

Veritas NetBackup™ 53xx Appliance Initial Configuration Guide

Release 3.1.2

Document revision 1

Veritas NetBackup™ 53xx Appliance Initial Configuration Guide

Legal Notice

Copyright © 2019 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

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	5
	Guidelines for NetBackup 53xx initial configuration	5
	Command limitations on appliances that are not configured	12
	About IPv4-IPv6-based network support	13
	Overview of the initial configuration pages in the NetBackup Appliance	
	Web Console	14
	About the NetBackup appliance initial configuration checklist	24
	NetBackup appliance initial configuration checklist	25
	About configuring the maximum transmission unit size	29
Chapter 2	Initial configuration procedures	30
	Configuring a master server to communicate with an appliance media	
	server	30
	Performing the initial configuration on NetBackup 53xx series	
	appliances from the NetBackup Appliance Web Console	33
	Performing the initial configuration on a NetBackup 53xx series	
	appliance from the NetBackup Appliance Shell Menu	49
	Configuring a NetBackup 53xx high availability setup	62
	Performing the initial configuration on the partner node for a NetBackup	
	53xx high availability configuration	67
	Adding the partner node to the NetBackup 53xx high availability	
	configuration	75
Chapter 3	Post configuration procedures	82
	About NIC1 (eth0) port usage on NetBackup appliances	82
	Downloading NetBackup client packages to a client from a NetBackup	
	appliance	83
	Installing NetBackup client software through an NFS share	85
Index		89

Preparing for initial configuration

This chapter includes the following topics:

- [Guidelines for NetBackup 53xx initial configuration](#)
- [About IPv4-IPv6-based network support](#)
- [Overview of the initial configuration pages in the NetBackup Appliance Web Console](#)
- [About the NetBackup appliance initial configuration checklist](#)
- [About configuring the maximum transmission unit size](#)

Guidelines for NetBackup 53xx initial configuration

Review the following guidelines before you perform the initial configuration on a new 53xx appliance:

Table 1-1 NetBackup 53xx appliance configuration guidelines

Parameter	Description
Connectivity during initial configuration	<p>When you perform the appliance initial configuration, you must take precautions to avoid loss of connectivity. Any loss of connectivity during initial configuration results in failure.</p> <p>The computer that you use to configure the appliance should be set up to avoid the following events:</p> <ul style="list-style-type: none"> ■ 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
Required names and addresses	<p>Before the configuration, gather the following information:</p> <ul style="list-style-type: none"> ■ Network IP addresses, netmask, and gateway IP addresses for the appliance ■ Network names for all appliances ■ DNS or host information <p>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.</p> <p>Note: The Domain Name Suffix is appended to the host name and cannot be changed after the initial configuration is completed. If you need to change the suffix or move the appliance to a different domain at a later time, you must perform a factory reset first, and then perform the initial configuration again.</p> <ul style="list-style-type: none"> ■ Names for NetBackup storage units <p>The Storage Name fields appear only when you configure the appliance as a media server. You can change the default names or leave them.</p> <p>Note: Only the storage unit name can be customized during the media server role configuration.</p> <p>The default values that appear in the NetBackup Administration Console for the storage units and disk pools are as follows:</p> <ul style="list-style-type: none"> ■ For the AdvancedDisk: <ul style="list-style-type: none"> Default storage unit name: stu_adv_<hostname> Default disk pool name: dp_adv_<hostname> ■ For the NetBackup Deduplication: <ul style="list-style-type: none"> Default storage unit name: stu_disk_<hostname> Default disk pool name: dp_disk_<hostname> <p>Note: The short host name for the appliance always appears in the default storage unit and disk pool names.</p>

Table 1-1 NetBackup 53xx appliance configuration guidelines (*continued*)

Parameter	Description
Default user name and password	<p>New NetBackup appliances are shipped with the following default log-in credentials:</p> <ul style="list-style-type: none"> ■ User name: admin ■ Password: P@ssw0rd <p>Note: When you perform the initial configuration, you are not required to change the default password. However, to increase the security of your environment Veritas recommends that you change the default password immediately. As a best practice, the password should be changed periodically. Make sure to keep a record of the current password in a secure location.</p>
Default Maintenance user password	<p>The appliance comes configured with a known default password for the <code>Maintenance</code> 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 <code>Maintenance</code> user password to Veritas Technical Support in the event that the appliance requires troubleshooting services.</p> <p>Each initial configuration procedure includes a step that describes how to change the default <code>maintenance user password</code>.</p>
Firewall port usage	<p>Make sure that the following ports are open on any firewall that exists between a master server and a media server:</p> <ul style="list-style-type: none"> ■ 13724 (<code>vnetd</code>) ■ 13720 (<code>bprd</code>) ■ 1556 (<code>PBX</code>) <p>For more information about firewall ports for NetBackup and the NetBackup appliance, see the following tech note on the Veritas Support website:</p> <p>https://www.veritas.com/support/en_US/article.TECH178855</p>

Table 1-1 NetBackup 53xx appliance configuration guidelines (*continued*)

Parameter	Description
Media server role	<p>The NetBackup 53xx series appliances can only be configured as a media server.</p> <p>Before you configure this 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.</p> <p>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:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>To deploy the host ID-based certificate:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>If the security certificates have been deployed on the appliance media server, you are not requested to deploy them again during the role configuration.</p> <p>For more information about security certificates, refer to the chapter Security certificates in NetBackup in the <i>NetBackup Security and Encryption Guide</i>.</p> <p>See “Configuring a master server to communicate with an appliance media server” on page 30.</p>

Table 1-1

NetBackup 53xx appliance configuration guidelines *(continued)*

Parameter	Description
High Availability	

Table 1-1 NetBackup 53xx appliance configuration guidelines (*continued*)

Parameter	Description
	<p>Starting with appliance release version 3.1, you can deploy 53xx series appliances for a high availability (HA) solution. An HA configuration uses two NetBackup 53xx appliances that are designated as a compute node and a partner node. These nodes are connected to each other and also to specific channels on the same Primary Storage Shelf.</p> <p>A NetBackup appliance HA configuration must use two identical appliances with regard to the model number, the hardware configuration, and the appliance software version as follows:</p> <ul style="list-style-type: none"> ■ Model number and hardware configuration The model number and the I/O configuration of both appliances must match. For example, use two model 5330 appliances with configuration D or two model 5340 appliances with configuration D. You cannot use one model 5330 appliance with configuration D and one model 5340 appliance with configuration D. ■ Appliance software version Both appliances must use the same software version. The appliance master server that is used must also use the same software version as the HA appliances. If a traditional (non-appliance) master server is used, it must use the NetBackup software version that is associated with the appliance software version. For example, if the HA appliances use version 3.1, the traditional NetBackup master server must use NetBackup version 8.1. <p>You can set up an HA configuration as follows:</p> <ul style="list-style-type: none"> ■ New system installations Perform the initial configuration on one NetBackup 53xx appliance (compute node), then set up the HA configuration on this same node. Next, perform the initial configuration on the other appliance (partner node). Finally, complete the HA configuration on the compute node by adding the configured partner node. ■ Existing systems The existing components must first be upgraded as follows: Master server: Traditional NetBackup (non-appliance) master servers must be upgraded to NetBackup release version 8.1 or later. NetBackup appliance master servers must be upgraded to appliance release version 3.1 or later. Media server (existing model 53xx): This appliance must be upgraded to appliance release version 3.1 or later. After these upgrades are completed, set up the HA configuration on the existing 53xx compute node. Next, perform the initial configuration on the partner node. Finally, complete the HA configuration on the compute node by adding the partner node. ■ Host name and IP address requirements In an HA setup, three host names with corresponding IP addresses are required as follows: <ul style="list-style-type: none"> ■ Physical nodes A dedicated host name and IP address must be assigned to each of the two physical media server nodes. Each host name should resolve to its corresponding IP address in the same subnet. ■ Virtual host name and IP address

Table 1-1 NetBackup 53xx appliance configuration guidelines (*continued*)

Parameter	Description
	<p>This host name and its corresponding IP address are used for the HA identity that encompasses the two physical nodes with the common attached storage. The virtual host name and IP address work as a pointer within the HA setup between the two nodes. For example, if one node is not running properly or is down for an upgrade or maintenance, the virtual host name automatically points to the node that is still operational.</p> <p>Before you configure the HA setup, all of the HA host names and IP addresses must be added to the Host Name Mappings property in the NetBackup Administration Console. This task must be performed on the associated master server. If the mappings property is not updated before the initial configuration of the physical nodes, the HA setup configuration process can fail. Starting with appliance release 3.1.2, the host name mappings also require approval.</p> <p>For complete details on adding host name mappings and approval, see the <i>NetBackup Security and Encryption Guide</i>.</p> <p>When you set up the HA configuration, the host name and the IP address of the first configured or existing media server are automatically elevated as the virtual host name and IP address for the HA configuration. You must provide a new host name and IP address for this media server at that time.</p> <p>Note: If you plan to use Active Directory (AD) authentication, do not set up the HA configuration until after you update the AD server with the host names and IP addresses of the HA configuration. The virtual host name and virtual IP address, along with the host name and IP address for each node are required on the AD server before setting up the HA configuration. Otherwise, AD users may experience problems when they access the system.</p> <p>If you plan to use a NetBackup client to manage the NetBackup jobs, add the three host names to the <code>bp.conf</code> file on the client: the host name of the two nodes and the new host name.</p>
Disk storage option licenses	<p>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 <i>NetBackup Appliance Administrator's Guide</i> for information and instructions on how to view and change a license key.</p> <p>Replace the NFR keys with permanent keys before they expire.</p>

Table 1-1 NetBackup 53xx appliance configuration guidelines (*continued*)

Parameter	Description
Optimized Share Reserve storage	<p>If you plan to use the Copilot feature, it is recommended that you create any Optimized Share Reserve during the initial configuration. An Optimized Share Reserve can also be created after the initial configuration is completed. For example, when you add an Expansion Storage Shelf to an existing or operational 53xx appliance.</p> <p>An Optimized Share Reserve can be created only as follows:</p> <ul style="list-style-type: none"> ■ The configuration must be performed through the NetBackup Appliance Shell Menu. ■ The appliance hardware configuration must include at least one Expansion Storage Shelf. ■ All storage space on the Expansion Storage Shelf must be dedicated for Optimized Share Reserve use. The minimum size for a reserve is 114 TB. ■ AdvancedDisk and MSDP partitions must reside on a different shelf. They cannot coexist on the dedicated shelf with the Optimized Share Reserve.
NetBackup version compatibility	<p>NetBackup appliance Release 3.1.2 includes NetBackup version 8.1.2.</p> <p>For this appliance media server, the associated master server and clients must use the appropriate software version as follows:</p> <ul style="list-style-type: none"> ■ Appliance master server The appliance master server that you plan to use with this appliance media server must use appliance software version 3.1.2 or later. If the appliance master server currently uses an earlier version, it must be upgraded to version 3.1.2 before you configure this appliance. ■ Traditional NetBackup master server To use this appliance media server with a traditional NetBackup master server, the master server must use NetBackup version 8.1.2 or later. If the NetBackup master server currently uses an earlier version, it must first be upgraded to version 8.1.2 before you configure this appliance. ■ Clients 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 8.1.2 can only be used with an appliance server with version 3.1.2 or earlier. Client add-ons must also be the same version as the client version.

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:

- 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.
- 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*.

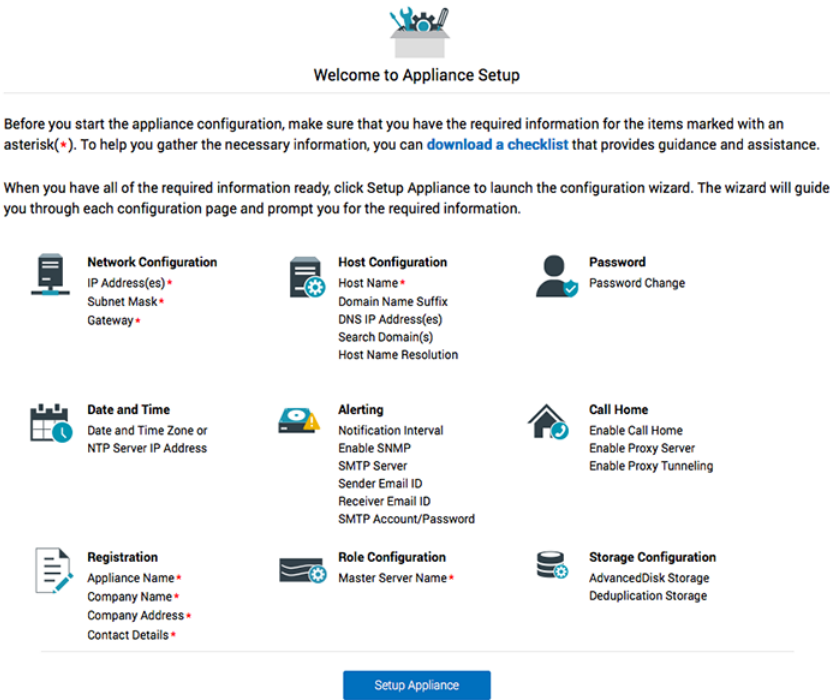
Overview of the initial configuration pages in the NetBackup Appliance Web Console

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

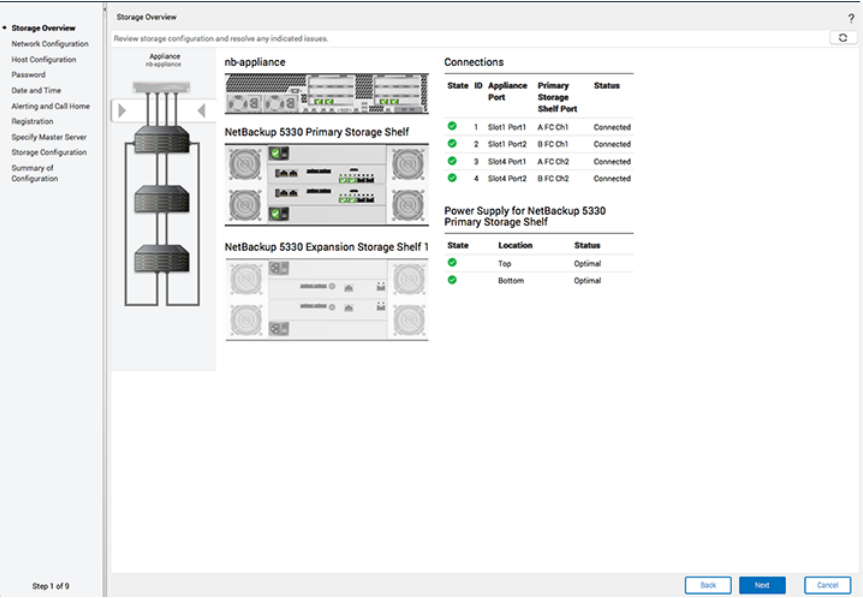


Note: This page provides a link to download a checklist that provides descriptions for all of the data entry fields on all pages in the initial configuration. Before you begin the initial configuration, Veritas recommends that you click on the **download a checklist** link, print the file, and record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

Storage Overview

This page shows the current status of all system hardware components. This page identifies any component cabling problems between the appliance server and the Primary Storage Shelf or the Expansion Storage Shelf. Disk drive problems are also identified if any exist.

Figure 1-2 Storage Overview page for the 5330 appliance



The following shows the status that is displayed for the Fibre Channel (FC) connections between a NetBackup 5340 compute node and the Primary Storage Shelf.

Figure 1-3 Storage overview page for the 5340 appliance

Storage Connections

nbapp111.engba.veritas.com

Connections: Compute node to Primary shelf

State	ID	Compute node	Primary shelf	Status
	1	Slot1 Port1	A FC Ch1	Disconnected
	2	Slot1 Port2	B FC Ch1	Connected
	3	Slot4 Port1	A FC Ch2	Connected
	4	Slot4 Port2	B FC Ch2	Connected

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 1-4 Network Configuration page

Network Configuration

Network Settings

Update or add the Network and Routing configurations for this appliance.

Interface Properties Routing Properties

Total	View Details	Edit	Delete	Filter by Network Interface				
Network Interface	Description	IP Address (IPv4)	Subnet Mask	Speed	Cable State	Link State	Link Aggregation	Reserved
<input type="checkbox"/>	eth0	192.168.229.2...	255.255.255.0	10G/s	UNPLUGGED	UP		Yes
<input type="checkbox"/>	eth1	10.132.0.185	255.255.248.0	10G/s	PLUGGED	UP		No
<input type="checkbox"/>	eth2			10G/s	UNPLUGGED	UP		No
<input type="checkbox"/>	eth3			10G/s	UNPLUGGED	UP		No
<input type="checkbox"/>	eth4			100G/s	PLUGGED	UP		No
<input type="checkbox"/>	eth5			100G/s	PLUGGED	UP		No

Network Configuration:

Create Bond

Tag VLAN

Add Static Route

Step 2 of 9

BackNextCancel

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 1-5 Host Configuration page

Storage Overview

Network Configuration

Host Configuration

Password

Date and Time

Alerting and Call Home

Registration

Specify Master Server

Storage Configuration

Summary of Configuration

?

The host name that you specify here is applied to this appliance. See the Help (?) for exceptions when using the Fully Qualified Domain Name. After you finish configuring the appliance, you cannot change the host name until you perform a factory reset on the appliance.

Host Name*

Short name or Fully Qualified Domain Name (FQDN) allowed

For systems that use DNS, complete the Domain Name System section. For systems that do not use DNS, complete the Host Name Resolution section.

Domain Name System

For systems that use DNS

Domain Name Suffix

engba.veritas.com

DNS IP Address(es)

172.16.8.2

Search Domain(s)

engba.veritas.com

engba.symantec.com

Host Name Resolution

For systems that do not use DNS

IP Address

10.132.0.186

Fully qualified host name

nbapp537.engba.verita

Short host name

nbapp537

To edit the hosts file manually click [here](#).

Back

Next

Cancel

Step 3 of 9

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 1-6 Password change page

✓ Storage Overview

✓ Network Configuration

✓ Host Configuration

• Password

Date and Time

Alerting and Call Home

Registration

Specify Master Server

Storage Configuration

Summary of Configuration

Step 4 of 9

BackNextCancel

?

Old admin password:

New admin password:

Confirm new admin password:

Please review the password policy before setting the new password:

• Passwords must contain at least eight characters.

• Passwords must contain at least one lower case letter (a-z) and one number (0-9).

• 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.

Click the help icon ? for more information.

• Password change is not mandatory but strongly recommended. Click Next, if you want the password to remain the same.

Date & Time

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

Figure 1-7 Date & Time page

✓ Storage Overview

✓ Network Configuration

✓ Host Configuration

✓ Password

• **Date and Time**

Alerting and Call Home

Registration

Specify Master Server

Storage Configuration

Summary of Configuration

Date & Time

?

Configure time zone, date and time for this appliance

Select the time zone, then manually specify the date and time or synchronize with one or more NTP servers. After setting the date and time or synchronizing with NTP server(s), the current login session may time out. In such a case, you must log back in to the appliance.

The use of NTP servers to synchronize NetBackup servers is strongly encouraged.

Select Time zone

Los Angeles

Set Date and Time

☒ Use NTP server date and time settings

Server IP or Host name

☐ Specify date and time

Date: June 2016

S	M	T	W	T	F	S
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Time: 07:58:52 (hh:mm:ss)

BackNextCancel

Step 5 of 9

Alerting and Call Home

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

Figure 1-8 Alerting and Call Home page

✓ Storage Overview

✓ Network Configuration

✓ Host Configuration

✓ Password

✓ Date and Time

• Alerting and Call Home

Registration

Specify Master Server

Storage Configuration

Summary of Configuration

Alerting and Call Home

To configure the SMTP and SNMP settings use the Alert Configuration section. To apply Proxy Settings for the Call Home functionality use the Call Home Configuration section.

Alert Configuration

This field is applicable for configuring the SNMP settings and SMTP settings. The notification interval cannot be set to 0 (zero) and should be in multiples of 15.

Notification Interval: 1440 (in minutes)

SNMP Server Configuration

☐ Enable SNMP Alert


SNMP Server:

SNMP Port: 162

SNMP Community: public

To set up the appliance SNMP manager to receive hardware monitoring related traps, click the following link and copy the contents of the MIB file.

[View SNMP-MIB file](#)

Click the help icon  for more information.

SMTP Server Configuration

SMTP Server:

Software Administrator Email:

Hardware Administrator Email:

Sender Email:

SMTP Account:

Password:

To enter multiple email addresses, separate each address with a semicolon (;).

Call Home Configuration

The appliance can communicate with the Veritas Call Home server and upload hardware and software information. [Read privacy policy](#)

☒ Enable Call Home

☐ Enable Proxy Server

☒ Enable Proxy Tunneling

Proxy Server:

Proxy Port:

Proxy Username:

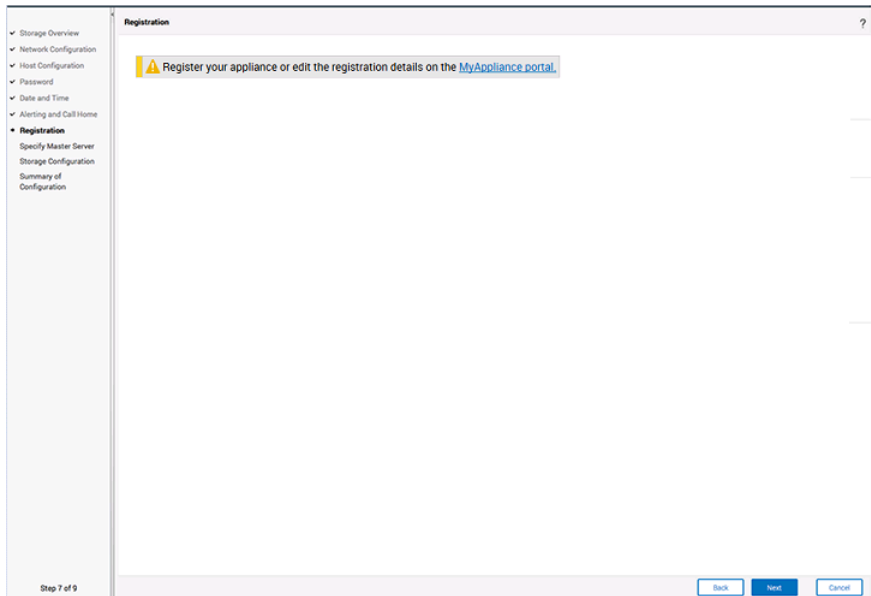
Proxy Password:

Step 5 of 9

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.

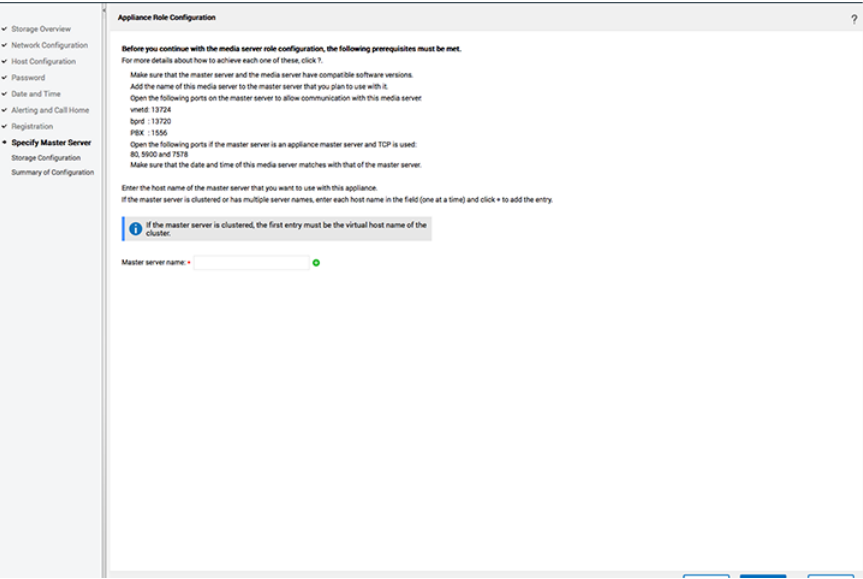
Figure 1-9 Registration page



Specify Master Server

This page is used to identify the master server that you want to use with this media server. Before you select the master server, you must first add the name of this appliance media server to server list on the master server.

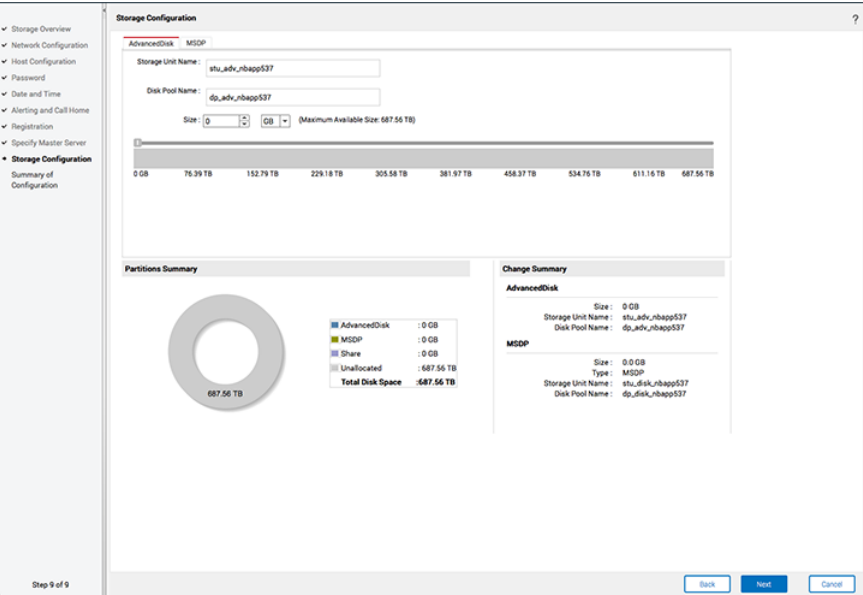
Figure 1-10 Specify Master Server page



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

Storage Configuration

Type: **MSDP**

Storage Unit Name:

Disk Pool Name:

Size: GB (Maximum Available Size: 687.56 TB)

An MSDP Catalog partition of size 32.74 TB will be created on the Meta disks.

0 GB 76.39 TB 152.79 TB 229.18 TB 305.58 TB 381.97 TB 458.37 TB 534.76 TB 611.16 TB 687.56 TB

Partitions Summary

AdvancedDisk	: 0 GB
MSDP	: 0 GB
Share	: 0 GB
Unallocated	: 687.56 TB
Total Disk Space	: 687.56 TB

Change Summary

AdvancedDisk

Size: 0 GB
Storage Unit Name: stu_disk_nbapp537
Disk Pool Name: dp_disk_nbapp537

MSDP

Size: 0 GB
Type: MSDP
Storage Unit Name: stu_disk_nbapp537
Disk Pool Name: dp_disk_nbapp537

Step 9 of 9

[Back](#) [Next](#) [Cancel](#)

About the NetBackup 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 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**.

- Online
To obtain a PDF file of the latest version of this checklist, see the following link:
https://www.veritas.com/support/en_US/article.000100480

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 1-2 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 1-3 Network Configuration - Create Bond

Field	Setting
Network Interface	
Bond Mode	
IP Address	
Subnet Mask	

Table 1-4 Network Configuration - Tag VLAN

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

Table 1-5 Network Configuration - Add Static Route

Field	Setting
Destination IP	
Destination Subnet Mask	
Gateway	
Network Interface	

Table 1-6 Host Configuration

Field	Setting
Host Name	
Domain Name System (DNS)	DNS: <div> <div>■ Domain Name Suffix</div> <div>■ DNS IP Address</div> <div>■ Search Domain(s)</div> </div> <div> <div>■ _____</div> <div>■ _____</div> <div>■ _____</div> </div>

Table 1-6 Host Configuration (continued)

Field	Setting
Host Name Resolution (no DNS)	No DNS:
<ul style="list-style-type: none"> IP address Fully qualified host name Short host name 	<ul style="list-style-type: none">

Table 1-7 Password change

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

Table 1-8 Date and time configuration

Field	Setting
Time zone	
NTP Server IP	
Date and Time	

Table 1-9 Alerting Configuration

Field	Setting
Notification Interval (in 15-minute intervals)	
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	

Table 1-9 Alerting Configuration (*continued*)

Field	Setting
Sender email address	
SMTP account	
Password	

Table 1-10 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 1-11 AdvancedDisk storage configuration

Field	Setting
Storage Unit name	
Disk Pool Name	
Size	

Table 1-12 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*.

Initial configuration procedures

This chapter includes the following topics:

- [Configuring a master server to communicate with an appliance media server](#)
- [Performing the initial configuration on NetBackup 53xx series appliances from the NetBackup Appliance Web Console](#)
- [Performing the initial configuration on a NetBackup 53xx series appliance from the NetBackup Appliance Shell Menu](#)
- [Configuring a NetBackup 53xx high availability setup](#)
- [Performing the initial configuration on the partner node for a NetBackup 53xx high availability configuration](#)
- [Adding the partner node to the NetBackup 53xx high availability configuration](#)

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:
 - If the master server is a traditional (non-appliance) NetBackup master server:
- 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 NetBackup 53xx series appliances from the NetBackup Appliance Web Console”](#) on page 33.

Performing the initial configuration on NetBackup 53xx series appliances from the NetBackup Appliance Web Console

This topic describes how to configure NetBackup 53xx series appliances that are new or have been reset to the factory defaults (factory reset).

This method requires that you connect a laptop directly to appliance port **NIC1** (eth0). A NetBackup 53xx appliance can only be configured as a media server.

For high availability configurations, use this procedure to configure the 53xx appliance that you use for the setup procedure. After this appliance (compute node) is configured, see step 18 for details to continue and complete the high availability configuration.

Before you perform the initial configuration on this media server, verify that you have already performed the following tasks:

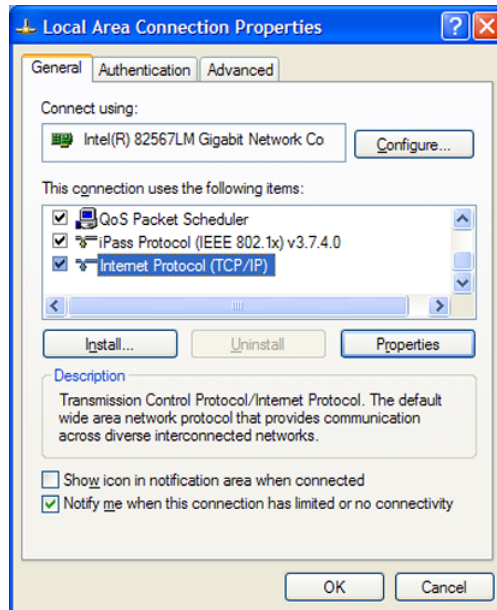
- Verified that the master server and this media server have compatible software versions.
- Added the host name of this media server to the `SERVERS` list on the master server that you plan to use with it.
For high availability configurations, added the host name of the node that you use for the setup procedure.
See [“Configuring a master server to communicate with an appliance media server”](#) on page 30.
- Opened the appropriate ports on the master server if a firewall exists between the master server and this media server.
See [“Configuring a master server to communicate with an appliance media server”](#) on page 30.
- Completed the initial configuration checklist.

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 17 in the following procedure describes how to change the `Maintenance` user password.

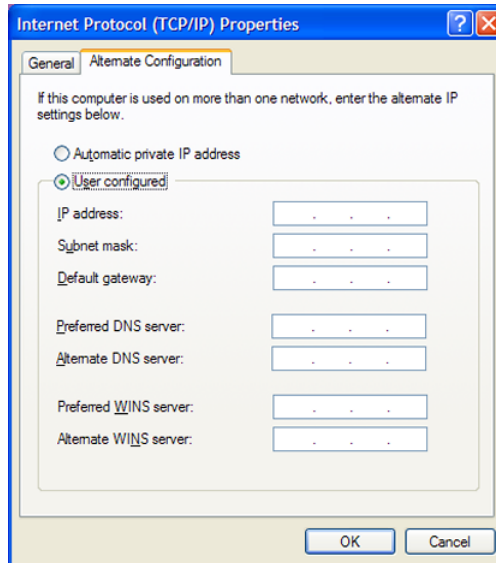
To perform the initial configuration on a NetBackup 53xx media server appliance from the NetBackup Appliance Web Console

- 1 Connect a laptop to appliance port **NIC1**. Next, 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:
- http://192.168.229.233**
- Make sure to confirm the security exception to proceed.
- 3 Log on to the appliance with the default credentials as follows:
- **User Name:** admin
 - **Password:** 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**
If you have not previously filled out the checklist in the *NetBackup 53xx Initial Configuration Guide*, click this link to access an electronic version. Veritas recommends that you first print this file, then fill it out for use as you

perform the configuration. After you have completed the initial configuration, store the checklist 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 On the **Storage Overview** page, check and verify the status of the connected hardware components.

The diagrams use specific icons to indicate whether any component cable or disk drive problems exist. The following describes the general icons that may appear:

Note: Click the help (?) icon at the top right of the page to see a complete list of icon descriptions.



OK



Warning

Indicates a problem that can be fixed later and lets you proceed with the initial configuration. However, such problems can prevent access to the affected devices. Click the icon to see a description of the problem.



Error

Indicates a critical problem that requires immediate resolution before you can proceed with the initial configuration. Click the icon to see a description of the problem.



Information

Click the icon to learn more about the specific area.

If there are no problems identified, click **Next** to start the initial configuration. Otherwise, use the following guidelines to resolve any problems:

- Click on the warning or the error icon to see a description of the problem.

- Verify that all cables are connected correctly and secured.
- Verify that all disk drives are installed and seated properly.
- Verify that all units are turned on and have booted up completely.
- Verify that you have checked all of the items on the hardware check list.
- After you have verified the previous items or made any changes, click **Refresh**. Any warning or error icons that disappear indicate that the problem has been fixed.
Veritas recommends that you resolve all problems before you start the initial configuration.

Note: If you cannot resolve any error problems after verifying all of the previous items and refreshing, stop here and contact Veritas Technical Support.

6 The **Network Configuration** page contains the following taskbars to complete specific tasks with the associated data entry fields to configure network connectivity:

- **Create Bond** - Use to create a bond between two or more network interfaces.
- **Tag VLAN** - Use to configure VLANs in your existing network environments.
- **Add Static Route** - Use to add a route configuration to your network.

Expand each taskbar to enter the relevant network configuration information. These functions are independent of each other and do not require configuration in the order in which they appear.

Note: 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.

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

Create Bond data entry fields

■ Network Interface

Click on the drop-down box and select the ethernet NIC port to use for a network connection.

■ 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

Enter the IP address for this appliance server.

■ 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 bond 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 from 1 to 4094 for the VLAN.
- **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:

Routing Configuration 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 13.
- **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 13.
- **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.

- 7 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.

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

Host Name

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

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 Domain Name Suffix is appended to the host name and cannot be changed after the initial configuration is completed. If you need to change the suffix or move the appliance to a different domain at a later time, you must perform a factory reset first, and then perform the initial configuration again.

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

- **Domain Name Suffix**
Enter the suffix name of the DNS server.
- **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 13.
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 13.
- **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**.

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

Note: To continue with the initial configuration, you are not required to change the default password. However, to increase the security of your environment Veritas recommends that you change the 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	<div>Enter the new password.</div> <div>Valid passwords must include the following:</div> <div><ul style="list-style-type: none">■ Eight or more characters■ At least one lowercase letter■ At least one number (0-9)</div> <div>Uppercase letters and special characters can be included, but they are not required.</div> <div>The following describes password restrictions:</div> <div><ul style="list-style-type: none">■ 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.</div>
Confirm new password	Re-enter the new password for confirmation.

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

- 9
- On the **Date & Time** page, enter the appropriate date and time for this appliance. The date and time for this media server must match the date and time of the associated master server.

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 an NTP server, select this option and enter the appropriate NTP **Server IP** address.

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

- 10** 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

- **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

- **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**.

- 11 On the **Registration** page, click on the link to the [MyAppliance portal](https://my.appliance.veritas.com) at <https://my.appliance.veritas.com> to register the appliance and enter your contact information.

- 12 On the **Specify Master Server** page, enter the name of the master server that you plan to use 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 the first host name or IP address in the field and click **Add**. If the master server is clustered, the first entry must be the virtual host name of the cluster.
Enter each additional host name or IP address in the same manner (one at a time), and click **Add** after each entry.

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.
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*.

Note: After you complete the role configuration, the storage initialization starts. Depending on the number of disk drives in the system, the storage initialization can take up to 46 hours to complete. As a result, appliance backup and restore performance is degraded until the storage initialization process has completed.

- 13 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.

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**.

- 14** 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.

- 15** 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.

- 16** After the configuration has completed successfully, wait about 10 minutes for the NetBackup services to start. You must then use the fully qualified host name to reconnect and log into the appliance.

- 17** 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*.

- 18 For high availability solutions, you must set up a high availability configuration on this configured appliance (compute node) before you perform the initial configuration on the partner node. To continue and complete the high availability configuration, perform the following tasks in the order as shown:

See [“Configuring a NetBackup 53xx high availability setup”](#) on page 62.

See [“Performing the initial configuration on the partner node for a NetBackup 53xx high availability configuration”](#) on page 67.

See [“Adding the partner node to the NetBackup 53xx high availability configuration”](#) on page 75.

- 19 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 83.

See [“Installing NetBackup client software through an NFS share”](#) on page 85.

Performing the initial configuration on a NetBackup 53xx series appliance from the NetBackup Appliance Shell Menu

This topic describes how to configure a NetBackup 53xx series appliance that is new or has been reset to the factory defaults (factory reset).

This method requires that you connect a laptop directly to appliance port **NIC1** (eth0). A NetBackup series 53xx appliance can only be configured as a media server.

For high availability configurations, use this procedure to configure the node that you use for the setup procedure. After this appliance (compute node) is configured, see step 17 for details to continue and complete the high availability configuration.

Before you perform the initial configuration on this media server, verify that you have already performed the following tasks:

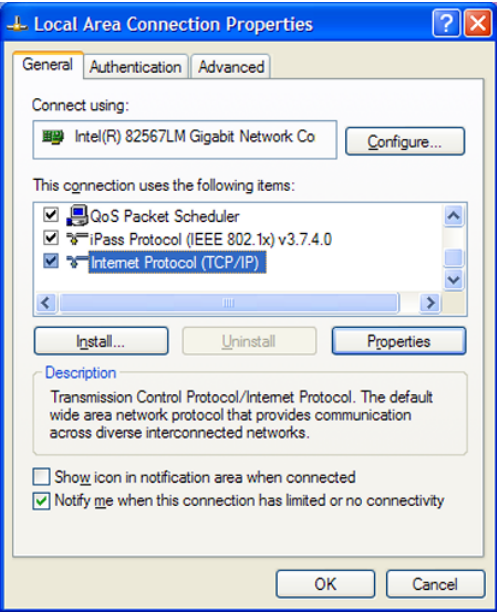
- Verified that the master server and this media server have compatible software versions.
- Added the host name of this media server to the `SERVERS` list on the master server that you plan to use with it.
For high availability configurations, added the host name of the node that you use for the setup procedure.
See “[Configuring a master server to communicate with an appliance media server](#)” on page 30.
- Opened the appropriate ports on the master server if a firewall exists between the master server and this media server.
See “[Configuring a master server to communicate with an appliance media server](#)” on page 30.
- Completed the initial configuration checklist.

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.

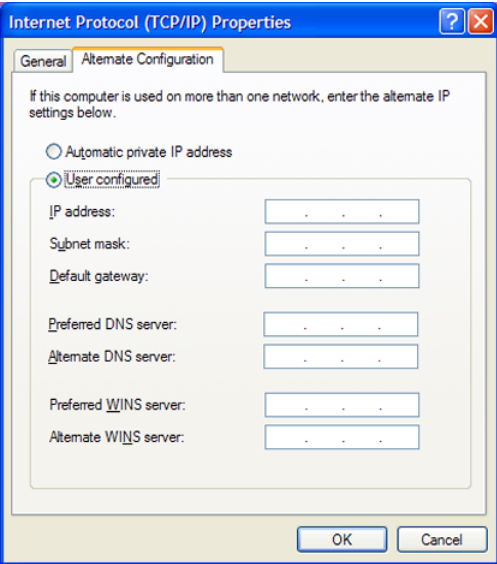
To perform the initial configuration on a NetBackup 53xx media server appliance from the NetBackup Appliance Shell Menu

- 1 Connect a laptop to appliance port `NIC1`. Next, 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`.
- 3** Log on to the appliance with the default credentials as follows:
- **User Name:** `admin`
 - **Password:** `P@ssw0rd`

A welcome message appears in the shell menu and the prompt is at the **Main_Menu** view.

Note: To continue with the initial configuration, you are not required to change the default password. However, to increase the security of your environment Veritas recommends that you change the password periodically. Make sure to keep a record of the current password in a secure location. To change the password when logged into the NetBackup Appliance Shell Menu, from the **Main_Menu** view, enter `Settings > Password`.

- 4** Before you begin the initial configuration, check and verify the status of the connected hardware components by entering the following command:

```
Support > Test Hardware
```

A **Warning** indicates a problem that can be fixed later and lets you proceed with the initial configuration. However, such problems can prevent access to the affected devices.

An **Error** indicates a critical problem that requires immediate resolution before you can proceed with the initial configuration.

If the command output identifies any problems, check the following items:

- Verify that all cables are connected correctly and secured.
- Verify that all disk drives are installed and seated properly.
- Verify that all units are turned on and have booted up completely.
- Verify that you have checked all of the items on the hardware check list.
- After you have verified the previous items, re-run the command. Any warning or error icons that disappear indicate that the problem has been fixed.

Performing the initial configuration on a NetBackup 53xx series appliance from the NetBackup Appliance Shell Menu

Veritas recommends that you resolve all problems before you start the initial configuration.

Note: If you cannot resolve any **Error** problems after verifying all of the previous items and re-running the command, stop here and contact Veritas Technical Support.

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

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

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

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

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

See [“About IPv4-IPv6-based network support”](#) on page 13.

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`.

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

Note: If you do not use DNS, you can proceed to [Step 9](#).

DNS Domain *Name*

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

- 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 13.

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

- 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.

- 9 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 13.

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

```
Hostname Set Name
```

Where *Name* is the 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 Domain Name Suffix is appended to the host name and cannot be changed after the initial configuration is completed. If you need to change the suffix or move the appliance to a different domain at a later time, you must perform a factory reset first, and then perform the initial configuration again.

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
```

- 11 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.

- To create a bond between two or more network interfaces, use the following command:

```
Network > LinkAggregation Create
```

- To tag a VLAN to a physical interface or bond interface, enter the following command:

```
Network > VLAN Tag
```

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

- 12 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 (HH:MM:SS).

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

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

Enter the SMTP server name `Email SMTP Add smtp [acct] [pass]`

Where *smtp* is the host name of the target SMTP server, *acct* is the account name for authentication to the SMTP server, and *pass* is the password for authentication to the SMTP server.

Enter email addresses `Email Software Add eaddr`

Where *eaddr* is the Email address where you want to receive failure alerts from the appliance.

To enter multiple addresses, separate each address with a semi-colon.

14 Identify the master server that you want to use with this media server.

Note: Before you continue, make sure that you have added this media server name to the master server. See [“Configuring a master server to communicate with an appliance media server”](#) on page 30.

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	<p>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.</p> <pre>Media MasterServerName</pre>
Multihomed master server	<p>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.</p> <pre>Media MasterNet1Name,MasterNet2Name</pre>
Clustered master server	<p>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.</p> <pre>Media MasterClusterName,ActiveNodeName,PassiveNodeName</pre>

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, and enter **yes**:

```
>> 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.

Note: After the role configuration completes, the storage initialization process begins. Depending on the number of disk drives in the system, storage initialization can take up to 46 hours to complete. As a result, appliance backup and restore performance is degraded until the storage initialization process has completed.

15 When the storage initialization process begins, 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 to enter a 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 (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 Deduplication (MSDP). 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.

16 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*.

- 17** For high availability solutions, you must set up a high availability configuration on this configured appliance (compute node) before you perform the initial configuration on the partner node. To continue and complete the high availability configuration, perform the following tasks in the order as shown:

See [“Configuring a NetBackup 53xx high availability setup”](#) on page 62.

See [“Performing the initial configuration on the partner node for a NetBackup 53xx high availability configuration”](#) on page 67.

See [“Adding the partner node to the NetBackup 53xx high availability configuration”](#) on page 75.

- 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 83.

See [“Installing NetBackup client software through an NFS share”](#) on page 85.

Configuring a NetBackup 53xx high availability setup

You can configure a high availability (HA) setup from either the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu.

Before you create the HA setup, review the following information:

- During this procedure, the host name and the IP address of the first configured node are elevated to become the virtual host name and IP address for the HA setup. This elevation requires that you assign a new host name and a new IP address to the first node. Before you create the HA setup, you must first add the new host name to the **Host Name Mappings** property on the associated master server.
- If you use a NetBackup client to manage the NetBackup jobs, add the following information in the `bp.conf` file on the client:
 - The virtual host name for the HA setup
 - The host name of the first node
 - The host name of the partner node
- If network bonds exist on the eth2 and eth3 ports of the first node, remove the bonds.

Caution: After the HA setup is complete, you cannot change the host name of the node until you perform a factory reset.

Note: If you are converting an existing 53xx appliance for HA, the configuration for the HA setup may fail and report the following error message: **[Error]**

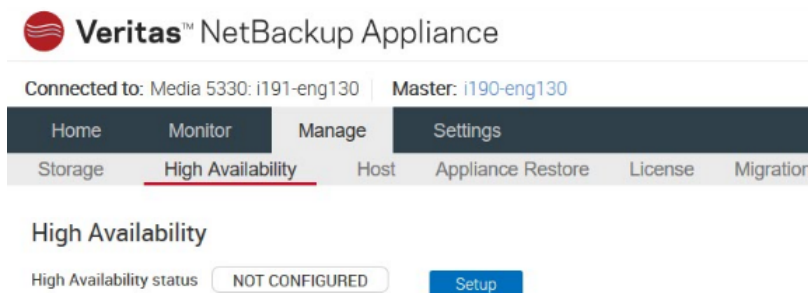
V-409-955-4011: Failed to create the MSDP disk service. Refer to the TechNote 000127738. If this problem occurs, do not refer to TechNote 000127738 which only applies to an HA setup failure with a new 53xx appliance. Instead, contact Veritas Support and inform the representative to see article 100044266 to help you resolve the issue.

To configure an HA setup from the NetBackup Appliance Web Console

- 1 On the associated master server, log in to the NetBackup Administration Console and add the new host name for the first configured node to the **Host Name Mappings** property. You must add both the short name and the fully qualified domain name (FQDN).


For details, refer to the section *Host ID to Host Name Mappings* in the *NetBackup Security and Encryption Guide*.

- 2 On the first configured node, log on to the NetBackup Appliance Web Console as `admin`.
- 3 On the **Welcome to Veritas NetBackup Appliance Web Console** page, click **Manage > High Availability**.
- 4 On the **High Availability** page, click **Setup**.



- 5 On the **High Availability > Setup** page, do the following:
 - Enter a new host name for this node.

- Enter a new IP address for this node.
- To have the new host name and IP address added to the `/etc/hosts` file, click the **Make a hosts file entry automatically** check box.
- Click **Setup**.

 Veritas™ NetBackup Appliance

Connected to: Media 5330: i191-eng130 | Master: i190-eng130

Home

Monitor

Manage

Settings

Storage

High Availability

Host


Appliance Restore

License

Migration Utility

Software Updates


High Availability ▶ Setup

 The current hostname and IP address will be elevated as the virtual hostname and virtual IP address for the high availability configuration.

Virtual hostname: i191-eng130

Virtual IP address: 10.220.130.191

Provide a new hostname and IP address for this node:

 The host name specified below is assigned to the current node. See help for exceptions when using the Fully Qualified Domain Name. After you finish the setup, you cannot change the hostname until you perform a factory reset on the node.

* New hostname: i192-eng130

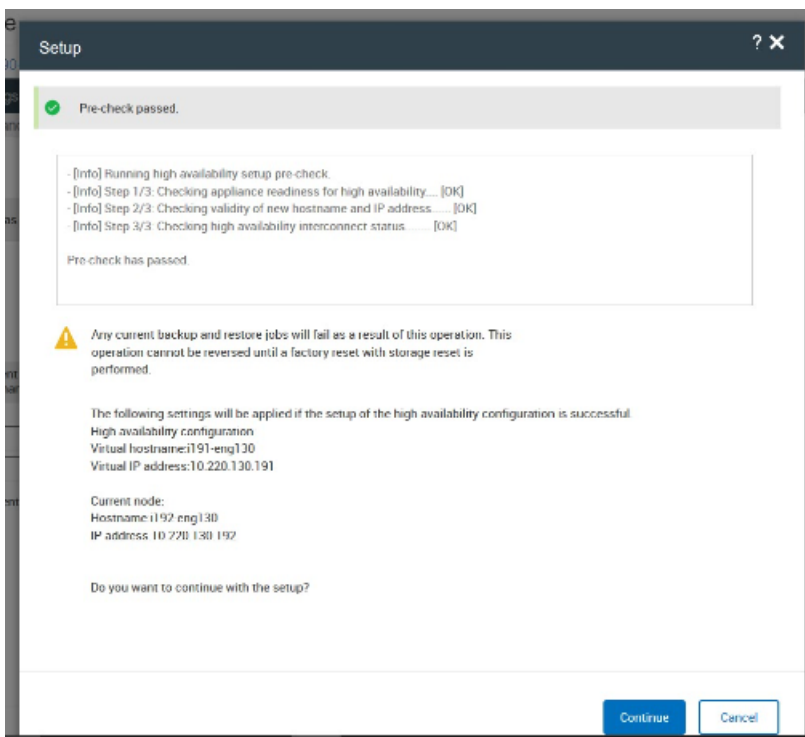
* New IP address: 10.220.130.192

☐ Make a hosts file entry automatically

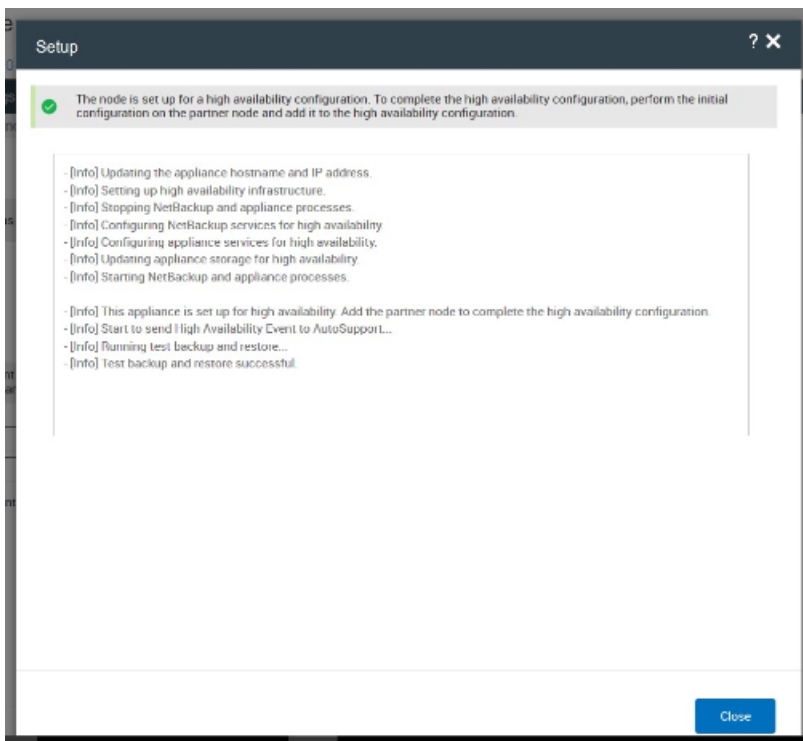
Setup

Cancel

- 6 When the **Setup** window shows that the pre-check is passed, click **Continue**.



- 7 When the **Setup** window updates and shows that the node is set up for the HA, click **Close**.



- 8 After the host name and the IP address have been changed, restart the NetBackup services on this node and on the master server to ensure that they both recognize the changes and the HA setup.

To set up a NetBackup 53xx HA configuration from the NetBackup Appliance Shell Menu

- 1 On the associated master server, log in to the NetBackup Administration Console and add the new host name for the first configured node to the **Host Name Mappings** property. You must add both the short name and the fully qualified domain name (FQDN).

For details, refer to the section *Host ID to Host Name Mappings* in the *NetBackup Security and Encryption Guide*

- 2 On the first configured node, log on to the NetBackup Appliance Shell Menu as `admin`.

Performing the initial configuration on the partner node for a NetBackup 53xx high availability configuration

- 3 Go to `Main > Manage > HighAvailability`.
- 4 Use the following command to assign the new host name and IP address to the configured node:

```
Setup NewHostname NewIPAddress
```

Where *NewHostname* is the new host name of the node, and *NewIPAddress* is the new IP address of the node.

- 5 After the host name and the IP address have been changed, restart the NetBackup services on this node and on the master server to ensure that they both recognize the changes and the HA setup.

Once the node is set up, the new network information of the node is added automatically to the additional server list on the master server.

Next steps

To complete the HA setup, perform the following procedures in the order as shown:

- Perform the initial configuration on the partner node.
See [“Performing the initial configuration on the partner node for a NetBackup 53xx high availability configuration”](#) on page 67.

- Add the partner node to the HA configuration and approve all host name mappings for the HA setup in the NetBackup Administration Console.
See [“Adding the partner node to the NetBackup 53xx high availability configuration”](#) on page 75.

All host name mappings must be approved. Otherwise, the MSDP service will not be online after a switchover. The referenced procedure includes a step that describes how to approve the host name mappings.

For additional details about host name mappings, refer to the section "Host ID to Host Name Mappings" in the *NetBackup Security and Encryption Guide*.

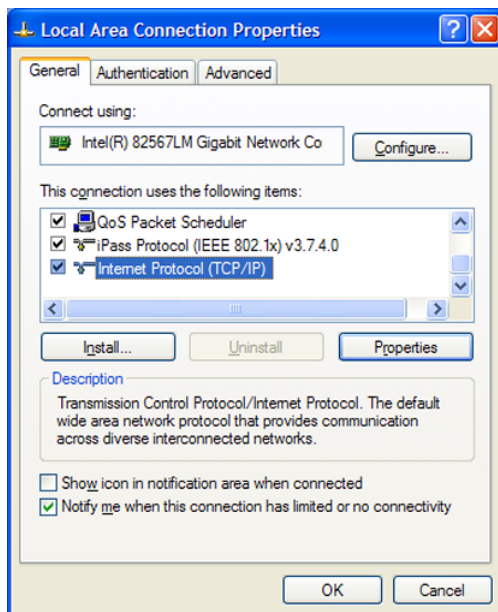
Performing the initial configuration on the partner node for a NetBackup 53xx high availability configuration

The partner node is the additional 53xx compute node used in a high availability (HA) configuration. You only need to configure the network settings and the time zone information on the partner node.

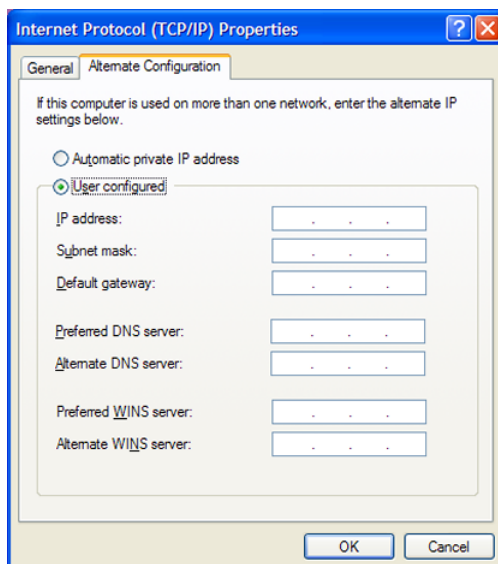
To configure the partner node

- 1 Connect a laptop to the port **NIC1** on the partner node. Next, 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** and click **OK**.
- 2** On the laptop that is connected to the partner node, open an SSH session to 192.168.229.233.
- 3** Log on to the partner node with the default credentials as follows:
- **User Name:** **admin**
 - **Password:** **P@ssw0rd**

A welcome message appears in the shell menu and the prompt is at the **Main_Menu** view.

Note: To continue with the initial configuration, you are not required to change the default password. However, to increase the security of your environment Veritas recommends that you change the password periodically. Make sure to keep a record of the current password in a secure location. To change the password when logged into the NetBackup Appliance Shell Menu, from the **Main_Menu** view, enter `Settings > Password`.

- 4** Before you begin the initial configuration, check and verify the status of the connected hardware components by entering the following command:

```
Support > Test Hardware
```

A **Warning** indicates a problem that can be fixed later and lets you proceed with the initial configuration. However, such problems can prevent access to the affected devices.

An **Error** indicates a critical problem that requires immediate resolution before you can proceed with the initial configuration.

If the command output identifies any problems, check the following items:

- Verify that all cables are connected correctly and secured.
- Verify that all disk drives are installed and seated properly.
- Verify that all units are turned on and have booted up completely.
- Verify that you have checked all of the items on the hardware check list.
- After you have verified the previous items, re-run the command. Any warning icons or error icons that disappear indicate that the problem has been fixed.

Veritas recommends that you resolve all problems before you start the initial configuration.

Note: If you cannot resolve any **Error** problems after verifying all of the previous items and re-running the command, stop here and contact Veritas Technical Support.

- 5 From the **Main_Menu > Network** view, enter the following command to configure the IP address of a single network that you want the partner node to connect to:

```
Configure IPAddress NetmaskGatewayIPAddress [[InterfaceName]]
```

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

The *IPAddress* or *GatewayIPAddress* 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 13.

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`.

- 6 From the **Main_Menu > Network** view, enter the following command to set the DNS domain name of the partner node:

Note: If you do not use DNS, you can proceed to [Step 9](#).

```
DNS Domain Name
```

Where *Name* is the domain name for the partner node.

- 7 From the **Main_Menu > Network** view, enter the following command to add the DNS name server to the configuration of the partner node:

```
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 13.

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

- 8 From the **Main_Menu > Network** view, use the following command to add a DNS search domain to the partner node configuration so that it can resolve to the host names in different domains:

```
DNS Add SearchDomain SearchDomain
```

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

- 9 This step is optional. Continue only if you want to add the IP addresses of other hosts to the `hosts` file. Otherwise, skip to the next step.

From the **Main_Menu > Network** view, enter the following command to add host entries to the `hosts` file on the partner node:

```
Hosts Add IPAddress FQHN ShortName
```

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

See [“About IPv4-IPv6-based network support”](#) on page 13.

- 10 From the **Main_Menu > Network** view, enter the following command to set the hostname for the partner node:

```
Hostname Set Name
```

Where *Name* is the short hostname or the fully qualified domain name (FQDN) of the partner node.

The hostname is applied to the entire 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 node has been factory reset and you want to import any of its previous backup images, the hostname of the node must meet one of the following rules:

- The hostname must be exactly the same as the one used before the factory reset.
- If you want to change the hostname 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 hostname to a short hostname, 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 hostname.

Note: The hostname 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 partner node. See the *NetBackup appliance Administrator's Guide* for more information.

With this step, NetBackup is re-configured to operate with the new hostname. 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 hostname 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
```

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

- 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 (HH:MM:SS).

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

Veritas recommends that you set the same date and time as the existing node in the HA configuration.

- 12 To ensure that both nodes properly communicate and detect the storage array, perform the following tasks before you add the partner node to the HA setup:

- Reboot the partner node as follows:

```
Support > Reboot
```

- On the first configured compute node, run the following command and wait for it to complete:

```
Manage > Storage > Scan
```

- On the partner node, run the following command and wait for it to complete:

```
Manage > Storage > Scan
```

- 13 Add the partner node to the HA setup.

See [“Adding the partner node to the NetBackup 53xx high availability configuration”](#) on page 75.

Adding the partner node to the NetBackup 53xx high availability configuration

Once the partner node is configured, use this procedure to complete the HA setup as follows:

- Add the partner node to the HA setup
You can add the partner node by using the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu.
- Approve the host name mappings
Starting with release 3.1.2, to complete the HA setup you must approve all host name mappings in the NetBackup Administration Console on the associated master server. If the mappings are not approved, the MSDP service will not be online after a switchover. The last step in each procedure describes how to approve the mappings.

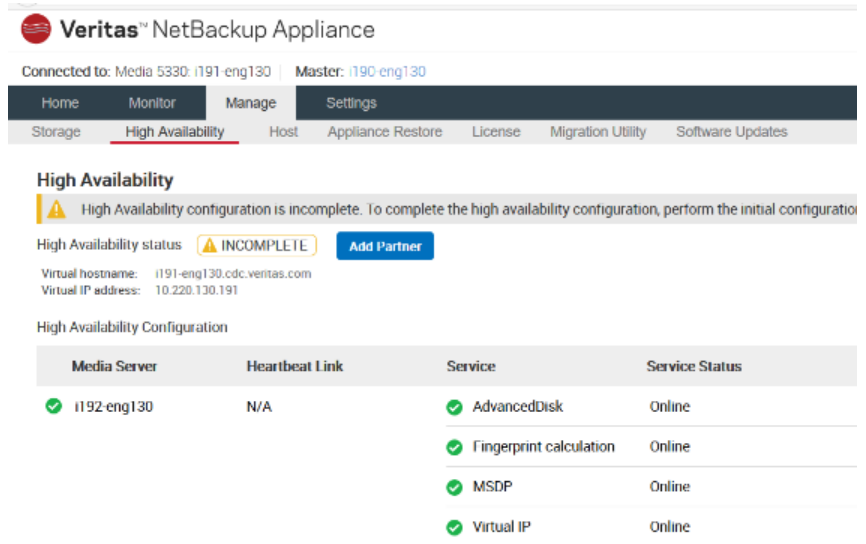
Once the partner node is added, the network information of the partner node is automatically added to the additional server list on the master server. The firmware on each node and the shared Primary Storage Shelf in the HA setup are attached with the same asset tag automatically.

Warning: Do not change the time and date settings on the two nodes once the HA setup is complete.

To add the partner node from the NetBackup Appliance Web Console

- 1 On the node that you set up the HA configuration, log on to the NetBackup Appliance Web Console as `admin`.
- 2 On the **Welcome to Veritas NetBackup Appliance Web Console** page, click **Manage > High Availability**.

- 3 On the **High Availability** page, the current status of the HA configuration is identified as incomplete. Click **Add Partner**.



Veritas™ NetBackup Appliance

Connected to: Media 5330: i191-eng130 | Master: i190-eng130

Home Monitor **Manage** Settings

Storage High Availability Host Appliance Restore License Migration Utility Software Updates

High Availability

⚠ High Availability configuration is incomplete. To complete the high availability configuration, perform the initial configuration.

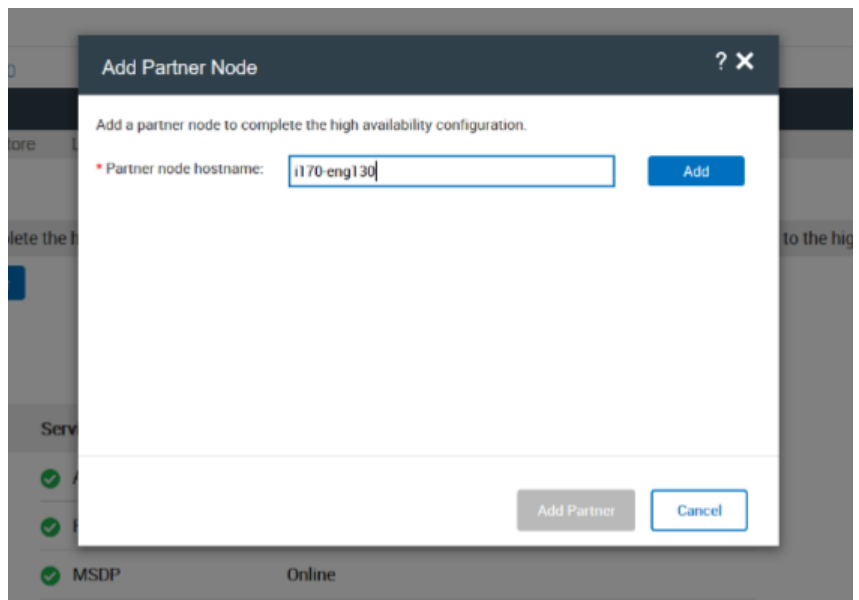
High Availability status: ⚠ INCOMPLETE [Add Partner](#)

Virtual hostname: i191-eng130.cdc.veritas.com
Virtual IP address: 10.220.130.191

High Availability Configuration

Media Server	Heartbeat Link	Service	Service Status
✓ i192-eng130	N/A	✓ AdvancedDisk	Online
		✓ Fingerprint calculation	Online
		✓ MSDP	Online
		✓ Virtual IP	Online

- 4 On the **Add Partner Node** dialog box, enter the configured hostname of the partner node and click **Add**.



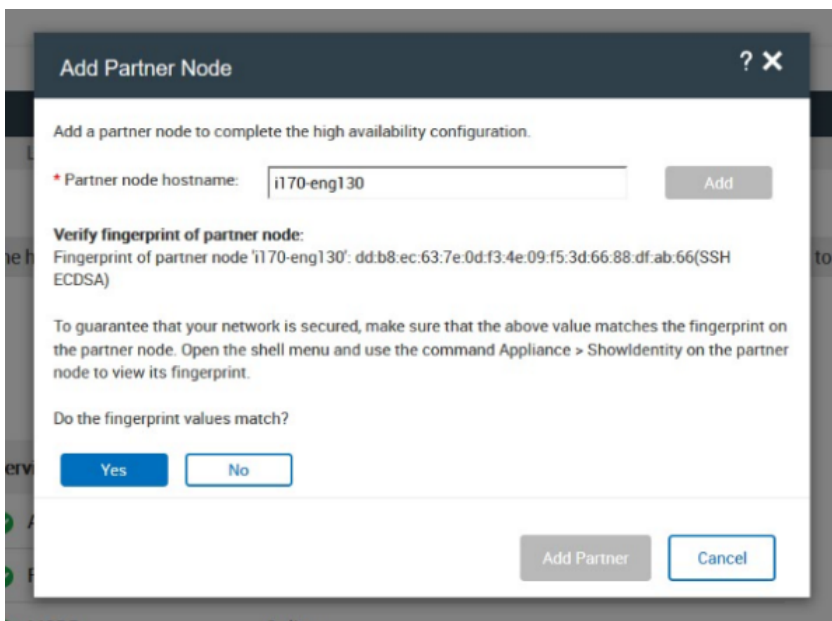
Add Partner Node ? X

Add a partner node to complete the high availability configuration.

* Partner node hostname: [Add](#)

[Add Partner](#) [Cancel](#)

- 5 If the fingerprint values match, click **Yes**.



The image shows a 'Add Partner Node' dialog box. At the top, it says 'Add a partner node to complete the high availability configuration.' Below this, there is a field for 'Partner node hostname' with the value 'i170-eng130' and an 'Add' button. A section titled 'Verify fingerprint of partner node:' displays the fingerprint 'dd:b8:ec:63:7e:0d:f3:4e:09:f5:3d:66:88:df:ab:66' for the node 'i170-eng130'. It includes instructions to verify this fingerprint on the partner node using the 'ShowIdentity' command. At the bottom, it asks 'Do the fingerprint values match?' with 'Yes' and 'No' buttons. At the very bottom right, there are 'Add Partner' and 'Cancel' buttons.

Add Partner Node ? X

Add a partner node to complete the high availability configuration.

* Partner node hostname:

Verify fingerprint of partner node:
Fingerprint of partner node 'i170-eng130': dd:b8:ec:63:7e:0d:f3:4e:09:f5:3d:66:88:df:ab:66(SSH ECDSA)

To guarantee that your network is secured, make sure that the above value matches the fingerprint on the partner node. Open the shell menu and use the command Appliance > ShowIdentity on the partner node to view its fingerprint.

Do the fingerprint values match?

- 6 Enter the password of the `admin` user for the partner node, and click **Add Partner**.

Add Partner Node ? X

Add a partner node to complete the high availability configuration.

✓ Fingerprint of the partner node is verified successfully.

* Partner node hostname: Add

* Admin user password for the partner node:

Add Partner Cancel

- 7 When the message **Do you want to continue?** appears, click **Continue**.
- 8 If the **Certificate Verification** dialog box appears, enter the authorization or the reissue token and click **Deploy Certificate**.

Certificate Verification X

The specified partner node needs to trust the host certificate from the master server to proceed.

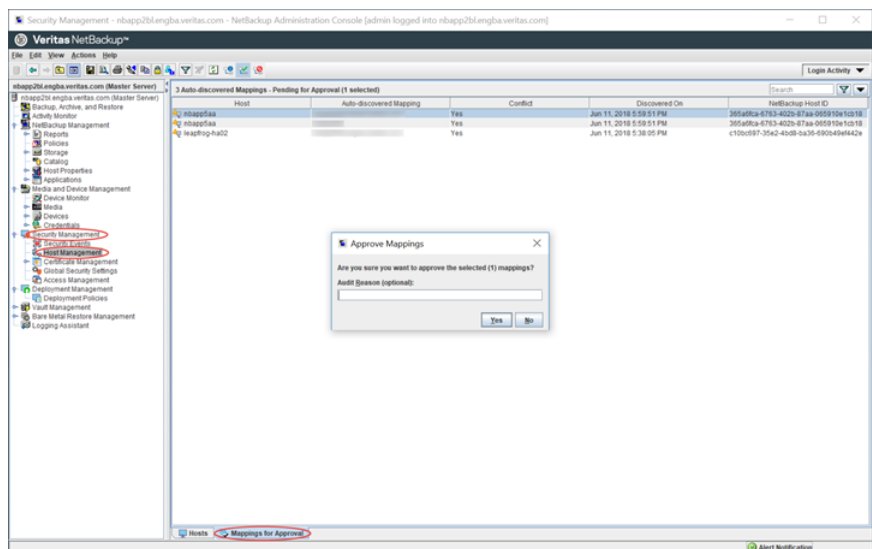
Master server name: i166-eng136
 Partner node hostname: i159-eng136

Reissue token is mandatory. Enter the reissue token for the required host to obtain a host-ID based certificate.

Enter token: *

Deploy Certificate Cancel

- 9 When a message shows that the process was successful, click **Close**.
- 10 To complete the HA setup, approve the host name mappings on the associated master server.
 - On the associated master server, log in to the NetBackup Administration Console.
 - In the left pane, click **Security Management** to expand its properties, then click **Host Management**.
 - In the lower-left of the right pane, click **Mappings for Approval**.
 - At the top of the right pane, click on any host mapping that is pending approval. When the **Approve Mappings** dialog box appears that prompts for approval, click **Yes**. Repeat this task for each host mapping that is pending approval.



To add the partner node from the NetBackup Appliance Shell Menu

- 1 On the node where you set up the HA configuration, log on to the NetBackup Appliance Shell Menu as `admin`.
- 2 Go to `Main > Manage > HighAvailability`.

- 3 Add the partner node to complete the HA configuration by entering the command:

```
AddNode hostname
```

Where *hostname* is the short host name or the fully qualified domain name (FQDN) of the partner node.

- 4 When the following message appears, make sure that you checked the SSH ECDSA fingerprint directly on the partner node:

```
Do the fingerprint values match? [yes, no] (no)
```

To guarantee that the network is safe, you need to confirm that the SSH ECDSA fingerprint of the partner node is correct. For the instructions on how to check the identity of the appliance, refer to *NetBackup Appliance Command Reference Guide*.

If the values match, enter **yes**.

- 5 After the pre-check has passed, when either of the following messages appears, enter an authority token or a reissue token to trust the host ID-based certificate:

Authorization token is mandatory. Enter an authorization token.
For more information about the authorization token, refer to the NetBackup Security and Encryption Guide.

Enter token:

or

Reissue token is mandatory. Enter the reissue token for the required host to obtain a host-ID based certificate. For more information about the reissue token, refer to the NetBackup Security and Encryption Guide.

Enter token:

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

- 6 When the following message appears, enter **yes** to continue:

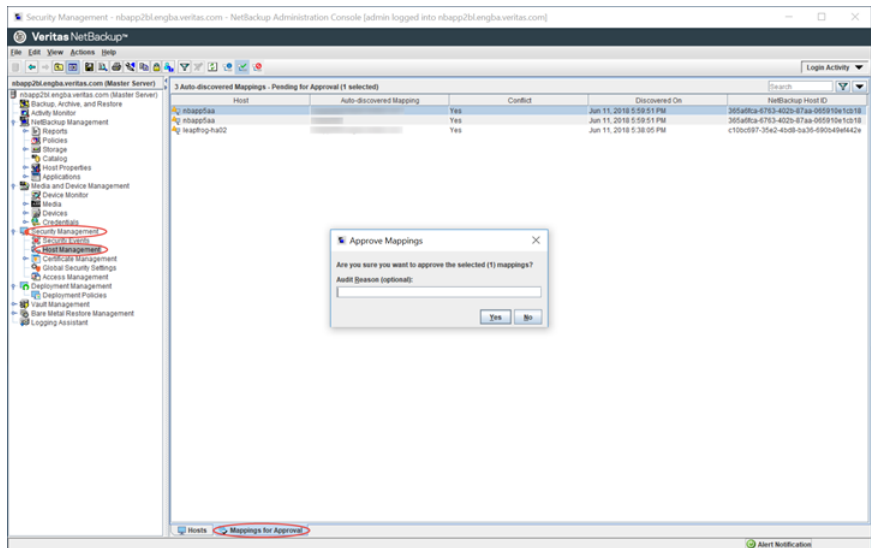
```
>> Do you want to continue? [yes, no] (no)
```

A message should appear that shows the process was successful.

- 7 Approve the host name mappings as follows:

- On the associated master server, log in to the NetBackup Administration Console.

- In the left pane, click **Security Management** to expand its properties, then click **Host Management**.
- In the lower-left of the right pane, click **Mappings for Approval**.
- At the top of the right pane, click on any host mapping that is pending approval. When the **Approve Mappings** dialog box appears that prompts for approval, click **Yes**. Repeat this task for each host mapping that is pending approval.



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](#)
- [Installing NetBackup client software through an NFS share](#)

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

Downloading NetBackup client packages to a client from a NetBackup appliance

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.

Note: Starting with the 3.1.2 release, the Windows client add-on is no longer included with the NetBackup Appliance client add-on package. If you need to install or upgrade the Windows client add-on, log in to your Veritas Entitlement Management System (VEMS) account and download it.

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

- All
- Linux
- Solaris
- AIX
- HP
- BSD
- 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.

For example, on Linux or UNIX platforms, download the package to `/tmp`.

Note: If the message **No packages found** appears after you make a selection, that client package is not currently installed on the appliance. 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 Untar the package.
- 6 Install the client software as follows:
On UNIX systems, run the `.install` script.
- 7 After you have successfully installed the client software, add the appliance 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/opensv/netbackup`
- Enter `ls` to see the contents of the directory.
- Open the `bp.conf` file in a text editor.
- Enter the fully qualified host name of the appliance master server.
- Save the changes and close the file.

See [“Installing NetBackup client software through an NFS share”](#) on page 85.

Installing NetBackup client software through an NFS share

After all appliance configuration has been completed, you can open an NFS share to install NetBackup client software on the UNIX clients that you plan to use with your configured appliance.

Note: Starting with the 3.1.2 release, the Windows client add-on is no longer included with the NetBackup Appliance client add-on package. If you need to install or upgrade the Windows client add-on, log in to your Veritas Entitlement Management System (VEMS) account and download it.

Before the installation, make sure that you have downloaded the NetBackup client software package to the appliance and verified that it exists in the following NFS share:
`<appliance-name>:/inst/client`

NetBackup UNIX client software installation through an NFS share

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

- 1 Log on to the 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.x_CLIENTS2 and/or NetBackup_8.x_CLIENTS1
- .packages
- clientconfig
- quickinstall.exe
- PC_Cln
- 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/opensv/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 83.

Index

A

- access appliance from NetBackup Appliance Shell Menu 52
- access appliance from NetBackup Appliance Web Console 35
- appliance media server
 - configure master server to communicate with 30

C

- command limitations
 - appliances not configured 12
- configuration
 - of maximum transmission unit size 29
- configure high availability setup
 - from shell menu 62
 - from web console 62
- configure master server
 - to communicate with appliance media server 30
- connectivity
 - during initial configuration 6

D

- default log-in credentials 7
- default maintenance user password 7
- default password 7, 52
- default user name 7, 52
- disk storage option licenses 11
- download NetBackup client packages from NetBackup appliance 83

F

- firewall port usage 7

G

- guidelines
 - NetBackup 53xx initial configuration 5

H

- High Availability
 - configuration guidelines 9

I

- initial configuration checklist
 - about 24
 - NetBackup appliance 25
- initial configuration from the NetBackup Appliance Shell Menu
 - NetBackup 53xx 49
- initial configuration from the NetBackup Appliance Web Console
 - NetBackup 53xx 33
- initial configuration on the partner node
 - High Availability 67
- initial configuration pages
 - NetBackup Appliance Web Console 14
- IPv4 and IPv6 support 13

M

- maximum transmission unit size
 - about configuration for 29
- media server role 8

N

- NetBackup 53xx
 - initial configuration from the NetBackup Appliance Shell Menu 49
 - initial configuration from the NetBackup Appliance Web Console 33
- NetBackup 53xx initial configuration
 - guidelines 5
- NetBackup appliance
 - initial configuration checklist 25
- NetBackup Appliance Shell Menu
 - add DNS name server to appliance 55
 - add DNS search domain 55
 - add host entries to appliance host file 56
 - configure alerts 58

NetBackup Appliance Shell Menu *(continued)*

- configure gateway IP address 55, 72
- configure IPv4 or IPv6 IP address 54, 71
- create bond 57
- enter disk pool name 61
- enter email for alerts 58
- enter SMTP server name 58
- enter storage pool name 61
- identify master server 59
- network configuration 54
- set appliance host name 56
- set date and time 57
- set DNS domain name 55
- set time zone 57
- tag VLAN 57
- test hardware - server and storage status 52

NetBackup Appliance Web Console

- change password 41
- configuration progress 48
- configure alerts - SNMP and SMTP server configuration 43
- configure call home 45
- host configuration - DNS or non-DNS 40
- identify master server 46
- initial configuration pages 14
- network configuration - add static route 39
- network configuration - create bond 37
- network configuration - tag VLAN 38
- set date and time 42
- storage configuration - AdvancedDisk 47
- storage configuration - deduplication (MSDP) 48
- storage overview 36
- summary of configuration 48

NetBackup appliances

- NIC1 (eth0) port usage 82

NetBackup client packages

- download from NetBackup appliance 83

NetBackup client software

- install using a share 85

NetBackup version compatibility 12**NIC1 (eth0) port usage**

- on NetBackup appliances 82

P**password**

- default 7, 52

R

- required names and addresses for initial configuration 6

S**shares**

- install NetBackup client software 85

storage overview page

- icon descriptions 36

U**user name**

- default 7, 52