

# Veritas NetBackup™ Appliance Upgrade Guide

Release 3.2

Document revision 2

**VERITAS™**

# Veritas NetBackup™ Appliance Upgrade Guide

Last updated: 2020-04-27

## Legal Notice

Copyright © 2020 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

<http://www.veritas.com>

## Technical Support

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

<https://www.veritas.com/support>

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

<https://my.veritas.com>

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

Worldwide (except Japan)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto: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](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](mailto:APPL.docs@veritas.com)

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

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

## Veritas Services and Operations Readiness Tools (SORT)

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

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

<b>Chapter 1</b>	<b>Introduction</b> .....	<b>6</b>
	About upgrading to NetBackup appliance software version 3.2 .....	6
	Supported upgrade paths .....	6
	About corresponding NetBackup software versions .....	7
	About the Appliance Install Manager .....	7
<b>Chapter 2</b>	<b>Upgrade planning</b> .....	<b>9</b>
	Requirements and best practices for upgrading NetBackup appliances .....	9
	About upgrades for NetBackup Appliance HA setups .....	13
	Upgrade time estimation .....	15
<b>Chapter 3</b>	<b>Performing the upgrade</b> .....	<b>16</b>
	Methods for downloading appliance software release updates .....	16
	Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console .....	16
	Downloading software updates directly to a NetBackup appliance .....	17
	Downloading software updates to a NetBackup appliance using a client share .....	19
	Installing a NetBackup appliance software update using the NetBackup Appliance Shell Menu .....	21
<b>Chapter 4</b>	<b>Post upgrade tasks</b> .....	<b>27</b>
	Post upgrade tasks .....	27
<b>Chapter 5</b>	<b>NetBackup client upgrades with VxUpdate</b> .....	<b>28</b>
	About VxUpdate .....	28
	VxUpdate repository management .....	29
	Deployment policy management .....	32
	Manually initiating upgrades from the master server using VxUpdate .....	36
	Manually initiating upgrades from the client using VxUpdate .....	40

	Deployment job status .....	41
Chapter 6	<b>Troubleshooting</b> .....	43
	Troubleshooting upgrade issues .....	43
Index .....		44

# Introduction

This chapter includes the following topics:

- [About upgrading to NetBackup appliance software version 3.2](#)

## About upgrading to NetBackup appliance software version 3.2

To upgrade to versions 3.1 or later, use the IPMI console to log in to the NetBackup Appliance Shell Menu or use the **Appliance Management Console**. To upgrade the nodes in a high availability (HA) setup, you must use the NetBackup Appliance Shell Menu. The **Appliance Management Console** does not support upgrades for HA nodes.

Before you begin any upgrades, review the following topics:

See [“Supported upgrade paths”](#) on page 6.

See [“About upgrades for NetBackup Appliance HA setups”](#) on page 13.

See [“About corresponding NetBackup software versions ”](#) on page 7.

See [“About the Appliance Install Manager”](#) on page 7.

### Supported upgrade paths

- Direct upgrade paths
  - 5230, 5240, or 5330 appliances with versions 2.7.3, 3.0, 3.1, 3.1.1, and 3.1.2
  - 5340 appliances with versions 3.1, 3.1.1, and 3.1.2
- Two-step upgrade path

## About upgrading to NetBackup appliance software version 3.2

Appliances with software versions 2.7.2 and earlier must be upgraded twice to get to version 3.2. It is recommended that these systems first be upgraded to version 2.7.3, and then upgraded to version 3.2.

---

**Note:** Although multi-path upgrades from versions 2.5.x or 2.6.x to version 3.2 are supported, these upgrades may fail if the preflight check detects insufficient space on the `/boot` partition. For example, if the appliance was upgraded from version 2.5.3 to 2.6.1 and then to version 2.7.3 or 3.0, an upgrade to version 3.2 will fail if insufficient `/boot` space is detected. This problem occurs because the `/boot` partition is completely allocated on appliances that once used the older versions and it cannot be resized. If you experience this problem, you must reimage the appliance with the version that existed before the failed upgrade attempt, and then upgrade to version 3.2. Using the example just described (version 2.6.1 to 3.1 to 3.2), the appliance must be reimaged with version 3.1 before upgrading it to version 3.2.

---

## About corresponding NetBackup software versions

NetBackup software version 8.2 is included with NetBackup appliance release 3.2. [Table 1-1](#) lists the corresponding NetBackup versions for the recent NetBackup appliance software releases.

**Table 1-1** Appliance software releases and the corresponding NetBackup software versions

Appliance software release	NetBackup software version
2.7.3	7.7.3
3.0	8.0
3.1	8.1
3.1.1	8.1.1
3.1.2	8.1.2
3.2	8.2

## About the Appliance Install Manager

Starting with the 3.1 release, you can switch to the **Appliance Install Manger (AIM)** window for viewing the upgrade progress. This window shows the estimated completion time, the upgrade progress bar, the main upgrade steps, the upgrade logs, and other useful information.

If you log on to the shell menu from the IPMI console during an upgrade, press **Alt + F2** from the soft keyboard to open the **AIM** window.

The following upgrade scenarios describe when the AIM window becomes available:

- For upgrades from 2.7.x and 3.0, after the third reboot has completed.
- For upgrades from 3.1, as soon as you start the upgrade to any later release.

The **AIM** window has the following view modes:

- **Main**

This default view shows the main upgrade steps and task results.

- **Verbose**

This view shows the detailed upgrade logs.

To change from the **Main** view to the **Verbose** view, press the **V** key.

To change from the **Verbose** view to the **Main** view, press the **M** key.

To pause the upgrade, press the **P** key.

To close the **AIM** window and return to the shell menu, press the **S** key.

To show the **AIM** window again, enter the following command:

```
Main_Menu > Manage > Software >UpgradeStatus
```



# Upgrade planning

This chapter includes the following topics:

- [Requirements and best practices for upgrading NetBackup appliances](#)

## Requirements and best practices for upgrading NetBackup appliances

This topic describes the requirements and best practices that you should follow anytime you plan to upgrade appliance software.

- For a complete list of required updates prior to 3.2 upgrades, refer to the following article:  
[https://www.veritas.com/support/en\\_US/article.100046066](https://www.veritas.com/support/en_US/article.100046066)
- Make sure that your appliance environment currently uses software version 2.7.3, 3.0, 3.1, 3.1.1, or 3.1.2. Only these versions support a direct upgrade to version 3.2.
- Starting with software version 3.1, you can perform upgrades from the **Appliance Management Console**. Appliances that use software versions 2.7.3 and 3.0 are also supported for upgrades through the console, if the appropriate EEB is installed before the upgrade. After you review all upgrade guidelines and perform the required pre-upgrade tasks, refer to the *Veritas Appliance Management Guide* for the upgrade procedure.

---

**Note:** The **Appliance Management Console** does not currently support upgrading appliances (nodes) in an HA setup. You must use the NetBackup Appliance Shell Menu to upgrade these appliances.

---

- Always perform a full disaster recovery (DR) backup before an upgrade.

- Master servers
 

Make sure that you have a recent and complete NetBackup Catalog backup.
- MSDP and CloudCatalyst configurations
 

Make sure to configure your deduplication pool catalog backup policy and perform a successful backup. For details, refer to the following article:  
[https://www.veritas.com/support/en\\_US/article.100046592](https://www.veritas.com/support/en_US/article.100046592)
- Export and re-import IPsec certificates.
 

If IPsec functionality is configured on any appliance that you plan to upgrade, the IPsec certificates may not be retained after the upgrade has completed. To avoid this issue, you must export the IPsec certificates before upgrading those appliances. Use the `Network > Security > Export` command to perform this task. The `Export` command copies two `.pfx` files (`serialnumber.pfx` and `.serialnumber.pfx`) to a location that you specify when you run the command. Export the IPsec certificates before an upgrade as follows:

  - Log in to the NetBackup Appliance Shell Menu and navigate to the following view:  
`Network > Security > Export`
  - Enter the following export option details:  
`Export [EnterPasswd] [PathValue]`  
 Where `[EnterPasswd]` is the field used to answer the question, "Do you want to enter a password?". You must enter **yes** or **no**.  
 Where `[PathValue]` is the location where you want to place the exported certificates.
  - After the export has completed, back up both of the `.pfx` files to a non-appliance location.  
 After the upgrade has completed, re-import the IPsec certificates.  
 See "Post upgrade tasks" on page 27.
- Delete previously downloaded release updates, client packages, and client add-ons.
 

To make sure that there is enough space in the `/inst` partition during the upgrade, first delete all previously downloaded release updates, client packages, and client add-ons from the appliance. As a best practice, always remove downloaded packages after all appliances and clients have been upgraded. If you do not delete the previously downloaded packages and the `/inst` directory on the appliance does not contain enough space, the preflight check and the Appliance Upgrade Readiness Analyzer tool prevent the upgrade. Even if enough space exists to allow the upgrade to start, the upgrade may fail if the old client add-ons are not removed. For downloaded packages on high availability (HA) nodes, you must remove the packages from both nodes.

The following describes the package removal methods for appliances that never had version 2.6.0.1 installed:

### NetBackup Appliance Web Console

- On the appliance to be upgraded, select **Manage > Software Updates**.
- In the **Downloaded Software Updates** table, click the radio button to the left of a release update, client package, or client add-on in the list, then click **Delete**.

### NetBackup Appliance Shell Menu

- On the appliance to be upgraded, check for all downloaded release updates and client packages by entering the following command: `Manage > Software > List Downloaded`.
- To remove each downloaded release update and client package, enter the following command: `Manage > Software > Delete update_name`. Where `update_name` is the release update or the client package file name.
- To see a list of all downloaded client add-ons, enter the following command: `Manage > Software > List AddOns`.
- To remove each downloaded client add-on, enter the following command: `Manage > Software > Rollback eeb_name`. Where `eeb_name` is the client add-on file name.

**Note:** You must include the `.rpm` extension when you enter the client add-on file name.

**Note:** You must include the `.rpm` extension when you enter the client add-on file name.

If the appliance that you want to upgrade has ever had appliance version 2.6.0.1 installed, it requires a different method for client package removal. The client packages for that version remain on the appliance even if it has been upgraded to a later version. If the appliance was purchased with version 2.6.0.1 or if you ever upgraded to version 2.6.0.1, you must perform the following tasks to delete the 2.6.0.1 client packages. The only exception is if the appliance was re-imaged to a version different than 2.6.0.1.

To delete version 2.6.0.1 client packages from an appliance:

- Open a web browser or an SSH session to the Veritas appliance software update release page.
- Download and install any later version of the client packages onto the appliance.
- Delete the newly installed client packages from the NetBackup Appliance Shell Menu. This action also deletes the 2.6.0.1 client packages.

---

**Note:** The client packages cannot be deleted from the NetBackup Appliance Web Console.

---

- Follow the same upgrade order for appliances as for traditional NetBackup upgrades. If you use NetBackup OpsCenter, upgrade it first. Then upgrade appliances starting with the master server appliance, followed by all media server appliances.
- If you have multiple media servers to upgrade, you must perform the upgrade process on each individual media server.  
Appliance media servers (nodes) in an HA setup are updated one at a time. Both nodes must use the same appliance software version. Once you have upgraded one node, you must upgrade the other node immediately.  
See [“About upgrades for NetBackup Appliance HA setups”](#) on page 13.
- If a traditional NetBackup master server is used with a media server appliance, that master server must have the same NetBackup version or later as the media server appliance. For example, before you upgrade a media server appliance with NetBackup appliance version 3.2, first upgrade the NetBackup software on the master server to version 8.2.  
See [“About corresponding NetBackup software versions”](#) on page 7.
- Make sure that the NetBackup master server is active and running throughout the duration of an appliance media server upgrade. In addition, make sure that the NetBackup processes are started or running on both the master server and the media server.

---

**Note:** Only NetBackup services should be active during an upgrade. All jobs must be stopped, suspended, or prevented from running during an upgrade.

---

- If you have enabled the STIG feature on an appliance and you need to upgrade it or install an EEB on it, do not plan such installations during the 4:00am - 4:30am time frame. By following this best practice, you can avoid interrupting the automatic update of the AIDE database and any monitored files, which can cause multiple alert messages from the appliance.
- NetBackup clients must use the same or an earlier software version as the appliance. Clients cannot run at a later version than the appliance. For example, a client with NetBackup version 8.2 can only be used with an appliance server with version 3.2 or later. Client add-ons must also be the same as the client version.  
See [“About corresponding NetBackup software versions”](#) on page 7.

- Use a compatible version of the NetBackup Administration Console to manage the NetBackup services.  
The NetBackup Administration Console is backward-compatible. A patch release (x.x.x.x) console is compatible with a major (x.x) or minor NetBackup release (x.x.x) that shares the same first and second digits.

## About upgrades for NetBackup Appliance HA setups

The following describes the upgrade requirements for nodes in a high availability (HA) setup:

- NetBackup Appliance Shell Menu  
Use this interface to upgrade the nodes.

---

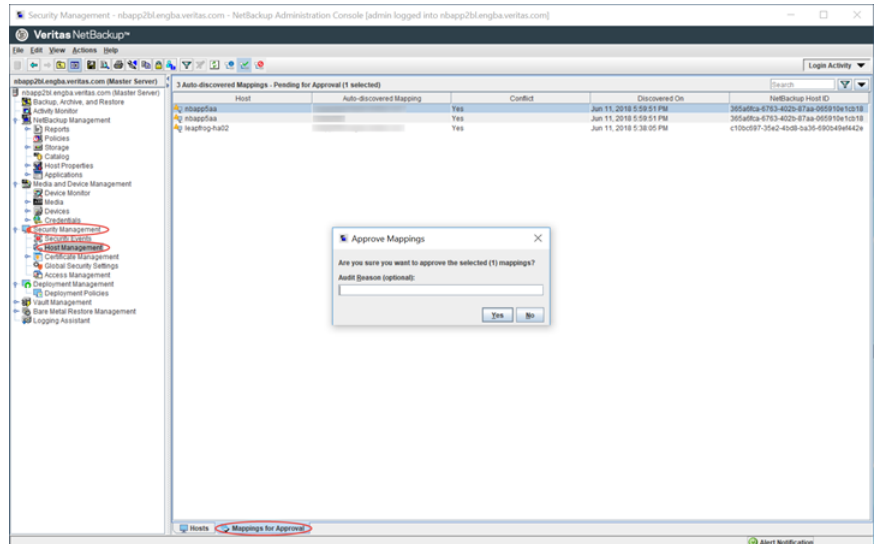
**Note:** The **Appliance Management Console** does not support upgrades for HA nodes.

---

- One or two nodes in the HA setup  
HA nodes must be upgraded from within the HA setup. If you remove a node from the HA setup, you can still upgrade the node that remains.
- One node at a time  
Only one node can be upgraded at a time so that the workload can continue on the other node.
- One software version  
Both nodes must use the same appliance software version. Once you have upgraded one node, you must upgrade the other node immediately.
- Node upgrade order  
Either node can be upgraded first. However, the node that runs the MSDP services cannot be upgraded while those services are in progress.  
The first node that is configured and then used to create the HA setup runs the MSDP services by default. To upgrade this node, you must first perform a switchover to transfer the MSDP services and workload to the partner node. After the upgrade on the first node has completed, perform the following tasks on that node to prepare for the partner node upgrade:
  - On the upgraded node, run the `Manage > High Availability > Switchover` command to switch the MSDP services from the partner node over to the upgraded node.
  - On the upgraded node, run the `Support > Test Software` command to verify the status of various appliance software components. If the test passes, log in to the partner node and upgrade it.

- **MSDP configuration**  
 To upgrade the nodes in an HA setup, MSDP configuration is required on both nodes. Upgrades on appliance HA nodes are not supported if MSDP is not configured.
- **Downloading packages from the NetBackup Appliance Shell Menu**  
 You only need to download rpm packages to one node. After you run the `Manage > Software > List Downloaded` command on the HA node with the downloaded package, run the command on the other node to make the package available on that node.
- **Approve host name mappings**  
 Before you upgrade from software versions 3.1.1 and earlier, you must first approve the host name mappings for HA appliances in the NetBackup Administration Console on the associated master server. Otherwise, the preflight check does not allow the upgrade to start.  
 To approve the host name mappings, do the following:
  - On the associated master server, log in to the NetBackup Administration Console.
  - In the left pane, click **Security Management** to expand its properties, then click **Host Management**.
  - In the lower-left of the right pane, click **Mappings for Approval**
  - At the top of the right pane, click on any host mapping that is pending approval. When the **Approve Mappings** dialog box appears that prompts for approval, click **Yes**. Repeat this task for each host mapping that is pending approval.

## Requirements and best practices for upgrading NetBackup appliances



- Perform a switchover for appliances in an HA setup

Appliances (nodes) in an HA setup are updated one at a time. Both nodes must use the same appliance software version. Once you have upgraded one node, you must upgrade the other node immediately.

Either node can be upgraded first. However, upgrades cannot be performed on the node where MSDP services and jobs are in progress. Before you begin an upgrade on the node that is running MSDP, you must first perform a switchover to transfer the MSDP workload to the partner node. Use the following command to perform a switchover:

```
Main_Menu > Manage > HighAvailability > Switchover hostname
```

Where *hostname* is the physical host name or IP address of the partner node.

When the upgrade on this node has completed, perform another switchover to transfer the MSDP workload from the partner node to the upgraded node. Immediately upgrade the partner node.

## Upgrade time estimation

Appliance upgrades can take from 2 - 3.5 hours, depending on the hardware configuration and the current software version.

# Performing the upgrade

This chapter includes the following topics:

- [Methods for downloading appliance software release updates](#)
- [Installing a NetBackup appliance software update using the NetBackup Appliance Shell Menu](#)

## Methods for downloading appliance software release updates

Starting with NetBackup Appliance release 3.2, release updates are available from the Veritas Download Center website:

[https://www.veritas.com/content/support/en\\_US/downloads](https://www.veritas.com/content/support/en_US/downloads)

Appliance software and client packages can be downloaded manually through a share. Updates must first be downloaded onto the appliance before you can initiate an upgrade.

The following describes the methods you can use to download appliance software release updates:

- [Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console](#)
- [Downloading software updates directly to a NetBackup appliance](#)
- [Downloading software updates to a NetBackup appliance using a client share](#)

## Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console

Use the following procedure to download a software release update to an appliance using the NetBackup Appliance Web Console.



---

**Note:** This method is not supported for downloading software release updates 3.1.1 or later to appliances that use versions 2.7.1 or 2.7.2. To download 3.1.1 or later release updates to appliances with these versions, you must download the updates manually. For instructions, refer to the following topic:

See [“Downloading software updates to a NetBackup appliance using a client share”](#) on page 19.

---

**To download a software release update onto the appliance using the NetBackup Appliance Web Console**

- 1** Open a web browser and log on to the appliance through the NetBackup Appliance Web Console.
- 2** Select **Manage > Software Updates**.
- 3** On the **Software Updates** page, in the **Downloaded Software Updates** table, check to make sure that the software update has not already been downloaded.
  - If the table contains the software update that you want to install, proceed to software installation as follows.
  - If the table does not contain a software update that you want to install, proceed to the next step.
- 4** In the **Online Software Updates** table on the page, select a software update and click **Download**.

The **Download Progress** column shows the download status. After the download has completed successfully, the software update appears in the **Available Software Updates** column of the **Downloaded Software Updates** table.

---

**Note:** Starting with appliance software version 3.1, the web console no longer supports the installation of upgrade or EEB packages. After you have downloaded these packages from the web console, you must perform the installation from the NetBackup Appliance Shell Menu.

---

## Downloading software updates directly to a NetBackup appliance

Use the following procedure to download a software release update to an appliance using the NetBackup Appliance Shell Menu.

---

**Note:** This method is not supported for downloading software release updates 3.1.1 or later to appliances that use versions 2.7.1 or 2.7.2. To download 3.1.1 or later release updates to appliances with these versions, you must download the updates manually. For instructions, refer to the following topic:

See [“Downloading software updates to a NetBackup appliance using a client share”](#) on page 19.

---

For high availability (HA) setups, you only need to download the package to one node. After you complete the package download on the first node, see [step 4](#) for details to make the package available on the other node.

### To download software release updates directly onto the appliance

- 1 Open an SSH session and log on to the appliance as an administrator using the NetBackup Appliance Shell Menu.
- 2 To determine if a software update is available from the Veritas Support website, enter the following command:

```
Main_Menu > Manage > Software > List AvailablePatch
```

- 3 To download an available software update or a client package, enter the appropriate command as follows:

- For appliance server updates:

```
Main_Menu > Manage > Software > Download  

SYMC_NBAPP_update-<release-version>.x86_64.rpm
```

Where *release* is the software release number and *version* is the version number of the software release. For example:

```
Main_Menu > Manage > Software > Download  

SYMC_NBAPP_update-3.1.x86_64.rpm
```

- For a UNIX client package:

```
Main_Menu > Manage > Software > Download  

SYMC_NBAPP_addon_nbclient_<platform>-<release>-<date>.x86_64.rpm
```

Where *<platform>* is the client platform operating system, *<release>* is the software release number, and *<date>* is the NetBackup client package date.

For example:

```
Main_Menu > Manage > Software > Download  

SYMC_NBAPP_addon_nbclient_Solaris-7.7.1-20150910.x86_64.rpm
```

- For a Windows client package:

```
Main_Menu > Manage > Software > Download
SYMC_NBAPP_addon_nbwin-<release>-<date>.x86_64.rpm
```

- 4 To verify that the rpm has downloaded successfully, enter the following command:

```
Main_Menu > Manage > Software > List Downloaded
```

After you run this command on the HA node with the downloaded package, run the command on the other node to make it available on that node.

See [“Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console”](#) on page 16.

## Downloading software updates to a NetBackup appliance using a client share

Use this procedure to download the software release updates or client packages to an appliance using a CIFS or an NFS client share.

For high availability (HA) setups, you only need to download the package to one node. After you complete the package download on the first node, see [step 8](#) for details to make the package available on the other node.

---

**Note:** If downloading the software updates directly to the appliance fails, use this method to download the appliance software release update or client package onto the appliance.

---

Perform this method from a computer that is connected to the appliance and that also has Internet access. Internet access is needed to download the files or packages from the Veritas Download Center.

### To download software release updates or client packages to the appliance using a CIFS or an NFS client share:

- 1 Open an SSH session and log on to the appliance as an administrator using the NetBackup Appliance Shell Menu.
- 2 To open an NFS or a CIFS share, enter the following command:

```
Main_Menu > Manage > Software > Share Open
```

- 3 Map or mount the appliance share directory as follows:

- Windows CIFS share
 

```
\\<appliance-name>\incoming_patches
```
- UNIX NFS share
 

```
mkdir -p /mount/<appliance-name>
```

```
mount
<appliance-name>:/inst/patch/incoming/mount/<appliance-name>
```

- 4 Go to the Veritas Download Center website and download the following items:
  - NetBackup Appliance 3.2 release update package
  - NetBackup 8.2 client and add-on packages
- 5 Copy the release update or client package to the mounted share.

---

**Note:** During the copy process, do not run any commands on the appliance. Doing so can cause the copy operation to fail.

---

- 6 After you have successfully copied the release update or client package into the mounted share, unmap or unmount the shared directory.
- 7 On the appliance, enter the following command to close the NFS and the CIFS shares:

```
Main_Menu > Manage > Software > Share Close
```

If you run any of the following commands before you close the share, the downloaded release update or client package is moved from the share directory location to its proper location. However, you must still run the `Share Close` command to ensure that the NFS and the CIFS shares are closed.

- `List Version`
- `List Details All`
- `List Details Base`
- `Share Open`
- `Share Close`

- 8 To list the available release updates or client packages on the appliance, enter the following command and note the name of the downloaded files:

```
Main_Menu > Manage > Software > List Downloaded
```

Running this command validates and moves the release update or the client package from the share directory to its proper location. You are not notified that this move has occurred.

After you run this command on the HA node with the downloaded package, run the command on the other node to make it available on that node.

See [“Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console”](#) on page 16.

# Installing a NetBackup appliance software update using the NetBackup Appliance Shell Menu

Use the following procedure to start the appliance upgrade.

---

**Note:** If you have enabled the STIG feature on an appliance and you need to upgrade it or install an EEB on it, do not plan such installations during the 4:00am - 4:30am time frame. By following this best practice, you can avoid interrupting the automatic update of the AIDE database and any monitored files, which can cause multiple alert messages from the appliance.

---

## To install a downloaded release update using the NetBackup Appliance Shell Menu

- 1 Check to make sure that the following required updates and pre-upgrade tasks have already been performed:
  - All required pre-upgrade updates have been completed. For a complete list of required updates prior to 3.2 upgrades, refer to the following article: [https://www.veritas.com/support/en\\_US/article.100046066](https://www.veritas.com/support/en_US/article.100046066)
  - All jobs have been stopped or suspended and all SLPs have been paused.
  - The `Support > Test Software` command has been run and it returned a **Pass** result.
- 2 Log in to the NetBackup Appliance Shell Menu from the IPMI console.

---

**Note:** Veritas recommends that you log in using the shell menu from the IPMI console instead of an SSH session. The IPMI console is also known as the Veritas Remote Manager interface. For details about how to access and use the Veritas Remote Manager, refer to the following document: *NetBackup Appliance Hardware Installation Guide*.

---

- 3 To install the software release update, run the following command:

```
Main_Menu > Manage > Software > Install patch_name
```

Where *patch\_name* is the name of the release update to install. Make sure that this patch name is the one that you want to install.

- 4 Monitor the preflight check and watch for any **Check failed** messages.
  - If no **Check failed** messages appear, you are prompted to continue to the next step to start the upgrade.

- If any **Check failed** messages appear, the upgrade is not allowed. You must resolve the reported failures, then launch the upgrade script again so that the preflight check can verify that the failures have been resolved. Click on the UMI links (V-409-xxx-xxxx) for information about how to resolve the reported issues.
  - If any **Check failed** messages indicate that a RHEL version third-party plug-in was not found, you must obtain the plug-in from the appropriate vendor. Refer to the following topic for installation details:
- 5** After all preflight check items have passed, and before the upgrade begins, you must first select how the upgrade process should respond if any errors occur during the upgrade. The following prompt appears:

```
If an error occurs during the upgrade, do you want to immediately enforce
```

Enter **yes** to immediately enforce an automatic rollback.

Enter **no** to pause the upgrade process and investigate the errors.

- 6** After all preflight check items have passed, you may need to trust the CA certificate and the host ID-based certificate to start the upgrade process.

To trust and deploy the CA certificates, do the following:

- Verify the CA certificate detail and enter **yes** to trust the CA certificate, as follows:

To continue with the upgrade, verify the following CA certificate detail and enter "yes" to trust the CA certificate.

CA Certificate Details:

```
Subject Name : /CN=nbatd/OU=root@abc.example.com/O=vx
Start Date   : Jul 14 12:59:18 2017 GMT
Expiry Date  : Jul 09 14:14:18 2037 GMT
SHA1 Fingerprint : 31:E9:97:2E:50:11:51:7C:D6:25:7F:32:86:3D:
                6B:D5:33:5C:11:E2
```

```
>> Do you want to trust the CA certificate? [yes, no] (yes)
```

- If the security level of the master server is **Very High**, you must manually enter an authorization token to deploy the host ID-based certificate on the appliance, as follows:

```
>> Enter token:
```

---

**Note:** If the appliance is ever factory reset or re-imaged after it has been upgraded to version 3.1 or later, a reissue token is required for the next upgrade.

---

- If the security level of the master server is **High** or **Medium**, the authentication token is not required. The host ID-based certificate is automatically deployed onto the appliance.

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

**7** Master server upgrades from software versions 3.1.1 and earlier require you to provide a registration key for the Veritas Smart Meter feature. The upgrade process displays the following instructions to obtain the key file and upload it to the appliance:

- Log in to the [Veritas Smart Meter](#) site with your VEMS credentials and go to the **Registration Keys** page.

- The following shares have been opened on this appliance:

```
CIFS share \hostname or
```

```
ip>\incoming_patches\customer_registration/
```

```
NFS share <hostname or
```

```
ip>:/inst/patch/incoming/customer_registration/
```

Mount one of these share paths.

- Upload the `veritas_customer_registration_key.json` file to the mounted share path.

Once the file is uploaded, you can continue with the upgrade for this Master server.

If you need assistance, contact Veritas Support.

- 8 To check the upgrade status before the **AIM** window appears, enter the following command:

```
Main_Menu > Manage > Software > UpgradeStatus
```

The system reboots at least two times during the upgrade process. After the first reboot, the NetBackup Appliance Web Console and any SSH-based connections to the server are unavailable until the reboot process has completed. This condition may last two hours or more, depending on the complexity of the appliance configuration. It is important that you do not attempt to manually reboot the appliance during this time. You can use the Veritas Remote Management interface (IPMI) to view the system status. In addition, you may view the logs under `/log` or wait for the appliance to send an email upon completion of the upgrade process.

During the upgrade process, you can open the **AIM** window to view the upgrade progress and the estimated remaining time.

- 9 If problems are detected during the post-upgrade self-test, the **AIM** window shows the upgrade status as **Paused**. Other SSH sessions and email notifications also indicate this status.

To clear the **Paused** status, perform the following tasks:

- Press the **V** key to switch to the **Verbose** view to see the logs. If there are any Unique Message Identification (UMI) codes for the errors, search for them on the [Veritas Support website](#) to get more detailed information.
- Try to fix the problem that the **AIM** window reports.  
If you need to use the shell menu, log on to the NetBackup Appliance Shell Menu through an SSH session. When the **AIM** window appears, press the **S** key to close it.
- Go back to the **AIM** window on the IPMI console.  
If you tried fixing the problem, press the **A** key to attempt the self-test again. If you cannot fix the problem, contact Technical Support or press the **R** key to roll back the appliance to the previous software version.

---

**Note:** Starting with the 3.1.2 release, if the post-upgrade self-test fails, an automatic rollback is no longer enforced. If you select **Attempt again** and the self-test still fails, the upgrade pauses again and prompts with the same options.

---



- 10** After the upgrade has completed, the **AIM** window shows a summary of the upgrade results.

After

the disk pools are back online, the appliance runs a self-diagnostic test. Refer to the following file for the test results:

```
/log/selftest_report_<appliance_serial>_<timedate>.txt
```

If SMTP is configured, an email notification that contains the self-test result is sent.

- 11** Complete this step only if your backup environment includes SAN client computers.

The Fibre Channel (FC) ports must be re-scanned to allow any SAN client computers to reconnect to the Fibre Transport (FT) devices. The re-scan must be done from the NetBackup CLI view on the appliance.

To re-scan the FC ports:

- Enter the following command to see a list of NetBackup user accounts:

```
Manage > NetBackupCLI > List
```

- Log on to this appliance as one of the listed NetBackup users.
- Run the following command to rescan the FC ports:

```
nbftconfig -rescanallclients
```

- If any SAN clients still do not work, run the following commands on each of those clients in the order as shown:

On UNIX clients:

```
/usr/opensv/netbackup/bin/bp.kill_all
```

```
/usr/opensv/netbackup/bin/bp.start_all
```

On Windows clients:

```
<install_path>\NetBackup\bin\bpdown
```

```
<install_path>\NetBackup\bin\bpup
```

- If any SAN clients still do not work, manually initiate a SCSI device refresh at the OS level. The refresh method depends on the operating system of the client. Once the refresh has completed, attempt the `nbftconfig -rescanallclients` command again.
- If any SAN clients still do not work, reboot those clients.

---

**Note:** If you have SLES 10 or SLES 11 SAN clients that still do not work, Veritas recommends upgrading the QLogic driver on those clients. For the affected SLES 10 clients, upgrade to version 8.04.00.06.10.3-K. For the affected SLES 11 clients, upgrade to version 8.04.00.06.11.1.

---

# Post upgrade tasks

This chapter includes the following topics:

- [Post upgrade tasks](#)

## Post upgrade tasks

After the upgrade process has completed successfully, refer to the following article for a checklist of any required or recommended updates that you should install:

[https://www.veritas.com/support/en\\_US/article.100046589](https://www.veritas.com/support/en_US/article.100046589)

# NetBackup client upgrades with VxUpdate

This chapter includes the following topics:

- [About VxUpdate](#)
- [VxUpdate repository management](#)
- [Deployment policy management](#)
- [Manually initiating upgrades from the master server using VxUpdate](#)
- [Manually initiating upgrades from the client using VxUpdate](#)
- [Deployment job status](#)

## About VxUpdate

Veritas introduces VxUpdate as the replacement for LiveUpdate. The main component of VxUpdate is the new deployment policy that serves as a client upgrade tool. With the release of VxUpdate, Veritas no longer supports LiveUpdate.

With support for policies, Veritas provides a simplified tool for client upgrades. No additional external tools are required and the configuration is in a familiar policy-based format, similar to a backup policy. Signed packages are verified and installed into the VxUpdate repository on the master server. Once the packages are installed, they become available for use with deployment policies. Additionally, you can use the deployment policies to automate the installation of emergency engineering binaries, as provided by Veritas.

---

**Note:** You can only cancel queued deployment jobs. Once a VxUpdate job enters the active state it cannot be canceled.

---

The deployment policies are not located with the other policies in the NetBackup Administrative Console. Deployment policies are located in the NetBackup Administration Console under **Deployment Management > Deployment Policies**.

To successfully create and use deployment policies, Veritas recommends:

**Table 5-1**

Step	Action	Additional information
1	Populate the NetBackup repository	See <a href="#">“VxUpdate repository management”</a> on page 29.
2	Create the deployment policy	See <a href="#">“Deployment policy management”</a> on page 32.
3	(Optional) Manually run the upgrade from the master server or the client	See <a href="#">“Manually initiating upgrades from the master server using VxUpdate”</a> on page 36.  See <a href="#">“Manually initiating upgrades from the client using VxUpdate”</a> on page 40.

## VxUpdate repository management

The appliance `VxUpdate` commands control the VxUpdate package repository contents. Do not attempt to manually modify or update the repository without the use of the `VxUpdate` commands. If you populate the repository with all the client packages for all platforms, you need approximately 20 GB of space on the appliance master server. This amount does not include any engineering binaries or hotfixes. Note that this is the approximate amount of space that is required for all packages for all platforms for each NetBackup version.

The `AddPkg` option verifies and populates the repository with supported VxUpdate client and NetBackup EEB packages. Veritas signs the VxUpdate packages. Attempts to populate the repository with unofficial or unsigned packages fails. These packages are referenced in the deployment policies that install NetBackup on target hosts. When you use the `AddPkg` option to populate the repository, be mindful of the required disk space. The master server must have enough disk space to store packages for the NetBackup versions and platforms that are specified in deployment policies.

The package types you can load into the repository include:

- **VxUpdate client packages**  
 You can upgrade NetBackup clients to a newer version of NetBackup with VxUpdate. These packages are slightly different from standard NetBackup client

packages. The packages include additional components to support the various VxUpdate operations.

- **Emergency binaries (EEBs) and hotfixes**  
You can use VxUpdate to deploy emergency binaries and hotfixes to NetBackup 8.1.2 and later clients. You can obtain VxUpdate formatted EEBs from support in the same way you obtain traditional EEBs. These EEBs are only for NetBackup version 8.1.2 and later. Any client hotfixes that Veritas creates for NetBackup 8.1.2 and later releases include VxUpdate formatted fixes.

VxUpdate formatted packages are available from the [myveritas.com](https://myveritas.com) licensing portal. Emergency binaries and hotfixes are obtained from the standard locations. You should download the VxUpdate versions of these packages and place them in a location accessible to the master server. Once they are accessible to your master server, you can add them to the VxUpdate package repository.

### Downloading Veritas approved NetBackup client packages

- 1 Go to the [myveritas.com](https://myveritas.com) licensing portal.
- 2 Enter your user name and password.
- 3 Select **Licensing**.
- 4 Enter or select your account number.
- 5 Select **Apply Filters**
- 6 Select your account number from the resulting table.  
This action presents a listing of your entitlements. From here, you have the ability to download the associated software.
- 7 Select **Downloads**
- 8 Use the filter options to limit the results to the NetBackup product line and the appropriate product version.  
Add your filters and select **Apply Filters**.
- 9 Under **Actions**, select the download icon
- 10 In the resulting table, select the VxUpdate packages and then select **Download**.  
The client packages follow the naming convention shown:  
`vxupdate_nbclient_version_operatingsystem_platform.sja`
- 11 Download and extract the files to `/inst/patch/incoming` on the appliance.

- 12 Run the following command to verify that all packages have been downloaded and extracted:

```
Main > Manage > Software > List Downloaded
```

- 13 After you have verified that all of the downloaded and extracted packages are listed, add the packages to the NetBackup package repository.

See [the section called “Adding packages to the VxUpdate package repository”](#) on page 31.

## Adding packages to the VxUpdate package repository

VxUpdate can only use the Veritas signed packages that you add to the VxUpdate package repository. Use the VxUpdate `AddPkg` option to add packages to the repository. This command also adds metadata to the EMM database and places the packages in the repository directory structure on the file system. You can use the `ListPkgs` option to list the contents of the package repository to verify that a package was added.

### To add packages to the repository

- 1 On the appliance master server, log in to the NetBackup Appliance Shell Menu as an administrator and navigate to the following menu:

```
Main > Manage > Software > VxUpdate
```

- 2 Run the `AddPkg package_name` option, where `package_name` is the client package name.

Example: `AddPkg vxupdate_nbclient_8.2_suse_ppc64le.sja`

- 3 To view the repository and verify that the package was added, run the `ListPkgs` option.
- 4 To see the package details, run the `ShowPkgDetails n` option, where `n` is the package ID number.

## Deleting packages from the VxUpdate package repository

You can delete packages from the repository either when they are no longer needed or to conserve disk space. For example, delete the NetBackup 8.1.2 packages once all of the clients are upgraded to that version. Use the `DelPkg` option to delete packages. To verify that a package was deleted, use the `ListPkgs` option to list all existing packages.

### To delete packages from the repository

- 1 On the appliance master server, log in to the NetBackup Appliance Shell Menu as an administrator and navigate to the following menu:

```
Main > Manage > Software > VxUpdate
```

- 2 To view a list of the packages in the repository, run the `ListPkgs` option and take note of the ID number that identifies each package.
- 3 Run the `DelPkg ID` option to delete any unused packages.

Example: `DelPkg 1`

For more information about `VxUpdate` command options, see the *NetBackup Appliance Commands Reference Guide*.

## Deployment policy management

Use the procedures that are shown to create, modify, and delete your deployment policies.

### Creating a deployment policy

---

**Note:** You must add packages to the VxUpdate repository before you can create a working deployment policy. You can create deployment policies without packages in the repository, but those policies fail to run successfully. More information about the management of the VxUpdate repository is available.

---

- 1 In the NetBackup Administration Console, in the left pane, select **Deployment Management > Deployment Policies**.
- 2 From the **Actions** menu, select **New Deployment Policy**.
- 3 Enter a unique name for the new policy in the **Add a New Deployment Policy** dialog box.
- 4 Click **OK**.
- 5 Specify the information that is shown on the **Attributes** tab in the **Change Deployment Policy** window:
  - **Package:** Select the package that you want deployed from the drop-down menu.



---

**Note:** Specifying a package that supports external certificate authority certificates presents you with an additional tab titled **Security**. That tab is covered later in this procedure.

---

- **Media server:** Specify the media server from drop-down. The media server that is specified is used to connect and transfer files to the NetBackup hosts that are included in the policy. The media server also caches the files from the NetBackup repository. The media server must be version NetBackup 8.1.2 or later. Since the repository resides on the master server, the master server is the default value for the media server field.
  - (Conditional): Select the **Limit simultaneous jobs** option and specify a value for **jobs** to limit the total number of concurrent jobs that can run at a time. The minimum value is 1 and the maximum value is 999. If the check box is selected, the default value is 3. If you do not select the check box, no limit is enforced for the simultaneous upgrade jobs. You can set unlimited simultaneous upgrade jobs through command line interface by setting the value as 0.
  - **Select hosts:** Select hosts from the **Available hosts** list and select **Add** to add hosts to the deployment policy. The list is generated from hosts in the host database and backup policies. Once you select **Add**, the hosts are shown under **Selected hosts**.
- 6** Select the **Schedules** tab in the **Change Deployment Policy** window.  
You can see a summary of all schedules within that policy.
- 7** Select **New**.
- 8** Specify the information that is shown in the **Add Deployment Schedule** window.
- **Name:** Enter a name for the new schedule.
  - **Type:** Specify the type of schedule you want created.  
Schedule types:
    - **Precheck**  
Performs the various precheck operations, including confirming there is sufficient space on the client for the update. The precheck schedule type does not exist for EEB packages.
    - **Stage**  
Moves the update package to the client, but does not install it. Also performs the precheck operation.
    - **Install**

Installs the specified package. Also performs the precheck and the stage package operations. If you already performed the stage package operation, the install schedule does not move the package again.

---

**Note:** Please be aware that adding multiple different schedule types to the same deployment schedule window has unpredictable results. VxUpdate has no defined behavior to determine which schedule type runs first. If a single deployment schedule window has precheck, stage, and install jobs, there is no way to specify the order in which they run. The precheck or the stage schedules can fail, but the install completes successfully. If you plan to use precheck, stage, and install schedules, Veritas recommends that you create separate schedules and separate windows for each.

---

- **Starts:** Specify the date and time you want the policy to start in the text field or with the date and the time spinner. You can also click the calendar icon and specify a date and time in the resulting window. You can select a schedule by clicking and dragging over the three-month calendar that is provided at the bottom of the window.
  - **Ends:** Specify the date and time you want the policy to end as you specified the start time.
  - **Duration:** Optionally, you can specify a duration in days, hours, minutes, and seconds instead of an end time for the policy. The minimum value is 5 minutes and the maximum is 99 days.
  - Select **Add/OK** and the schedule is created. Select **OK** to save and create your policy.
- 9** A **Security** tab appears when you select a deployment package that contains support for external certificate authorities.

By default, the **Use existing certificates when possible** option is selected. This option instructs NetBackup to use the existing NetBackup CA or external CA certificates, if available.

---

**Note:** If you specify this option and certificates are not available, your upgrade fails.

---

Deselecting the **Use existing certificates when possible** option lets you specify the location for external certificate authority information for both UNIX and Linux computers and Windows computers.

- 10** Windows clients have **Use Windows certificate store** selected by default.

You must enter the certificate location as *Certificate Store Name\Issuer Distinguished Name\Subject Distinguished Name*.

---

**Note:** You can use the `$hostname` variable for any of the names in the certificate store specification. The `$hostname` variable evaluates at run time to the name of the local host. This option provides flexibility when you push NetBackup software to a large number of clients.

---

Alternatively, you can specify a comma-separated list of Windows certificate locations. For example, you can specify:

```
MyCertStore\IssuerName1\SubjectName,  
MyCertStore\IssuerName2\SubjectName2,  
MyCertStore4\IssuerName1\SubjectName5
```

Then select the Certificate Revocation List (CRL) option from the radio buttons shown:

- **Do not use a CRL.** No additional information is required.
- **Use the CRL defined in the certificate.** No additional information is required.
- **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

**11** For both UNIX and Linux clients and Windows clients that select the **From certificate file path (for file-based certificates)** option, specify the information as shown:

- **Certificate file:** This field requires you to provide the path to the certificate file and the certificate file name.
- **Trust store location:** This field requires you to provide the path to the trust store and the trust store file name.
- **Private key path:** This field requires you to provide the path to the private key file and the private key file name.
- **Passphrase file:** This field requires you to provide the path of the passphrase file and the passphrase file name. This field is optional.
- Then specify the correct CRL option for your environment:
  - **Do not use a CRL.** No additional information is required.
  - **Use the CRL defined in the certificate.** No additional information is required.

- **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

**To change a deployment policy**

- 1 Right click on the deployment policy and select **Change**.
- 2 Navigate through the deployment policy tabs and make any necessary changes to the policy.
- 3 Select **OK** and the policy is updated.

**Deleting a deployment policy**

- 1 Right click on the deployment policy and select **Delete**.
- 2 Select **OK**.
- 3 Confirm the deletion of the policy.

## Manually initiating upgrades from the master server using VxUpdate

You can manually initiate upgrades with VxUpdate using one of two methods. You can manually initiate an upgrade based on an existing policy. You can also initiate an upgrade without an associated policy.

Manually initiate deployment policies when you are logged into the master server locally and need to force an immediate update. Or you can initiate an immediate upgrade for emergency binaries. VxUpdate also provides the ability to launch upgrades from the client with the command line. More information is available.

See [“Manually initiating upgrades from the client using VxUpdate”](#) on page 40.

**To manually initiate an upgrade of all clients in a policy from the administration console**

- 1 In the NetBackup Administration Console, navigate to **Deployment Management > Deployment Policies**.
- 2 In the middle pane, expand the master server, and select the policy you want to run.
- 3 Right-click on the policy you want to start, and select **Manual Deployment**.
- 4 Alternatively, after selecting the policy you want to run, you can select **Actions > Manual Deployment**.

### To manually initiate an upgrade of a specific client in a policy from the administration console

- 1 Select **NetBackup Management > Host Properties > Clients** in the NetBackup Administrative Console.
- 2 Right click on the host you want to upgrade in the right pane.
- 3 Select **Upgrade Host**.
- 4 In the **Upgrade Host** dialog:
  - Select the package you want to use from the **Package** drop-down.

---

**Note:** Specifying a package that supports external certificate authority certificates presents you with an additional button titled **Configure**. That button is covered in the next step.

---

- Specify the type of schedule you want to run from the **Type** drop-down.
  - Select the media server you want to use from the **Media server** drop-down.
  - Confirm that the host you want upgraded is listed under **Selected hosts**.
- 5 (Conditional) If present, click on the **Configure** button to configure external certificate authority information.

By default, the **Use existing certificates when possible** option is selected. This option instructs NetBackup to use the existing NetBackup CA or external CA certificates, if certificates available.

---

**Note:** If you specify this option and certificates are not available, the upgrade fails.

---

Deselecting the **Use existing certificates when possible** option lets you specify the location for external certificate authority information for both UNIX and Linux computers and Windows computers.

- 6 Windows clients have **Use Windows certificate store** selected by default.

You must enter the certificate location as *Certificate Store Name\Issuer Distinguished Name\Subject Distinguished Name*.

---

**Note:** You can use the `$hostname` variable for any of the names in the certificate store specification. The `$hostname` variable evaluates at run time to the name of the local host. This option provides flexibility when you push NetBackup software to a large number of clients.

---

Alternatively, you can specify a comma-separated list of Windows certificate locations. For example, you can specify:

```
MyCertStore\IssuerName1\SubjectName,  
MyCertStore\IssuerName2\SubjectName2,  
MyCertStore4\IssuerName1\SubjectName5
```

Then select the Certificate Revocation List (CRL) option from the radio buttons shown:

- **Do not use a CRL.** No additional information is required.
- **Use the CRL defined in the certificate.** No additional information is required.
- **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

**7** For both UNIX and Linux clients and Windows clients that select the **From certificate file path (for file-based certificates)** option, specify the information as shown:

- **Certificate file:** This field requires you to provide the path to the certificate file and the certificate file name.
- **Trust store location:** This field requires you to provide the path to the trust store and the trust store file name.
- **Private key path:** This field requires you to provide the path to the private key file and the private key file name.
- **Passphrase file:** This field requires you to provide the path of the passphrase file and the passphrase file name. This field is optional.
- Then specify the correct CRL option for your environment:
  - **Do not use a CRL.** No additional information is required.
  - **Use the CRL defined in the certificate.** No additional information is required.
  - **Use the CRL at the following path:** You are prompted to provide a path to the CRL.

**8** Select **OK** to launch the upgrade.

---

**Note:** You can also launch an upgrade job from the **Policies** section of the NetBackup Administrative Console. Select **NetBackup Management > Policies** in the NetBackup Administrative Console. In the middle pane, select **Clients**. Then right-click on the client you want to upgrade in the right pane and select **Upgrade Host**. Then follow the procedure shown.

---

### To manually initiate an upgrade from the command line for all clients in a policy

Use this procedure to manually start an upgrade for all clients in a policy.

---

**Note:** This procedure starts the upgrade for all clients in the specified policy. You can start an upgrade on selected clients. More information is available.

[To manually initiate an upgrade from the command line for selected clients in a policy](#)

---

- 1 Open a command prompt and navigate to the directory shown:

Windows: `install_path\netbackup\bin`

UNIX or Linux: `/usr/opensv/netbackup/bin`

- 2 Use the `nbinstallcmd` command as shown to launch a policy:

Where *policy\_name* is the name of the deployment policy, *schedule* is the name of the schedule, and *master* is the name of the master server.

### To manually initiate an upgrade from the command line for selected clients in a policy

Use this procedure to manually start an upgrade for selected clients in a policy.

---

**Note:** This procedure starts the upgrade on selected clients in the specified policy. You can start an upgrade for all clients in a policy. More information is available.

[To manually initiate an upgrade from the command line for all clients in a policy](#)

---

- 1 Open a command prompt and navigate to the directory shown:

Windows: `install_path\netbackup\bin`

UNIX or Linux: `/usr/opensv/netbackup/bin`

- 2 Use the `nbinstallcmd` command as shown:

```
nbinstallcmd -policy policy_name -schedule schedule
{-host_filelist filename|-hosts client1, client2, clientN}
```

Where:

- *policy\_name* is the name of the deployment policy
- *schedule* is the name of the schedule
- *filename* is the name of a file that contains a list of clients to upgrade.
- *client1, client2, clientN* is a list of clients to upgrade.

You can manually initiate the upgrade of a single client from the command line without an associated policy. The options required for the `ninstallcmd` command vary depending on your security configuration. Please refer to the `ninstallcmd` command documentation for a list of all possible options and examples of command usage.

[NetBackup Commands Reference Guide](#)

## Manually initiating upgrades from the client using VxUpdate

Manually initiate deployment jobs when you are logged into the client locally and want to force an immediate update. You can either use a deployment policy to initiate an immediate upgrade or specify an upgrade without an associated policy. You can use the upgrade to update the NetBackup version or for other upgrades such as emergency binaries.

Among the reasons for a client initiated upgrade using VxUpdate is mission critical systems with specific maintenance windows. One example of these systems is database servers with limited available down time.

---

**Note:** You can only launch updates on the local client. You cannot use the `ninstallcmd` command on a client to launch jobs on other clients. If you want to launch updates on other clients, you must initiate them from the master server.

---

VxUpdate also provides the ability to launch upgrades from the master server with the command line. More information is available.

See [“Manually initiating upgrades from the master server using VxUpdate”](#) on page 36.



### To start a client initiated deployment job based on an existing policy

- 1 Navigate to the binary directory from a command prompt.

UNIX or Linux: `/usr/opensv/netbackup/bin`

Windows: `install_path\netbackup\bin`

- 2 Use the `nbininstallcmd` as shown:

```
nbininstallcmd -policy policy -schedule schedule -master_server  
name
```

**Example:** `nbininstallcmd -policy all_clients -schedule install812  
-master_server master1`

If the job initiated successfully, you are returned to the command prompt without an error message.

- 3 Monitor upgrade status with the NetBackup administrator and the Activity Monitor in the NetBackup Administrative Console.

You can start a client initiated deployment job without an associated policy from the command line. The options required for the `nbininstallcmd` command vary depending on your security configuration. Please refer to the `nbininstallcmd` command documentation for a list of all possible options and examples of command usage.

[NetBackup Commands Reference Guide](#)

## Deployment job status

Monitor and review deployment job status in the Activity Monitor in the NetBackup Administration Console. The **Deployment** job type is the new type for VxUpdate policies. Deployment policy parent jobs that exit with a status code 0 (zero) indicate that all the child jobs successfully completed. Parent jobs that finish with a status code 1 indicate that one or more of the child jobs succeeded, but at least one failed. Any other status code indicates failure. Review the status of the child jobs to determine why they failed. Otherwise, there are no differences between deployment jobs and other NetBackup jobs.

Your deployment job may receive a status code 224. This error indicates that the client's hardware and operating system are specified incorrectly. You can correct this error by modifying the deployment policy with the `bpplclients` command found in:

UNIX or Linux: `/usr/opensv/netbackup/bin/admincmd`

Window: `install_path\netbackup\bin\admincmd`.

Use the syntax shown:

```
bpplclients deployment_policy_name -modify client_to_update -hardware
new_hardware_value -os new_os_value
```

Deployment policies use a simplified naming scheme for operating system and hardware values. Use the values as shown for the `bpplclients` command:

**Table 5-2** Deployment policy operating system and hardware

Operating system	Hardware
hpux	ia64
debian	x64
redhat	x64
suse	x64
redhat	ppc64le
suse	ppc64le
redhat	zseries
suse	zseries
aix	rs6000
solaris	sparc
solaris	x64
windows	x64

Security certificates are not deployed as part of the VxUpdate upgrade if the **Security Level for certificate deployment** is set to **Very High**. This setting is located in the **NetBackup Global Security Settings** in the NetBackup Administration Console.

If you cannot communicate with your clients after you use VxUpdate to upgrade your clients, please ensure that the proper security certificates were issued during upgrade. You may need to manually deploy the certificates. Refer to the technote that is shown for additional details:

[https://www.veritas.com/support/en\\_US/article.000127129](https://www.veritas.com/support/en_US/article.000127129)

# Troubleshooting

This chapter includes the following topics:

- [Troubleshooting upgrade issues](#)

## Troubleshooting upgrade issues

If the upgrade fails or if you experience other upgrade issues, access the following information to help resolve the issues.

- [Rollback after NetBackup appliance upgrade failure causes inactive media server](#)
- [Preflight checkpoint creation failure prevents NetBackup appliance upgrade from starting](#)
- [Old checkpoints remain after interrupting a NetBackup appliance upgrade or rollback](#)

# Index

## A

- Appliance Install Manager (AIM) 7
- appliance server or client package
  - download directly 17
- appliance upgrades
  - requirements and best practices 9

## C

- client share
  - download software updates 19

## D

- download directly
  - appliance server or client package 17
- download methods
  - release updates 16
- download software updates
  - from NetBackup Appliance Web Console 16
  - using client share 19

## I

- install update from NetBackup Appliance Shell Menu
  - version 3.2 21

## R

- requirements and best practices
  - appliance upgrades 9

## S

- software updates
  - download from NetBackup Appliance Web Console 16

## T

- troubleshoot upgrade issues 43

## U

- upgrade
  - version 3.2 with RHEL operating system 6
- upgrade time estimation 15
- upgrades
  - supported upgrade paths 6

## V

- version 3.2
  - install update from NetBackup Appliance Shell Menu 21
- version 3.2 upgrades
  - RHEL operating system 6