# Veritas NetBackup™ Appliance Decommissioning and Reconfiguration Guide

Release 5.1.1, 5.3

VERITAS
now part of Cohesity

# Veritas NetBackup™ Appliance Decommissioning and Reconfiguration Guide

Last updated: 2025-10-09

## Legal Notice

Copyright © 2025 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
2625 Augustine Drive
Santa Clara, CA 95054

https://www.veritas.com

## Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

## Documentation

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

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

## Documentation feedback

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

APPL.docs@veritas.com

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

https://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 Decommissioning a NetBackup appliance ..... 5

About decommissioning a NetBackup 52xx Appliance ..... 5
Performing pre-installation checks for role compatibility and version compatibility ..... 6
Decommissioning a NetBackup 52xx primary server appliance ..... 7
Decommissioning a NetBackup 52xx or 53xx media server appliance ..... 7

Chapter 2 Reconfiguring a NetBackup appliance ..... 15

About reconfiguring a NetBackup appliance ..... 15
Reimaging a NetBackup appliance from the USB drive ..... 17
Reimaging an appliance using the MyVeritas portal ..... 22
Reconfiguring a 52xx primary server appliance using the NetBackup Appliance Shell Menu ..... 27
Configuring a primary server to communicate with an appliance media server ..... 37
Reconfiguring a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu ..... 39
About the NetBackup Appliance USB flash drive ..... 55
About NIC1 (eth0) port usage on NetBackup appliances ..... 55

Appendix A Migration from Cloud Catalyst to MSDP direct cloud tiering ..... 57

Migrating from NetBackup Cloud Catalyst Appliance to MSDP direct cloud tiering ..... 57

Appendix B LUN reconfiguration ..... 64

About NetBackup Appliance LUN reconfiguration using the DMPDR tool ..... 64

Index ..... 66

Chapter 1

# Decommissioning a NetBackup appliance

This chapter includes the following topics:


- About decommissioning a NetBackup 52xx Appliance
- Performing pre-installation checks for role compatibility and version compatibility
- Decommissioning a NetBackup 52xx primary server appliance
- Decommissioning a NetBackup 52xx or 53xx media server appliance


## About decommissioning a NetBackup 52xx Appliance

To decommission an appliance means to physically remove or eliminate the appliance from the backup environment. When you decide which appliance to decommission, you must make sure that the appliance is not configured as a backup destination for any clients.

You may need to decommission an appliance for any of the following reasons:

- The appliance has issues and needs to be reset to factory settings.
- The appliance has hardware issues and needs to be replaced.
- The appliance is no longer needed (down-sizing your backup environment).
- The appliance may need to be removed from the network domain to be repaired.
- The appliance is no longer supported and needs to be replaced.

After you determine that you need to decommission a media appliance, you can provision a new appliance to act as a target for all backups. With this technique the

load is decreased on the existing appliance and moved to the new appliance. The existing can be removed from the domain eventually.

# Performing pre-installation checks for role compatibility and version compatibility

From NetBackup Appliance 5.0, checks have been added to the role configuration process for role compatibility and version compatibility. When a NetBackup Appliance is re-imaged and role configuration is performed, if the storage setting is not erased using the `Support > Storage Reset` or `Support > FactoryReset` command, the following checks are performed before role configuration is done.

Checking for role compatibility

The existing storage setting is checked to verify if the previous role matches the current role. If the roles are not exactly the same, a warning message is displayed and the role configuration process is stopped. For example, if an appliance was installed and configured as a primary server, and if you try to re-image it and configure it as a media server, role configuration is stopped.

You can fix this issue by performing the following steps:

- `Support > Storage Reset`
- `Support > FactoryReset`
- Switch to configure role as previous role.

Checking for version compatibility

The appliance records and upgrades the Appliance version on the external disk. If you try to re-image an appliance with a version later than the current release version, a version check is triggered. You can re-image the appliance and reconfigure the role only if the appliance version remains the same. If the previous version and current version do not match, the role configuration process will be stopped.

You can fix this issue by performing the following steps:

- `Support > Storage Reset`
- `Support > FactoryReset`
- Switch to configure role as previous version.

# Decommissioning a NetBackup 52xx primary server appliance

When you decommission a 52xx primary server appliance it means all of the catalog and backup images that are stored on the disk are lost. You can use Factory Reset command to reset this appliance.

**To decommission a 52xx primary server appliance**

1. Open an SSH session on the primary appliance.
2. Log on as admin.
3. Run the following command and follow any additional prompts to reset the appliance to factory default settings.

   `Main_Menu` > `Support` > `FactoryReset`

# Decommissioning a NetBackup 52xx or 53xx media server appliance

When you decommission a 52xx or 53xx media server appliance it means all of the backup images that are stored on the disk are lost. You can use `Factory Reset` command to decommission and reset a NetBackup appliance media server.

---

**Note:** Factory reset does not remove an appliance from the NetBackup domain. Before performing a factory reset, ensure that the media server is fully decommissioned within NetBackup. It is recommended that you decommission the media server using the `nbdecommission` command. You can also follow the manual process to decommission the media server.

---

---

**Note:** If the NetBackup 53xx media server appliance is a node in a high availability (HA) configuration, you need to remove the node from the HA configuration first and perform the following procedure to decommission it.

For more information on how to remove a node from an HA configuration, refer to *NetBackup Appliance Commands Reference Guide*.

---

**To decommission a media server using the nbdecommission utility**

- This is the preferred method for decommissioning a media server. Run the following command:

  ```
  nbdecommission -oldserver <old_server> -newserver
  <new_server>
  ```

  For more details on this command, refer to the *NetBackup Commands Reference Guide* for the installed version.

Manually decommissioning and removing a media server from a NetBackup configuration involves several steps. Note the following before you do this procedure.

- If devices connected to the media server hold NetBackup media, move that media to a new media server.
- If the media is no longer usable or valid, remove it from the NetBackup configuration.
- If you do not decommission and remove the media server using the manual procedure, and a subsequent restore requires media associated with the old server, you have to import that media, which takes a longer time than if you used the procedure.
- If the server is configured for MSDP (Media Server Deduplication Pool), refer to the KB article 100004810, which provides steps to remove the related configuration.
- All commands referenced in the manual procedure can be found in the following directories:
  - `UNIX/Linux: /usr/openv/netbackup/bin/admincmd`
  - `Windows: install_path\NetBackup\bin\admincmd`
- To discover references to the media server to be decommissioned, you can run the following command on the primary server:

  ```
  nbdecommission -list_ref -oldserver <old_server>
  ```

  You can also save this output as a text file.

**To manually decommission a 52xx or 53xx media server**

1. Determine which tapes on the old server contain NetBackup images that have not expired using the `bpmedialist` command, where the `-l` option produces one line of output per tape:

   ```
   bpmedialist -mlist -l -h <old_server>
   ```

2. Use the NetBackup Administration Console to move the tapes in the robots that are attached to old server to a non-robotic status (standalone).
   - Select each robot that is attached to the old server.
   - Select all of the tapes and move them to standalone by selecting **Actions > Move**.

**3** Choose another server or the primary server to manage the tapes from the decommissioned server. Logically move the media from the old server to the new server by running the following command:

**bpmedia -movedb -allvolumes -oldserver *<old_server>* -newserver *<new_server>***

---

**Note:** This command updates the NetBackup image database and replaces the media server entry in the header files of all backups from the old server with the new server entry.

---

Example of an image header file before you run the `bpmedia` command:

```
# FRAG: c# f# K rem mt den fn id/path host bs off md dwo f_flags
f_unused1 exp mpx rl chkpt rsm_nbr seq_no media_subtype keep_date
copy_date i_unused1
FRAGMENT 1 1 890 0 0 0 0 C:\backup\windows_client_1320927029_C1_F1
windowsmaster 262144 0 0 -1 0 windowsmaster 1322136629 0 65537
0 0 0 1 0 1320927040 0
BACKUP_ID windows_client_1320927029
```

---

**Note:** The images reside in `C:\backup`. Move the images to the same location on the new media server to restore the backups. The operating system must be identical to maintain path accessibility.

---

Run the following command:

**bpmedia -movedb -allvolumes -oldserver windowsmaster -newserver linuxmedia**

The header file now looks like this:

```
# FRAG: c# f# K rem mt den fn id/path host bs off md dwo f_flags
f_unused1 exp mpx rl chkpt rsm_nbr seq_no media_subtype keep_date
copy_date i_unused1
FRAGMENT 1 1 890 0 0 0 0 C:\backup\windows_client_1320927029_C1_F1
linuxmedia 262144 0 0 -1 0 windowsmaster 1322136629 0 65537
0 0 0 1 0 1320927040 0
BACKUP_ID windows_client_1320927029
```

**4** Run `tpconfig` or `vmoprcmd` command to ensure that no entries for the old media server remain.

5. Use the Administration Console to configure NetBackup so that restore requests are directed to the new server. In the **General Server** host properties of the primary server, add a **Media Host Override** entry that specifies the old server for the **Original backup server** and the new server as the **Restore server**.
6. Use the NetBackup Administration Console to delete the following in the given order:
   - All storage units that use the robots that are associated with the old server.
   - Drives from the old server.
   - Robots from the old server.

   If NetBackup is already removed from the media server, deleting devices from the GUI can trigger an error stating that the volume manager daemon on that server is not running. In such a scenario, run the following command from the primary (EMM) server:

   ```
   nbemmcmd -deletealldevices -machinename <old_server> -machinetype media
   ```
7. Modify any policies that specify the storage units on the old server. Change the policies to point to any other defined storage units in the NetBackup configuration or to any available storage units.
8. Use the NetBackup Administration Console to remove any reference to the decommissioned media server in the Servers host properties of the primary server, all media servers, and all clients.
9. Restart the NetBackup daemons or services on any system that was updated.
10. To remove reference to the media server from EMM, run the following command:

    ```
    nbemmcmd -deletehost -machinename <old_server> -machinetype media
    ```
11. Verify that all references have been removed by running the following command:

    ```
    nbemmcmd -listhosts
    ```
12. Remove any files having the same name as the old server in the `remote_versions` directory:
    - UNIX/Linux: `/opt/openv/netbackup/remote_versions/`
    - Windows: `*install_path\NetBackup\Remote_Versions*`
13. If any robots from the old server are reused on other media servers, perform the following actions:

- Shut down the affected servers and disconnect the robots from the old servers. Connect the robots to the new media servers. Verify that the operating systems on the new media servers recognize the robots.
- Use the **NetBackup Device Configuration Wizard** to add the robots and drives to the media servers.
- Use the **NetBackup Administration** Console to create the appropriate NetBackup storage units.
- Use the **NetBackup Administration** Console to inventory the robots that are attached to the new server. The inventory updates the location of all tapes in these robots.

---

**Note:** This procedure is also applicable to a SAN media server. A SAN media server is the same as a media server except it only backs up itself and does not backup remote clients.

---

After the appliance media server is decommissioned within the NetBackup domain, reset the appliance back to a factory state using the `factory reset` command.

**To decommission a 52xx or 53xx media server appliance**

1. Open an SSH session on the media server appliance.
2. Log on as admin.
3. Run the following command and follow any additional prompts to reset the appliance to factory default settings.

   `Main_Menu` > `Support` > `FactoryReset`

To decommission a non-appliance media server, you must log in to the NetBackup Appliance Shell Menu from a primary appliance. Use the procedure below to decommission a non-appliance media server.

**To decommission a non-appliance media server**

1. Open an SSH session to the primary appliance.
2. Log on as admin.

3 Enter the following command to remove media server and move the ownership of the tape library:

`Main_Menu` > `Appliance` > `Remove` *`MediaServer TargetMediaServer`*

The variable *`MediaServer`* is the host name of the non-appliance media server that you want to decommission. And *`TargetMediaServer`* is the host name of the media server that you have selected to receive the media. The *`TargetMediaServer`* media server can be an appliance or non-appliance media server.

You can specify **NONE** for the *`TargetMediaServer`* variable if you do not need to move the media. If you specify **NONE** for the *`TargetMediaServer`* variable, then all of the backup images on the media that are attached to the media server are lost.

4 Enter `Yes`, to confirm that you want to remove this media server.

---

**Note:** If the media server that you are about to decommission has a deduplication pool storage unit configured, you must manually expire the images on that storage unit before you attempt to remove the media server.

---

5 If you designated a valid media server in the *`TargetMediaServer`* variable, enter the following command on each of the appliances to shut them down after a successful decommission of the appliance

`Main_Menu` > `Support` > `Shutdown`

6 You must cable the tape library to the target media server.

7 Run the following command to turn on the media server.

`Main_Menu` > `Support` > `Reboot`

**8** Enter the following command to configure the tape library to a media server that is defined in the *TargetMediaServer* variable.

`Main_Menu` > `Manage` > `Libraries` > `Configure` *`MediaServer`*

---

**Note:** If you want to use a media server that is not an appliance media server, then you must use the NetBackup Administration Console to configure the tape library to that media server.

---

Where *`MediaServer`* is the media server that you connected to the tape library and need to configure.

**9** From the decommissioned media server, run the following command and follow any additional prompts to reset the appliance to factory default settings.

`Main_Menu` > `Support` > `FactoryReset`

Once you have completed the factory reset process and finished decommissioning the media server, you can configure it to serve any role that you choose. If you configure it as a primary server, then you can use the `Main_Menu > Settings > NetBackup AdditionalServers Add` command to add a media appliance.

Chapter 2

# Reconfiguring a NetBackup appliance

This chapter includes the following topics:


- About reconfiguring a NetBackup appliance


## About reconfiguring a NetBackup appliance

If you experience problems with the appliance software, you can attempt to roll back the appliance software to a checkpoint or you can perform a factory reset operation. With the factory reset option, you can reset the appliance to its original default settings or if checkpoints exist, you can reset the appliance to an existing checkpoint. If you chose to perform a factory reset, you have the option to preserve your catalog configuration and existing data.

In a disaster recovery situation you must determine if you have lost all of the data and any software updates that were currently on the media or primary server appliance. Or you may determine that you have an opportunity to save all of the data. No matter which scenario you face, you must image the appliance and then reconfigure the appliance in the same way you did as a new appliance. Veritas recommends that you record all of your initial configuration information so that you can reference that information should you need to reconfigure.

---

**Note:** During the reimaging process, all storage shelves that were already attached to the appliance should remain attached. In addition, do not attach any additional storage shelves.

---

## Best practices before you begin reconfiguring your appliance

Before you reconfigure your appliance, you should consider the following with regards to license keys:

- If you intend to preserve data during the reconfiguration process, you must use the NetBackup Appliance Shell Menu. Reconfiguration using the NetBackup Appliance Web Console is not supported.
- If during the reconfiguration process, the media or primary server appliance goes through an initial configuration, then you must use the NetBackup Appliance Shell Menu to install the license keys before the initial configuration process begins. In addition, the user name and password may be set back to the default values if a factory reset operation was performed.

## Record your configuration information before you begin a reconfiguration

Before you begin a reimage process, Veritas recommends that you record the configuration information that you entered when you performed the initial configuration process on the appliance. If a factory reset is run after the reimage process completes, you should enter the same configuration information to connect to the appliance. In addition, after a factory reset the user name and password are reset to the default values.

- Network configuration:
  - Network interface
  - IP address
  - Subnet mask
  - Gateway
  - Network name
- Host configuration:
  - For Domain Name System (DNS) - Domain name suffix, DNS IP address, and the Search domain
  - For non-DNS systems - IP address, Fully qualified host name, and the short host name
- User name and password - Default user name is `admin` and the default password is `P@ssw0rd`.
- Role configuration - It is important that you configure the appliance using the same role as you did when it was initially configured.

- Storage configuration - If your media server appliance that has backup data on a disk that you want to preserve, you can record the following information so you have it available when you are ready to configure your storage.
  - Storage pool size
  - Disk pool name
  - Storage unit name
  - Deduplication password

See "Reconfiguring a 52xx primary server appliance using the NetBackup Appliance Shell Menu" on page 27.

See "Reconfiguring a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu" on page 39.

# Reimaging a NetBackup appliance from the USB drive

The following procedure describes the steps required to install a new image on a media server appliance. Existing backup data on the storage volumes are preserved automatically. To complete the data recovery the appliance must be reconfigured from the NetBackup Appliance Shell Menu. The NetBackup Appliance Web Console cannot be used if you want to preserve the previous storage configuration.

**To re-image an appliance from the USB drive**

1. If you can log into the appliance and you can access the NetBackup Appliance Shell Menu, export (copy) and move the device certificates. Use the following steps and then continue with Step 2.

   ---

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

   Contact Veritas Technical Support if you cannot log on to the appliance to export device certificates. More in-depth assistance is needed in this situation.

   ---

   - Open a CIFS and an NFS share with the following command:

     `Manage > Software > Share Open`

   - To export (copy) the device certificates, enter the following command:

     `Network > Security > Export <yes/no> /inst/patch/incoming`

     Where *<yes/no>* is for whether you want password protection.

**Note:** The output from the `export` command creates a backup `.pfx` file of the actual certificate. If you select `yes` to use a password, the file name is a number with the `.pfx` extension (`nnnnnnn.pfx`). If you select `no` for no password, a period precedes the file name (`.nnnnnnn.pfx`).

If you use a password, retain the name of the password to use when you run the `Import` command later in this procedure.

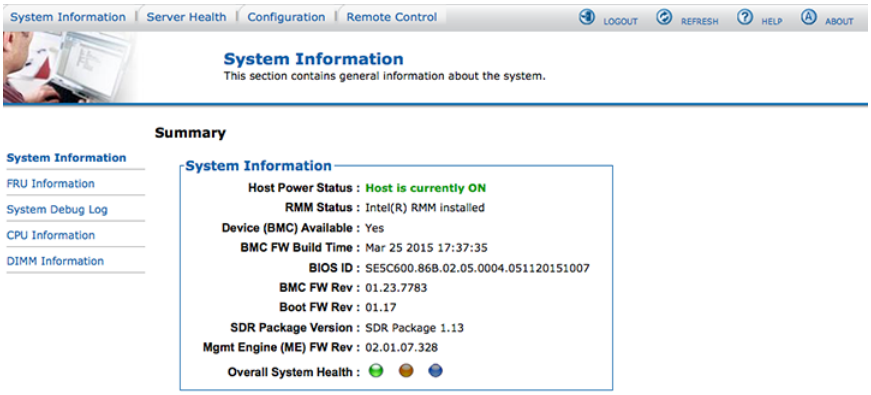
- To move the `.pfx` files into a local directory on a remote computer, create and mount a mount point and then move the files as follows:

  Windows — This example assumes that the Windows system uses Samba.
  - Create and mount a mount point as follows:
    `net use <AnAvailableDriveLetter>: \\<appliance-host>\"incoming_patches"`
  - Copy the `.pfx` file as follows:
    `# copy /inst/patch/incoming/*.pfx /mnt/<computer_name>`

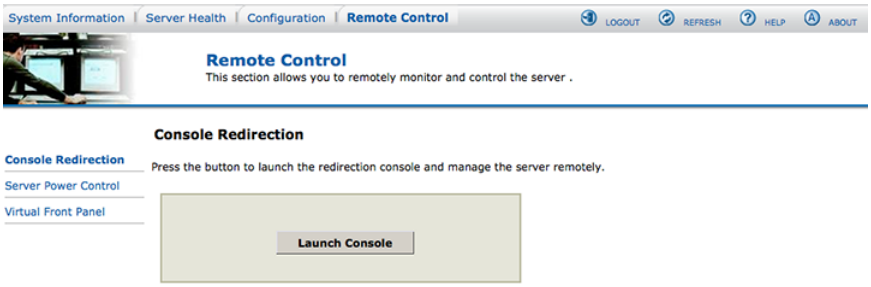
  UNIX or Linux — This example assumes that the UNIX or Linux system uses NFS.
  - Create and mount a mount point as follows:
    `# mkdir -p /mnt/<computer_name>`
    `# mount -t nfs <computer_name>:/<share_name> /mnt/<computer_name>`
  - Copy the .pfx file as follows:
    `# cp /inst/patch/incoming/*.pfx /mnt/<computer_name>`

2. Insert the USB drive into an appliance USB port on the media server appliance that you want to re-image.
3. Connect the remote management (IPMI) port of the appliance that you are reconfiguring to the corporate network, then do the following:
   - Log on to the remote management port of media server appliance from a remote machine, using the IP address that you assigned to the remote management port.


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




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




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

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

- Select the **Reset Server** radial button.

- Click **Perform Action**.

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

7 After you select the USB drive, press the ESC key. A screen appears that lets you select which type of installation you want to perform. You can choose to install the full NetBackup appliance installation or a smaller version that excludes the installation of the client packages.

Make your selection and press **Enter** to begin the reimage operation.

8 When the installation of the new appliance package is complete, you receive a **Welcome** message in the **JViewer** application window. Enter the default appliance password (`P@ssw0rd`). You are now logged on to the NetBackup Appliance Shell Menu.

---

**Note:** Before you begin the reconfiguration process, you may want to reference the configuration information that you recorded before beginning the re-image operation.

---

---

**Note:** Starting with the NetBackup Appliance 5.0 release, during the re-image of a NetBackup 5240/5340 Appliance from the USB drive/CDROM or in case of a factory reset or upgrade, a copy of the ISO being installed is saved in the newly added partition, `/dev/mapper/system-iso`.

---

---

**Note:** Starting with the NetBackup Appliance 5.0 release, during the re-image of a NetBackup 5250/5350 Appliance from the USB drive/CDROM, the ISO in the SSD is updated with the current ISO being installed. The boot menu entry in the SSD is also updated. During the re-imaging process, copying the ISO from the CDROM to the SSD will take approximately one hour of additional time.

---

9 Import the device certificates, `.pfx` files, from the remote computer where you exported them earlier:

- Open a share from the NetBackup Appliance Shell Menu as follows:

  `Main_Menu > Manage > Software > Share Open`

  The CIFS share `\\<appliance-name>\incoming_patches` and the NFS share `<appliance-name>:/inst/patch/incoming` are now open on this appliance.

- To move the earlier saved `.pfx` files to the open share location, create and mount a mount point and then move the files as follows:

  Windows — This example assumes that the Windows system uses Samba.
  - Create and mount a mount point as follows:
    `net use <AnAvailableDriveLetter>:\\<appliance-host>\"incoming_patches"`
  - Move the `.pfx` files back to the appliance as follows:
    `# move /mnt/computer_name/*.pfx /inst/patch/incoming/`

  UNIX or Linux — This example assumes that the UNIX or Linux system uses NFS.
  - Create and mount a mount point as follows:
    `# mkdir -p /mnt/computer_name`
    `move <directory where the pfx file was save>/*.pfx <mounted drive>`
  - Move the .pfx files back to the appliance as follows:
    `mv <local directory where the pfx file was kept>/*.pfx <mount point>`

- Import the files by entering the following command:
  `Main_Menu > Network > Security > Import <yes/no>/inst/patch/incoming`

  **Note:** If you used a password in Step 1 when you performed the `Export` command, then you must enter the same password when you run the `Import` command.

- Close the share from the NetBackup Appliance Shell Menu as follows:
  `Main_Menu > Manage > Software > Share Close`

**10** Type `Return` twice to return to the main menu.

**11** Verify that you are at the main menu.

The appliance is now ready for initial configuration.

Refer to the following topics to reconfigure your NetBackup appliance:

See "Reconfiguring a 52xx primary server appliance using the NetBackup Appliance Shell Menu" on page 27.

See “Reconfiguring a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu” on page 39.

# Reimaging an appliance using the MyVeritas portal

You can use an ISO image from MyVeritas.com to reimage your appliance with the same version or a different version of NetBackup appliance software. You need your maintenance serial number to access the ISO image. You can find your serial number on the license certificate you received with your initial purchase or on your Version Upgrade Notification. If you need help locating your serial number, email customercare@veritas.com.

---

**Warning:** When you use an ISO to install a different version of NetBackup appliance software than is currently installed, the storage must be reset. If you want to keep your existing storage, you can only install an ISO image of the same version. Further, if NetBackup appliance software 2.6 or later is installed on your appliance and you want to install an ISO image earlier than 2.6, you must perform a storage reset before you install the ISO.

---

To perform this procedure, you must be able to access the appliance remotely through the Intelligent Platform Management Interface (IPMI) network. Before you begin, make sure that IPMI networking is configured on your appliance and that you can access the Veritas Remote Management interface.

---

**Note:** Due to the bandwidth required to install an ISO image through the IPMI network, the ISO installation works best if the appliance and the remote computer are located at the same physical site. If you try to remotely reimage an appliance over a WAN, the process can fail. Therefore, Veritas does not recommend performing an ISO reimage over a WAN.

---

## Downloading the ISO image from the MyVeritas portal

**To download the ISO image**

1. On the computer from which you remotely access the appliance, go to MyVeritas.com.
2. Log on to the MyVeritas portal using your credentials.

3 Follow the prompts until you have downloaded the new NetBackup Appliance ISO image. If you need help with the downloading the ISO, refer to the following link:

https://www.veritas.com/support/en_US/article.000100418

---

**Warning:** To prevent technical or service issues with your appliance, ensure that you download the correct ISO image for your appliance model and series. These images are for use only with the correct physical appliance type. If you have purchased a 52xx Appliance that is under a current Veritas Support contract, you are only authorized to download and install on that appliance the ISO image for the 52xx Appliance. If you have purchased a 50xx Appliance that is under a Support contract, you are only authorized to download and install on that appliance the ISO image for the 50xx Appliance. Use of any ISO image that is not authorized for the correct physical appliance type may cause errors and malfunctions, and may void the warranty rights that Veritas provides for that physical unit.

---

4 Save the ISO image to a local drive of the remote computer.

## Installing the ISO image on your appliance

**To install the ISO image**

1 If a firewall exists between the appliance and the remote devices that manage the appliance, make sure that the following ports are open:

| | |
|---|---|
| 5120 | RMM ISO/CD |
| 7578 | RMM CLI |

2 Turn off your appliance.

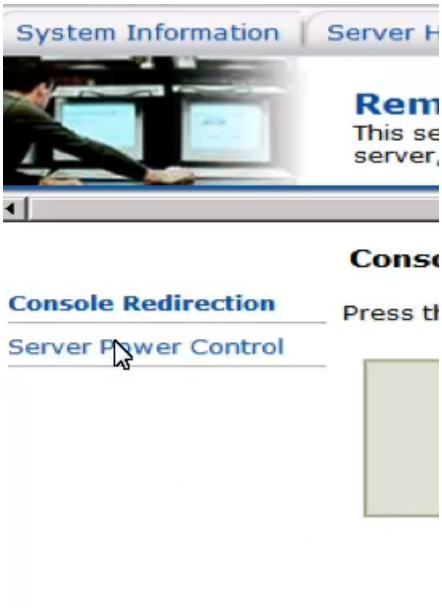
3 On the computer that you use to remotely access the appliance, open a supported browser. Enter the remote management (IPMI) port IP address that is assigned to the appliance and log on to the Veritas Remote Management interface.

4 Navigate to the **Remote Control** tab and click **Launch Console**.

5 When the redirection console launches, click on the **Device** drop-down menu on the console and select **Redirect ISO**.


6 From the **Open** pop-up window that appears, choose the ISO image that you want to install and click **Open**.

7 Return to the Veritas Remote Management interface and select **Server Power Control** on the left side of the **Remote Control** page.




8 The **Power Control and Status** page appears.

Since the server is currently off, the only available option is **Power ON Server**. Click **Perform Action**.

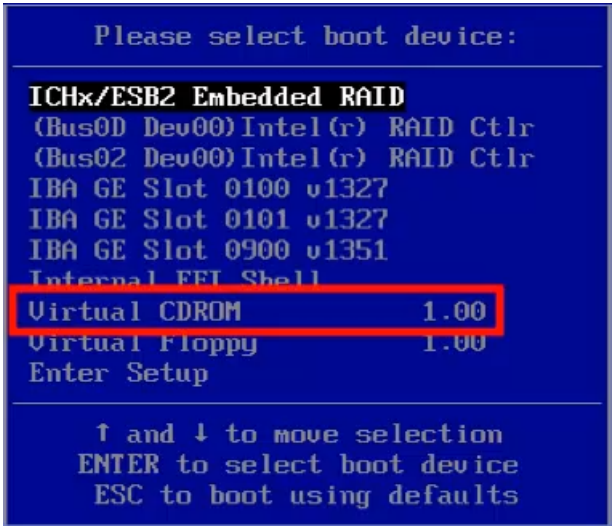
9 Return to the remote console and wait for the system to turn on. When the splash screen appears, immediately press **F6** to enter the boot menu.

---

**Note:** You only get a window of a few seconds to perform this task. If you miss the window, the operating system loads, and you cannot access the boot menu.

---

**10** When the boot menu appears, scroll down to **Virtual CDROM** and press **Enter**.




**11** The system begins to boot from the ISO image you selected earlier. It then presents the following options:

For reimaging to versions 3.1.2 and earlier:

- **Boot from Hard Disk**
- **Install NetBackup Appliance**

Select **Install NetBackup Appliance** and press **Enter**.

For reimaging to versions 3.2 and later:

- **Boot from local drive**
- **Install Veritas Optimized Operating System**
- **Rescue A Red Hat Enterprise Linux system**

Select **Install Veritas Optimized Operating System** and press **Enter**.

The installation begins. Once the installation completes, you can log on and configure the system with the new version of NetBackup Appliance.

**Note:** The IPMI ISO installation is sensitive to the quality of the network connection. If an installation failure occurs, try the installation again. If the problem persists, try to improve the quality of the IPMI network connection. You can also burn the ISO image onto a DVD and install it with a USB DVD-ROM drive that you physically connect to the appliance.

See "Reimaging a NetBackup appliance from the USB drive" on page 17.

See "Reconfiguring a 52xx primary server appliance using the NetBackup Appliance Shell Menu" on page 27.

See "Reconfiguring a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu" on page 39.

# Reconfiguring a 52xx primary server appliance using the NetBackup Appliance Shell Menu

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

The initial configuration process requires that you change the default passwords for the **admin**, **maintenance**, and **sysadmin** (IPMI) user accounts. The default admin password is valid only for the initial appliance login. The prompt to change the default passwords appears when you enter the **Main_Menu** > **Appliance** command to set the appliance role.

**Note:** The **nbasecadmin** account is created automatically when you perform the initial configuration on an appliance primary server. Once created, this account is assigned the default appliance password. This user cannot log in to the NetBackup Web UI until the default password is changed.

The following procedure describes how to configure a new or a re-imaged 52xx primary server appliance from the NetBackup Appliance Shell Menu.

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

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

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

1 Before performing the reconfiguration process, make sure you have followed the re-image procedure. See "Reimaging a NetBackup appliance from the USB drive" on page 17.

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

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

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

The *IPAddress* or the *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`

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

| | |
|---|---|
| Configure the IP address of each network | Use either of the following commands depending on whether you want to configure an IPv4 or an IPv6 address for the network interface:<br><br>To configure the IPv4 address of a network interface:<br><br>`IPv4` *`IPAddress Netmask`* `[InterfaceName]`<br><br>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.<br><br>To configure the IPv6 address of a network interface:<br><br>IPv6 <*IP Address*> <Prefix> [InterfaceNames]<br><br>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]`<br><br>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.<br><br>The *GatewayIPAddress* or the *TargetNetworkIPAddress* can be an IPv4 or an IPv6 address.<br><br>Remember that you should not use both IPv4 and IPv6 addresses in the same command. For example, you cannot use `Gateway Add 9ffe::3 255.255.255.0 eth1`. You should use `Gateway Add 9ffe::3 6ffe:: 64 eth1`. |

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

**Note:** If you do not use DNS, then you can proceed to Step 6.

`DNS Domain` *`Name`*

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

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

`DNS Add NameServer` *`IPAddress`*

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

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

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

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

`DNS Add SearchDomain` *`SearchDomain`*

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

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

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

```
Hosts Add IPAddress FQHN ShortName
```

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

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

---

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

---

```
Hostname Set Name
```

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

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

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

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

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

**Note:** The 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
```

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

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

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

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

- Set the time zone by entering the following command:

  `TimeZone Set`

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

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

  Where *Month* is the name of the month.

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

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

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

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

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

**11** Set the role for the appliance to a primary server.

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

```
Primary
```

The following prompts appear for you to complete the role configuration task.

- Default passwords

  The following prompt appears to change the default passwords:

  ```
  - [Info] Default password change is required for the following user(s): admin, maintenance, sysadmin
  ```

  Change each user account password as prompted.

  Review the following password policy before setting a new password:

  - Passwords must contain at least eight characters.
  - Passwords must contain at least one lowercase letter (a-z) and one number (0-9).
  - Dictionary words are considered weak passwords and are not accepted.
  - Passwords for the sysadmin (IPMI) user must contain no more than 20 characters.
  - The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.

**Note:** If you enter five consecutive invalid passwords for any user account, the appliance aborts the initial configuration process automatically. You must start the initial configuration process again.

- Veritas Usage Insights customer registration key
  Starting with release 4.0, when you select this role you are required to provide a Veritas Usage Insights customer registration key. You cannot complete the role configuration until you provide the registration key. To obtain a key, follow the onscreen prompts.
- Call Home settings test
  Starting with release 5.0, a settings test for the Call Home feature is performed automatically. The test is performed to ensure that the appliance can communicate with the Veritas Call Home server. If the test fails, the following message appears:

  **Warning:** The appliance is not able to connect to the Veritas Call Home server to upload hardware and software telemetry. Providing the Call Home information to Veritas allows for an improved support experience and recommendations through the NetInsights Console. It is recommended that you enable Call Home and ensure the system can reach the Veritas Call Home server through correct name resolution or proxy server setting.

  You can ignore this message and continue with the initial configuration.
- `AutoUpdate` for `UpgradeReadinessCheck`
  Starting with release 5.1.1, a prompt appears for you to enable the `AutoUpdate` option for the `UpgradeReadinessCheck` feature. When the feature is enabled and a new analyzer tool version is available, the analyzer tool on the appliance is updated automatically. If an analyzer tool does not already exist on the appliance when you enable this feature, the latest version of the analyzer tool is downloaded automatically. You can also download the latest version of the analyzer tool from the Veritas Download Center. Veritas recommends that you enable AutoUpdate.

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

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

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

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

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

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

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

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

To configure storage partitions, you must do the following:

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

Note the following for MSDP partition sizes:

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

The storage prompts appear in the following order:

```
NetBackup Catalog partition size in GB/TB:
AdvancedDisk partition size in GB/TB: (1 GB)
AdvancedDisk diskpool name:
AdvancedDisk storage unit name:
MSDP partition size in GB/TB: (10 GB)
MSDP diskpool name:
MSDP storage unit name:
MSDP Catalog partition size in GB/TB:
```

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

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

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

**14** If you plan to use this primary server with a media server in a NAT network, perform the following tasks:

- Enable the `NetBackup DNAT` feature on this primary server as follows:

  `Main > Settings > NetBackup DNAT Enable`
- Add the name of the media server to the NetBackup Servers list on this primary server as follows:

  `Main > Settings > NetBackup NATServers Add`

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

---

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

See "About NIC1 (eth0) port usage on NetBackup appliances" on page 55.

---

16 If you have a media server that needs reconfiguration, now is the time to configure the primary server to communicate with it, then reconfigure your media server.

See "Configuring a primary server to communicate with an appliance media server" on page 37.

See "Reconfiguring a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu" on page 39.

17 If you want to configure the appliance for MSDP cloud, log in to the NetBackup web UI as the **nbasecadmin** user and configure the MSDP cloud storage as follows:

- Run the following command to change the default password for the **nbasecadmin** user:

  `Main > Settings > Password nbasecadmin`

- Log in to the NetBackup web UI as the nbasecadmin user and configure the MSDP cloud storage as follows:
  - Create a disk pool.
  - Create a storage unit.
    For details, see the *NetBackup Web UI Administrator's Guide*.

# Configuring a primary server to communicate with an appliance media server

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

Before you configure a re-imaged media server appliance, you must ensure that the primary server you plan to use with it is configured. That allows for appropriate communication to occur between the primary server and the reconfigured media server appliance.

The following procedure describes how to configure a primary server to communicate with an appliance media server.

**To configure a primary server to communicate with a new media server**

**1** Log in to the primary server as the administrator and make sure that the media server appliance name is added to the primary server:

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

**2** Open the following ports on the primary server as follows to allow it to communicate with the associated media server:

- Traditional (non-appliance) NetBackup primary server
  If a firewall exists between this primary server and the media server, open the following ports and make sure to set all of them for bidirectional (inbound and outbound) communication:

  **Note:** You must log in to the primary server as the administrator to change port settings.

  ```
  https: 443
  PBX: 1556
  vnetd: 13724
  ```

- NetBackup Appliance primary server
  If this primary server uses TCP, make sure that the IPMI iKVM port 7578 is accessible through the gateway firewall in your lab.
  Additionally, NetBackup ports that are used for NetBackup optional features may not be enabled by default on a NetBackup Appliance. To change NetBackup port settings on the appliance, log in to the appliance shell menu and use the `Settings > Security > Port > ModifyNBUPortRange` command. For complete details, see the *NetBackup Appliance Commands Reference Guide*.

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

# Reconfiguring a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu

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

The initial configuration process requires that you change the default passwords for the **admin**, **maintenance**, and **sysadmin** (IPMI) user accounts. The default admin password is valid only for the initial appliance login. The prompt to change the default passwords appears when you enter the **Main_Menu** > **Appliance** command to set the appliance role.

External certificate authority certificates are supported. This feature provides an alternative to using the NetBackup Certificate Authority for host verification and security. This procedure includes the necessary information to deploy these certificates. For more information about security certificates, see the chapter "External CA support in NetBackup" in the *NetBackup Security and Encryption Guide*.

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

See "Configuring a primary server to communicate with an appliance media server" on page 37.

- Make sure that the primary server and this media server have compatible software versions.
- Add the name of this media server to the SERVERS list on the primary server that you plan to use with it.
- If a firewall exists between the primary server and this media server, open the appropriate ports as described in the link above.
- Make sure that the date and time of this media server matches the date and time on the primary server.
- If you plan to use this media server in a NAT network, make sure to enable the DNAT feature on the primary server and to also add this media server name to the NAT servers list on the primary server.

The following procedure describes how to configure a new or a re-imaged 52xx or 53xx media server appliance from the NetBackup Appliance Shell Menu.

---

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

---

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

---

**To reconfigure a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu**

1 Before performing the reconfiguration process, make sure you have followed the re-image procedure. See “Reimaging a NetBackup appliance from the USB drive” on page 17.

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

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

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

The *IPAddress* or the *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 addresses in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1.`. You should use `Configure 9ffe::46 64 9ffe::49 eth1`

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:<br><br>To configure the IPv4 address of a network interface:<br><br>`IPv4` *`IPAddress Netmask`* `[InterfaceName]`<br><br>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.<br><br>To configure the IPv6 address of a network interface:<br><br>IPv6 <*IP Address*> <Prefix> [InterfaceNames]<br><br>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]`<br><br>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.<br><br>The *GatewayIPAddress* or the *TargetNetworkIPAddress* can be an IPv4 or an IPv6 address.<br><br>Remember that you should not use both IPv4 and IPv6 address in the same command. For example, you cannot use `Gateway Add 9ffe::3 255.255.255.0 eth1`. You should use `Gateway Add 9ffe::3 6ffe:: 64 eth1`. |

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

**Note:** If you do not use DNS, then you can proceed to Step 6.

`DNS Domain` *`Name`*

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

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

`DNS Add NameServer` *`IPAddress`*

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

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

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

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

`DNS Add SearchDomain` *`SearchDomain`*

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

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

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

```
Hosts Add IPAddress FQHN ShortName
```

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

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

---

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

---

```
Hostname Set Name
```

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

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

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

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

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

**Note:** The 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
```

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

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

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

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

- Set the time zone by entering the following command:

  `TimeZone Set`

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

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

  Where *Month* is the name of the month.

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

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

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

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

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

**11** If you plan to use this media server in a NAT network, perform the following tasks on the associated primary server before you set the appliance role:

- Enable the `DNAT` feature on the primary server.
- Add the name of this media server to the NetBackup Servers list on the primary server.
  See "Configuring a primary server to communicate with an appliance media server" on page 37.

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

---

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

---

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

`Media` *`PrimaryServer`*

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

| | |
|---|---|
| Standalone primary server | This scenario shows one primary server host name. This name does not need to be a fully qualified name as long as your appliance recognizes the primary server on your network. The following is an example of how the command would appear.<br>`Media PrimaryServerName` |
| Multihomed primary server | In this scenario, the primary 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.<br>`Media PrimaryNet1Name,PrimaryNet2Name` |
| Clustered primary server | In this scenario, the primary 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.<br>`Media PrimaryClusterName,ActiveNodeName,PassiveNodeName` |
| Multihomed clustered primary server | In this scenario, the primary 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.<br>`Media PrimaryClusterName,ActiveNodeName,`<br>`PassiveNodeName,PrimaryNet1Name,PrimaryNet2Name`<br>To prevent any future issues, when you perform the appliance role configuration, Veritas recommends that you provide all of the associated primary server names. |

Default passwords

Veritas Usage Insights customer registration key

Call Home settings test

`AutoUpdate` for `UpgradeReadinessCheck`

- Default passwords

  The following prompt appears to change the default passwords:

  ```
  - [Info] Default password change is required for the following user(s): admin, maintenance, sysadmin
  ```

  Change each user account password as prompted.

  Review the following password policy before setting a new password:

  - Passwords must contain at least eight characters.
  - Passwords must contain at least one lowercase letter (a-z) and one number (0-9).
  - Dictionary words are considered weak passwords and are not accepted.
  - Passwords for the sysadmin (IPMI) user must contain no more than 20 characters.
  - The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.

  **Note:** If you enter five consecutive invalid passwords for any user account, the appliance aborts the initial configuration process automatically. You must start the initial configuration process again.

- Call Home settings test

  Starting with release 5.0, a settings test for the Call Home feature is performed automatically. The test is performed to ensure that the appliance can communicate with the Veritas Call Home server. If the test fails, the following message appears:

  **Warning:** The appliance is not able to connect to the Veritas Call Home server to upload hardware and software telemetry. Providing the Call Home information to Veritas allows for an improved support experience and recommendations through the NetInsights Console. It is recommended that you enable Call Home and ensure the system can reach the Veritas Call Home server through correct name resolution or proxy server setting.

  You can ignore this message and continue with the initial configuration.

- `AutoUpdate` for `UpgradeReadinessCheck`

  Starting with release 5.1.1, a prompt appears for you to enable the `AutoUpdate` option for the `UpgradeReadinessCheck` feature. When the feature is enabled and a new analyzer tool version is available, the analyzer tool on the appliance is updated automatically. If an analyzer tool does not already exist on the appliance when you enable this feature, the latest version of the analyzer tool is downloaded automatically. You can also download the latest version of the analyzer tool from the Veritas Download Center. Veritas recommends that you enable AutoUpdate.

| | |
|---|---|
| Certificate provisioning | |
| Certificate revocation list (CRL) | |

After you have entered the primary server name, the appliance pings the primary server for the Certificate Authority (CA) status and shows the result. Each of the following bullet statements describes the possible status results. Follow the instructions that appear below the applicable status result to complete the certificate configuration.

If the primary server has an enabled External CA-signed certificate, the following appears:

- `The primary server <primary_server_name> has an enabled External CA-signed certificate. Do you want to import the External CA-signed certificate for this Media server now [yes,no](yes):`

  Press **Enter** to continue. The following message appears:

  `The following shares have been opened on the appliance for you to upload certificate files:`

  `NFS share <media_server_name>:/inst/share`

  `CIFS share \\<media_server_name>\general_share`

  Enter the following details for external certificate configuration:

  `Enter the certificate file path:`

  `Enter the trust store file path:`

  `Enter the private key path:`

  `Enter the password for the passphrase file path or skip security configuration (default: NONE):`

  Enter the following details for CRL usage:

  `Should a CRL be honored for the external certificate?`

  `1) Use the CRL defined in the certificate.`

  `2) Use the specific CRL directory.`

  `3) Do not use a CRL.`

  `q) Skip security configuration.`

  `CRL option:` Enter 1, 2, 3, or q.

  Verify the External CA details that you entered:

  `Certificate file name:`

  `Trust store file name:`

  `Private key file name:`

  `CRL check level:` (Shows the selected CRL option.)

  `Do you want to use the above certificate files? [yes, no](yes):`

  After verifying that the entered information is correct, press **Enter** to continue and answer the following prompt:

  `Is this correct? [yes, no](yes):`

  If all of the information is correct, press **Enter** to continue.

  The appliance performs an ECA health check and shows the result of each validation check. When the health check has completed successfully, the following messages appear:

```
ECA health check was successful.
The external certificate has been registered successfully.
```

- The primary server *<primary_server_name>* currently uses an external CA issued certificate and its own internal certificate. Would you like to proceed with the external CA issued certificate? [yes,no](yes):

  If you select **no**, the following message appears:

  ```
  This appliance will use a NetBackup issued certificate for
  secure communication.
  ```

  If you select **yes**, enter the following details for external certificate configuration:

  ```
  Enter the certificate file path:
  Enter the trust store file path:
  Enter the private key path:
  Enter the password for the passphrase file path or skip
  security configuration (default: NONE):
  ```

  Enter the following details for CRL usage:

  ```
  Should a CRL be honored for the external certificate?
  1) Use the CRL defined in the certificate.
  2) Use the specific CRL directory.
  3) Do not use a CRL.
  q) Skip security configuration.
  CRL option: Enter 1, 2, 3, or q.
  ```

  Verify the External CA details that you entered:

  ```
  Certificate file name:
  Trust store file name:
  Private key file name:
  CRL check level: (Shows the selected CRL option.)
  Do you want to use the above certificate files? [yes,
  no](yes):
  ```

  After verifying that the entered information is correct, press **Enter** to continue and answer the following prompt:

  ```
  Is this correct? [yes, no](yes):
  ```

  If all of the information is correct, press **Enter** to continue.

  The appliance performs an ECA health check and shows the result of each validation check. When the health check has completed successfully, the following messages appear:

  ```
  ECA health check was successful.
  The external certificate has been registered successfully.
  ```

- This appliance will use an External Certificate for secure communication.
  If the primary server has a disabled External CA-signed certificate, the following message appears:
  `The primary server <server_name> has a disabled External CA-signed certificate. Trust the certificate to continue the role configuration process.`
  `Do you trust the certificate? [yes, no], If you select yes, this appliance will continue to do storage configuration. If you select no, the role configuration will be aborted.`
- `This appliance will use a NetBackup issued certificate for secure communication.`
  No further certificate configuration is required. Click **Next** to continue

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 primary server is an FQDN, Veritas recommends that you use the FQDN to specify the primary server for the media server.

---

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

If storage objects are detected, you receive the following message:

```
NetBackup storage objects have been detected that belong to this
media server node. You have an option to clean up (delete and
recreate) or preserve any preexisting NetBackup storage objects
that are solely owned by this appliance node.

If you choose 'yes' the following occurs:
1. The NetBackup catalog images owned by this node are expired,
if applicable.
2. The storage servers, disk pools, and storage units are cleaned
up on the primary server.

Whether you chose 'yes' or 'no', the backup data on the disk is
preserved.

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

 >> Do you want to clean up existing storage objects? [yes,no]
```

If you enter `Yes` the following occurs:

- The NetBackup catalog images owned by this media server compute node are expired.
- The storage servers, disk pools, and storage units are cleaned up on the primary server.
- The backup data on the disk is preserved.

If you choose `No` the following occurs:

- NetBackup catalog images are retained.
- The backup data on the disk is preserved.

---

**Note:** If you want to remove the backup data, run the following command from the NetBackup Appliance Shell Menu before you proceed.

```
Main_Menu > Support > Storage Reset
```

---

**14** Enter the storage configuration properties to configure storage pools for AdvancedDisk, for Deduplication (MSDP), or both.

When you configure storage pool sizes after a reimage process, the default storage sizes are displayed. If you adjusted the storage pool sizes before the reimage, those new storage pool sizes become the new default values that appear. However, the default disk pool name and the storage unit name that appear are the same default names as in the initial configuration process. If you changed the disk pool name and the storage unit name before the reimage, you must enter the names that you had chosen again during the reconfiguration process.

---

**Note:** To skip this step enter 0 when you are prompted for the size. This also deletes any existing data for that partition.

If you enter a 0 when you are prompted and a storage partition does not exist, then a partition is not created. If you enter 0 and a partition already exists then the partition is deleted and any existing data is also deleted.

---

To configure an AdvancedDisk storage pool provide the following information:

- `AdvancedDisk partition size in GB/TB [1GB..4.51TB]: (1 GB) [1.6395 GB..51.8 TB]:`
- `AdvancedDisk diskpool name: (dp_adv_5240)`

- `AdvancedDisk storage unit name: (stu_adv_5240)`

To configure an MSDP storage pool provide the following information:

- `MSDP partition size in GB/TB [118GB..4.49TB]: (4.23 TB)`
- `MSDP diskpool name: (dp_disk_5240)`
- `MSDP storage unit name: (stu_disk_5240)`
- `MSDP Catalog partition size in GB/TB [19GB..294GB]: (19 GB)`

---

**Note:** You may need to reference the configuration notes that you recorded before starting this reimaging procedure so you can recreate the same storage pool configurations.

---

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

---

**Note:** The estimated time to configure storage can vary depending on the system load. It may also take several minutes to restart the NetBackup services. The greater the system load, the longer it takes to complete the operation.

---

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

**16** If you want to configure the appliance for MSDP cloud, do the following:

- Log in to the appliance primary server and run the following command to change the default password for the **nbasecadmin** user:
  `Main > Settings > Password nbasecadmin`
- Log in to the NetBackup web UI as the nbasecadmin user and configure the MSDP cloud storage as follows:
  - Create a disk pool.
  - Create a storage unit.
    For details, see the *NetBackup Web UI Administrator's Guide*.

# About the NetBackup Appliance USB flash drive

Included with each NetBackup appliance is a USB flash drive that contains the NetBackup appliance ISO image. The primary use of the USB flash drive is to reimage the appliance. The version of the image is identical to what comes installed on the appliance from the factory.

Other reasons for reimaging an appliance:

- Disaster recovery after an operating system-related failure.
- Redeploying the appliance with a different version of the appliance software.
- Reimaging a new appliance with a different version of the appliance software to deploy in an existing NetBackup appliance environment.

In addition to the NetBackup appliance ISO image, the client packages are also included on the USB flash drive. The client packages are automatically copied into the incoming patches directory, `/inst/patch/incoming`, when reimaging the appliance.

The client packages can be installed onto the appliance by navigating to `Manage > Software` and running the command `Install<rpm name>`. The `<rpm name>` is found using the `List Downloaded` command. Once the clients are installed on the appliance, they become available for installation when a client computer accesses the appliance.

If you have misplaced your original USB flash drive you can request another through Veritas Technical Support.

See the following topics for more information on how to reconfigure the appliance:

See “Reimaging a NetBackup appliance from the USB drive” on page 17.

See “Reconfiguring a 52xx primary server appliance using the NetBackup Appliance Shell Menu” on page 27.

See “Reconfiguring a 52xx or 53xx media server appliance using the NetBackup Appliance Shell Menu” on page 39.

# About NIC1 (eth0) port usage on NetBackup appliances

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

Once the initial configuration has been completed, you can connect NIC1 (eth0) to an administrative network that does not provide any backup data transfer. However, you may need to change the default IP address if your primary network uses the

same IP address range. NetBackup appliances do not support the use of any network configuration in the same range as the default IP address for the administrator interface on NIC1 (eth0).

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

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

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

---

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

---

Appendix A

# Migration from Cloud Catalyst to MSDP direct cloud tiering

This appendix includes the following topics:


- Migrating from NetBackup Cloud Catalyst Appliance to MSDP direct cloud tiering


## Migrating from NetBackup Cloud Catalyst Appliance to MSDP direct cloud tiering

Starting with NetBackup appliance release 4.1, the Cloud Catalyst feature is no longer supported. However, you are encouraged to move to MSDP direct cloud tiering. This technology offers improved performance, reliability, usability, and flexibility when compared to the earlier Cloud Catalyst product.

Details for migrating from Cloud Catalyst to MSDP direct cloud tiering are included in the *Veritas NetBackup Deduplication Guide, Appendix B*. You should review that information before proceeding with the migration.

This document provides the additional required information to convert a NetBackup Cloud Catalyst Appliance to use MSDP direct cloud tiering. The following describes the supported and unsupported migration scenarios, and the migration process.

---

**Note:** Note: The procedures in this appendix must be run on MSDP servers running appliance versions 5.0 and later. The master server may be running a newer version, but the MSDP server on which the `nbdecommission -migrate_cloudcatalyst` command is run, must be running one of these versions.

---

## Supported scenarios

- New NetBackup appliance installations
  You can deploy any new NetBackup Appliance with software version 5.0 and later and configure it to use MSDP direct cloud tiering.
- Existing Cloud Catalyst Appliance installations
  You can re-image most existing installations of Cloud Catalyst appliances with software version 5.0 to use MSDP direct cloud tiering.
- Existing NetBackup appliance media server installations that are used as an MSDP target server
  You can upgrade most existing NetBackup appliance media server installations with software version 5.0 to use MSDP direct cloud tiering.

## Unsupported scenario

Any NetBackup 5240 Appliance that used software version 3.1.x and was configured as a Cloud Catalyst storage server with a cloud bucket, and then modified as follows:

- The appliance was re-imaged with software version 3.2 or later.
- The re-imaged appliance was configured as a Cloud Catalyst storage server to use the same cloud bucket, without cleaning up the cloud bucket data. Therefore, the re-imaged appliance is using the same cloud bucket data that was first generated with version 3.1.x.

For this scenario, see the *Veritas NetBackup Deduplication Guide, Appendix B* for other migration options.

## Time estimates for migration

The actual time to complete the migration (Task 6: Perform migration steps) can vary, depending on the cloud provider involved and the available network bandwidth for downloading from the cloud. Most migrations should finish within 24 hours, and many require much less than 24 hours. However, in some cases it may take longer.

## Migration process

The following shows a summarized list of the required tasks to migrate to MSDP direct cloud tiering. Click on each link for the details of each task.

Task 1: Review migration documentation

Task 2: Upgrade primary server

Task 3: Collect required data to prepare for pre-migration steps

Task 4: Perform pre-migration steps

Task 5: Re-image and reconfigure Cloud Catalyst appliance

Task 6: Perform migration steps

Task 7: Perform post-migration steps

## Task 1: Review migration documentation

For complete details about migrating to MSDP direct cloud tiering, see the *Veritas NetBackup Deduplication Guide, Appendix B*.

For additional details about migrating a NetBackup Cloud Catalyst appliance to MSDP direct cloud tiering, review this entire topic.

## Task 2: Upgrade primary server

Upgrade the associated primary server as follows:

- For a NetBackup Appliance primary server, upgrade to appliance version 5.0 or later. See the *Veritas NetBackup Appliance Upgrade Guide*.
- For a traditional NetBackup primary server, upgrade to version 10.0 or later. See the *Veritas NetBackup Upgrade Guide*.

## Task 3: Collect required data to prepare for pre-migration steps

Before you start the migration, collect the following information about the existing Cloud Catalyst appliance and any new information as needed for the migrated MSDP direct cloud tier storage server. Use the right column in the table to enter the information.

**Table A-1** Data for pre-migration tasks

| Item | Configuration data |
|---|---|
| Cloud Catalyst appliance hostname | |
| Admin login credentials to elevate to maintenance mode | |
| Cloud Catalyst storage server name | |
| Cloud Catalyst bucket or container name | |
| KMS configuration/KMS Key Group Name | |

**Table A-1** Data for pre-migration tasks *(continued)*

| Item | Configuration data |
|---|---|
| Name to use for the new disk volume for the migrated MSDP direct cloud tier storage server | |
| Name to use for the new disk pool for the migrated MSDP direct cloud tier storage server | |
| Your cloud credentials | |
| Other cloud-specific configuration information | |
| List of policies and SLPs, that currently write to the Cloud Catalyst storage server | |

After you have completed collecting the information above, do the following:

- Create a NetBackupCLI user with administrator privileges on the associated appliance primary server and on the appliance media server.
- Sign in to the Veritas Download Center to obtain one of the following hot fixes (EEBs), based on the current software version on your Cloud Catalyst appliance:
  `NBAPP_EEB_ET4063815-5.0.0-1.x86_64.rpm` (for software versions 3.2)
  `NBAPP_EEB_ET4063818-5.0.0-1.x86_64.rpm` (for software version 3.3.0.1)

  **Note:** Hot fixes are not available for Cloud Catalyst appliances that use software versions earlier than 3.2. Before you can perform the migration for those appliances, you must first upgrade them to version 3.2 or 3.3.0.1.

  After you have manually performed the initial pre-migration steps in the following task, hot fix installation performs the remaining pre-migration steps.

## Task 4: Perform pre-migration steps

The following procedure describes the pre-migration tasks.

**To perform the pre-migration steps**

1. Stop all jobs on the Cloud Catalyst appliance as follows.
   - Deactivate all backup policies that write to the Cloud Catalyst storage server.

- Deactivate all storage lifecycle policies (SLPs) that write to the Cloud Catalyst storage server.
- Verify all active jobs that are targeted for the Cloud Catalyst storage server have been stopped.

**2** Log in to the primary appliance server as a NetBackupCLI Administrator and run the following command to clean up the NetBackup catalog:

```
bpimage -cleanup -allclients -prunetir
```

For a traditional NetBackup primary server, log in to the NetBackup Administration Console to run the command.

**3** To complete the pre-migration steps on the Cloud Catalyst appliance, install the EEB that you downloaded from the Vertias Download Center (in Task 3) and respond to the prompts as they appear.

## Task 5: Re-image and reconfigure Cloud Catalyst appliance

For a Cloud Catalyst appliance, you must re-image it with NetBackup Appliance release 5.0 and then reconfigure it.

---

**Caution:** Do not perform a factory reset before you re-image the Cloud Catalyst appliance.

---

For other NetBackup Appliance media servers that use a different MSDP server, upgrade them to NetBackup Appliance release 5.0.

For re-imaged or upgraded appliances, you must also reset the storage and delete the existing PureDisk storage unit and disk pool on the media server as described.

**After completing a re-image or an upgrade to NetBackup Appliance release 5.0**

**1** Reset the storage and remove all PureDisk storage elements as follows:

- Log in to the appliance shell menu and run the following command to reset the storage:

  ```
  Support > Storage Reset
  ```

- Log in to the NetBackup Web UI and delete the PureDisk storage unit and disk pool on the media server.

**2** For re-imaged appliances only:

- After resetting the storage as previously described, reconfigure the appliance and set the **Role** for **Media**. You must associate this server with the same primary server that was used before the re-image. Make sure that the

re-imaged appliance media server has an adequate amount of space for the MSDP partition.

- If the appliance was previously configured for KMS, make sure to configure it after you have completed the reconfiguration.
- Recreate the NetBackupCLI user with Administrator privileges (from Task 3), which was lost when you re-imaged the appliance.

## Task 6: Perform migration steps

After reconfiguration of a re-imaged Cloud Catalyst appliance to 5.0 or an upgrade of a NetBackup Appliance media server to 5.0, you are ready to perform the migration.

---

**Note:** The actual time to complete this task can vary, depending on the cloud provider involved and the available network bandwidth for downloading from the cloud. Most migrations should finish within 24 hours, and many require much less than 24 hours. However, in some cases it may take longer.

---

**To perform the migration steps**

1. Log in to the re-imaged or upgraded appliance as a NetBackupCLI Administrator and run the following command:

   ```
   bpnbat -Login -loginType WEBUI -requestApproval
   ```

2. To start the migration process, run the following command:

   ```
   sudo /usr/openv/netbackup/bin/admincmd/nbdecommission
   -migrate_cloudcatalyst
   ```

3. Monitor the migration and provide the following information or responses when prompted to do so:

   - The line number of the Cloud Catalyst server to migrate
   - Cloud bucket name
   - Cloud Catalyst server hostname
   - Indicate if MSDP KMS encryption is enabled for `cloudcatalyst_`*`server_name`*.
   - New disk volume name for the migrated Cloud Catalyst server
   - New disk pool name for the migrated Cloud Catalyst server
   - Cloud account username or access key
   - Cloud account password or secret access key

- Indicate if you want to migrate `cloudcatalyst_server_name` to the new MSDP cloud server.
- Verify that no jobs are currently running on the Cloud Catalyst server.
- Decide if you wish to skip migrating Cloud Catalyst image sharing information.
- Select how to handle the SLP-controlled images that are in-process or yet to be processed. Options are displayed.
- Select how to delete the Cloud Catalyst disk pool, storage unit, and storage server, or how to deactivate the policies that reference the Cloud Catalyst storage unit. Options are displayed.

## Task 7: Perform post-migration steps

Immediately after the migration process has completed successfully, perform the following tasks:

**After the migration process has completed successfully**

1. Log in to the appliance (image sharing server) as a NetBackupCLI Administrator and run the following command, and then restart the appliance:

   ```
   cacontrol --catalog buildcloudcatalystobjects
   <new_disk_volume_name>
   ```

   For details about this command, see the *Veritas NetBackup Deduplication Guide, Appendix B*.

2. Create a new storage unit for this disk pool that was created during the migration through the NetBackup Web UI. Use the new storage unit as the destination for your policies and SLPs through the NetBackup Java Console.

3. Re-enable any existing policies and SLPs that previously wrote to the migrated Cloud Catalyst server, as the migration process disables these policies.

4. Optional step: To clean up any unused Cloud Catalyst objects from the cloud bucket, log in to the media server appliance as a NetBackupCLI user and run the following command:

   ```
   cacontrol --catalog cleanupcloudcatalystobjects
   <new_disk_volume_name>
   ```

   For details about this command, see the *Veritas NetBackup Deduplication Guide, Appendix B*.

Appendix B

# LUN reconfiguration

This appendix includes the following topics:


- About NetBackup Appliance LUN reconfiguration using the DMPDR tool


## About NetBackup Appliance LUN reconfiguration using the DMPDR tool

To reduce the complexity of the multi-step dynamic LUN reconfiguration process, you can use the DMPDR tool which is available by logging in to the maintenance mode of an appliance. DMP refers to Dyanmic Multi-Pathing and DR refers to Dynamic Reconfiguration. The following command launches the tool:

```
# /usr/lib/vxvm/voladm.d/bin/dmpdr -o refresh
```

The DMPDR tool includes a non-interactive interface to help with the complex LUN reconfiguration process. The tool attempts to automate and perform the correct sequence of events on the host, which reduces the chance of human error without the need for manual intervention.

For example, the tool performs the following tasks:

- Performs the correct sequence of events on the appliance to detect any removed and newly added LUNs.
- Updates the underlying OS device handles for the DMP managed devices and refreshes the VxVM and DMP structures.
- Creates a log file under `/var/adm/vx/` for each LUN reconfiguration event.

The DMPDR tool works in connection only with Veritas DMP (Dynamic Multi-Pathing). Third-party multi-pathing drivers (such as MPxIO and EMC PowerPath) are not supported and will not work with the interface.

## Reconfiguring LUNs connected to an appliance server with the DMPDR tool

Separate DMPDR tool sessions are required when you physically add or remove LUNs. You cannot run the tool to reconfigure both added and removed LUNs in the same session, as it may cause problems with the various layers in the I/O stack.

The following procedure describes how to reconfigure LUNs after removing or adding LUNs at the storage array back-end.

**To reconfigure LUNs with the DMPDR tool**

1. Remove the intended LUNs from the storage array back-end.
2. Log in to the appliance as an administrator, then run the following command to log in to the maintenance mode:

   ```
   Main > Support > Maintenance
   ```

3. Run the DMPDR with the following command:

   ```
   # /usr/lib/vxvm/voladm.d/bin/dmpdr -o refresh
   ```

   ---

   **Note:** The SCSI **Peripheral Qualifier/Device Type** (PQ) attribute reports a nonzero value for LUNs that have been removed intentionally from the storage array back-end. For example:

   ```
   # /etc/vx/diag.d/vxscsiinq -d /dev/vx/dmp/emc0_00aa | head -3

   Inquiry for /dev/vx/dmp/emc0_00aa, evpd 0x0, page code 0x0
   Peripheral Qualifier/Device Type : 3f
   ```

   The DMPDR tool deletes only the stale OS device handles that report a nonzero value for the **Peripheral Qualifier/Device Type** (PQ) attribute.

   ---

   The command output provides details of the entire process. When the process has completed successfully, you can continue to the next step to add and reconfigure new LUNs.
4. Add the intended LUNs to the storage array back-end.
5. Run the DMPDR with the following command:

   ```
   # /usr/lib/vxvm/voladm.d/bin/dmpdr -o refresh
   ```

6. When the process has completed successfully, exit from the maintenance mode.

# Index


## Symbols

52xx media server appliance
    reconfigure from NetBackup Appliance Shell Menu 39
52xx primary server appliance
    initial configuration from NetBackup Appliance Shell Menu 27
    reconfigure from USB and NetBackup Appliance Shell Menu 27

## A

about
    decommissioning an appliance 5
    reconfiguring the appliance 15
appliance media server
    configure primary server to communicate with 37

## C

configure primary server
    to communicate with appliance media server 37

## D

decommissioning an appliance
    about 5

## I

initial configuration of 52xx primary server appliance
    from NetBackup Appliance Shell Menu 27
ISO image
    installing 22

## M

MyVeritas portal
    ISO image download and installation 22

## N

NetBackup appliance
    reconfigure 15
NetBackup appliances
    NIC1 (eth0) port usage 55
NIC1 (eth0) port usage
    on NetBackup appliances 55

## R

reconfiguration of 52xx or 53xx media server appliance
    from NetBackup Appliance Shell Menu 39
reconfiguration of 52xx primary server appliance
    from USB and NetBackup Appliance Shell Menu 27
reconfigure
    NetBackup appliance 15
reimage
    with MyVeritas ISO image 22

## U

USB content 55
USB purpose 55