Veritas NetBackup™ 52xx Appliance Initial Configuration Guide

Release 3.1

Document Revision 1

VERITAS™

Veritas NetBackup™ Appliance Initial Configuration Guide

Release 3.1, Document Revision 1

Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

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

This product may contain third party software for which Veritas is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third party legal notices document accompanying this Veritas product or available at:

https://www.veritas.com/about/legal/license-agreements

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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://sort.veritas.com/documents

Documentation feedback

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

APPL.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1 Preparing for initial configuration 6

About appliance configuration guidelines 6
About appliance system configuration sequence 10
About NetBackup 52xx appliance roles 11
Command limitations on appliances that are not configured 12
About IPv4-IPv6-based network support 12
Overview of the initial configuration pages in the NetBackup Appliance Web Console 14
About the NetBackup 52xx Appliance initial configuration checklist 25
NetBackup appliance initial configuration checklist 26
About configuring the maximum transmission unit size 30

Chapter 2 Initial configuration procedures 32

Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console 32
Performing the initial configuration on a 52xx master server appliance from the NetBackup Appliance Shell Menu 49
Configuring a master server to communicate with an appliance media server 58
Performing the initial configuration on a 52xx media server appliance from the NetBackup Appliance Shell Menu 60
Performing the initial configuration on a NetBackup 5240 CloudCatalyst Appliance 72
Deploying certificates for a credentials broker when the master server is an appliance 85

Chapter 3 Post configuration procedures 87

About NIC1 (eth0) port usage on NetBackup appliances 87
Downloading NetBackup client packages to a client from a NetBackup appliance 88
Downloading the NetBackup Administration Console to a Windows computer from a NetBackup appliance 91

Installing NetBackup client software through CIFS and NFS shares 92

Index 96

Chapter 1

Preparing for initial configuration

This chapter includes the following topics:

- About appliance configuration guidelines
- About appliance system configuration sequence
- About NetBackup 52xx appliance roles
- About IPv4-IPv6-based network support
- Overview of the initial configuration pages in the NetBackup Appliance Web Console
- About the NetBackup 52xx Appliance initial configuration checklist
- NetBackup appliance initial configuration checklist
- About configuring the maximum transmission unit size

About appliance configuration guidelines

Use the following configuration guidelines when you deploy new appliances:

Table 1-1 Appliance configuration guidelines

Parameter	Description
Connectivity during initial configuration	When you perform the appliance initial configuration, Veritas recommends that you take precautions to avoid loss of connectivity. Any loss of connectivity during initial configuration results in failure. The computer that you use to configure the appliance should be set up to avoid the following events: ■ Conditions that cause the computer to go to sleep ■ Conditions that cause the computer to shut down or to lose power ■ Conditions that cause the computer to lose its network connection
NetBackup Appliance Web Console access	Starting with NetBackup appliance software version 2.6.0.4, the NetBackup Appliance Web Console is accessible only over HTTPS on the default port 443. Port 80 over HTTP has been disabled. The exception to this change is in NetBackup appliance software version 2.6.1. With that version, the NetBackup Appliance Web Console is accessible only over HTTPS on the default port 80.
Required names and addresses	Before the configuration, gather the following information: ■ Network IP addresses, netmask, and gateway IP addresses for the appliance ■ Network names for all appliances ■ DNS or host information **Note:** If DNS is used, make sure that the network names of all appliances and the master server are DNS resolvable (FQDN and short name). If DNS is not used, make sure that you enter the proper host entries for the appliance during the initial configuration. ■ Password for appliance access The default password for appliance access is **P@ssw0rd**. ■ Names for NetBackup storage units The **Storage Name** fields appear when you configure the appliance role. You can change the default names or leave them. The default values that appear in the **NetBackup Administration Console** for the storage units and disk pools are as follows: ■ For the AdvancedDisk: Default storage unit name: **stu_adv_<hostname>** Default disk pool name: **dp_adv_<hostname>** ■ For the NetBackup Deduplication: Default storage unit name: **stu_disk_<hostname>** Default disk pool name: **dp_disk_<hostname>** **Note:** The short host name of the appliance appears as the default storage unit name and the disk pool name.

Table 1-1 Appliance configuration guidelines *(continued)*

Parameter	Description
Default user name and password	New NetBackup appliances are shipped with the following default log-in credentials: ■ User name: **admin** ■ Password: **P@ssw0rd** **Note:** When you perform the initial configuration, you are not required to change the default password. However, to increase the security of your environment you should change the password periodically. Make sure to keep a record of the current password in a secure location.
Default Maintenance user password	The appliance comes configured with a known default password for the `Maintenance` user account. You should change this password either before or immediately after the initial configuration to prevent unauthorized access to the appliance maintenance mode. Note that you must provide the `Maintenance` user password to Veritas Technical Support in the event that the appliance requires troubleshooting services. Each initial configuration procedure includes a step that describes how to change the default `Maintenance` user password.
Firewall port usage	Make sure that the following ports are open on any firewall that exists between a master server and a media server: ■ 13724 (`vnetd`) ■ 13720 (`bprd`) ■ 1556 (`PBX`) ■ 7578 (specific for the 5220 appliance when the TCP protocol is used) For more information about firewall ports for NetBackup and the NetBackup appliance, see the following tech note on the Veritas Support website: https://www.veritas.com/support/en_US/article.TECH178855

Table 1-1 Appliance configuration guidelines *(continued)*

Parameter	Description
Media server role	Before you configure a NetBackup appliance as a media server, the master server that you plan to use with it must be updated with the new appliance media server name. Whether the master server is a NetBackup appliance or a traditional NetBackup master server, the name of the new appliance media server must be added to the **Additional Servers** list on the master server. Adding the new appliance media server name to the master server before the new appliance is configured provides the following benefits when performing the initial configuration on the new appliance: ■ Provides the appropriate network communication that allows the media server to become part of the NetBackup domain. ■ Allows the media server to create the storage server and the disk pool entries. To configure this appliance as a media server, you have to deploy the security certificates on the appliance to trust the master server. A CA certificate and a host ID-based certificate must be deployed from the master server that you plan to use with this appliance. The CA certificate is automatically downloaded and deployed if you select to trust the master server. To deploy the host ID-based certificate: ■ If the security level of the master server is **Very High**, you need to manually enter an authorization token to deploy the host ID-based certificate to the media server. ■ If the security level of the master server is **High** or **Medium**, the authentication token is not required. The host ID-based certificate is automatically deployed to the media server. **Note:** Regardless of the master security level, if the appliance is ever factory reset or re-imaged, a reissue token is required when the appliance is reconfigured. If the security certificates have been deployed on the appliance media server, you are not requested to deploy them again during the role configuration. For more information about security certificates, refer to the chapter **Security certificates in NetBackup** in the *NetBackup Security and Encryption Guide*. See "Configuring a master server to communicate with an appliance media server" on page 58.
Disk storage option licenses	The appliance comes with a not for resale (NFR) license key that expires after a specific period of time. The appliance does not provide a warning message that this license key is about to expire. Therefore, Veritas recommends that you change this key to a permanent key after you install and configure the appliance. See the *NetBackup Appliance Administrator's Guide* for information and instructions on how to view and change a license key. Replace the NFR keys with permanent keys before they expire.

Table 1-1 Appliance configuration guidelines *(continued)*

Parameter	Description
NetBackup version compatibility	NetBackup appliance release 3.1 includes NetBackup version 8.1. If you plan to configure this appliance as a media server, use the following guidelines for the associated master server and clients: ■ Appliance master server The appliance master server that you plan to use with this appliance media server must use appliance software version 3.1 or later. If the appliance master server currently uses appliance software version 3.0 or earlier, it must be upgraded to version 3.1 before you configure this appliance. ■ Traditional NetBackup master server To use an appliance media server with a traditional NetBackup master server, the master server must use NetBackup version 8.1 or later. If the NetBackup master server currently uses NetBackup version 8.0 or earlier, it must first be upgraded to version 8.1 before you configure this appliance. ■ Clients and client add-ons NetBackup clients must use the same or an earlier software version as the appliance. Clients cannot run at a later version than the appliance. For example, a client with NetBackup version 2.7.1 can only be used with an appliance server with version 2.7.1 or later. Client add-ons must also be the same version as the client version.

See "About appliance system configuration sequence" on page 10.

About appliance system configuration sequence

If your system includes more than one appliance or a storage expansion unit, configuration must be done in a specific order.

The following describes the proper sequence for appliance configuration, based on the system components.

Table 1-2 Appliance configuration order

System	Configuration order
Single appliance system (standalone)	Configure the appliance as a master server. See "Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console " on page 32. See "Performing the initial configuration on a 52xx master server appliance from the NetBackup Appliance Shell Menu" on page 49.

Table 1-2 Appliance configuration order *(continued)*

System	Configuration order
Multiple appliance system (master server and media servers)	■ Configure the first appliance as a master server. See "Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console " on page 32. See "Performing the initial configuration on a 52xx master server appliance from the NetBackup Appliance Shell Menu" on page 49. ■ Add the host names of the new media servers to the configured master server. See "Configuring a master server to communicate with an appliance media server" on page 58. ■ After the master server has been updated with the new media server host names, configure the remaining appliances as media servers. See "Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console " on page 32. See "Performing the initial configuration on a 52xx media server appliance from the NetBackup Appliance Shell Menu" on page 60.
Systems that include a storage expansion unit	After all appliances have been configured, add the storage expansion unit to the server on which it is physically connected.

See "About appliance configuration guidelines" on page 6.

About NetBackup 52xx appliance roles

When you configure an appliance for the first time, you must select a role for it. The role refers to the server type as follows:

Table 1-3 Appliance role and mode descriptions

Role	Description
Master	Select this role to configure the appliance as a master server.

Table 1-3 Appliance role and mode descriptions *(continued)*

Role	Description
Media	Select this role to configure the appliance as a media server. You must also identify the master server that you plan to use with this appliance. The master server can be either a traditional NetBackup master server or a NetBackup appliance master server. When you select the media server role, you must also define the storage names for the following disk volumes: ■ **Deduplication volume** ■ **AdvancedDisk volume**

See "About the NetBackup 52xx Appliance initial configuration checklist" on page 25.

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 IPv4-IPv6-based network support

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

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

Review the following considerations for IPv6 addresses:

- NetBackup appliance does not support a pure IPv6 network. An IPv4 address must be configured for the appliance, otherwise the initial configuration (which

requires the command `hostname set`) is not successful. For this command to work, at least one IPv4 address is required.

For example, suppose that you want to set the `hostname` of a specific host to v46. To do that, first make sure that the specific host has at least one IPv4 address and then run the following command:

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

- Only global addresses can be used, not addresses with link-local or node-local scope. Global-scope and unique-local addresses are both treated as global addresses by the host.

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

- You cannot use both an IPv4 and an IPv6 address in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1`. You should use `Configure 9ffe::46 64 9ffe::49 eth1`.

- Embedding the IPv4 address within an IPv6 address is not supported. For example, you cannot use an address like 9ffe::10.23.1.5.

- You can add an appliance media server to the master server if the IPv6 address and the host name of the appliance media server are available.

  For example, to add an appliance media server to the master server, enter the IPv6 address of the appliance media server as follows:

  Example:

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

  ```
  Main > 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.

- Network File System (NFS) or Common Internet File System (CIFS) protocols are supported over an IPv4 network on appliance. NFS or CIFS are not supported on IPv6 networks.

- The NetBackup client can now communicate with the media server appliance over IPv6.

- The `Main_Menu > Network > Hosts` command supports multiple IPv6 addresses to be assigned to the same host name having one network interface card (NIC). However, only one IPv4 address can be assigned to a specific host name having one NIC using this command.

- You can add an IPv6 address of a network interface without specifying a gateway address.

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

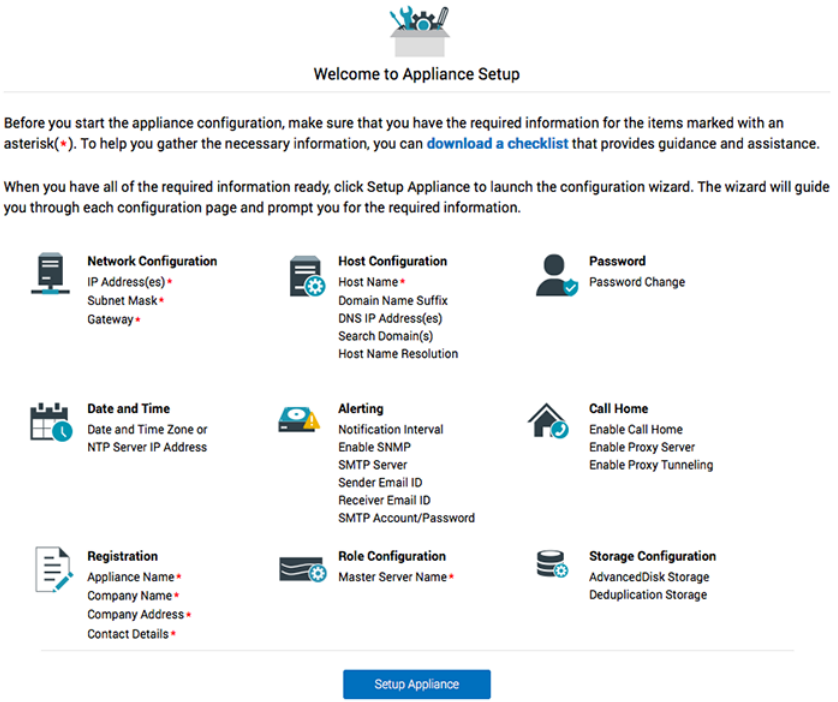
Overview of the initial configuration pages in the NetBackup Appliance Web Console

The NetBackup Appliance Web Console lets you perform the initial configuration through a series of pages where you enter the appropriate information. The following shows each page along with a brief description of the required information.

Welcome to Appliance Setup

This page appears when you log on to an appliance that is not configured. It provides a short summary of the necessary information for the initial configuration.

Figure 1-1 Welcome to Appliance Setup page

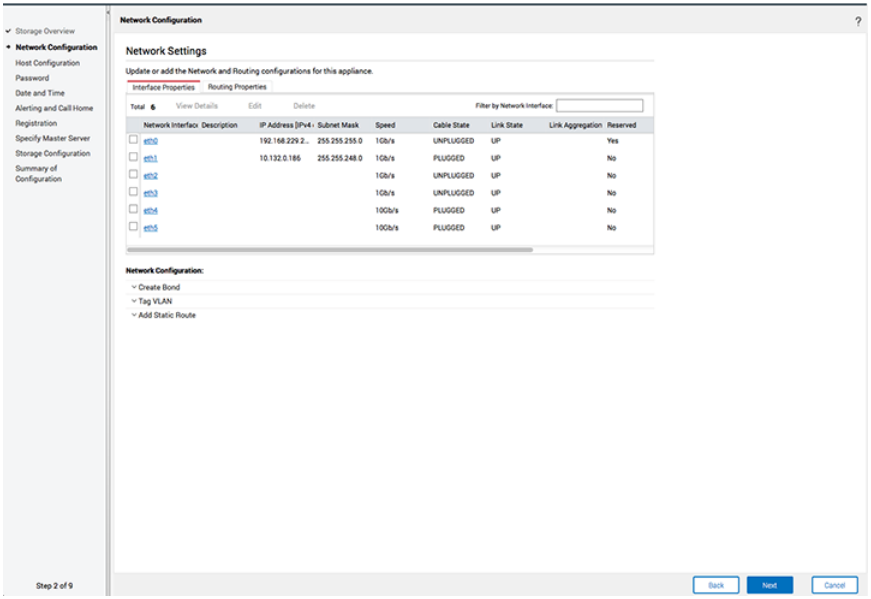


Note: This page provides a link to download a checklist that provides descriptions for all of the data entry fields on all pages in the initial configuration. Before you begin the initial configuration, Veritas recommends that you click on the **download a checklist** link, print the file, and record all of the necessary information.

Network Configuration

This page is used to enter your corporate network information. The upper table contains tabs for entering the **Interface Properties** and the **Routing Properties** information. The lower table contains drop down tabs that expand to enter the **Create Bond**, **Tag VLAN**, and **Add Static Route** information.

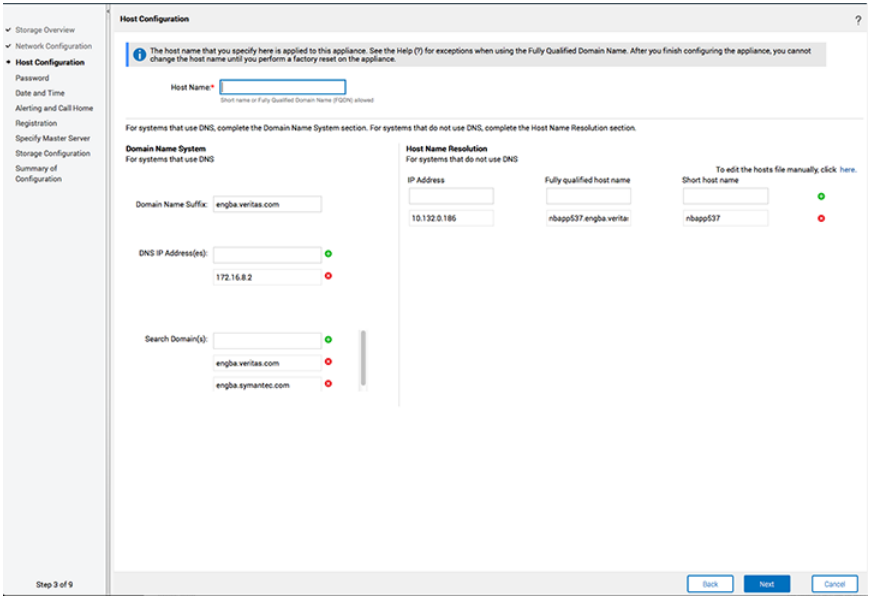
Figure 1-2 Network Configuration page



Host Configuration

This page is used to enter the host identification information for this appliance. The appliance host name (FQDN and short name), the IP address, and the domain name are all required.

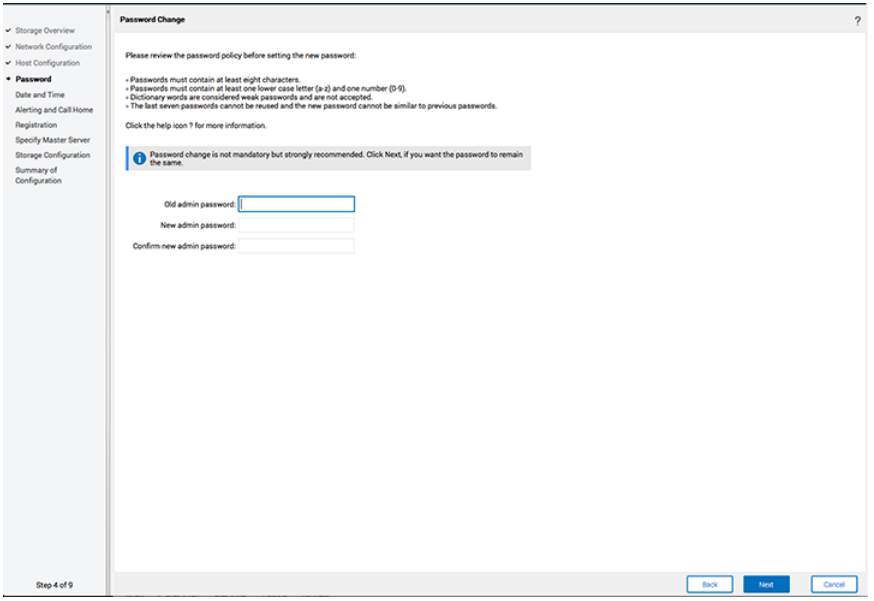
Figure 1-3 Host Configuration page



Password change

This page is used to change the password for this appliance server. Veritas recommends that you change the factory default password to a high security password when you perform the initial configuration.

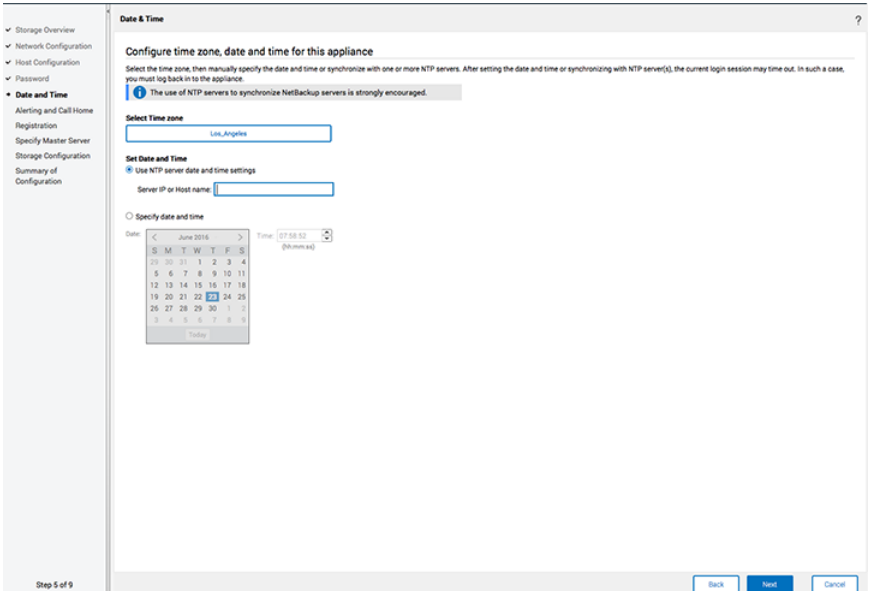
Figure 1-4 Password change page



Date & Time

This page is used to set the date, the time, and the time zone for the appliance location.

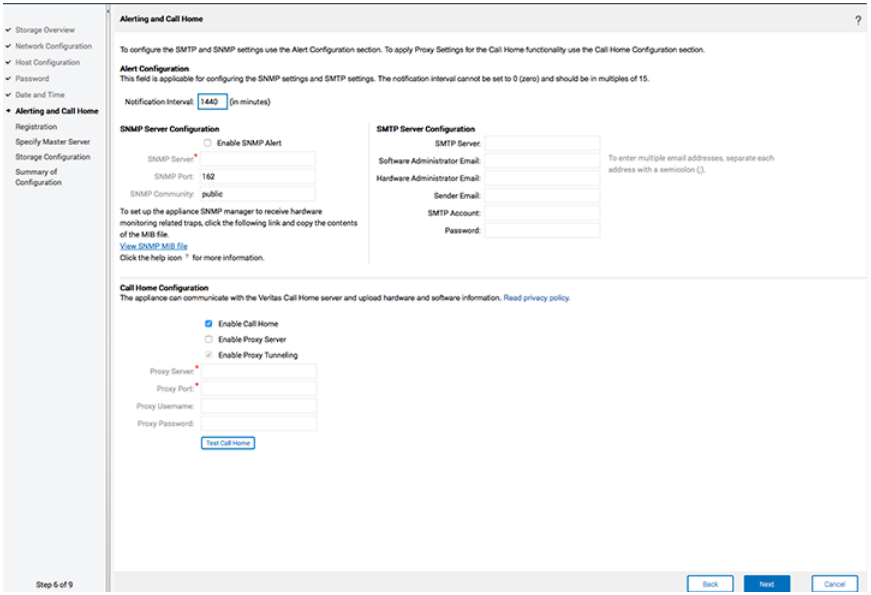
Figure 1-5 Date & Time page



Alerting and Call Home

This page is used to configure system alerts and the Call Home feature for reporting problems.

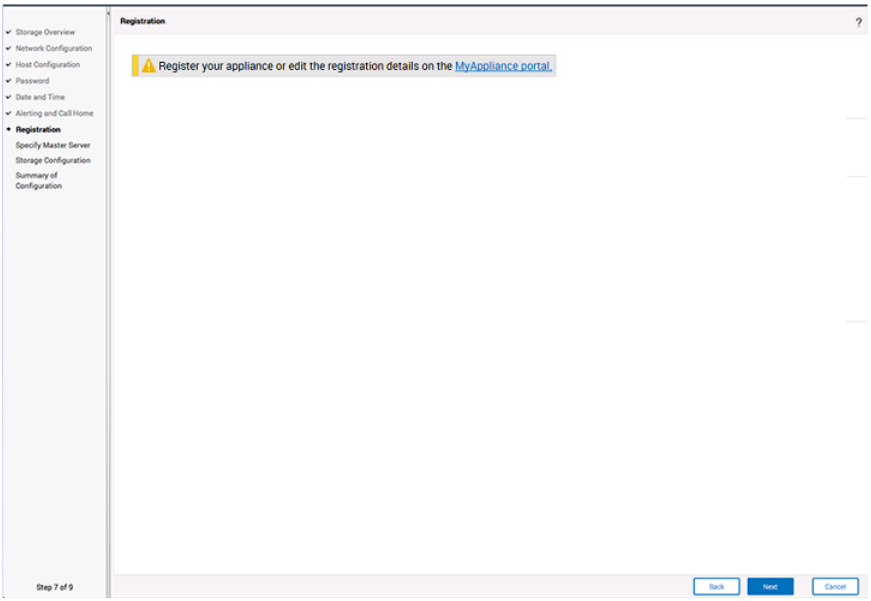
Figure 1-6 Alerting and Call Home page



Registration

This page provides a link to the MyAppliance portal. Register your appliance on the portal to make sure that you are alerted to product updates and other important updates about your appliance.

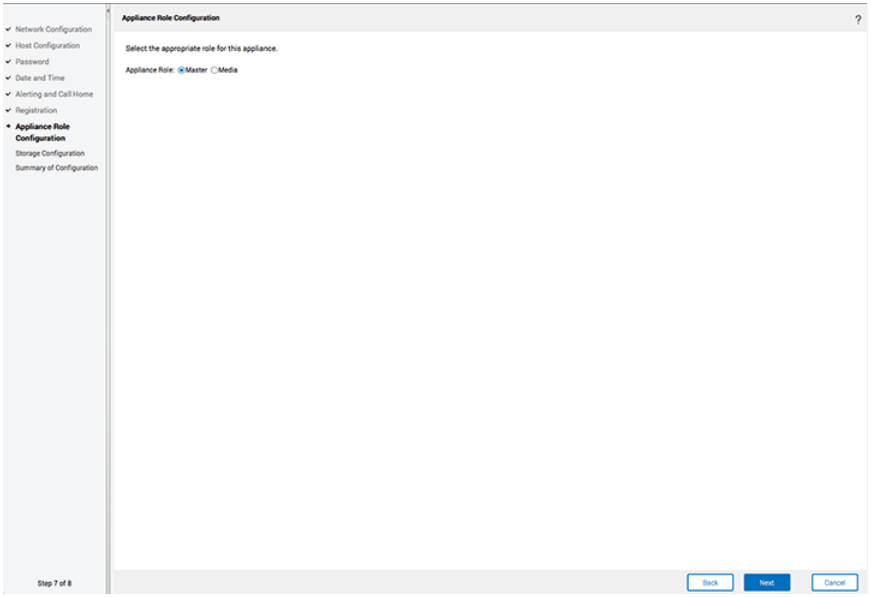
Figure 1-7 Registration page



Appliance Role Configuration - Master

This page is used to select the role for the appliance as either a master server or a media server. When you select **Master**, no further action is required. When you select **Media**, the page content changes to let you identify the associated master server (see Figure 1-9).

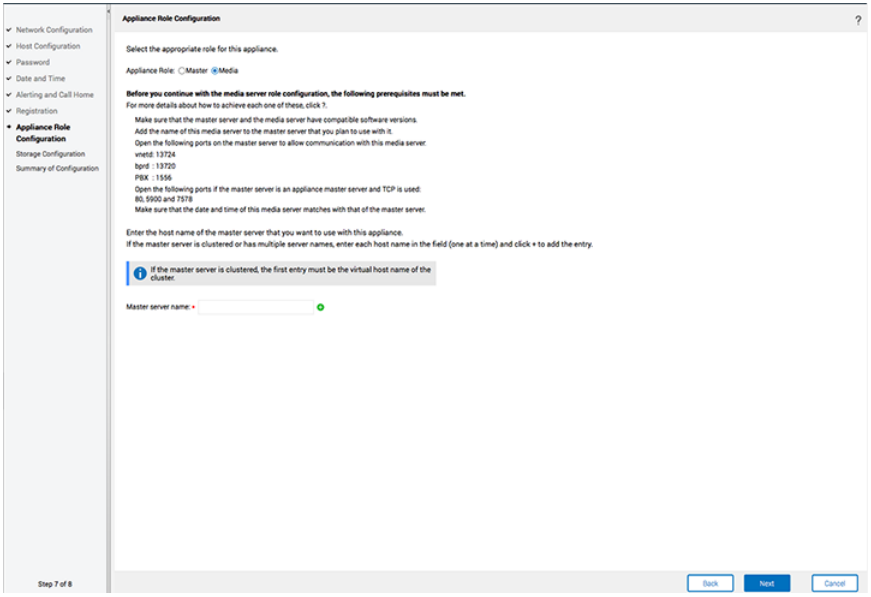
Figure 1-8 Appliance Role Configuration -Master page



Appliance Role Configuration - Media

When you select **Media**, a description of prerequisites appears, along with a data entry field to enter the name of the associated master server.

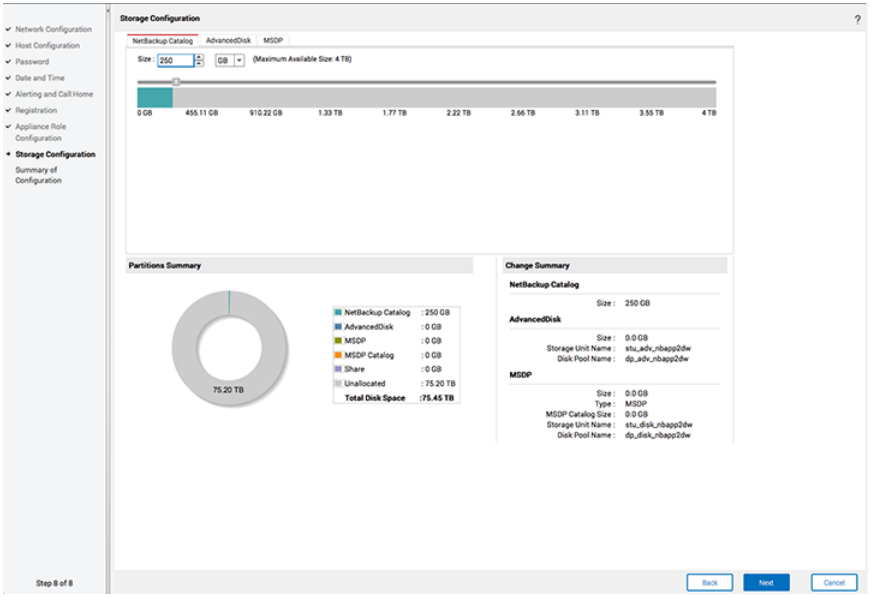
Figure 1-9 Appliance Role Configuration -Media page



Storage Configuration - NetBackup Catalog

The **NetBackup Catalog** tab on this page is used to set the size of the NetBackup catalog. This tab appears only when you select **Master** for the appliance role.

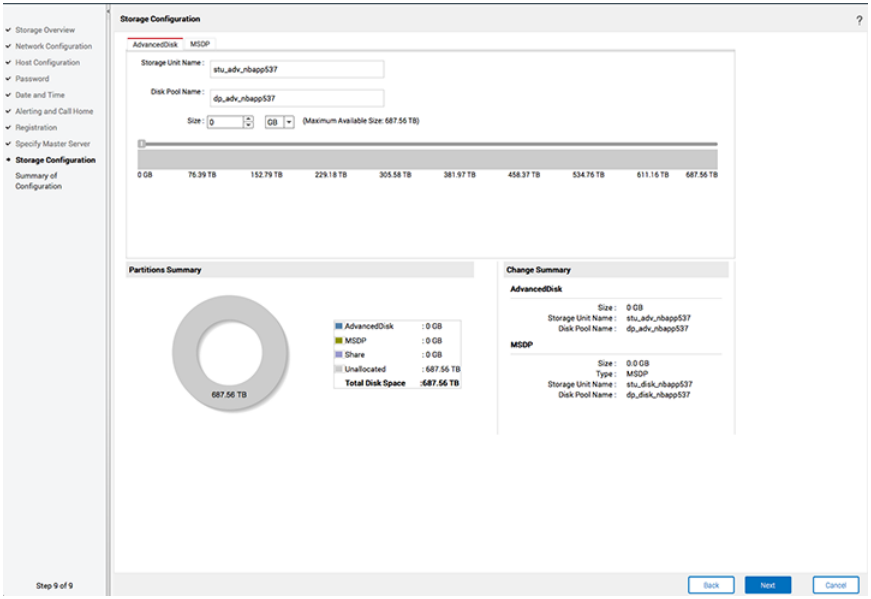
Figure 1-10 Storage Configuration page - NetBackup Catalog



Storage Configuration - AdvancedDisk

The **AdvancedDisk** tab on this page is used to allocate storage space for the AdvancedDisk partition and to name the storage unit and the disk pool.

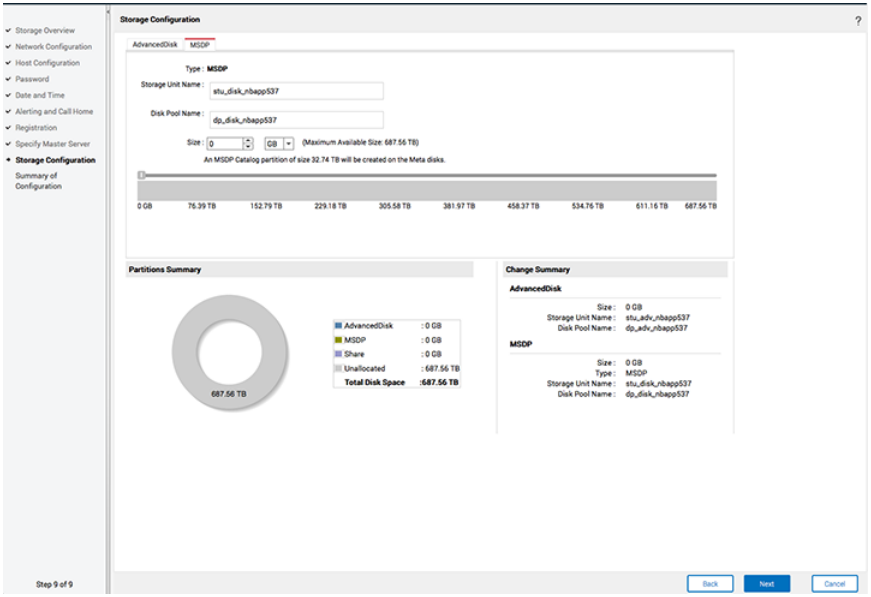
Figure 1-11 Storage Configuration page - AdvancedDisk



Storage Configuration - MSDP

The **MSDP** tab on this page is used to allocate storage space for the Media Server Deduplication Pool partition and to name the storage unit and the disk pool.

Figure 1-12 Storage Configuration page - MSDP



About the NetBackup 52xx Appliance initial configuration checklist

Use the initial configuration checklist to help plan for the initial configuration and for any future appliance reconfiguration.

The checklist consists of a series of tables that describe the data entry fields for each initial configuration page that appears in the NetBackup Appliance Web Console.

For a new appliance, use the checklist to record the initial configuration settings before you configure the appliance. If the appliance is ever factory reset or re-imaged, the appliance must be configured again. The recorded settings in the checklist can save time and help get the appliance back on line quickly.

The checklist can be found in the following locations:

- *NetBackup 5230 Appliance Initial Configuration Guide*
  This document is available at the following NetBackup appliance documentation website:
  https://www.veritas.com/support/en_US/58991/appliance-docs.html
- NetBackup Appliance Web Console

When you log in to the appliance for the first time through the NetBackup Appliance Web Console, a **download checklist** link appears on the **Welcome** page. Click on the link to open the checklist file. You can also access the checklist by clicking the online Help (?) icon from any page and searching for **checklist**.

- NetBackup appliance online documentation
  You can obtain a PDF version of the checklist to download and save to a location of your choice. To access the latest version of this checklist, see the following link:
  www.symantec.com/docs/DOC6675

See "Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console " on page 32.

See "Performing the initial configuration on a 52xx master server appliance from the NetBackup Appliance Shell Menu" on page 49.

See "Performing the initial configuration on a 52xx media server appliance from the NetBackup Appliance Shell Menu" on page 60.

NetBackup appliance initial configuration checklist

This checklist is intended to help you plan for the initial configuration of your appliance.

Use this checklist together with the initial configuration procedures in the *NetBackup Appliance Initial Configuration Guide*. That document also contains a copy of this checklist.

For a new appliance, use the following tables to record the initial configuration settings for this appliance. If this appliance is ever factory reset or re-imaged, the appliance must be configured again. The recorded settings in the checklist can save valuable time and help get the appliance back on line quickly.

When using the hard copy or printed version of this checklist, make sure to place the completed checklist in a secure location. You can also obtain a PDF version of the checklist to download and save to a location of your choice. To access the latest version of this checklist, see the following link:

https://www.veritas.com/support/en_US/article.000100480

IPMI port configuration

IPMI port configuration is separate from the initial configuration. To use this port for remote access to the appliance, you must first configure it for connectivity to your network. Use the following table to record the required parameter settings.

Table 1-4 IPMI port configuration

Parameter	Setting
IP Address	
Netmask	
Gateway IP Address	

Appliance initial configuration

The following tables identify the fields that appear on the initial configuration pages in the NetBackup Appliance Web Console. Use these tables to record your settings.

Table 1-5 Network Configuration - Create Bond

Field	Setting
Network Interface	
Bond Mode	
IP Address	
Subnet Mask	

Table 1-6 Network Configuration - Tag VLAN

Field	Setting
Select Interface	
Description (for Select Interface field above)	
VLAN Id	
IP Address (IPv4 or IPv6)	
Subnet Mask	

Table 1-7 Network Configuration - Add Static Route

Field	Setting
Destination IP	
Destination Subnet Mask	
Gateway	

Table 1-7 Network Configuration - Add Static Route *(continued)*

Field	Setting
Network Interface	

Table 1-8 Host Configuration

Field	Setting
Host Name	
Domain Name System (DNS) ■ Domain Name Suffix ■ DNS IP Address ■ Search Domain(s)	DNS: ■ _____ ■ _____ ■ _____
Host Name Resolution (no DNS) ■ IP address ■ Fully qualified host name ■ Short host name	No DNS: ■ _____ ■ _____ ■ _____

Table 1-9 Password change

Field	Setting
Old admin password	
New admin password	
Confirm new admin password	

Table 1-10 Date and time configuration

Field	Setting
Time zone	
NTP Server IP	
Date and Time	

Table 1-11 Alerting Configuration

Field	Setting
Notification Interval (in 15-minute intervals)	

Table 1-11 Alerting Configuration *(continued)*

Field	Setting
Enable SNMP Alert	
SNMP server (required only if you check **Enable SNMP Alert**)	
SNMP port	
SNMP community	
SMTP server	
Software administrator email address	
Hardware administrator email address	
Sender email address	
SMTP account	
Password	

Table 1-12 Call Home Configuration

Field	Setting
Enable Call Home	
Enable proxy server	
Enable proxy tunneling	
Proxy server (required only if you check **Enable proxy server**)	
Proxy port (required only if you check **Enable proxy server**)	
Proxy user name	
Proxy password	

Table 1-13 Role Configuration

Field	Setting
Master or Media	

Table 1-13 Role Configuration *(continued)*

Field	Setting
Master server name (required only if you check **Media**)	

Table 1-14 AdvancedDisk storage configuration

Field	Setting
Storage Unit name	
Disk Pool Name	
Size	

Table 1-15 Deduplication (MSDP) Disk Configuration

Field	Setting
Storage Unit name	
Disk Pool Name	
Size	

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*.

Chapter 2

Initial configuration procedures

This chapter includes the following topics:

- Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console
- Performing the initial configuration on a 52xx master server appliance from the NetBackup Appliance Shell Menu
- Configuring a master server to communicate with an appliance media server
- Performing the initial configuration on a 52xx media server appliance from the NetBackup Appliance Shell Menu
- Performing the initial configuration on a NetBackup 5240 CloudCatalyst Appliance

Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console

After you have installed, connected, and turned on all appliance system components, you are ready to configure the server.

If you plan to configure this appliance as a media server, complete the following tasks on the master server before you start the initial configuration. The following link provides specific instructions about how to accomplish the necessary tasks:

See "Configuring a master server to communicate with an appliance media server" on page 58.

- Make sure that the master server and this media server have compatible software versions.
- Add the name of this media server to the `SERVERS` list on master server that you plan to use with it.
- If a firewall exists between the master server and this media server, open the appropriate ports as described in the link above.
- Make sure that the date and time of this media server matches the date and time on the master server.

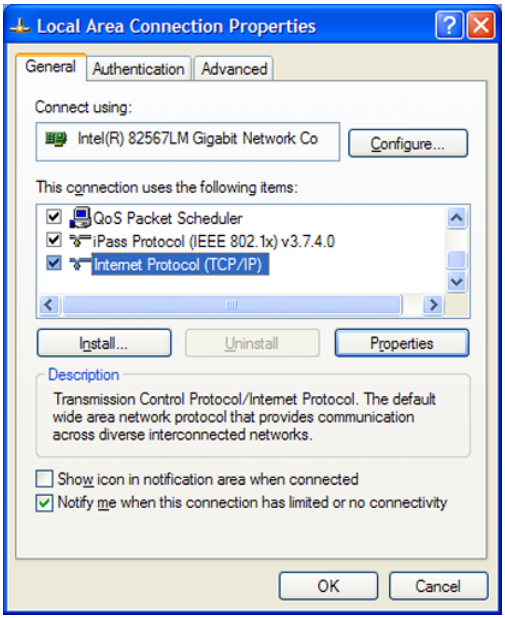
The following procedure describes how to configure a new or a re-imaged appliance from the NetBackup Appliance Web Console.

Caution: The appliance comes configured with a known default password for the `Maintenance` user account. You should change this password either before or immediately after the initial configuration to prevent unauthorized access to the appliance maintenance mode. Note that you must provide the `Maintenance` user password to Veritas Technical Support in the event that the appliance requires troubleshooting services. Step 16 in the following procedure describes how to change the `Maintenance` user password.

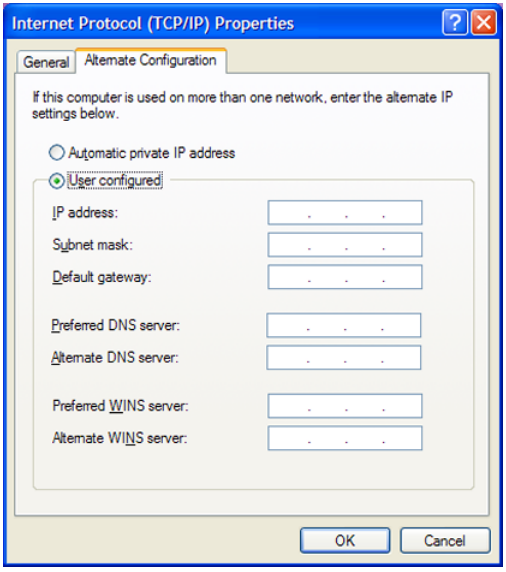
To perform the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console

1 On the laptop that is connected to the **NIC1** appliance port, navigate to the **Local Area Connection Properties** dialog box.

On the **General** tab, select **Internet Protocol (TCP/IP)** so that it is highlighted, then click **Properties**.



On the **Alternate Configuration** tab, perform the following tasks:



- Click **User Configured**.

- For the **IP address**, enter `192.168.229.nnn`, where `nnn` is any number from 2 through 254 except for 233.
- For the **Subnet mask**, enter **255.255.255.0**.
- Click **OK**.

2 On the laptop that is connected to the appliance, open a web browser to the following URL:

https://192.168.229.233

Note: Starting with NetBackup appliance software version 2.6.0.4, the NetBackup Appliance Web Console is accessible only over HTTPS on the default port 443. Port 80 over HTTP has been disabled. The exception to this change is in NetBackup appliance software version 2.6.1. With that version, the NetBackup Appliance Web Console is accessible only over HTTPS on the default port 80.

---

3 Log on to the appliance as follows:

- For **User Name**, enter **admin**.
- For **Password**, enter **P@ssw0rd**.

4 On the **Welcome to Appliance Setup** page, review the summary of information that you need to perform the initial configuration.

- **Download Configuration Checklist**
  To help with the initial configuration, click this link to open a file where you can record all of the configuration settings. Veritas recommends that you print this file and fill it out for use as you perform the configuration. Then store it in a secure location for future reference.
- **Setup Appliance**
  After you have filled out the configuration checklist, click this item to start the configuration.

5 The **Network Configuration** page contains the following taskbars to complete specific tasks with their necessary data entry fields to configure network connectivity. Expand taskbar to enter the relevant network configuration information:

- **Create Bond** - Use to create a bond between two or more network interfaces.
- **Tag VLAN** - Starting with NetBackup Appliances version 2.6.0.3, you can configure VLANs in your existing network environments using this taskbar.

- **Add Static Route** - Use to add a route configuration for your network.

Note: These functions are independent of the other and do not require configuration in the order in which they appear.

Enter the appropriate **Create Bond** information as follows:

Create Bond data entry fields

- **Network Interface**
  Click on the drop-down box and select the interface or the device name between which you want to create the bond.
- **Bond Mode**
  Click on the drop-down box and select the bond mode to use for the NIC ports that you want to bond.
  Bonding lets you combine (aggregate) multiple network interfaces into a single logical "bonded" interface. The behavior of the bonded interfaces depends upon the mode. The default bond mode is **balance-alb**.
  The available bonding modes from the drop-down list are as follows:
  - **balance-rr**
  - **active-backup**
  - **balance-xor**
  - **broadcast**
  - **802.3ad**
  - **balance-tlb**
  - **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
  After you have entered the appropriate data into all fields, you must click **+** to add and immediately plumb the selected network interface. To configure bonding, you must select multiple interfaces from the **Bond Mode** drop-down box. For IPv6 addresses, enter 64 as the **Subnet Mask**.
- **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 network address that identifies the IP address for this appliance server.
- After you have entered the appropriate data into all fields, click **+** to save and add the network configuration settings.

If required for your environment, enter the appropriate **Tag VLAN** information as follows:

Tag VLAN data entry fields

- **Select Interface**
  Select the network interface or the device name to which you want to tag the VLAN.
- **Description**
  Enter a description for the VLAN. For example, Finance or Human Resource.
- **VLAN Id**
  Enter a numeric identifier for the VLAN. VLAN IDs can range between 1- 4094. 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.
- Click **Add** to add the configuration information for tagging VLAN into to your existing network environment.
  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.

Enter the appropriate **Add Static Route** information as follows:

Add Static Route data entry fields

- **Destination IP**
  Enter the network IP address of a destination network. 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 12.
- **Destination Subnet Mask**
  Enter the subnet value that corresponds to the **Destination IP** address.
  For the initial 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. 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 12.
- **Network Interface**
  Click on the drop-down box and select the ethernet NIC port to use for a network connection.
- After you have entered the appropriate data into all fields, click **+** to save and add the routing configuration settings.

After clicking **+** to save the entered network configuration settings, click **Next** at the bottom of the page to continue.

6 On the **Host Configuration** page, you can enter the host resolution information as follows:

- **To edit the hosts file manually, click here**
  Add the IP address, the fully qualified host name, and the short host name directly into the `/etc/hosts` file. Click **here** to open and edit the `/etc/hosts file` file.

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

- Enter the appliance host name and the related host resolution information in the following fields:

Host Name

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

Enter the short host name or the fully qualified domain name (FQDN) of this appliance.

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

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

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

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

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

For DNS systems: Enter the following **Domain Name System** information:

- **Domain Name Suffix**
  Enter the suffix name of the DNS server. If you entered the FQDN in the Host Name field, this field is populated automatically.
- **DNS IP Address(es)**
  Enter the IP address of a DNS server, then click the **+** icon to add the address. Repeat as necessary for the number of addresses that you want to add.
  The address can be either IPv4 or IPv6. For IPv6 addresses, only global-scope or unique-local addresses are allowed.
  See "About IPv4-IPv6-based network support" on page 12.
  To remove an address, select it from the list that appears below the data entry field and click the **x** icon.
- **Search Domain(s)**
  If required for your environment, enter a search domain name, then click the **+** icon to add the name. Repeat as necessary for the number of search domains that you want to add.
  To remove a search domain, select it from the list that appears below the data entry field and click the **x** icon.

After you have entered all of the necessary information, click **Next**.

For the systems that do not use DNS: Enter the following **Host name resolution** information:

- **IP**
  Enter the IP address of the appliance.
  The address can be either IPv4 or IPv6. For IPv6 addresses, only global-scope or unique-local addresses are allowed.
  See "About IPv4-IPv6-based network support" on page 12.
- **Fully qualified host name**
  Enter the fully qualified host name (FQHN) of the appliance.
- **Short host name**
  Enter the short name of the appliance.
  To enter two or more names, add a comma with no space between each name.

After you have populated all fields, click the **+** icon. The added entries now appear below the fields.

After you have entered all of the necessary information, click **Next**.

7 On the **Password change** page, enter a new password to replace the default password as follows:

Note: To continue with the initial configuration of the appliance, you are not required to change the default password. However, to increase the security of your environment Veritas recommends that you change the administrator password periodically. Make sure to keep a record of the current password in a secure location.

Old admin password	Enter the factory default password (`P@ssw0rd`)
New admin 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.

After you have entered all of the necessary information, click **Next**.

8 On the **Date & Time** page, enter the appropriate date and time for this appliance.

You can enter the information manually or use a Network Time Protocol (NTP) server to synchronize the appliance date and time over the network.

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.

Specify date & time	To enter the date and the time manually, select this option and enter the following information: ■ In the first field, enter the date by using the `mm/dd/yyyy` format. Or, click on the calendar icon and select the appropriate month, day, and year. ■ In the second field, enter the time by using the `hh:mm:ss` format. Entries must be in the 24 hour format (`00:00:00 - 23:59:59`).
NTP	To synchronize the appliance with a Network Time Protocol (NTP) server, select this option and enter the NTP **Server IP** address.

After you have entered all of the necessary information, click **Next**.

9 On the **Alerting and Call Home** page, enter the information for the appliance to send alerts or to upload status reports by email to a Veritas Call Home server.

For alerts, enter the appropriate **Alerting Configuration** information as follows:

Alerting Configuration data entry fields

To configure the appliance to upload alerts, enter the following information:

- **Notification interval (in minutes)**
  Enter the interval for the appliance to upload alerts to the Veritas Call Home server. Entries must be in increments of 15 minutes.
- **Enable SNMP Alert**
  Click this check box and enter the following SNMP information:
  - **SNMP server**
    Enter either the SNMP server host name or its IP address to define this computer. The IP address can be either IPv4 or IPv6. For IPv6, only global-scope and unique-local addresses are allowed.
  - **SNMP port**
    Enter the port number of the SNMP server to allow communication with this appliance.
  - **SNMP community**
    Enter the community name where the alerts or traps are sent.
    For example, you can enter the same information that you used for the **SNMP server**. You can also enter a company name or another name like, admin_group, public, or private. If you do not enter anything, the default value is **Public**.
  - **View SNMP MIB file**
    To set up the appliance SNMP Manager to receive hardware monitoring related traps, click this link to view the content of the MIB file. Then, copy the file to another location and use the content to update the SNMP Manager.
    The appliance can only accept traps in the SNMPv2c format.
- **SMTP server**
  Enter either the SMTP server host name or its IP address to define this computer.
- **Software administrator email address**
  Enter the email address of your software administrator so that they can receive and notifications.
- **Hardware administrator email address**
  Enter the email address of your hardware administrator so that they can receive and notifications.
- **Sender email address**
  Enter the email address of the appliance so that recipients can identify the source of the report.
- **SMTP account**
  Enter an account name for the SMTP server.
- **Password**
  To increase security, enter a password for the SMTP server.

You can configure this server to send email reports to a proxy server or to the Veritas Call Home server.

The following describes the supported proxy servers:

- Squid
- Apache
- TMG

Note: NTLM authentication in the proxy configuration is also supported.

For Call Home, enter the appropriate **Call Home Configuration** information as follows:

Call Home Configuration data entry fields

To configure the appliance to send email reports to a proxy server or to the Veritas Call Home server, enter the following information:

- **Enable Call Home**
  Click this check box to enable the appliance to send email reports to the Veritas Call Home server.
- **Enable proxy server**
  Click this check box to use a proxy server for email notification and provide the proxy information that follows.
- **Enable proxy Tunneling**
  To enable proxy tunneling, click this check box and provide the following proxy information:
  - **Proxy server**
    Enter the IP address of the server.
    The IP address can be either IPv4 or IPv6. For IPv6, only global-scope and unique-local addresses are allowed.
  - **Proxy port**
    Enter the port number of the proxy server to allow communication with this appliance.
  - **Proxy username**
    Enter the user name for the proxy server.
  - **Proxy password**
    Enter the password of the proxy server.
  - **Test Call Home**
    After you have entered all of the necessary information, Veritas recommends that you click **Test Call Home** to verify communication with the Veritas server.
    If the test fails, check that you have entered all names, IP addresses, and port numbers correctly. If the test fails again, contact Veritas Technical Support.

After you have entered all of the necessary information, click **Next**.

10 On the **Registration** page, click on the link to the MyAppliance portal at https://my.appliance.veritas.com to register the appliance and enter your contact information.

11 Configure the role for this appliance server as follows:

Option or data entry field	Description

Appliance Role	■ **Master**
	When you select this role, no further action is required. Click **Next** to continue.
	■ **Media**
	If you select this role, do not continue configuration until you have performed or verified the following configuration on the master server that you want to use with this media server. The following link provides specific instructions about how to accomplish the necessary tasks:
	See "Configuring a master server to communicate with an appliance media server" on page 58.
	■ Make sure that the master server and this media server have compatible software versions.
	■ Add the name of this media server to the `SERVERS` list on the master server that you plan to use with it.
	■ Open the following ports on the master server to allow communication to this media server:
	`vnetd: 13724`
	`bprd: 13720`
	`PBX: 1556`
	■ Open the following ports if the master server is an appliance master server and TCP is used: 443, 5900, and 7578.
	■ Make sure that the date and time of this media server matches with that of the master server.

Option or data entry field	Description
Master server name	If you selected the **Media Server** role, identify the name of the master server that must communicate with this media server as follows: ■ For master servers with only one name and IP address: Enter the host name or the IP address of the master server and click **Add**. ■ For clustered master servers or master servers with multiple names and IP addresses: Enter each host name or IP address in the field (one at a time) and click **Add**. **Note:** If the master server is clustered, the first entry must be the virtual host name of the cluster. **Note:** If the host name of the master server is an FQDN, Veritas recommends that you use the FQDN to specify the master server for the media server.

After you have entered all of the necessary information, click **Next**. The **Certificate Verification** dialog box appears, see the following:

Confirm the CA certificate detail and click **Deploy** to deploy the CA certificate to the media server.

Enter the token if it is required , and click **Deploy** to deploy the host ID-based certificate to the media server.

For more information about security certificates, refer to the chapter **Security certificates in NetBackup** in the *NetBackup Security and Encryption Guide*.

12 On the **Storage Configuration** page, create names for the storage units and the disk pools that you plan to use, and configure the size of the disk partitions.

You can configure storage partitions for AdvancedDisk, for Deduplication (MSDP), or for both.

Note: If you choose to configure MSDP storage, a policy is automatically created to protect the MSDP catalog. Veritas recommends reviewing this policy and activating it once your appliance is configured.

NetBackup Catalog

This tab lets you set the size of the NetBackup catalog partition on the master server. This tab appears only for the appliances that are configured as a master server.

To change the size of the partition, enter a precise number in the **Size** field, or click and drag the box on the gray slide bar to the desired size. The size can be set in GB or TB units, depending on the maximum available space.

AdvancedDisk

Enter the following information:

- **Storage Unit Name**
  Enter the name that you want to use to identify this storage unit. The 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.
- **Disk Pool Name**
  Enter the name that you want to use to identify this disk pool. The 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.
- **Size**
  Set the size for this partition by entering a precise number in the **Size** field, or click and drag the box on the gray slide bar to the desired size. The size can be set in GB or TB units, depending on the maximum available space.

Deduplication Disk (MSDP) Enter the following information:

- **Storage Unit Name**
  Enter the name that you want to use to identify this storage unit. The 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.
- **Disk Pool Name**
  Enter the name that you want to use to identify this disk pool. The 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.
- **Size**
  Set the size for this partition by entering a precise number in the **Size** field, or click and drag the box on the gray slide bar to the desired size
  The size can be set in GB or TB units, depending on the maximum available space.

After you have entered all of the necessary information, click **Next**.

13 On the **Configuration Progress** page, you can monitor the progress of the appliance as it applies all of the data input from the configuration pages.

The amount of time for the configuration to complete varies and depends on the complexity of your environment.

14 On the **Summary of Configuration** page, review the results of the configuration. Examine the results to make sure that the configuration completed successfully.

This page also identifies any errors that may have occurred. You may need to perform the initial configuration again if errors appear in the results.

15 After the configuration has completed successfully, wait about 5 minutes for the NetBackup services to start. You must then use the fully qualified host name to reconnect and log into the appliance.

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

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

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

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

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

See "About NIC1 (eth0) port usage on NetBackup appliances" on page 87.

---

18 After all appliances are configured and operational, you are ready to install client software on the computers that you want to back up.

See "Downloading NetBackup client packages to a client from a NetBackup appliance" on page 88.

See "Installing NetBackup client software through CIFS and NFS shares" on page 92.

Performing the initial configuration on a 52xx master server appliance from the NetBackup Appliance Shell Menu

After you have installed, connected, and turned on all appliance system components, you are ready to configure the server.

The following procedure describes how to configure a new 52xx master server appliance from the NetBackup Appliance Shell Menu.

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

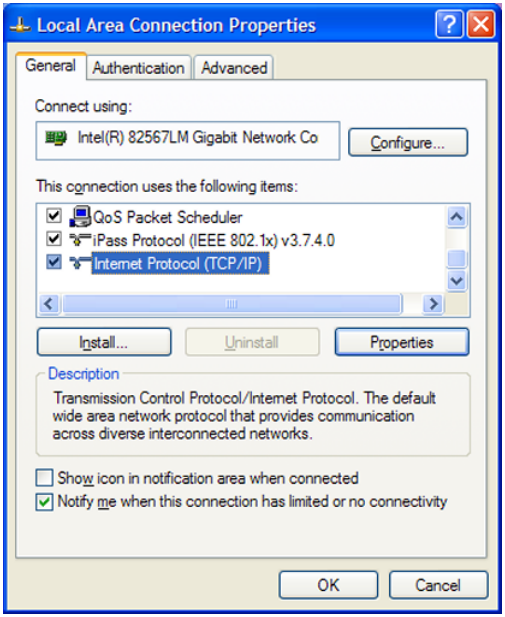
Note: You cannot remove an IP address if the appliance host name resolves to that IP address.

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

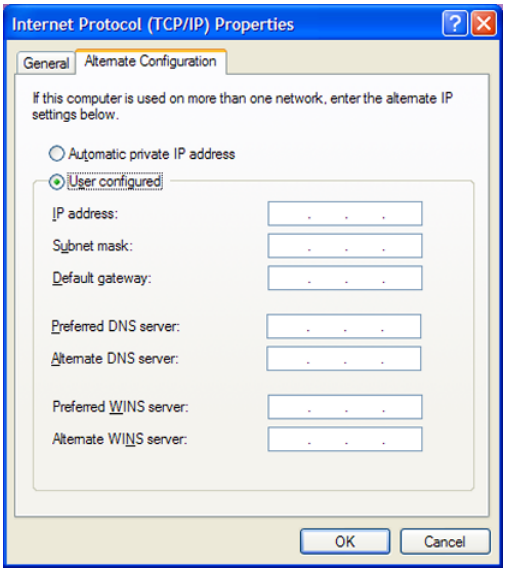
To perform the initial configuration on a 52xx master server appliance from the NetBackup Appliance Shell Menu

1 On the laptop that is connected to the **NIC1** appliance port, navigate to the **Local Area Connection Properties** dialog box.

On the **General** tab, select **Internet Protocol (TCP/IP)** so that it is highlighted, then click **Properties**.



On the **Alternate Configuration** tab, perform the following tasks:



- Click **User Configured**.
- For the **IP address**, enter `192.168.229.nnn`, where `nnn` is any number from 2 through 254 except for 233.
- For the **Subnet mask**, enter **255.255.255.0**.
- Click **OK**.

2 On the laptop that is connected to the appliance, open an SSH session to 192.168.229.233 and log on to your appliance.

The logon is `admin` and the default password is `P@ssw0rd`.

After you log on, the welcome message appears in the shell menu and the prompt is at the **Main_Menu** view.

3 From the **Main_Menu** > **Network** view, enter the following command to configure the IP address of a single network that you want your appliance to connect to.

`Configure` *`IPAddress Netmask GatewayIPAddress`* `[InterfaceNames]`

Where *IPAddress* is the new IP address, *Netmask* is the netmask, and *GatewayIPAddress* is the default gateway for the interface. The `[InterfaceNames]` option is optional.

The *IP Address* or the *Gateway IP Address* can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.

Remember that you should not use both IPv4 and IPv6 address in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1.`. You should use `Configure 9ffe::46 64 9ffe::49 eth1`

See "About IPv4-IPv6-based network support" on page 12.

If you want to configure multiple networks, you must first configure the IP address of each network that you want to add. Then you configure the Gateway address for each network you added. Make sure that you add the default Gateway address first. Use the following two commands:

Configure the IP address of each network	Use either of the following commands depending on whether you want to configure an IPv4 or an IPv6 address for the network interface: To configure the IPv4 address of a network interface: `IPv4` *`IPAddress Netmask`* `[InterfaceName]` Where *IPAddress* is the new IP address, *Netmask* is the netmask, and `[InterfaceName]` is optional. Repeat this command for each IP address that you want to add. To configure the IPv6 address of a network interface: IPv6 <*IP Address*> <Prefix> [InterfaceNames] Where *IPAddress* is the IPv6 address, *Prefix* is the prefix length, and `[InterfaceName]` is optional.

Configure the gateway address for each network that you added	`Gateway Add` *`GatewayIPAddress`* `[TargetNetworkIPAddress] [Netmask] [InterfaceName]` Where *GatewayIPAddress* is the gateway for the interface and *TargetNetworkIPAddress*, *Netmask*, and `InterfaceName` are optional. Repeat this command to add the gateway to all of the destination networks. The *Gateway IP Address* or the *TargetNetworkIPAddress* can be an IPv4 or an IPv6 address. Remember that you should not use both IPv4 and IPv6 addresses in the same command. For example, you cannot use `Gateway Add 9ffe::3 255.255.255.0 eth1`. You should use `Gateway Add 9ffe::3 6ffe:: 64 eth1`.

4 From the **Main_Menu** > **Network** view, use the following command to set the appliance DNS domain name.

Note: If you do not use DNS, then you can proceed to Step 7.

`DNS Domain` *`Name`*

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

5 From the **Main_Menu** > **Network** view, use the following command to add the DNS name server to your appliance configuration.

`DNS Add NameServer` *`IPAddress`*

Where *IPAddress* is the IP address of the DNS server.

The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed.

See "About IPv4-IPv6-based network support" on page 12.

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

6 From the **Main_Menu** > **Network** view, use the following command to add a DNS search domain to your appliance configuration so the appliance can resolve the host names that are in different domains:

`DNS Add SearchDomain` *`SearchDomain`*

Where *SearchDomain* is the target domain to add for searching.

7 This step is optional. It lets you add the IP addresses of other hosts in the appliance hosts file.

From the **Main_Menu** > **Network** view, use the following command to add host entries to the hosts file on your appliance.

```
Hosts Add IPAddress FQHN ShortName
```

Where *IPAddress* is the IPv4 or the IPv6 address, *FQHN* is the fully qualified host name, and *ShortName* is the short host name.

See "About IPv4-IPv6-based network support" on page 12.

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

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

```
Hostname Set Name
```

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

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

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

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

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

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

With this step, NetBackup is re-configured to operate with the new host name. This process may take a while to complete.

For the command `Hostname set` to work, at least one IPv4 address is required. For example, you may want to set the host name of a specific host to v46. To do that, first ensure that the specific host has at least an IPv4 address and then run the following command.

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

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

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

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

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

- Set the time zone by entering the following command:

  `TimeZone Set`

  Select the appropriate time zone from the displayed list.
- Set the date and the time by entering the following command:

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

  Where *Month* is the name of the month.

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

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

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

11 From the **Main_Menu > Settings > Alerts > Email** view, use the following commands to enter the SMTP server name and the email addresses for appliance failure alerts.

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

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

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

```
Master
```

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

To configure storage partitions, you must do the following:

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

The storage prompts appear in the following order:

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

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

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

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

14 Change the `Maintenance` user password as follows:

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

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

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

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

See "About NIC1 (eth0) port usage on NetBackup appliances" on page 87.

---

16 After all appliances are configured and operational, you are ready to install client software on the computers that you want to back up.

See "Downloading NetBackup client packages to a client from a NetBackup appliance" on page 88.

See "Installing NetBackup client software through CIFS and NFS shares" on page 92.

Configuring a master server to communicate with an appliance media server

Before you configure a new appliance for the **Media** server role, you must first update the configuration on the master server that you plan to use with it. To ensure communication between the master server and the new media server, the new media server host name must be added to the **Additional Servers List** on the master server.

For high availability configurations, you must add the host name of the node that you use for the setup procedure.

The following procedure describes how to configure a master server to communicate with a new appliance media server.

To configure a master server to communicate with a new media server

1. Before the appliance is configured for the media server role, verify that the software version is compatible with the master server as follows:
   - If the master server is a NetBackup appliance:
     The master server must use appliance software version 3.1 or later.
   - If the master server is a traditional (non-appliance) NetBackup master server:
     The master server must use NetBackup version 8.1 or later, and the new media server must use appliance software version 3.1 or later.
2. Log in to the master server as the administrator and add the media server name to it as follows:

For an appliance master server:	From the NetBackup Appliance Web Console: ■ Click **Manage > Additional Servers > Add**. ■ In the **Appliance Hostname** field, enter the fully qualified host name (FQHN) of the appliance media server that you want to add. ■ Click **Add**. If the appliance has more than one host name, you must add all of the names. From the NetBackup Appliance Shell Menu: ■ From the **Main_Menu** > **Settings** view, run the following command: `Settings > NetBackup AdditionalServers Add media-server` Where *media-server* is the fully qualified host name (FQHN) of the appliance media server that is not yet configured. If the appliance has more than one host name, you must add all of the names.
For a traditional NetBackup master server:	■ Log on to the NetBackup Administration Console as the administrator. ■ On the main console window, in the left pane, click **NetBackup Management > Host Properties > Master Servers**. ■ In the right pane, click on the master server host name. ■ On the **Host Properties** window, in the left pane, click **Servers**. ■ In the right pane, in the **Additional Servers** section, click **Add** and enter your appliance host name. The appliance host name should appear in the top **Additional Servers** section. If the appliance has more than one host name, you must add all of the names. ■ Click **OK** and close the **Master Server Properties** window.

3 If a firewall exists between the master server and the media server, open the following ports on the master server to allow communication with the media server:

Note: You must be logged in as the administrator to change port settings.

- vnetd: 13724
- bprd: 13720
- PBX: 1556
- If the master server is a NetBackup appliance that uses TCP, open the following ports:
  443, 5900, and 7578.

4 Make sure that the date and time of the media server matches the date and time on the master server. You can use an NTP server or set the time manually.

See "Performing the initial configuration on a NetBackup 52xx appliance from the NetBackup Appliance Web Console " on page 32.

See "Performing the initial configuration on a 52xx media server appliance from the NetBackup Appliance Shell Menu" on page 60.

Performing the initial configuration on a 52xx media server appliance from the NetBackup Appliance Shell Menu

After you have installed, connected, and turned on all appliance system components, you are ready to configure the server.

If you plan to configure this appliance as a media server, you must complete the following tasks on the master server before you start the initial configuration. The following link provides specific instructions about how to accomplish the necessary tasks:

See "Configuring a master server to communicate with an appliance media server" on page 58.

- Make sure that the master server and this media server have compatible software versions.
- Add the name of this media server to the SERVERS list on the master server that you plan to use with it.
- If a firewall exists between the master server and this media server, open the appropriate ports as described in the link above.
- Make sure that the date and time of this media server matches the date and time on the master server.

The following procedure describes how to configure a new 52xx media server appliance from theNetBackup Appliance Shell Menu.

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

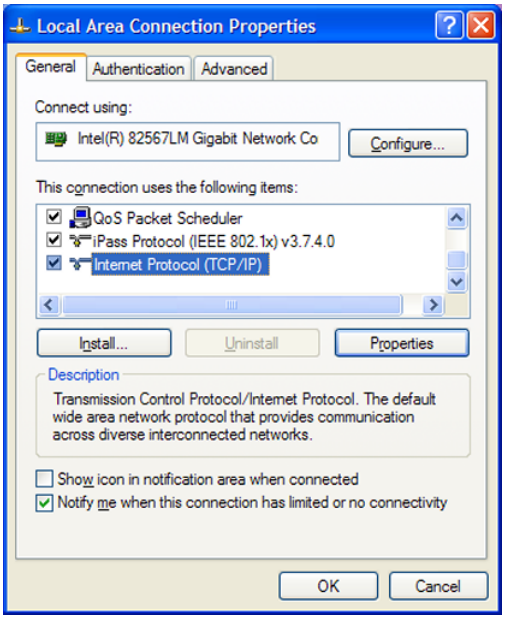
Note: You cannot remove an IP address if the appliance host name resolves to that IP address.

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

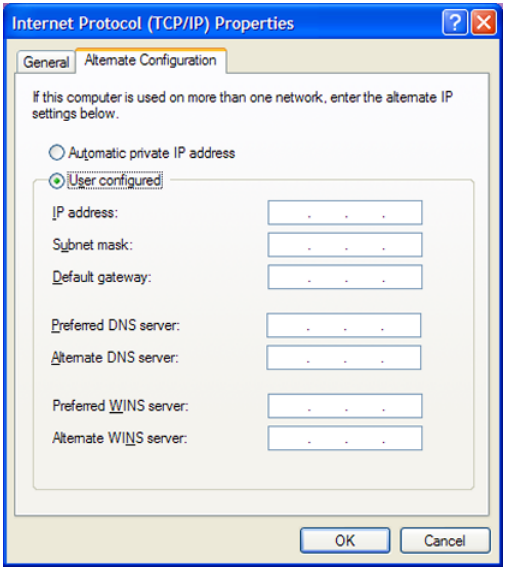
To perform the initial configuration on a 52xx media server appliance from the NetBackup Appliance Shell Menu

1 On the laptop that is connected to the **NIC1** appliance port, navigate to the **Local Area Connection Properties** dialog box.

On the **General** tab, select **Internet Protocol (TCP/IP)** so that it is highlighted, then click **Properties**.



On the **Alternate Configuration** tab, perform the following tasks:



- Click **User Configured**.

- For the **IP address**, enter `192.168.229.nnn`, where `nnn` is any number from 2 through 254 except for 233.
- For the **Subnet mask**, enter **255.255.255.0**.
- Click **OK**.

2. On the laptop that is connected to the appliance, open an SSH session to 192.168.229.233 and log on to your appliance.

   The logon is `admin` and the default password is `P@ssw0rd`.

   After you log on, the welcome message appears in the shell menu and the prompt is at the **Main_Menu** view.

3 From the **Main_Menu** > **Network** view, enter the following command to configure the IP address of a single network that you want your appliance to connect to.

`Configure` *`IPAddress Netmask GatewayIPAddress`* `[InterfaceNames]`

Where *IPAddress* is the new IP address, *Netmask* is the netmask, and *GatewayIPAddress* is the default gateway for the interface. The `[InterfaceNames]` option is optional.

The *IP Address* or the *Gateway IP Address* can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.

Remember that you should not use both IPv4 and IPv6 addresses in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1.`. You should use `Configure 9ffe::46 64 9ffe::49 eth1`

See "About IPv4-IPv6-based network support" on page 12.

If you want to configure multiple networks you must first configure the IP address of each network that you want to add. Then you configure the Gateway address for each network you added. You must make sure that you add the default Gateway address first. Use the following two commands:

Configure the IP address of each network	Use either of the following commands depending on whether you want to configure an IPv4 or an IPv6 address for the network interface: To configure the IPv4 address of a network interface: `IPv4` *`IPAddress Netmask`* `[InterfaceName]` Where *IPAddress* is the new IP address, *Netmask* is the netmask, and `[InterfaceName]` is optional. Repeat this command for each IP address that you want to add. To configure the IPv6 address of a network interface: IPv6 <*IP Address*> <Prefix> [InterfaceNames] Where *IPAddress* is the IPv6 address, *Prefix* is the prefix length, and `[InterfaceName]` is optional.

Configure the gateway address for each network that you added	`Gateway Add` *`GatewayIPAddress`* `[TargetNetworkIPAddress] [Netmask] [InterfaceName]` Where *GatewayIPAddress* is the gateway for the interface and *TargetNetworkIPAddress*, *Netmask*, and `InterfaceName` are optional. Repeat this command to add the gateway to all of the destination networks. The *Gateway IP Address* or the *TargetNetworkIPAddress* can be an IPv4 or an IPv6 address. Remember that you should not use both IPv4 and IPv6 address in the same command. For example, you cannot use `Gateway Add 9ffe::3 255.255.255.0 eth1`. You should use `Gateway Add 9ffe::3 6ffe:: 64 eth1`.

4 From the **Main_Menu** > **Network** view, use the following command to set the appliance DNS domain name.

Note: If you do not use DNS, then you can proceed to Step 7.

```
DNS Domain Name
```

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

5 From the **Main_Menu** > **Network** view, use the following command to add the DNS name server to your appliance configuration.

```
DNS Add NameServer IPAddress
```

Where *IPAddress* is the IP address of the DNS server.

The address can be either IPv4 or IPv6. Only global-scope and unique-local IPv6 addresses are allowed.

See "About IPv4-IPv6-based network support" on page 12.

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

6 From the **Main_Menu** > **Network** view, use the following command to add a DNS search domain to your appliance configuration so the appliance can resolve the host names that are in different domains:

```
DNS Add SearchDomain SearchDomain
```

Where *SearchDomain* is the target domain to add for searching.

7 This step is optional. It lets you add the IP addresses of other hosts in the appliance hosts file.

From the **Main_Menu** > **Network** view, use the following command to add host entries to the hosts file on your appliance.

```
Hosts Add IPAddress FQHN ShortName
```

Where *IPAddress* is the IPv4 or IPv6 address, *FQHN* is the fully qualified host name, and *ShortName* is the short host name.

See "About IPv4-IPv6-based network support" on page 12.

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

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

```
Hostname Set Name
```

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

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

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

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

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

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

With this step, NetBackup is re-configured to operate with the new host name. This process may take a while to complete.

For the command `Hostname set` to work, at least one IPv4 address is required. For example, you may want to set the host name of a specific host to v46. To do that, first ensure that the specific host has at least an IPv4 address and then run the following command.

```
Main_Menu > Network > Hostname Set v46
```

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

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

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

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

- Set the time zone by entering the following command:

  `TimeZone Set`

  Select the appropriate time zone from the displayed list.
- Set the date and the time by entering the following command:

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

  Where *Month* is the name of the month.

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

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

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

11 From the **Main_Menu > Settings > Alerts > Email** view, use the following commands to enter the SMTP server name and the email addresses for appliance failure alerts.

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

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

Note: Before you configure this appliance as a media server, you must add the name of this appliance to the master server that must work with this appliance.

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

```
Media MasterServer
```

Where *MasterServer* is either a standalone master server, a multihomed master server, or a clustered master server. The following defines each of these scenarios:

Standalone master server	This scenario shows one master server host name. This name does not need to be a fully qualified name as long as your appliance recognizes the master server on your network. The following is an example of how the command would appear. `Media MasterServerName`
Multihomed master server	In this scenario, the master server has more than one host name that is associated with it. You must use a comma as a delimiter between the host names. The following is an example of how the command would appear. `Media MasterNet1Name,MasterNet2Name`
Clustered master server	In this scenario, the master server is in a cluster. Veritas recommends that you list the cluster name first, followed by the active node, and then the passive nodes in the cluster. This list requires you to separate the node names with a comma. The following is an example of how the command would appear. `Media MasterClusterName,ActiveNodeName,PassiveNodeName`

Multihomed clustered master server	In this scenario, the master server is in a cluster and has more than one host name that is associated with it. Veritas recommends that you list the cluster name first, followed by the active node, and then the passive nodes in the cluster. This list requires you to separate the node names with a comma. The following is an example of how the command would appear.
	`Media MasterClusterName,ActiveNodeName,`
	`PassiveNodeName,MasterNet1Name,MasterNet2Name`
	To prevent any future issues, when you perform the appliance role configuration, Veritas recommends that you provide all of the associated master server names.

When the CA certificate detail appears, confirm the detail, enter **yes**, and then respond to the following prompts:

```
>> Do you trust the CA certificate? [yes, no] yes
```

Enter a token when it is required to deploy the host ID-based certificate, see the following prompts:

```
>> Enter token:
```

For more information about security certificates, refer to the chapter **Security certificates in NetBackup** in the *NetBackup Security and Encryption Guide*.

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

---

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

To configure storage partitions, you must do the following:

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

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

The storage prompts appear in the following order:

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

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

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

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

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

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

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

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

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

See "About NIC1 (eth0) port usage on NetBackup appliances" on page 87.

16 After all appliances are configured and operational, you are ready to install client software on the computers that you want to back up.

See "Downloading NetBackup client packages to a client from a NetBackup appliance" on page 88.

See "Installing NetBackup client software through CIFS and NFS shares" on page 92.

Performing the initial configuration on a NetBackup 5240 CloudCatalyst Appliance

Review the following information before configuring the NetBackup 5240 CloudCatalyst Appliance:

- Check the following tech note to ensure that your cloud provider is supported and install any necessary provider compatibility updates on the appliance: https://www.veritas.com/support/en_US/article.000127518
- A NetBackup 5240 CloudCatalyst Appliance supports a single cloud storage bucket of up to 1 Petabyte in size.
- When configured for CloudCatalyst, the NetBackup 5240 Appliance does not support attached storage shelves. All of the appliance's internal storage is allocated as MSDP cache space.
- The NetBackup 5240 CloudCatalyst Appliance does not support the NetBackup Appliance Web Console. Once the appliance is configured, the NetBackup Appliance Web Console is disabled.
- NetBackup CloudCatalyst does not support IPv6. Ensure that you have an IPv4 network set up to support the appliance before you configure it.

After you have installed, connected, and turned on all appliance system components, you are ready to configure the server.

You must complete the following tasks on the master server before you start the initial configuration. The following link provides specific instructions about how to accomplish the necessary tasks:

See "Configuring a master server to communicate with an appliance media server" on page 58.

- Make sure that the master server and this media server have compatible software versions.
- Add the name of this media server to the `SERVERS` list on the master server that you plan to use with it.
- If a firewall exists between the master server and this media server, open the appropriate ports as described in the link above.
- Make sure that the date and time of this media server matches the date and time on the master server.

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

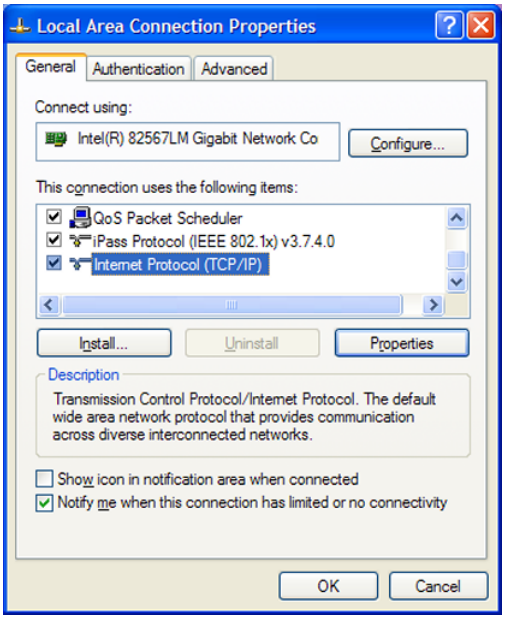
Note: You cannot remove an IP address if the appliance host name resolves to that IP address.

Caution: The appliance comes configured with a known default password for the `Maintenance` user account. You should change this password either before or immediately after the initial configuration to prevent unauthorized access to the appliance maintenance mode. Note that you must provide the `Maintenance` user password to Veritas Technical Support in the event that the appliance requires troubleshooting services. Step 19 in the following procedure describes how to change the `Maintenance` user password.

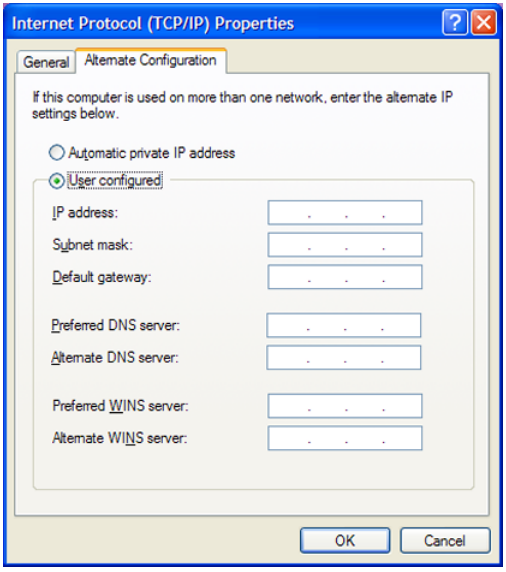
To perform the initial configuration on a NetBackup 5240 CloudCatalyst Appliance

1 On the laptop that is connected to the **NIC1** appliance port, navigate to the **Local Area Connection Properties** dialog box.

On the **General** tab, select **Internet Protocol (TCP/IP)** so that it is highlighted, then click **Properties**.



On the **Alternate Configuration** tab, perform the following tasks:



- Click **User Configured**.

- For the **IP address**, enter `192.168.229.nnn`, where `nnn` is any number from 2 through 254 except for 233.
- For the **Subnet mask**, enter **255.255.255.0**.
- Click **OK**.

2 On the laptop that is connected to the appliance, open an SSH session to 192.168.229.233 and log on to your appliance.

The logon is `admin` and the default password is `P@ssw0rd`.

After you log on, the welcome message appears in the shell menu and the prompt is at the **Main_Menu** view.

3 From the **Main_Menu** > **Network** view, enter the following command to configure the IP address of a single network that you want your appliance to connect to.

`Configure` *`IPAddress Netmask GatewayIPAddress`* `[InterfaceNames]`

Where *IPAddress* is the new IP address, *Netmask* is the netmask, and *GatewayIPAddress* is the default gateway for the interface. The `[InterfaceNames]` option is optional.

The *IP Address* or the *Gateway IP Address* must be an IPv4 address. NetBackup CloudCatalyst does not currently support IPv6.

If you want to configure multiple networks you must first configure the IP address of each network that you want to add. Then you configure the Gateway address for each network you added. You must make sure that you add the default Gateway address first. Use the following two commands:

Configure the IP address of each network	To configure the IPv4 address of a network interface: `IPv4` *`IPAddress Netmask`* `[InterfaceName]` Where *IPAddress* is the new IP address, *Netmask* is the netmask, and `[InterfaceName]` is optional. Repeat this command for each IP address that you want to add.
Configure the gateway address for each network that you added	`Gateway Add` *`GatewayIPAddress`* `[TargetNetworkIPAddress] [Netmask] [InterfaceName]` Where *GatewayIPAddress* is the gateway for the interface and *TargetNetworkIPAddress*, *Netmask*, and `InterfaceName` are optional. Repeat this command to add the gateway to all of the destination networks.

4 From the **Main_Menu** > **Network** view, use the following command to set the appliance DNS domain name.

Note: If you do not use DNS, then you can proceed to Step 7.

```
DNS Domain Name
```

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

5 From the **Main_Menu** > **Network** view, use the following command to add the DNS name server to your appliance configuration.

```
DNS Add NameServer IPAddress
```

Where *IPAddress* is the IP address of the DNS server.

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

6 From the **Main_Menu** > **Network** view, use the following command to add a DNS search domain to your appliance configuration so the appliance can resolve the host names that are in different domains:

```
DNS Add SearchDomain SearchDomain
```

Where *SearchDomain* is the target domain to add for searching.

7 This step is optional. It lets you add the IP addresses of other hosts in the appliance hosts file.

From the **Main_Menu** > **Network** view, use the following command to add host entries to the hosts file on your appliance.

```
Hosts Add IPAddress FQHN ShortName
```

Where *IPAddress* is the IPv4 address, *FQHN* is the fully qualified host name, and *ShortName* is the short host name.

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

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

```
Hostname Set Name
```

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

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

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

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

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

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

With this step, NetBackup is re-configured to operate with the new host name. This process may take a while to complete.

For the command `Hostname set` to work, at least one IPv4 address is required. For example, you may want to set the host name of a specific host to v46. To do that, first ensure that the specific host has at least an IPv4 address and then run the following command.

```
Main_Menu > Network > Hostname Set v46
```

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

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

- Use the `Network > VLAN Tag` command to tag a VLAN to a physical interface or bond interface.

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

10 (Optional) Configure the appliance to use a proxy server for cloud access.

If your environment requires a proxy server to connect to cloud services, you can use the following procedure:

- From the `Main_Menu > Settings > Alerts` view, type the following command:

  `CallHome Proxy Add <server> <port>`

  Where <*server*> is the fully qualified host name or IP address of the proxy server, and <*port*> is port number used by the proxy server.

  From the `Main_Menu > Settings > Alerts` view, type the following command:

  `CallHome Proxy Enable`

Note: The Call Home functionality is not turned on when you configure the proxy settings.

---

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

- Set the time zone by entering the following command:

  `TimeZone Set`

  Select the appropriate time zone from the displayed list.

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

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

  Where *Month* is the name of the month.

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

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

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

12 From the **Main_Menu > Settings > Alerts > Email** view, use the following commands to enter the SMTP server name and the email addresses for appliance failure alerts.

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

13 (Optional) Configure and start the NetBackup Key Management Service (KMS) on the master server.

To encrypt backups, use the following command to configure KMS:

```
/usr/openv/netbackup/bin/nbkms -createemptydb
```

As part of the setup, enter:

- A pass phrase and an ID for the host master key (HMK).
- A pass phrase and ID for the key protection key (KPK).

To start KMS, run the following command on the master server:

```
/usr/openv/netbackup/bin/nbkms
```

14 On the master server, run the following command to generate a set of credentials for the appliance:

```
/usr/openv/netbackup/bin/bpnbat -addmachine<mediaservername>
<password>
```

Where <*mediaservername*> is the host name of the appliance, and <*password*> is an arbitrary password that you will use to verify the host name-based certificate later in the configuration process.

15 Set the role for the appliance to a media server.

Note: Before you configure this appliance as a media server, you must add the name of this appliance to the master server that must work with this appliance. See "Configuring a master server to communicate with an appliance media server" on page 58.

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

```
Media MasterServer
```

Where *MasterServer* is either a standalone master server, a multihomed master server, or a clustered master server. The following defines each of these scenarios:

Standalone master server	This scenario shows one master server host name. This name does not need to be a fully qualified name as long as your appliance recognizes the master server on your network. The following is an example of how the command would appear. `Media MasterServerName`
Multihomed master server	In this scenario, the master server has more than one host name that is associated with it. You must use a comma as a delimiter between the host names. The following is an example of how the command would appear. `Media MasterNet1Name,MasterNet2Name`
Clustered master server	In this scenario, the master server is in a cluster. Veritas recommends that you list the cluster name first, followed by the active node, and then the passive nodes in the cluster. This list requires you to separate the node names with a comma. The following is an example of how the command would appear. `Media MasterClusterName,ActiveNodeName,PassiveNodeName`

Multihomed clustered master server	In this scenario, the master server is in a cluster and has more than one host name that is associated with it. Veritas recommends that you list the cluster name first, followed by the active node, and then the passive nodes in the cluster. This list requires you to separate the node names with a comma. The following is an example of how the command would appear.
	`Media MasterClusterName,ActiveNodeName,`
	`PassiveNodeName,MasterNet1Name,MasterNet2Name`
	To prevent any future issues, when you perform the appliance role configuration, Veritas recommends that you provide all of the associated master server names.

When the CA certificate detail appears, confirm the detail, enter **yes**, and then respond to the following prompts:

```
>> Do you trust the CA certificate? [yes, no] yes
```

Enter a token when it is required to deploy the host ID-based certificate, see the following prompts:

```
>> Enter token:
```

For more information about security certificates, refer to the chapter **Security certificates in NetBackup** in the *NetBackup Security and Encryption Guide*.

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

---

16 The following prompt appears:

```
>> Do you want to configure the appliance as a dedicated media
server for NetBackup CloudCatalyst? [yes, no] (yes):
```

Type **yes**.

17 The following prompt appears:

```
>> Enter the password for the host name-based certificate:
```

Type the password that you created in Step 14

18 Complete the NetBackup CloudCatalyst Appliance Configuration Wizard for your desired cloud provider.

A NetBackup 5240 CloudCatalyst Appliance can only be configured with one cloud storage provider. For example, the appliance cannot be used with Amazon S3 and Amazon GovCloud at the same time.

For detailed information about the required parameters in NetBackup CloudCatalyst Appliance Configuration Wizard, refer to the *NetBackup Cloud Administrator's Guide*.

- Amazon S3

Step 1: Cloud storage provider	Select Amazon.
Step 2a: Cloud storage region	Select or create a storage region.
Step 2b: NetBackup KMS encryption	Type **yes** if you enabled NetBackup KMS on the master server in Step 13.
Step 2c: SSL	Authentication only: Select this option, if you want to use SSL only at the time of authenticating users while they access the cloud storage. Data Transfer: Select this option, if you want to use SSL to authenticate users and transfer the data from NetBackup to the cloud storage.
Step 2d: Storage class	Select a storage class for Amazon cloud storage, such as `STANDARD` or `STANDARD - Infrequent Access`.
Step 3: Access details	Enter the access key ID and secret access key for your Amazon account.
Step 4: Configure storage bucket	Select or create a storage bucket.
Step 5a: MSDP cache diskpool	Enter a name for the MSDP cache diskpool.
Step 5b: MSDP cache storage unit	Enter a name for the MSDP cache storage unit.

- Amazon GovCloud

Step 1: Cloud storage provider	Select Amazon GovCloud
Step 2a: Cloud storage region	Select or create a storage region.

Step 2b: NetBackup KMS encryption	Type **yes** if you enabled NetBackup KMS on the master server in Step 13.
Step 2c: SSL	Authentication only: Select this option, if you want to use SSL only at the time of authenticating users while they access the cloud storage. Data Transfer: Select this option, if you want to use SSL to authenticate users and transfer the data from NetBackup to the cloud storage.
Step 3a: Credentials broker	Select whether to use a credentials broker or standard access details.
Step 3b: Credentials broker information	Enter the credentials broker details. Ensure that the necessary Certificate and Private key files reside at the `db/cloud` location on the NetBackup master server. ■ UNIX: `/usr/openv/netbackup/db/cloud` ■ Windows: `install_dir\NetBackup\db\cloud` ■ Appliance master: See "Deploying certificates for a credentials broker when the master server is an appliance" on page 85.
Step 3b: Access details	Enter the access key ID and secret access key for your Amazon account.
Step 4: Configure storage bucket	Select or create a storage bucket.
Step 5a: MSDP cache diskpool	Enter a name for the MSDP cache diskpool.
Step 5b: MSDP cache storage unit	Enter a name for the MSDP cache storage unit.

- Microsoft Azure and Azure Government

Step 1: Cloud storage provider	Select Microsoft Azure.
Step 2a: Blob service endpoint	Select a blob service endpoint.

Step 2b: NetBackup KMS encryption	Type **yes** if you enabled NetBackup KMS on the master server in Step 13.
Step 2c: SSL	Authentication only: Select this option, if you want to use SSL only at the time of authenticating users while they access the cloud storage. Data Transfer: Select this option, if you want to use SSL to authenticate users and transfer the data from NetBackup to the cloud storage.
Step 3: Access details	Enter the storage account and access key ID for your Azure account.
Step 4: Configure container	Select or create a container.
Step 5a: MSDP cache diskpool	Enter a name for the MSDP cache diskpool.
Step 5b: MSDP cache storage unit	Enter a name for the MSDP cache storage unit.

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

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

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

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

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

See "About NIC1 (eth0) port usage on NetBackup appliances" on page 87.

21 After all appliances are configured and operational, you are ready to install client software on the computers that you want to back up.

See "Downloading NetBackup client packages to a client from a NetBackup appliance" on page 88.

See "Installing NetBackup client software through CIFS and NFS shares" on page 92.

Deploying certificates for a credentials broker when the master server is an appliance

To use a credentials broker to authenticate with your cloud provider, you need to deploy certificate files on the NetBackup master server before you can configure the NetBackup CloudCatalyst Appliance. If the master server is an appliance, you need to deploy these certificates using a NetBackupCLI user account.

To deploy certificates on an appliance master server

1 Gather the client certificate, CA certificate, and client key into the same directory. In this example, the file names are as follows:

```
client.pem
cacert.pem
client-key.pem
```

2 Use the following `scp` command to copy the PEM files to the appliance master server:

```
scp *.pem <NetBackupCLI_user>@master123.example.com:/home/nbusers
```

Where *<NetBackupCLI_user>* is the user name of the NetBackupCLI user.

3 Use SSH to log onto the appliance as the NetBackupCLI user.

4 Type the following command to append the CA certificate to the NetBackup cloud store CA certificate bundle:

```
nbcldutil appendcert -sourceCert cacert.pem
```

5 Type the following commands to copy the client certificate and the client key to the default NetBackup cloud directory (`/usr/openv/netbackup/db/cloud`):

```
nbcldutil copycert -sourcecert client.pem
```

```
nbcldutil copycert -sourcecert client-key.pem
```

Chapter 3

Post configuration procedures

This chapter includes the following topics:

- About NIC1 (eth0) port usage on NetBackup appliances
- Downloading NetBackup client packages to a client from a NetBackup appliance
- Downloading the NetBackup Administration Console to a Windows computer from a NetBackup appliance
- Installing NetBackup client software through CIFS and NFS shares

About NIC1 (eth0) port usage on NetBackup appliances

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

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

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

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

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

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

Downloading NetBackup client packages to a client from a NetBackup appliance

You can download NetBackup client software from a NetBackup appliance to any client that you want to back up. The NetBackup Appliance Web Console logon page provides a **Download Packages** section to download the client packages.

The packages are listed by operating system type in a drop-down box as follows:

- All
- Windows
- Linux
- Solaris
- AIX
- HP
- BSD
- Mac OS

- VMware vCenter Plug-in

Note: If you download Linux, UNIX, Solaris, AIX, or BSD packages, Veritas recommends GNU tar version 1.16 or higher to extract the .tar packages.

For more information, see the following Technote on the Veritas Support website:

https://www.veritas.com/docs/TECH154080

In addition to the downloading instructions, this procedure also includes the steps to extract and install the downloaded files on to the client.

To download NetBackup client packages from a NetBackup appliance to a client

1. Log in to the client that you want to back up.
2. Open a browser window and enter the appliance URL.
3. In the middle of the landing page, in the section **Download Packages**, click on the drop-down box to see the list of packages.
4. Right-click the selected package and specify the location to download it onto the client.

   Example locations are as follows:

   - On Windows platforms, download the package to `C:\temp` or to the desktop.
     To determine the type of hardware on your Windows system, right-click **My Computer** and select **Properties**.
   - On Linux or UNIX platforms, download the package to `/tmp`.

   Note: If the message **No packages found** appears after you make a selection, that client package is not currently installed on the appliance. This situation is most likely to occur if the appliance has been re-imaged from the USB flash drive. To download and install client packages on to the appliance, see the *NetBackup Appliance Administrator's Guide*. In the chapter "Managing a NetBackup Appliance from the NetBackup Appliance Web Console", refer to the topic "Uploading NetBackup appliance software release updates or client packages using a manual download method".

   ---

5. Unzip or untar the package.
6. Install the client software as follows:

   - Windows systems
     Click the **setup.exe** file.

- UNIX systems
  Run the `.install` script.

7 After you have successfully installed the client software, add the appliance master server name to the client as follows:

Windows systems

- After NetBackup has been installed on the client, open the Backup, Archive, and Restore interface.
  Start > All Programs > 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 master server and click **OK**.
- Close the Backup, Archive, and Restore interface.
- Restart the NetBackup Client Services by opening a Windows Command prompt. Then, enter `services.msc` and press **Enter**.

UNIX systems

- On the client, navigate to the following location:
  `cd /usr/openv/netbackup`
- Enter `ls` to see the contents of the directory.
- Open the `bp.conf` file in a text editor.
- Enter the fully qualified host name of the appliance master server.
- Save the changes and close the file.

See "Installing NetBackup client software through CIFS and NFS shares" on page 92.

See "Downloading the NetBackup Administration Console to a Windows computer from a NetBackup appliance" on page 91.

Downloading the NetBackup Administration Console to a Windows computer from a NetBackup appliance

You can download the NetBackup Administration Console software from a NetBackup appliance to a Windows computer that you want to use to access the appliance. The Windows computer does not require NetBackup installation to use the administration console. The logon page of the NetBackup Appliance Web Console provides a **Download Packages** section to download the NetBackup Administration Console package.

In addition to the downloading instructions, this procedure also includes the steps to extract and install the downloaded files on to the client.

To download the NetBackup Administration Console package from a NetBackup appliance appliance to a Windows computer

1. Log into the Windows computer that you want to use for appliance access.
2. Open a browser window and enter the appliance URL.
3. In the middle of the landing page, in the section **Download Packages**, click on the drop-down box and select **Windows**.
4. When the package file name appears under the drop-down box, right-click on it and select either **Download Linked File** or **Download Linked File As**, then specify the location to download the package onto the Windows computer.

   For example, download the package to `C:\temp` or to the desktop.
5. Unzip the package.
6. Install the administration console software as follows:
   - On the client, navigate to the `Addons/JavaInstallFiles` directory.
   - Click on the **setup.exe** file.

See “Downloading NetBackup client packages to a client from a NetBackup appliance” on page 88.

See “Installing NetBackup client software through CIFS and NFS shares” on page 92.

Installing NetBackup client software through CIFS and NFS shares

After all appliance configuration has been completed, you can use the following procedures to install NetBackup client software on the Windows and UNIX clients that are used with your NetBackup appliance. These procedures describe how to install the client software through a CIFS or an NFS share.

Note: Before the installation, make sure that you have downloaded the NetBackup client software package to the appliance and it exists on the NFS or CIFS share for client installation.

The shares for client installation are as follows:

NFS: `<appliance-name>:/inst/client`

CIFS: `\\<appliance-name>\install`

NetBackup Windows client software installation through a CIFS share

To install NetBackup client software on a Windows client through a CIFS share

1. On the appliance where the client software resides, log on to the NetBackup Appliance Shell Menu with your administrator credentials.
2. Open the CIFS share using the following command:

   ```
   Main > Settings > Share ClientInstall Open
   ```

3. On the Windows client computer where you want to install the NetBackup client software, log on as the administrator.
4. Open a map or a directory to the following CIFS shared folder on the appliance:

   `\\<appliance_name>\install`

5. Click on the Windows executable, **quickinstall.exe**.

   This action installs the NetBackup client software and adds the appliance master server name on the client.

6. On the appliance, close the shared directory using the following command:

   ```
   Main > Settings > Share ClientInstall Close
   ```

NetBackup UNIX client software installation through an NFS share

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

1. Log on to the master appliance from the NetBackup Appliance Shell Menu with your administrator credentials.
2. Add the client host names to the additional servers list of the master server appliance using the following command:

   ```
   Main > Settings > NetBackup AdditionalServers Add
   ```

3. Open the NFS share using the following command:

   ```
   Main > 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_8.1_CLIENTS2 and/or NetBackup_8.1_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:

```
MASTERSERVER=master123.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 master 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 88.

See "Downloading the NetBackup Administration Console to a Windows computer from a NetBackup appliance" on page 91.

Index

Symbols

52xx master server appliance
    initial configuration from NetBackup Appliance Shell Menu 49
    reconfigure from USB and NetBackup Appliance Shell Menu 49
52xx media server appliance
    initial configuration from NetBackup Appliance Shell Menu 60

A

about
    appliance configuration guidelines 6
appliance configuration
    about guidelines 6
appliance media server
    configure master server to communicate with 58
appliance roles
    for NetBackup 52xx 11
appliance system
    configuration sequence 10

C

CIFS and NFS shares
    install NetBackup client software 92
CloudCatalyst
    configure 72
    credentials broker 85
command limitations
    appliances not configured 12
configuration
    of maximum transmission unit size 30
configuration sequence
    for appliance systems 10
configure 52xx appliance
    from NetBackup Appliance Web Console 32
configure master server
    to communicate with appliance media server 58

D

download NetBackup client packages from NetBackup appliance 88

G

guidelines
    appliance configuration 6

I

initial configuration
    52xx appliance from NetBackup Appliance Web Console 32
initial configuration checklist
    about NetBackup 52xx 25
    NetBackup appliance 26
initial configuration of 52xx master server appliance
    from NetBackup Appliance Shell Menu 49
initial configuration of 52xx media server appliance
    from NetBackup Appliance Shell Menu 60
initial configuration pages
    NetBackup Appliance Web Console 14
IPv4 and IPv6 support 12

M

maximum transmission unit size
    about configuration for 30

N

NetBackup 52xx initial configuration checklist
    about 25
NetBackup Adminstration Console
    download to Windows computer from NetBackup appliance 91
NetBackup appliance
    initial configuration checklist 26
NetBackup Appliance Web Console
    initial configuration pages 14
NetBackup appliances
    NIC1 (eth0) port usage 87

NetBackup client packages
download from NetBackup appliance 88
NetBackup client software
install using CIFS and NFS shares 92
NIC1 (eth0) port usage
on NetBackup appliances 87

R

reconfiguration of 52xx master server appliance
from USB and NetBackup Appliance Shell Menu 49

S

sequence
for appliance system configuration 10