1000 to 1999 only for local appliance users. For remote AD and LDAP users, reserve a user ID and group ID range greater than 1999.
- NetBackup appliance uses general CIFS shares for some of its internal operations such as storing patches and installation files, uploading logs to support, forwarding logs to an external server, and uploading OST plug-ins. Starting with appliance software version 4.0, you must manage access to the general CIFS shares for all local users and Active Directory users and user groups (except the **admin** user). Use the `Settings > Security > Authentication > CIFSShare` command to manage access to the general CIFS shares.
  - Guest users: Replace a Guest user by creating a new local user.
  - Existing local users: Change the passwords for these users.

About authorizing NetBackup appliance users

Table 5-17 describes the options that are provided for authorizing new and existing users or user groups through the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu:

Table 5-17 User authorization management

Task	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Manage users	The following options are available under **Settings > Authentication > User Management** ■ View all of the users that have been added to the appliance. ■ Expand and view all belonging users to a single user group. ■ Add and delete local users. ■ Add and delete LDAP or AD users and user groups.	Use the `Settings > Security > Authentication` commands to add, delete, and view appliance users. See "About configuring user authentication" on page 275.
Manage user permissions (roles)	The following options are available under **Settings > Authentication > User Management**: ■ Grant and revoke the Administrator role for users and user groups. ■ Grant and revoke the NetBackupCLI role for users and user groups. ■ Synchronize members of registered user groups with Administrator role.	The following commands and options are available under `Main > Settings > Security > Authorization`: ■ `Grant` Grant the Administrator and NetBackupCLI roles to specific users and users groups that have been added to the appliance. ■ `List` List all of the users and user groups that have been added to the appliance, along with their designated roles. ■ `Revoke` Revoke the Administrator and NetBackupCLI roles from specific users and users groups that have been added to the appliance. ■ `SyncGroupMembers` Synchronize members of registered user groups.

Notes about user management

- You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from the NetBackup Appliance Shell Menu.
- The NetBackupCLI role can be assigned to a maximum of nine user groups at any given time.
- Active Directory (AD) user groups and user names support the use of a hyphen character in those names. The hyphen must appear between the first and the last character of a user name or a user group name. AD user names and user group names cannot begin or end with a hyphen.
- You can list all users of a group that has maximum to 2000 users from the NetBackup Appliance Web Console. To list all of a group that has more than 2000 users, use the `List` command from the NetBackup Appliance Shell Menu.

NetBackup appliance user role privileges

User roles determine the access privileges that a user is granted to operate the system or to change the system configuration. The user roles that are described in this topic are specific to LDAP and Active Directory (AD) users.

The following describes the appliance user roles and their associated privileges:

Table 5-18 User roles and privileges

User role	Privileges
NetBackupCLI	Users can only access the NetBackup CLI.
Administrator	Users can access the following: ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup Administration Console
AMSadmin	A user account that is assigned the **AMSadmin** role is provided administrative privileges to access the Appliance Management Console that is hosted on the AMS. An AMS user is allowed to perform all the functions on the Appliance Management Console and centrally manage multiple appliances. The AMS user cannot log on the NetBackup Appliance Shell Menu for AMS. An Administrator can create AMS users.

A role can be applied to an individual user, or it can be applied to a group that includes multiple users.

A user cannot be granted privileges to both user roles. However, a NetBackupCLI user can also be granted access to the NetBackup Appliance Shell Menu in the following scenarios:

- The user with the NetBackupCLI role is also in a group that is assigned the Administrator role.
- The user with the Administrator role is also in a group that is assigned the NetBackupCLI role.

Note: When granting a user to have privileges to the NetBackupCLI and the NetBackup Appliance Shell Menu, an extra step is required. The user must enter the `switch2admin` command from the NetBackup CLI to access the NetBackup Appliance Shell Menu.

Granting privileges to users and user groups can be done as follows:

- From the NetBackup Appliance Web Console, on the **Settings > Authentication > User Management** page, click on the **Grant Permissions** link.
- From the NetBackup Appliance Shell Menu, use the following commands in the `Settings > Security > Authorization` view:

```
Grant Administrator Group
Grant Administrator Users
Grant Administrator SSO_Groups
Grant Administrator SSO_Users
Grant NetBackupCLI Group
Grant NetBackupCLI Users
Grant AMS Group
Grant AMS Users
Grant AMS SSO_Groups
Grant AMS SSO_Users
```

See “About configuring user authentication” on page 275.

See “About authorizing NetBackup appliance users” on page 280.

Settings > Authentication

The NetBackup appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support various authentication methods. The following directory service users can be configured and registered to log on to the appliance:

- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD)
- Single sign-on (SSO)
  Configure SSO users to log in with their corporate credentials. SSO access is supported only to the NetBackup Appliance Web Console using a supported external provider. To configure SSO, click this link to obtain the following documents:
  NetBackup Appliance Security Guide
  NetBackup Appliance Commands Reference Guide

Settings > Authentication > LDAP

You can use the **Settings > Authentication** page of the NetBackup Appliance Web Console to configure the appliance to use LDAP server as a directory source to access user information and authenticate the users and user groups to access the appliance. You can also import or export the LDAP configuration settings between multiple appliances.

Prerequisites

- You must have NetBackup appliance 2.6 or higher installed to configure LDAP user authentication.
- LDAP schema must be RFC 2307 or RFC 2307bis compliant.
- The following firewall ports must be open:
  - LDAP 389
  - LDAP OVER SSL/TLS 636
  - HTTPS 443
- Ensure that the LDAP server is available and is set up with the users and user groups that you want to register with the appliance.
- If you are going to select the **Active Directory** as the LDAP directory type, you must configure the appliance with a DNS server that can forward DNS requests to the AD DNS server that you want to use. Alternatively, configure the appliance to use the AD DNS server as the name service data source.

Adding an LDAP server configuration

You can use the **Authentication Server Configuration** tab to add the details of an LDAP server and configure it with your appliance. The LDAP server enables you to access and maintain distributed directory information services for your

appliance. The following procedure describes the steps to configure LDAP user authentication.

To configure an LDAP server

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication >LDAP** to expand the **LDAP Server Configuration**.
3. Select **Add new configuration**.

   The appliance displays the fields to create a new configuration.
4. Enter the configuration information based on the following fields:

Field	Description	Example
Server Name/IP	Enter the FQDN or IP address of your LDAP server. **Note:** The specified LDAP server should comply with RFC2307bis. The RFC2307bis specifies that hosts with IPv6 addresses must be written in their preferred form, such that all components of the address are indicated and leading zeros are omitted.	
Base DN	Enter the base directory name which is the top level of the LDAP directory tree.	**OU= ExampleUsers, dc= mydomain**
Bind DN	Enter the bind directory name. The **Bind DN** is used as an authentication to externally search the LDAP directory within the defined search base.	**DC=com**
Password	Enter the password to access the LDAP server.	
Common User Name	Enter the name of an existing LDAP user on your LDAP server.	**NBUApplianceAdmin**
Common Group Name	Enter the name of an existing LDAP user group on your LDAP server.	

Field	Description	Example
SSL Certificate Required	Displays a drop-down list to enable SSL certificate for your LDAP server. The drop-down list displays the following options: ■ **Yes** - Select to enable adding an SSL certificate ■ **No** - Select to continue configuring the LDAP server without the SSL certificate ■ **Start TLS** **Note:** When you use the **Start TLS** and **Yes** options during LDAP configuration, the initial setup is done over a non-SSL channel. After the LDAP connection and initial discover phase is over, the SSL channel is turned on. Even at this phase, the established SSL channel doesn't do the server-side certificate validation. This validation starts after the server's root certificate is explicitly set using the **Set Certificate** option. For more information, refer to See "Setting the SSL certification" on page 288.	
Directory Type	Select the LDAP directory type from the drop-down list. The available options are: ■ **OpenLDAP** ■ **ActiveDirectory** ■ **Others** Select **OpenLDAP** if you use a typical OpenLDAP directory service. Select **ActiveDirectory** if you use AD as an LDAP directory service. Select **Others** if you use a different type of LDAP directory service.	
Validate UIDs and GIDs for Conflicts	Select the check-box to validate the User IDs and Group IDs and identify conflicting entires between the NetBackup appliance and the LDAP server.	

Note: The **Common User Name** and **Common Group Name** fields are not required to complete LDAP configuration. However, if you do not complete those fields, no LDAP users or LDAP groups appear under **Settings > Authentication > User Management** until you manually add them.

5 Click **Configure** to configure LDAP authentication using the entered parameters.

The appliance configures and enables the new LDAP server and displays the **Attribute Mappings** and **Configuration Parameters** table.

Note: When the directory type is **ActiveDirectory** and the `Settings > Security > Authentication > LDAP > Users Add` command is used to add an LDAP user, you must use the following command to add the groups that the user belongs to on the LDAP server to the appliance: `Settings > Security > Authentication > LDAP > Groups Add`

Importing an LDAP server configuration

You can use the **Authentication Server Configuration** tab to import the details of an LDAP server and configure it with your appliance. The following procedure describes the steps to import a `.xml` file that includes the LDAP server configuration details. The NetBackup appliance configures and connects to the LDAP server using these details.

Note: The `.xml` file must be saved and made available in the `/inst/patch/incoming` directory on the appliance.

To import an LDAP server configuration

1 Log on to the NetBackup Appliance Web Console.

2 Click **Settings > Authentication >LDAP** to expand the **LDAP Server Configuration**.

3 Select the **Import existing configuration** option.

The appliance displays the **File Name** field.

4 Enter the absolute path to the `.xml` file in the **File Name** field.

The `.xml` file must be saved and made available in the `/inst/patch/incoming` directory on the appliance.

5 Click **Import**.

The appliance imports the `.xml` file. The appliance configures and connects to the LDAP server using the XML details.

Setting the SSL certification

You can use the **Authentication Server Configuration** tab to import and set the SSL certificate for your LDAP server. The following procedure describes the steps to set the SSL certification for your LDAP server.

Note: The **Set SSL certificate** option is enabled only after the LDAP server is configured. The SSL certificate must be saved and made available in the `/inst/patch/incoming` directory on the appliance.

To set the SSL certificate

1 Log on to the NetBackup Appliance Web Console.

2 Click **Settings > Authentication**.

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

3 Click on the **Set Certificate** option that is displayed at the end of the tab.

The appliance displays a pop-up box to enter the path to the SSL certificate.

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

---

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

The SSL certificate must be saved and made available in the `/inst/patch/incoming` directory on the appliance.

5 Click **OK**.

The appliance imports the SSL certificate and is used to authenticate the LDAP Server.

Exporting an LDAP configuration

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

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

To export the configuration file

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

   The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server.
3. Click on the **Export** option that is displayed at the end of the tab.

   The appliance displays a pop box to enter the path for exporting the `.xml` file.
4. Enter a name for the `.xml` file.

   You can only save the `.xml` file to the `/inst/patch/incoming` directory on the appliance.
5. Click **OK**.

   The appliance converts the configuration details into an `.xml` file and exports it to the specified location.

Unconfiguring LDAP user authentication

You can use the **Authentication Server Configuration** tab to unconfigure LDAP user authentication. The following procedure describes the steps to unconfigure the LDAP server configuration.

Note: Before you unconfigure the LDAP server, you must revoke the roles from all of the LDAP users that have been added to the appliance. Otherwise the operation fails.

Warning: Unconfiguring LDAP user authentication disables and deletes the current LDAP configuration. The LDAP users are deleted from the appliance, but not from the LDAP server.

To unconfigure an LDAP server

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

   The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server.
3. Click on the **Unconfigure** option that is displayed at the end of the tab.

   The appliance displays the following message:

   ```
   Do you want to unconfigure the LDAP server?
   ```
4. Click **OK** to continue unconfiguring the LDAP server.

   The appliance deletes the LDAP settings.

Enabling the LDAP server configuration

You can use the **Authentication Server Configuration** tab to enable the disabled LDAP configuration. The following procedure describes the options to enable the LDAP configuration for user authentication.

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

To enable the configured server

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

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

   If the LDAP configuration is disabled, the following message is displayed on the **Server Configuration** tab next to the **Enable** option:

   ```
   LDAP authentication is disabled.
   ```
3. Click on the **Enable** option.

   The appliance displays the following message:

   ```
   Are you sure you want to enable the configuration?
   ```
4. Click **OK** to enable the LDAP configuration.

   The appliance enables the LDAP Server.

Disabling the LDAP server configuration

You can use the **Authentication Server Configuration** tab to disable LDAP authentication without unconfiguring it. The following procedure describes the options to disable LDAP user authentication.

To disable the configured server

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

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

   If the LDAP configuration is enabled, the following message is displayed on the **Server Configuration** tab next to the **Disable** option.

   ```
   LDAP authentication is enabled.
   ```

3. Click on the **Disable** option.

   The appliance displays the following message:

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

4. Click **OK** to disable the LDAP server.

   The appliance disables the LDAP server.

Deleting LDAP configuration parameters

When you configure LDAP user authentication, the server configuration parameters that you added or imported are displayed in the **Configuration Parameters** table on the **Authentication Server Configuration** tab. The following procedure describes the steps to delete LDAP configuration parameters.

To delete a configuration parameter

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

   The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Configuration Parameters** table.

3. Select the configuration parameter you want to delete.

4 Click the **Delete** option that is displayed at the top of the **Configuration Parameters** table.

The appliance displays the following message:

```
Are you sure you want to delete the configuration parameter?
```

5 Click **Yes** to proceed.

The deleted configuration parameter is removed from the **Configuration Parameters** table.

Adding LDAP configuration parameters

When you configure LDAP user authentication, the server configuration parameters that you added or imported are displayed in the **Configuration Parameters** table on the **Authentication Server Configuration** tab. The following procedure describes the steps to delete LDAP configuration parameters.

To add a configuration parameter

1 Log on to the NetBackup Appliance Web Console.

2 Click **Settings > Authentication**.

The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Configuration Parameters** table.

3 Click the **Add** option that is displayed at the top of the **Configuration Parameters** table.

The appliance displays a new row in the **Configuration Parameters** table with the **Update** and **Cancel** options.

4 Enter the name of the new configuration parameter in the **Name** field.

5 Enter the value of the configuration parameter in the **Value** field.

6 Click **Update**.

The new configuration parameter is added to the **Configuration Parameters** table.

Adding an LDAP attribute mapping

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

To add an attribute mapping

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

   The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Attribute Mappings** table.
3. Click the **Add** option that is displayed at the top of the **Attribute Mappings** table.

   The appliance displays a new row in the **Attribute Mappings** table with the **Update** and **Cancel** options.
4. Enter the mapping type in the **Map Type** field.
5. Enter the NSS value in the **NSS Value** field.
6. Enter the LDAP value for the attribute in the **LDAP Value** field.
7. Click **Update**.

   The new attribute mapping is added to the **Attribute Mappings** table.

Deleting an LDAP attribute mapping

When you add a new LDAP configuration, its attribute mappings are added or imported and displayed in the **Attribute Mappings** table on the **Authentication Server Configuration** tab. The following procedure describes the steps to delete an attribute mapping from the LDAP server configuration.

To delete an attribute mapping

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

   The appliance displays the **Authentication Server Configuration** tab with the details of the configured LDAP server in the **Attribute Mappings** table.
3. Select the attribute mapping you want to delete in the **Attribute Mappings** table.
4. Click the **Delete** option that is displayed at the top of the **Attribute Mappings** table.

   The appliance displays the following message:

   ```
   Are you sure you want to delete the configuration parameter?
   ```
5. Click **Yes** to proceed.

   The deleted attribute mapping is removed from the **Attribute Mappings** table.

Settings > Authentication > Active Directory

You can use the **Settings > Authentication** page of the NetBackup Appliance Web Console to configure the appliance to use Active Directory (AD) server as a directory source to access user information and authenticate the users and user groups to access the appliance.

Prerequisites

- You must have NetBackup appliance 2.6.0.3 or higher installed to configure AD user authentication.
- Ensure that the AD service is available and is set up with the users and user groups that you want to register with the appliance.
- Ensure that the authorized domain user credentials are used to configure the AD server with the appliance.
- Configure the NetBackup appliance with a DNS server that can forward DNS requests to an AD DNS server. Alternatively, configure the appliance to use the AD DNS server as the name service data source.

Adding an Active Directory server configuration

This topic describes how to add the details of an Active Directory (AD) server and configure it with your appliance. The Active Directory server enables you to access the directory information services for your appliance. The following procedures describe the steps to configure Active Directory user authentication from the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu.

Note: Before you configure new Active Directory authentication, first verify that the DNS of the appliance directs to the Active Directory server or Active Directory DNS server.

To configure an Active Directory server from the NetBackup Appliance Web Console

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Authentication**.

   Three types of authentication server appear.
3. Click **Active Directory** to expand the Active Directory configuration list.

4 Enter the necessary information into the following fields:

Field	Description	Example
Server Name or IP	Enter the Active Directory server name or IP address. The recommended method is to use the Fully Qualified Domain Name (FQDN) for the Active Directory server. Do not use a space as the first character.	**10.200.210.229**
Username	Enter the user name of the AD server Administrator. Do not use a space as the first character.	**admin**
Password	Enter the password of the AD server Administrator. Do not use a space as the first character.	**P@ssw0rd**

5 Click **Configure** to apply the Active Directory authentication parameters to the appliance.

You can check the authentication status when the configuration process is complete.

6 Click **Configure** to complete the Active Directory configuration.

To configure an Active Directory server from the NetBackup Appliance Shell Menu

1 Log on to the NetBackup Appliance Shell Menu.

2 Navigate to the Network view as follows:

```
Main_Menu > Network
```

3 Use th following command to enter the host properties:

```
Hosts add <appliance ip address> <appliance shortname>.<dns
domain> <appliance shortname>
```

4 Navigate to the Active Directory view as follows:

```
Main_Menu > Settings > Security > Authentication > ActiveDirectory
```

5 Use the following command to enter the Active Directory fully qualified host name or IP address, then press **Enter**. You are then prompted to enter the AD server Administrator user name and password to complete this step.

```
Configure <hostname or IP Address>
```

When the `Username` prompt appears, enter the user name of the AD server Administrator, then press **Enter**.

When the `Password` prompt appears, enter a password for the AD server Administrator, then press **Enter**.

The message **Command was successful** should appear.

See "Unconfiguring the Active Directory user authentication " on page 296.

Unconfiguring the Active Directory user authentication

You can stop authenticating the AD user from the appliance. The following procedure describes the steps to unconfigure the Active Directory server configuration.

Note: To unconfigure the Active Directory authentication from the appliance, you must have the Administrator authority on the AD server.

Note: You must remove the roles of all Active Directory users and user groups before the unconfigure process begins.

To unconfigure an Active Directory server

1 Log on to the NetBackup Appliance Web Console.

2 Click **Settings > Authentication**.

The details of the configured Active Directory server are displayed.

3 Enter the **Username** and **Password** of an administrator on Active Directory server.

4 Click **Unconfigure**.

A warning dialog box pops up.

5 Click **Yes** to continue with the unconfigure process.

Click **No** to cancel the unconfigure process.

Settings > Authentication > User Management

You can use the **Settings > Authentication > User Management** page of the NetBackup Appliance Web Console to do the following tasks:

- View all of the users that have been added to the appliance.
- Expand and view all of the users belonging to a single user group.
- Add and delete local users.
- Add and delete LDAP users and user groups.
- Grant Administrator user permissions to local, LDAP, and AD users.
- Grant Administrator user permissions to LDAP and AD user groups.
- Grant NetBackupCLI user permissions to LDAP and AD users.
- Grant NetBackupCLI user permissions to LDAP and AD user groups.
- Revoke Administrator user permissions for local, LDAP, and AD users.
- Revoke Administrator user permissions for LDAP and AD user groups.
- Revoke NetBackupCLI user permissions for LDAP and AD users.
- Revoke NetBackupCLI user permissions for LDAP and AD user groups.
- Sync group members with the Administrator role.

Adding appliance users

You can use the **User Management** tab to add new users to the NetBackup appliance. The following procedure describes how to add new users.

To add new users

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

   The appliance displays the **User Management** tab.
3. Click on the **Add User** option that is displayed at the end of the **User Management** tab.

   The appliance displays the **Add User** pop-up dialog box.
4. Select the type of user from the **User Type** drop-down list. The drop-down list displays the following options depending on your configuration:
   - **Local** - Select this option to add a local user to the appliance database.
   - **LDAP** - Select this option to register a user that is already present on the LDAP server that you have configured with your appliance.

Note: If you do not register (add) a remote (LDAP, etc.) user with the appliance, that user cannot access the appliance.

5 Enter the name of the user in the **User Name** field.

Note: Do not use non-alphanumeric characters (special characters: !, $, #, %, etc.) for the **User Name** field.

6 If you selected a **Local** user type from the **User Type** drop-down list, enter a password for the new user in the **Password** field. Valid passwords must include the following:

- Eight or more characters
- At least one lowercase letter
- At least one number (0-9)

Uppercase letters and special characters can be included, but they are not required.

The following describes password restrictions:

- Dictionary words are considered weak passwords and are not accepted.
- The last seven passwords cannot be reused, and the new password cannot be similar to previous passwords.

You or the new user can change their password at a later time on the **Settings > Password > Password Management** page.

7 Reenter the password in the **Confirm Password** field.

8 Click **Save**.

The appliance adds the new user and displays the following message:

```
User added successfully.
```

9 Click **OK** to continue.

The new user is added to the list of users on the **User Management** tab.

Deleting appliance users

As a matter of best practice, you should delete a registered user or user group from the NetBackup appliance before deleting it from the LDAP server or the Active Directory (AD) server. If a user is removed from the remote directory first (and not

removed from the appliance), the user is listed as an authorized user but cannot log on.

You can use the **User Management** tab to delete users from the NetBackup appliance. The following procedure describes how to delete existing users.

To delete existing users

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

   The appliance displays the **User Management** tab.
3. Select the user that you want to delete.
4. Click on the **Delete User** option that is displayed at the end of the **User Management** tab.

   The appliance displays the following message:

   ```
   User Deleted Successfully
   ```

5. Click **OK** to continue.

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

Adding appliance user groups

You can use the **User Management** tab to add new user groups to the NetBackup appliance from a registered directory service, such as LDAP. The following procedure describes how to add new user groups.

To add user group

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

   The appliance displays the **User Management** tab.
3. Click on the **Add Group** option that is displayed at the end of the **User Management** tab.

   The appliance displays the **Add Group** pop-up dialog box.
4. Enter the name of the user group in the **Group Name** field.

Note: If you do not register (add) a remote (LDAP, etc.) user group with the appliance, the users belonging to that user group cannot access the appliance.

---

5 Click **Save**.

The appliance adds the new user group and displays the following message:

```
Group Added Successfully
```

6 Click **OK** to continue.

The user group is added to the list of users and user groups on the **User Management** tab.

Deleting appliance user groups

As a matter of best practice, you should delete a registered user or user group from the NetBackup appliance before deleting it from the LDAP server or the Active Directory (AD). If a user is removed from the remote directory first (and not removed from appliance), the user is listed as an authorized user but cannot log on.

You can use the **User Management** tab to delete user groups from the NetBackup appliance. The following procedure describes how to delete existing user groups.

To delete user groups:

1 Log on to the NetBackup Appliance Web Console.

2 Click the **Settings > Authentication > User Management** tab.

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

3 Select the user group that you want to delete.

4 Click on the **Delete Group** option that is displayed at the end of the **User Management** tab.

5 Click **OK** to continue.

The appliance displays the following message:

```
Group Deleted Successfully
```

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

Granting roles to users and user groups

You can use the **User Management** tab to grant roles to appliance users and user groups that grant them different types of permissions to access the appliance. The following procedure describes how to grant roles to existing users and user groups.

To grant administrative roles to users and user groups

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

   The appliance displays the **User Management** tab.
3. Select a user or user group that has **NoRole** displayed in the **Role** column.
4. Click on the **Grant Permission** option that is displayed at the end of the **User Management** tab.

   Depending on your configuration, the appliance displays the **Grant Permissions** pop-up dialog box:

   - Select the **Administrator** option to grant the Administrator user role to the selected user or user group.
   - Select the **NetBackupCLI** option to grant the NetBackupCLI user role to the selected user or user group.

   Note: You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from the NetBackup Appliance Shell Menu.
5. Click **OK** to continue.

   The term **Administrator** or **NetBackupCLI** is displayed in the **Role** column for the selected user.

Revoking roles from users and user groups

You can use the **User Management** tab to revoke roles from appliance users and user groups to limit their permissions to access the appliance. The following procedure describes how to revoke roles from existing users and user groups.

To revoke roles

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

   The appliance displays the **User Management** tab.
3. Select a user or user group that has the **Administrator** or **NetBackupCLI** role displayed in the **Role** column.

4 Click on the **Revoke Permission** option that is displayed at the end of the **User Management** tab.

5 Click **OK** to continue.

The appliance displays the following message:

```
User Un-authorized Successfully
```

The term **NoRole** is displayed in the **Role** column for the selected user or user group.

Synchronizing the user groups

You can use the **User Management** tab to synchronize the user group members. The following procedure describes how to synchronize the user groups between the appliance and the servers for LDAP and AD.

You can also schedule a sync start time by using the `Settings > Security > Authorization > SyncGroupMembers` command in the NetBackup Appliance Shell Menu. For more information, refer to the *NetBackup Appliance Command Reference Guide*.

To sync the user groups

1 Log on to the NetBackup Appliance Web Console.

2 Click the **Settings > Authentication > User Management** tab.

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

3 Select a user group from the list.

4 Click on the **Sync Group Members** option that is displayed on the right top corner of the **User Management** tab.

5 Click **Sync** to sync user group members immediately.

Settings > Password Management

After the initial configuration, you can change the appliance user password from the **Settings** > **Password** > **Password Management** page.

Note: For maximum security, Veritas recommends that you set a regular schedule for password changes and keep a record of all passwords in a secure location.

When the password is changed here, it is also updated for use with the command-line interface. If you change this password from the command-line interface, the new password is also used to log on to the appliance user interface.

Table 5-19 describes the data entry fields on the **Password Management** page.

Table 5-19 Data entry fields for administrator password change

Field	Description
User Name	Enter your current user name.
Old Password	Enter the current password. If the current password is the factory default password, enter **`P@ssw0rd`**.
New Password	Enter the new password. Valid passwords must include the following: ■ Eight or more characters ■ At least one lowercase letter ■ At least one number (0-9) Uppercase letters and special characters can be included, but they are not required. The following describes password restrictions: ■ Dictionary words are considered weak passwords and are not accepted. ■ The last seven passwords cannot be reused, and the new password cannot be similar to previous passwords.
Confirm New Password	Re-enter the new password for confirmation.
Reset Password	Click this item to commit the password change.
Clear Fields	Click this item to remove the data from all fields and start over.

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

See "About modifying the appliance settings" on page 231.

Chapter 6

Troubleshooting

This chapter includes the following topics:

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 shell menu. The `LOGROOT/>` prompt appears.
2. To display the available log directories on your appliance, type `ls` at the `LOGROOT/>` prompt.
3. To see the available log files in any of the log directories, use the `cd` command to change directories to the log directory of your choice. The prompt changes to show the directory that you are in. For example, if you changed directories to the `OS` directory, the prompt appears as `LOGROOT/OS/>`. From that prompt you can use the `ls` command to display the available log files in the `OS` log directory.
4. To view the files, use the `less <FILE>` or `tail <FILE>` command. Files are marked with `<FILE>` and directories with `<DIR>`.

See "Where to find NetBackup appliance log files using the Browse command" on page 305.

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

1. You can view the 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. Log in to the log browser website with the `Main > Support > LogBrowser Start` command. Use the log browser desktop to map, share, and copy the logs.

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

- Upload the log files to Veritas Technical Support.
- Set log levels.

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

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

Where to find NetBackup appliance log files using the Browse command

Table 6-1 provides the location of the logs and the log directories that are accessible with the `Support > Logs > Browse` command.

Table 6-1 NetBackup appliance log file locations

Appliance log	Log file location
Configuration log	`<DIR> APPLIANCE` `config_nb_factory.log`

Table 6-1 NetBackup appliance log file locations *(continued)*

Appliance log	Log file location
Selftest report	<DIR> APPLIANCE selftest_report
Host change log	<DIR> APPLIANCE hostchange.log
NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the openv directory	<DIR> NBU ■ <DIR> netbackup ■ <DIR> openv ■ <DIR> volmgr
Operating system (OS) installation log	<DIR> OS boot.log messages
Operating system (OS) audit log	<DIR> APPLIANCE audit.log
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	/log/data-collect/sosreport*.tar.xz You can download the DataCollect.zip file by logging into the log browser website with the Main > Support > LogBrowser Start command. Use the log browser desktop to map, share, and copy the logs.

About disaster recovery

Numerous situations can cause fatal conditions and result in the need for disaster recovery. In a disaster recovery situation, it is critical to determine the cause of the disaster and recover as much data from the appliance as possible. Therefore, before you attempt to recover your appliance, contact Technical Support.

Note: A local drive backup and restore on the appliance is not supported and may leave the system in an inconsistent state. You must protect appliance data by using the backup policies and use the recommended disaster recovery procedures for restore.

The environment that you have configured around your appliance plays an important role on the level of recovery you can achieve. An environment that consists of a standalone primary (primary server) appliance offers the least number of recovery solutions. A failure that is severe enough to bring your appliance down, may mean that it is impossible to recover the data on the system. Veritas support engineers work with you to determine whether they can recover your appliance. If your appliance is not recoverable, then Support may suggest that you rebuild your appliance. If that option is not feasible, then you may need to replace your appliance completely.

However, an appliance that is configured with one or more secondary appliances, or configured with a tape storage unit, there is a much better chance that its data can be recovered.

You can also configure Auto Image Replication between appliances.

See “About Auto Image Replication between appliances” on page 219.

Veritas recommends that you review the following sections from within the NetBackup documentation before you operate the appliance:

- *NetBackup Administration Guide, Volume I*
  - In Section 5, “Configuring Backups", review the following topics:
    - "Creating backup policies"
    - "Protecting the NetBackup Catalog"
    - "Strategies that ensure successful NetBackup catalog backups"
  - Review the topics within Section 3, “Configuring Storage".
- *NetBackup Troubleshooting Guide*
  Review Chapter 8, "Disaster Recovery" for help with understanding disaster recovery fundamentals.
  The Troubleshooting Guide is located at the following location:
  http://www.veritas.com/docs/DOC5332

Recovering a NetBackup appliance primary server using NetBackup catalog restore

This section details how to recover a NetBackup appliance primary server using the NetBackup catalog restore function.

The following information is mandatory to complete this task:

- Copy of the NetBackup catalog from the affected primary server.

  Note: Make sure to set the passphrase for the NetBackup catalog backup policy. The passphrase is needed for a catalog recovery.

- Storage configuration from the affected primary server.
- Host name of the affected primary server.
- Network configuration, if a re-image is needed.
- Time zone of the affected primary server.

Note: This procedure requires that you have a copy of your NetBackup catalog stored on a separate server or computer. You need the catalog backup to recover the affected primary server.

To recover an appliance primary server using NetBackup catalog restore

1. Perform one of the following actions depending on the state of your primary server:
   - If you can log on to the primary server, perform a factory reset and retain the network settings. You can elect to delete all images and reset the storage configuration.
   - If you cannot log on to the primary server, perform a re-image of the server using the same network settings as before the disaster event.
2. Once you have completed the factory reset or re-image operation, log on to the NetBackup Appliance Shell Menu on the primary server and create an NetBackup CLI user.

   ```
   Main_Menu > Manage > NetBackupCLI > Create
   ```

3. Copy the NetBackup catalog files that were stored off-site onto the primary server.
4. Log out of the NetBackup Appliance Shell Menu, then log on as the NetBackup CLI user you created earlier.
5. Run `bp.kill_all`.
6. Run `nbhostidentity -import -infile` with the package file of the `.drpkg`
7. Run `bp.start_all`, then verify that the token, certifications, and security settings have been restored.

8 Configure the role on the factory state appliance as a primary server.

Note: Make sure to keep the same host name, time zone, and storage settings of the primary as before the disaster.

9 Run `bpsetconfig` to add the line: `MEDIA_SERVER=<media_server_name>` and register media servers on the new primary server. Use `Ctrl + D` to exit and save this entry.

10 Run `nbemmcmd` to add the media server's record to the EEM database manually:

```
nbemmcmd -addhost -machinename <media_server_name> -machinetype
media -primarieserver <primary_server_name> -operatingsystem linux
-netbackupversion <NetBackup_version>
```

11 Restart the NetBackup services on the media server.

Note: To ensure proper communication between the primary and the media server, you must perform this step before you create the MSDP storage information on the media server as described in the following step.

12 Create the media server AdvancedDisk and MSDP storage information using the following commands:

- AdvanvcedDisk

```
nbdevconfig -creatests -storage_server <media_server_name>
-stype AdvancedDisk -media_server <media_server_name> -st 5
nbdevconfig -createdp -dp dp_adv_<media_server_name> -stype
AdvancedDisk -storage_servers <media_server_name> -dvlist
dvlist.txt
bpstuadd -label stu_adv_<media_server_name> -dp
dp_adv_<media_server_name> -cj 20 -odo 1 -okrt 0 -nodevhost
-M <primary_server_name>
```

- MSDP

```
nbdevconfig -creatests -storage_server <media_server_name>
-stype PureDisk -media_server <media_server_name> -st 9
nbdevconfig -createdp -dp dp_disk_<media_server_name> -stype
PureDisk -storage_servers <media_server_name> -dvlist
dvlist.txt
```

```
bpstuadd -label stu_disk_<media_server_name> -dp
dp_disk_<media_server_name> -cj 20 -odo 1 -okrt 0 -nodevhost
-M <primary_server_name>
```

13 Restore the NetBackup catalog by performing one of the following actions:

- Run the `bprecover -wizard` command.
- Use the NetBackup Catalog Recovery Wizard in the NetBackup Administrator's Console.

14 During the role configuration, the nbasecadmin user is recreated and its user ID may change which prevents that user from logging in to the NetBackup Web Console. Before attempting to log in to the web console as nbasecadmin, open an SSH session as a NetBackupCLI user and run the following command:

```
bpnbaz -AddRBACPrincipal -User unixpwd:<appliancename>:nbasecadmin
```

If the following message appears, the nbasecadmin user ID has not changed and you can log in to the web console:

```
The user or user group provided already has Administrator
privileges.
```

If the above message does not appear, there are now two user IDs associated with the nbasecadmin username. To resolve this issue, perform the following tasks in the order as they appear:

- Log in to the NetBackup Web Console as nbasecadmin.
- Go to **RBAC > Role > Adminstrator**.
- Remove the nbasecadmin user rows, which disables the nbasecadmin user from logging in.
- Run the above `bpnbaz` command again to add nbasecadmin as an RBAC principal user. This step ensures that there is only one record for nbasecadmin in the NetBackup user database.

No other OS users are created or recreated during the role configuration. The catalog recovery may show users with the Administrator, or other roles that were associated with OS users that no longer exist. Those users should be removed from the NetBackup Web Console, then recreated on the appliance and assigned their appropriate roles in the NetBackup Web Console.

15 Run `bp.kill_all` and `bp.restart_all` to finish recovering the primary server.

16 Synchronize the MSDP storage server password as follows:

- For software versions 3.3.0.1 and later, log in to the appliance shell menu on the primary server and run the following command:

```
Main_Menu > Appliance > ShowDeDupPassword
```

- For software versions 3.1 through 3.2, log in to the appliance shell menu on the primary server and run the following command:

  ```
  Main_Menu > Appliance > ShowDeDupPassword
  ```

  Log in to the appliance primary server as a NetBackup CLI user and run the following command:

  ```
  tpconfig -update -storage_server <primary host name> -stype
  PureDisk -sts_user_id root -media_server <primary hostname>
  ```

  , then enter the dedupe password from the previous command output.

Gathering device logs on a NetBackup appliance

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

The DataCollect command collects the following logs:

- Release information
- Disk performance logs
- Command output logs
- iSCSI logs
- 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 one of the following commands to gather device logs:
   - `dataCollect`
   - `dataCollect advanced`
     Use this option to include detailed logs for a higher level of debugging.

   For appliance software versions 5.0 and later, the appliance generates the device log in the `/log/data-collect/sosreport*.tar.xz` file.
3. You can download the `DataCollect.zip` file by logging into the log browser website with the `Main > Support > LogBrowser Start` command. Use the log browser desktop to map, share, and copy the logs.
4. You can send the `DataCollect.zip` file to the Veritas Support team to resolve your issues.

Chapter 7

Deduplication pool catalog backup and recovery

This chapter includes the following topics:

Deduplication pool catalog backup policy

Creating a backup of the deduplication pool (MSDP) catalog is a very important step in protecting your data in the event of a disaster.

Policy creation depends on how the appliance has been configured, as follows:

- Standard NetBackup appliance configuration
  This configuration process automatically creates a policy to back up the MSDP catalog. In rare cases where the policy cannot be created, manual intervention may be necessary.
  See "Manually configuring the deduplication pool catalog backup policy" on page 317.
  For more details about catalog backup policies, see the Veritas *NetBackup Deduplication Guide* and refer to Chapter 5, "Configuring deduplication".

Caution: Veritas recommends that you contact your Veritas Support representative before you recover the deduplication pool catalog. The Support representative can help you determine if you need to recover the catalog or if other solutions are available.

The following topics provide more information about the deduplication pool catalog backup policy and the recovery process:

See "Automatic configuration of the deduplication pool catalog backup policy" on page 314.

See "Manually configuring the deduplication pool catalog backup policy" on page 317.

See "Manually updating the deduplication pool catalog backup policy" on page 318.

See "Recovering the deduplication pool catalog" on page 319.

Automatic configuration of the deduplication pool catalog backup policy

A policy is automatically created to protect the deduplication storage pool. The deduplication pool catalog can then be recovered in the event of a disaster. The deduplication pool catalog backup policy is automatically created in the following scenarios:

- When a deduplication storage pool is created during the initial configuration of the appliance.
- When `Manage>Storage>Resize MSDP` is run when a deduplication storage pool did not exist.
- When you upgrade an appliance that had a deduplication storage pool already configured.

The deduplication pool catalog backup policy can be viewed once it is created by one of the above scenarios.

Veritas recommends that you activate this policy to protect the deduplication pool catalog. Protecting the deduplication pool catalog can prove beneficial in a disaster recovery situation.

If a policy to backup the deduplication storage pool catalog already exists, the configuration of this policy is updated.

When configuring the deduplication storage pool backup policy, take the following into consideration:

- The residence must be set and should not be local to the appliance.

- You can adjust properties such as schedules, frequency, and backup window.
- Do not modify the policy type, client name, or backup selection in the policy properties.
- The policy must be activated manually.

The name of this policy is `SYMC_NBA_Dedupe_Catalog_<appliance-short-name>` where `<appliance-short-name>` is the short name you have given to your appliance.

Note: If MSDP storage is not configured during initial configuration, the policy is not created.

The creation of the policy is automatic so be sure to check the output messages to make sure that the policy has been successfully created.

Email notifications are sent to the email addresses that have been configured to receive software alerts. These email addresses are configured through the NetBackup Appliance Web Console or by running the following command: `Settings>Alerts>Email Software Add`.

Table 7-1 Deduplication storage pool catalog backup policy success messages

Message	Definition
A backup policy, <policy-name>, has been configured to protect the deduplication pool catalog. Review the policy configuration and make changes to its schedules, backup window, and residence as required. Make sure to activate the policy to protect the catalog. For more information, refer to the *NetBackup Appliance Administrator's Guide*.	This message is displayed in the following scenarios: ■ The deduplication pool catalog backup policy did not exist and was created successfully. ■ The deduplication pool catalog backup policy has existed and was updated successfully.
An existing backup policy, <policy-name>, has been found that conflicts with the required deduplication pool backup policy. The policy type has been updated to 'Standard' to protect the deduplication pool catalog. The policy type was set to <previous-policy-type> before this update.	The policy type of the pre-existing deduplication pool policy has been updated to standard. The policy type was set to <previous policy type>. Review the policy configuration and make sure that the previous backup configuration is not affected.

Table 7-2 Deduplication storage pool catalog backup policy failure messages

Message	Definition
Failed to create a deduplication pool catalog backup policy. The policy is required to protect the deduplication pool catalog and recover it in case of disaster. Refer to the *NetBackup Appliance Administrator's Guide* for how to configure the policy manually.	The deduplication pool catalog backup policy did not exist and the policy creation has failed. To protect the deduplication pool catalog, you need to configure the backup policy manually. See "Manually configuring the deduplication pool catalog backup policy" on page 317.
Failed to update deduplication pool catalog backup policy, '<policy-name>', type to 'Standard.' An existing backup policy has been found that conflicts with the required deduplication pool catalog backup policy. Make sure to update the policy type to 'Standard' manually to protect the deduplication pool catalog. Refer to the NetBackup Appliance Administrator's Guide for how to configure the policy manually.	This message is displayed in the following scenarios: ■ The policy already exists and the policy type is not set to Standard. ■ The operation has failed to update the policy type to Standard. To protect the deduplication pool catalog, you need to change the policy type manually. See "Manually updating the deduplication pool catalog backup policy" on page 318.
Failed to update the client and the backup selection properties of the deduplication pool catalog backup policy <policy-name>. Refer to the *NetBackup Appliance Administrator's Guide* for how to configure the policy manually.	The deduplication pool catalog backup policy pre-exists but the operation has failed to update the policy properties, which include Client and Backup Selection. To protect the deduplication pool catalog, you need to update the Client and Backup selection manually. See "Manually updating the deduplication pool catalog backup policy" on page 318.

Caution: Veritas recommends that you contact your Veritas Support representative before you recover the deduplication pool catalog. The Support representative can help you determine if you need to recover the catalog or if other solutions are available.

See "Manually configuring the deduplication pool catalog backup policy" on page 317.

See "Manually updating the deduplication pool catalog backup policy" on page 318.

See "Recovering the deduplication pool catalog" on page 319.

Manually configuring the deduplication pool catalog backup policy

The following procedure is provided in case the deduplication pool catalog backup policy is not automatically created. Creating a backup policy to protect the deduplication pool catalog is critical in protecting your data in the event of a disaster.

Manually configuring the deduplication pool catalog backup policy

1. Log on to the Appliance with a NetBackupCLI user account.

   See "Creating NetBackup administrator user accounts" on page 215.

2. Enter the following command to create the deduplication pool catalog backup policy:

   ```
   # drcontrol --new_policy --policy <policy-name> --hardware
   <appliance model> --OS 'NetBackup-Appliance' --log_file ~/<log
   file name>
   ```

   - Replace <*policy-name*> with: `SYMC_NBA_Dedupe_Catalog_<appliance-short-name>` where `<appliance-short-name>` is the short name you have given to your appliance.
   - Replace `<appliance model>` with the model of the Appliance. For example, 5240 or 5340.
   - Replace `<log file name>` with the name of the log file the `drcontrol` tool creates.

     Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

See "Automatic configuration of the deduplication pool catalog backup policy" on page 314.

See "Manually updating the deduplication pool catalog backup policy" on page 318.

See "Recovering the deduplication pool catalog" on page 319.

Manually updating the deduplication pool catalog backup policy

The following procedure is provided in case the deduplication pool catalog backup policy is not automatically updated. Creating a backup policy to protect the deduplication pool catalog is critical in protecting your data in the event of a disaster.

Manually updating the deduplication pool catalog backup policy

1. Log on to the Appliance with a NetBackupCLI user account.

   See "Creating NetBackup administrator user accounts" on page 215.

2. Update the policy type. Enter the following command to update the policy type to Standard:

   ```
   # bpplinfo <policy-name> -modify -pt Standard
   ```

   Replace *<policy-name>* with `SYMC_NBA_Dedupe_Catalog_<appliance-short-name>` where *<appliance-short-name>* is the short name you have given to your appliance.

3. Identify the client name:

   - Determine if the appliance is added as a client by entering the following command:

     ```
     # bpplclients <policy-name> -l
     ```

   - If the client has not been added, run the following command to identify the client name:

     ```
     # bpgetconfig CLIENT_NAME | cut -f3 -d' '
     ```

4. Update the client and the backup selection by entering the following command:

   ```
   # drcontrol --update_policy --policy <policy name> --client
   <client name> --hardware <appliance model> --OS
   'NetBackup-Appliance' --log_file ~/<log file name>
   ```

   - Replace *<client name>* with the name of the client that is identified in the previous step.
   - Replace *<appliance model>* with the model of the Appliance. For example, 5240.
   - Replace *<log file name>* with the name of the log file the `drcontrol` tool creates.

Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

See "Automatic configuration of the deduplication pool catalog backup policy" on page 314.

See "Manually configuring the deduplication pool catalog backup policy" on page 317.

See "Recovering the deduplication pool catalog" on page 319.

Recovering the deduplication pool catalog

This section outlines how to recover the deduplication pool catalog in the event of a disaster.

Caution: Veritas recommends that you contact your Veritas Support representative before you recover the deduplication pool catalog. The Support representative can help you determine if you need to recover the catalog or if other solutions are available.

Recovering the deduplication pool catalog

1. Log on to the Appliance with a NetBackupCLI user account

   See "Creating NetBackup administrator user accounts" on page 215.

2. Enter the following command to identify the space requirements:

   ```
   # drcontrol --print_space_required --policy <policy-name>
   --log_file ~/<log file name>
   ```

   Replace *<log file name>* with the name of the log file the`drcontrol` tool creates.

   Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

3. Log on to the Appliance as an Appliance Administrator.
4. Run hardware monitoring commands to make sure that there are no errors.

5 Run hardware self-test to make sure that all hardware components are in place and functioning correctly.

6 Run `Manage > Storage > Show` to make sure that all the storage components are in place and functional. Also verify that the deduplication pool catalog partition size meets the space requirements.

7 If the size requirement is not met, run `Manage > Storage Resize MSDPCatalog` to expand the partition.

8 Log on to the Appliance with a NetBackupCLI user account.

9 Perform the catalog recovery using `drcontrol` and other tools as documented in the MSDP catalog recovery section of the *NetBackup Deduplication Guide*.

Note: If the `drcontrol` tool is run without the log file option the tool creates a file that is not accessible to the NetBackupCLI user. Make sure to choose a directory accessible by the NetBackupCLI user, such as the home directory of the NetBackupCLI user.

See "Automatic configuration of the deduplication pool catalog backup policy" on page 314.

See "Manually configuring the deduplication pool catalog backup policy" on page 317.

See "Manually updating the deduplication pool catalog backup policy" on page 318.

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W