

# Veritas NetBackup™ Appliance Upgrade Guide

Release 3.1

Document Revision 1

Red Hat Enterprise Linux (RHEL)  
Operating System

**VERITAS™**

# Veritas NetBackup™ Appliance Upgrade Guide - Red Hat Enterprise Linux (RHEL) Operating System

Release 3.1, Document Revision 1

## Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

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

<http://www.veritas.com>

## Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

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

Japan

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

## Documentation

The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

## Documentation feedback

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

[APPL.docs@veritas.com](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 upgrades to NetBackup appliance software version 3.1 and the Red Hat Enterprise Linux operating system .....	6
	Supported upgrade paths .....	7
	Preflight check before the upgrade .....	7
	Third-party plug-ins for RHEL .....	8
	Appliance behavior during upgrades .....	8
	Changes during upgrades .....	10
	About corresponding NetBackup software versions .....	10
	About the Appliance Install Manager .....	10
<b>Chapter 2</b>	<b>Upgrade planning</b> .....	<b>12</b>
	Guidelines and best practices for upgrading NetBackup appliances .....	12
	Upgrade time estimation .....	12
	Upgrade guidelines .....	13
<b>Chapter 3</b>	<b>Pre-upgrade tasks</b> .....	<b>16</b>
	Pre-upgrade tasks for appliance upgrades .....	16
	Stop all backup jobs and run a software self-test .....	16
	Delete previously downloaded release updates, client packages, and client add-ons .....	17
	Obtain necessary third-party plug-ins .....	19
	Update firewall rules for new Veritas servers .....	20
	Update disk drive firmware .....	20
<b>Chapter 4</b>	<b>Performing the upgrade</b> .....	<b>22</b>
	Methods for downloading appliance software release updates .....	22
	Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console .....	22
	Downloading software updates directly to a NetBackup appliance .....	23
	Downloading software updates to a NetBackup appliance using a client share .....	24

	Installing a NetBackup appliance software update using the NetBackup Appliance Shell Menu .....	28
Chapter 5	Post upgrade tasks .....	33
	Post upgrade tasks for 3.1 upgrades .....	33
Chapter 6	Troubleshooting .....	35
	Troubleshooting upgrade issues .....	35
Index .....		36

# Introduction

This chapter includes the following topics:

- [About upgrades to NetBackup appliance software version 3.1 and the Red Hat Enterprise Linux operating system](#)

## About upgrades to NetBackup appliance software version 3.1 and the Red Hat Enterprise Linux operating system

---

**Note:** NetBackup Appliance release 3.1 has been updated as of November 8, 2017. This updated release helps to ensure a successful upgrade and it also includes an automatic EEB installation that resolves a kernel panic problem. If you have already upgraded successfully to appliance release 3.1 before November 8, 2017, you do not need to upgrade again. To resolve an existing kernel panic problem or to prevent one in the future, refer to the following article to obtain an EEB to fix the issue: [www.veritas.com/docs/100040686](http://www.veritas.com/docs/100040686)

---

Starting with NetBackup appliance software version 2.7.1, Red Hat Enterprise Linux (RHEL) replaces the SUSE Linux Enterprise Server (SLES) operating system. You can upgrade any existing 5220, 5230, 5240 or 5330 appliances that currently use earlier software versions to version 3.1. In some situations, you may need to upgrade twice to get to version 3.1.

---

**Note:** The NetBackup 5200 Appliance does not support upgrade to versions 2.7.1 and later, due to Intel components that are not supported by RHEL version 6.6 or later.

---

---

**Note:** Appliance upgrades to software version 3.1 and later are not supported from the NetBackup Appliance Web Console. To upgrade to version 3.1, use the IPMI console to log in to the NetBackup Appliance Shell Menu.

---

This topic covers the following information that you should review before an upgrade to version 3.1:

[Supported upgrade paths](#)

[Preflight check before the upgrade](#)

[Third-party plug-ins for RHEL](#)

[Appliance behavior during upgrades](#)

[Changes during upgrades](#)

[About corresponding NetBackup software versions](#)

[About the Appliance Install Manager](#)

## Supported upgrade paths

The following describes the supported upgrade paths to version 3.1:

- Direct upgrade path  
The following appliances can be upgraded directly to version 3.1:
  - Any NetBackup 5220, 5230, or 5330 appliances with version 2.6.1, 2.6.1.x, 2.7.x, and 3.0
  - NetBackup 5240 appliance with version 2.7.3 and 3.0
- Two-step upgrade path  
Any NetBackup 5220 or 5230 appliances with versions earlier than 2.6.1 must be upgraded twice to get to version 3.1. It is recommended that these systems first be upgraded to version 2.6.1.2, then upgraded to version 3.1.

---

**Note:** For appliances with versions earlier than 2.6.1, refer to the following document for upgrade instructions: *NetBackup Appliance Upgrade Guide - Software Releases through 2.6.1.2 - SUSE Linux Enterprise Server (SLES) Operating System*. Then use this document to upgrade to version 3.1.

---

## Preflight check before the upgrade

For upgrades to versions 2.7.1 and later, the upgrade script runs a preflight check to determine if the appliance is ready for an upgrade. The preflight check analyzes

several system parameters and provides information about what was found and whether an upgrade can proceed. If the preflight check detects any issues that fail to meet the upgrade requirements, the upgrade is not allowed to proceed. You must address all of the reported issues before the upgrade is allowed.

Refer to the following topic for more information:

See [“Pre-upgrade tasks for appliance upgrades”](#) on page 16.

---

**Note:** Upgrades to version 2.7.1 and later are not supported if you have installed Teradata binaries on the appliance. The RHEL operating system does not currently support the use of these binaries. The upgrade cannot proceed if the preflight check finds Teradata binaries on the appliance.

---

## Third-party plug-ins for RHEL

Since all NetBackup appliances with version 2.6.1.2 and earlier use SLES version third-party plug-ins, upgrades to version 2.7.1 and later require use the appropriate RHEL versions to replace these plug-ins. The upgrade cannot proceed until all required RHEL third-party plug-ins are available in the preflight upgrade script.

---

**Note:** The preflight upgrade script only identifies those plug-ins that are required for the upgrade. At the time when version 2.7.1 was released, some third-party vendors had not yet completed development of their RHEL equivalent plug-ins. Make sure to check those vendor websites periodically for any additional plug-ins that you may need.

---

Refer to the following topic for installation details:

See [“Pre-upgrade tasks for appliance upgrades”](#) on page 16.

## Appliance behavior during upgrades

The upgrade mechanism takes the following measures to ensure that the upgrade process completes successfully:

- Determines if the available update is newer than the version of software that is currently installed.
- Determines if there is enough available space on the appliance to install the release update.
- Stops the processes that are currently active on the appliance.
- Checks for any active NetBackup jobs. The upgrade proceeds only if it is determined that no active jobs are detected.



The appliance software upgrade occurs only after all of these criteria are met.

- To view the upgrade progress, log in to the NetBackup Appliance Shell Menu from the IPMI console and run the following command:

```
Main > Manage > Software > UpgradeStatus
```

- The appliance reboots four times during the upgrade progress. The following describes what takes place at each reboot:
  - First reboot - installs the Red Hat Enterprise Linux (RHEL) operating system.
  - Second reboot - initializes the appliance using the new RHEL operating system.
  - Third reboot - restores the appliance configuration.
  - Fourth reboot - initializes the restored appliance configuration with the RHEL operating system.

After the first reboot, the NetBackup Appliance Web Console and any SSH-based connections to the server are unavailable until all reboots have completed. This condition may last 2 hours or more, depending on the complexity of the appliance configuration. Do not attempt to manually reboot the appliance during this time. You can use the Veritas Remote Management interface (IPMI) to view the system reboot 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.

After the third reboot occurs, the **Appliance Install Manager (AIM)** window appears and shows the upgrade progress.

See [“About the Appliance Install Manager”](#) on page 10.

- Before the upgrade can complete, a self-test is performed automatically. If the self-test fails, the upgrade pauses and you are prompted to select one of the following:
  - **Attempt again** to try the self-test again.
  - **Rollback now** to roll back to the previous version.

You must respond on the AIM window on the IPMI console within one hour, otherwise a rollback occurs automatically.

---

**Note:** If you select **Attempt again** and the self-test still fails, the upgrade pauses again and prompts with the same options.

---

See [“About the Appliance Install Manager”](#) on page 10.

- After a successful appliance upgrade, the Fibre Transport Media Server (FTMS) reboots automatically. As a result, the Fibre Channel (FC) ports must be

re-scanned to allow any SAN Client computers to reconnect to the Fibre Transport (FT) devices. The upgrade procedures include the details on how to re-scan the FC ports.

## Changes during upgrades

During the upgrade, the following change occurs:

- For upgrades from 2.6.1 or 2.6.1.x to 2.7.x or 3.0, the Symantec Critical System Protection (SCSP) feature is updated to version 6.5 and renamed as Symantec Data Center Security (SDCS). For all upgrades to 3.1 and later, the SDCS console and server are no longer included with NetBackup appliance software upgrade packages.

For more information, refer to the following topic:

See [“Post upgrade tasks for 3.1 upgrades”](#) on page 33.

## About corresponding NetBackup software versions

NetBackup software version 8.1 is included with NetBackup appliance release 3.1. [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

## About the Appliance Install Manager

Starting with the 3.1 release, the NetBackup Appliance Shell Menu includes the **Appliance Install Manager (AIM)** window. The **AIM** window appears in the NetBackup Appliance Shell Menu, after the third reboot during the upgrade process. This window shows the estimated completion time, the upgrade progress bar, the main upgrade steps, the upgrade logs, and other useful information.

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 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:

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

## Guidelines and best practices for upgrading NetBackup appliances

This topic describes the guidelines and best practices that you should follow anytime you plan to upgrade appliance software. Use the following information to help prepare for an appliance upgrade and to help avoid situations that can prevent a successful upgrade.

### Upgrade time estimation

**Table 2-1** Upgrade scenarios and related time estimations

Model	Upgrade path	Estimated base time	Additional time considerations
5220	2.6.1 -> 3.1 2.6.1.x -> 3.1 2.7.x -> 3.1 3.0 -> 3.1	2 - 2.5 hours	<ul style="list-style-type: none"><li>▪ For master server upgrades, add 30 minutes.</li><li>▪ For appliances that were previously upgraded from versions 2.0.x, 2.5.x, or 2.6.0.1, add 30 minutes.</li></ul>

**Table 2-1** Upgrade scenarios and related time estimations (*continued*)

Model	Upgrade path	Estimated base time	Additional time considerations
5230	2.6.1 -> 3.1 2.6.1.x -> 3.1 2.7.x -> 3.1 3.0 -> 3.1	2 - 2.5 hours	<ul style="list-style-type: none"> <li>■ For master server upgrades, add 15 minutes.</li> <li>■ For appliances that were previously upgraded from versions 2.5.4 or 2.6.0.1, add 30 minutes.</li> <li>■ For appliances with more than two Veritas Storage Shelf units, add 15 minutes.</li> </ul>
5330	2.6.1 -> 3.1 2.6.1.x -> 3.1 2.7.x -> 3.1 3.0 -> 3.1	2 - 2.5 hours	For appliances with Expansion Storage Shelf units, add 15 minutes for each unit.
5240	2.7.3 -> 3.1 3.0 -> 3.1	1.5 - 2 hours	N/A

For all the upgrade scenarios, refer to the following:

- Add 10 minutes for every 350,000 jobs on the master server. For example, add 30 minutes to a master server with a job list containing 1 million records.
- Add 5 minutes for every 250 VLANs that you have configured.

## Upgrade guidelines

Review the following guidelines before you begin the upgrade:

- Make sure that your appliance environment currently uses software version 2.6.1, 2.6.1.1, 2.6.1.2, 2.7.1, 2.7.2, 2.7.3 or 3.0. Only these versions support a direct upgrade to version 3.1.
- Always perform a full disaster recovery (DR) backup before an upgrade.
- To make sure that there is enough space for the upgrade, delete all previously downloaded release updates, client packages, and client add-ons from the appliance before the upgrade. As a best practice, always remove downloaded packages after all appliances and clients have been upgraded. 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.

See [“Pre-upgrade tasks for appliance upgrades”](#) on page 16.

- Follow the same upgrade order for appliances as for traditional NetBackup upgrades. Always begin by updating the master server appliance, then upgrade all media server appliances.
- If you have multiple media servers to upgrade, you must perform the upgrade process on each individual media server.
- 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 3.1, first upgrade the NetBackup on the master server to version 8.1.

See [“About corresponding NetBackup software versions”](#) on page 10.

- 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.

See [“Pre-upgrade tasks for appliance upgrades”](#) on page 16.

---

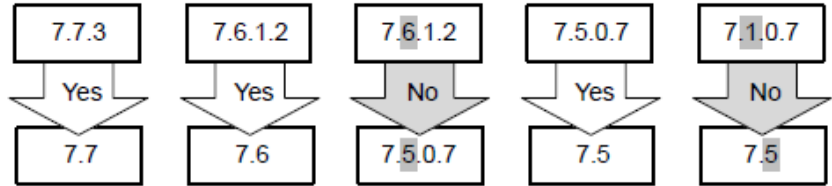
- Use a compatible version of NetBackup Administration Console to manage the NetBackup services.

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.

For example, the 7.6.1.2 console is compatible with a 7.6 NetBackup server. However, a NetBackup 7.6.1.2 console cannot administer a 7.5.0.7 NetBackup server. See [Figure 2-1](#) for various examples.

See [“About corresponding NetBackup software versions”](#) on page 10.

**Figure 2-1** Examples of supported and unsupported back-level console configurations



# Pre-upgrade tasks

This chapter includes the following topics:

- [Pre-upgrade tasks for appliance upgrades](#)

## Pre-upgrade tasks for appliance upgrades

To prepare for an upgrade to version 3.1, the following tasks must be performed on each appliance that you plan to upgrade:

[Stop all backup jobs and run a software self-test](#)

[Delete previously downloaded release updates, client packages, and client add-ons](#)

[Obtain necessary third-party plug-ins](#)

[Update firewall rules for new Veritas servers](#)

[Update disk drive firmware](#)

### Stop all backup jobs and run a software self-test

The preflight check verifies whether there are any active jobs. To help ensure a successful upgrade, perform the following:

- Log on to the NetBackup Administration Console as the administrator.
- Before master server upgrades, pause all jobs and any SLPs (Storage Lifecycle Policies).
- Before media server upgrades, stop all jobs that are currently running and suspend the jobs that may start during the upgrade. You must prevent jobs from attempting to start on the media server during an upgrade.
- After all jobs have been stopped or suspended and all SLPs have been paused, run the following command from the NetBackup Appliance Shell Menu for a validation test:



- Support > Test Software

The software self-test result must show **Pass**.

---

**Note:** This command performs a backup and restore test to the `/tmp` directory. If the `/tmp` directory for the appliance you are upgrading is on the NetBackup exclude list, you must remove it from that list before you run the self-test command. Otherwise, the self-test fails.

---

## Delete previously downloaded release updates, client packages, and client add-ons

To make sure that there is enough space for the installation of version 3.1, all previously downloaded release updates, client packages, and client add-ons must be removed from the appliance before the upgrade. If the appliance that you want to upgrade has ever had appliance version 2.6.0.1 installed, a different method is required for client package removal.

If you do not delete the previously downloaded packages and the `/inst` directory on the appliance does not contain enough space, the preflight check notifies you of the problem and prevents the upgrade.

---

**Note:** As a best practice, always remove downloaded packages after all appliances and clients have been upgraded.

---

The following table describes the package removal methods for appliances that never had version 2.6.0.1 installed. For appliances that had version 2.6.0.1 installed, refer to the information that appears below the table.

**Table 3-1** Deleting previously downloaded release updates, client packages, and client add-ons (for appliances that never had version 2.6.0.1 installed)

NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
<ul style="list-style-type: none"> <li>■ On the appliance to be upgraded, log on using the NetBackup Appliance Web Console.</li> <li>■ Select <b>Manage &gt; Software Updates</b>.</li> <li>■ In the <b>Downloaded Software Updates</b> table, click the radio button to the left of a release update, client package, or client add-on in the list, then click <b>Delete</b>.</li> </ul>	<ul style="list-style-type: none"> <li>■ On the appliance to be upgraded, log on using the NetBackup Appliance Shell Menu.</li> <li>■ To see a list of all downloaded release updates and client packages, enter the following command:  <pre>Manage &gt; Software &gt; List Downloaded</pre> </li> <li>■ To remove each downloaded release update and client package, enter the following command:  <pre>Manage &gt; Software &gt; Delete update_name</pre> <p>Where <i>update_name</i> is the release update or the client package file name.</p> </li> <li>■ To see a list of all downloaded client add-ons, enter the following command:  <pre>Manage &gt; Software &gt; List AddOns</pre> </li> <li>■ To remove each downloaded client add-on, enter the following command:  <pre>Manage &gt; Software &gt; Rollback eeb_name</pre> <p>Where <i>eeb_name</i> is the client add-on file name.</p> <p><b>Note:</b> Do not include the <code>.rpm</code> extension when you enter the client add-on file name.</p> </li> </ul>

**For appliances that once used version 2.6.0.1**

If the appliance that you want to upgrade has ever installed appliance version 2.6.0.1, the client packages for that version remains 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.

---

## Obtain necessary third-party plug-ins

For upgrades from 2.6.1 or 2.6.1.x to 2.7.1 and later, the existing SUSE Linux Enterprise Server (SLES) third-party plug-ins must be replaced with the appropriate Red Hat Enterprise Linux (RHEL) versions. The preflight upgrade script only identifies those plug-ins that are required for the upgrade. Software releases starting with version 2.7.1 contain the required RHEL third-party plug-ins to perform the upgrade. For any additional plug-ins that you use in your environment, check the vendor website for availability. For appliances that have already been upgraded to version 2.7.x, some third-party plug-ins that were not previously available may be available now.

To install RHEL plug-ins, do the following:

- Locate the appropriate RHEL plug-ins from the listed vendor websites:
  - <http://www.cleversafe.com>
  - <http://www.datadomain.com/products>
  - <http://www.dell.com>
  - <http://www.emc.com>
  - <http://www.exagrid.com>
  - <http://www.falconstor.com/en/pages/?pn=VTL>
  - <http://www.fujitsu.com/global>
  - <http://www.getgreenbytes.com>
  - <http://www.hds.com>
  - <http://www.hp.com/go/ebs>
  - <http://www.huawei.com>
  - <http://www.ibm.com>
  - <http://www.necam.com/HYDRAsTOR>
  - <http://www.nexenta.com>
  - <http://www.oracle.com>
  - <http://www.quantum.com>

<http://www.sepaton.com>

<https://www.veritas.com/product/backup-and-recovery/netbackup-appliances?themeid=nbu-appliance>

If you have other third-party plug-ins that you use, those must also be replaced with the appropriate RHEL versions. See the appropriate vendor website for details.

- Open the following share from the NetBackup Appliance Shell Menu:

```
Manage > OpenStorage > Share > Open.
```

This command opens the `/inst/plugin/incoming` share for NFS and the `\incoming_plugins` share for Windows. Copy the required plug-ins to these locations.

- Close the share as follows:

```
Manage > OpenStorage > Share > Close.
```

---

**Note:** For upgrades from 2.6.1 or 2.6.1.x, after the RHEL plug-in packages have been copied into the share and the share has been closed, do not run the `Manage > OpenStorage > List Available` command. The current 2.6.x SUSE appliance code flags the RHEL plug-in packages as invalid because the package naming conventions are different between SUSE and Red Hat environments. Since the appliance is still running on SLES, running the `List Available` command removes the RHEL plug-in packages from the share which prevents the upgrade.

---

## Update firewall rules for new Veritas servers

Due to the company separation of Veritas from Symantec, some important server changes occurred that affect NetBackup appliance environments. These changes affect SORT, the NetBackup Product Improvement Program, appliance registration, and AutoSupport. Depending on your firewall settings and your proxy settings, you may need to make updates to maintain existing functionality. For specific information on these changes, refer to the following Tech Alert on the Veritas Support website:

<https://www.veritas.com/docs/INFO2803>

## Update disk drive firmware

The preflight check for the disk drive firmware version alerts you if it detects a version that is earlier than 0006. Veritas recommends that before you upgrade the appliance software, you should first update the disk drive firmware to version 0006. This update addresses important disk drive performance issues.

---

**Note:** An earlier disk drive firmware version does not prevent the software upgrade from proceeding. If you do not update the disk drive firmware before the appliance software upgrade, Veritas recommends that you do so immediately afterward.

---

For complete details about updating the disk drive firmware, refer to following tech notes:

- NetBackup appliance models 5230 and 5330 with software versions 2.5 - 2.5.4  
[https://www.veritas.com/support/en\\_US/article.000108370](https://www.veritas.com/support/en_US/article.000108370)
- NetBackup appliance models 5230 and 5330 with software versions 2.6.0.1 - 2.6.1.2  
[https://www.veritas.com/support/en\\_US/article.000108372](https://www.veritas.com/support/en_US/article.000108372)

# 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

NetBackup appliance software release updates are available from the Veritas support website. Appliance software and client packages can be downloaded through the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu. 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.

**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

To use this method, the appliance requires Internet access to download the files or packages from the Veritas Support website.

**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-2.7.1-1.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
```

Where *<release>* is the software release number and *<date>* is the NetBackup client package date.

For example:

```
Main_Menu > Manage > Software > Download
SYMC_NBAPP_addon_nbwin-7.7.1-20150910.x86_64.rpm
```

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

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

See [“Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console”](#) on page 22.

## 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.

---

**Note:** For the 3.1 release, the server, client, and add-on packages are located on the Veritas SORT website, along with a text file that contains the MD5 and SHA1 checksums. This procedure includes links to access all of these items.

---



**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 Support website to the appliance.

**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 This step describes downloading the upgrade package files, the client and add-on packages, and where to find the MD5 and SHA1 checksums.

- Release updates

Click on each of the following links to download the split tar server files from the Veritas SORT website:

[http://sort.veritas.com/public/appliance/nba/patches/3.1/NB\\_Appliance\\_N\\_3.1-2x86\\_64-tar-split.1of3](http://sort.veritas.com/public/appliance/nba/patches/3.1/NB_Appliance_N_3.1-2x86_64-tar-split.1of3)

[http://sort.veritas.com/public/appliance/nba/patches/3.1/NB\\_Appliance\\_N\\_3.1-2x86\\_64-tar-split.2of3](http://sort.veritas.com/public/appliance/nba/patches/3.1/NB_Appliance_N_3.1-2x86_64-tar-split.2of3)

[http://sort.veritas.com/public/appliance/nba/patches/3.1/NB\\_Appliance\\_N\\_3.1-2x86\\_64-tar-split.3of3](http://sort.veritas.com/public/appliance/nba/patches/3.1/NB_Appliance_N_3.1-2x86_64-tar-split.3of3)

- Client packages

Click on any of the following links to download the specific client or add-on package from the Veritas SORT website:

[http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC\\_NBAPP\\_addon\\_rtdent\\_HPUXIA64810049x86\\_64.rpm](http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC_NBAPP_addon_rtdent_HPUXIA64810049x86_64.rpm)

[http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC\\_NBAPP\\_addon\\_rtdent\\_Linux810049x86\\_64.rpm](http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC_NBAPP_addon_rtdent_Linux810049x86_64.rpm)

[http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC\\_NBAPP\\_addon\\_rtdent\\_RS6000810049x86\\_64.rpm](http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC_NBAPP_addon_rtdent_RS6000810049x86_64.rpm)

[http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC\\_NBAPP\\_addon\\_rtdent\\_Solaris810049x86\\_64.rpm](http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC_NBAPP_addon_rtdent_Solaris810049x86_64.rpm)

[http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC\\_NBAPP\\_addon\\_rtdent\\_Solaris810049x86\\_64.rpm](http://sort.veritas.com/public/appliance/nba/patches/3.1/SYMC_NBAPP_addon_rtdent_Solaris810049x86_64.rpm)

- MD5 and SHA1 checksums

Click on the following link to a text file on the Veritas SORT website that contains the MD5 and SHA1 checksums:

[http://sort.veritas.com/public/appliance/backup/patches/3.1/NBBackup\\_Appliance\\_Release\\_31\\_MD5\\_SHA1.txt](http://sort.veritas.com/public/appliance/backup/patches/3.1/NBBackup_Appliance_Release_31_MD5_SHA1.txt)

Verify that the downloaded MD5 or SHA1 checksums match those in the file on the Veritas SORT web site.

## 5 Use the following commands to join (and extract) the release update `.rpm` files:

- For Windows:

```
copy /b NB_Appliance_N_<release-version>.x86_64-tar-split.1of3+
NB_Appliance_N_<release-version>.x86_64-tar-split.2of3+
NB_Appliance_N_<release-version>.x86_64-tar-split.3of3+
NB_Appliance_N_<release-version>.tar
```

---

**Note:** This command must be entered as one string. Make sure that the only space in the name is after `.3of3`. In addition, `<release>` is the software release number and `<version>` is the posted version number.

---

Use Windows WinRAR utilities to uncompress the

`NB_Appliance_N_<release-version>.tar` file. The resulting files are as follows:

- `SYMC_NBAPP_update-<release-version>.x86_64.rpm`
- `update.rpm.md5_checksum`
- `update.rpm.sha1_checksum`

- For UNIX:

```
cat
NB_Appliance_N_<release-version>.x86_64-tar-split.1of3<space>
NB_Appliance_N_<release-version>.x86_64-tar-split.2of3<space>
NB_Appliance_N_<release-version>.x86_64-tar-split.3of3 | tar
xvf -
```

Where `<release-version>` is the software release number, such as 3.1, and the version number of the software release, such as -1.

---

**Note:** This command is one string. In this example, there is one space between each split package that is identified with a "`<space>`".

---

The resulting files are as follows:

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

- `update.rpm.md5_checksum`
- `update.rpm.sha1_checksum`

---

**Note:** To extract packages on UNIX systems, Veritas recommends that you use GNU tar version 1.16 or higher instead of tar. See the following Technote for more information about extracting images:

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

---

- 6** For UNIX systems, run one of the following commands to compute the checksum value for the `.rpm` file:

```
md5sum SYMC_NBAPP_update-<release-version>.x86_64.rpm OR sha1sum
SYMC_NBAPP_update-<release-version>.x86_64.rpm.
```

Verify that the checksum value matches the content of the `update.rpm.md5_checksum` file or the `update.rpm.sha1_checksum` file.

- 7** Copy this release update or client package `.rpm` 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.

---

- 8** After you have successfully copied the release update or client package `.rpm` into the mounted share, unmap or unmount the shared directory.
- 9** 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.

---

**Note:** For upgrades from 2.6.1 or 2.6.1.x, the release update or the client package cannot be verified and moved unless the Symantec Critical System Protection (SCSP) scanning is complete.

For upgrades from 2.7.1 or later, the release update or the client package cannot be verified and moved unless the Symantec Data Center Security (SDCS) scanning is complete.

---

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

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

- 10** 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.

See [“Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console”](#) on page 22.

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

Use the following procedure to start the appliance upgrade.

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

- 1** Check to make sure that the following pre-upgrade tasks have already been performed:
  - 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.
  - All of the necessary RHEL plug-in packages have been copied into the appropriate location.

See [“Pre-upgrade tasks for appliance upgrades”](#) on page 16.

- 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.

After the preflight check has finished, proceed as follows:

- 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:  
 See [“Pre-upgrade tasks for appliance upgrades”](#) on page 16.

- 5 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
```

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

```
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, 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*.

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

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

The system reboots several 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.

After the third reboot occurs, the **AIM** window appears automatically and shows the upgrade progress and the estimated remaining time.

---

**Note:** Do not close the **AIM** window until after the upgrade has completed.

---

- 7 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.

---

**Note:** If a **Paused** status occurs, the **AIM** window on the IPMI console becomes locked and does not respond to keyboard input. Before you can clear the **Paused** status, you must unlock the **AIM** window as described below.

---

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

- Unlock the **AIM** window on the IPMI console as follows:
  - Press the **Enter** key several times until the login prompt appears.
  - Enter the user account name and the password to log in to the IPMI console again. After logging in, the **AIM** window reappears and should respond to keyboard input.
  - Continue with the following tasks to clear the **Paused** status.
- Press the **V** key to switch to the **Verbose** view to see the logs. If there are any Unique Message Identification (UMI) codes for the errors, search for them on the [Veritas Support website](#) to get more detailed information.
- Try to fix the problem that the **AIM** window reports.  
 If you need to use the shell menu, log on to the NetBackup Appliance Shell Menu through an SSH session. When the **AIM** window appears, press the **S** key to close it.
- Go back to the **AIM** window on the IPMI console.  
 If you tried fixing the problem, press the **A** key to attempt the self-test again. If you cannot fix the problem, contact Veritas Technical Support or press the **R** key to roll back the appliance to the previous software version.

---

**Note:** A rollback occurs automatically after one hour if there is no user response on the **AIM** window during a pause condition.

---

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

After the upgrade has completed and 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.

- 9** 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, restart 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 for 3.1 upgrades](#)

## Post upgrade tasks for 3.1 upgrades

After the upgrade process has completed successfully, perform the following tasks as needed for your environment:

- SDCS mode  
After an upgrade from 2.6.1 or 2.6.1.x, the Symantec Critical System Protection (SCSP) feature is renamed to Symantec Data Center Security (SDCS). This feature is set automatically to the un-managed mode (default). If the previous SCSP feature was set to the managed mode before the upgrade, make sure to change SDCS to the managed mode and apply the latest IDS and IPS policies after the upgrade has completed. For complete details, refer to one of the following documents:  
*NetBackup 52xx and 5330 Appliance Administrator's Guide*  
*NetBackup 52xx and 5330 Appliance Security Guide.*
- SDCS console and server  
Starting with software version 3.1, the SDCS console and the server are no longer included in NetBackup appliance software releases.  
For appliances that do not currently have an SDCS environment configured, you must obtain the console and the server binaries from the Veritas Support website before you can set it up.  
For appliances with an existing SDCS environment and console set up, you are only required to update the policy files and make sure that the SDCS agent points to the correct SDCS server. You do not need to obtain the binaries.  
For complete details, refer to one of the following documents:  
*NetBackup 52xx and 5330 Appliance Administrator's Guide*

*NetBackup 52xx and 5330 Appliance Security Guide.*

# 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](#)
- [During a NetBackup appliance upgrade, warning dialog appears with the message Error processing drive](#)
- [Preflight checkpoint creation failure prevents NetBackup appliance upgrade from starting](#)
- [Self-test failure during a NetBackup appliance upgrade](#)
- [AdvancedDisk storage pool error occurs after NetBackup appliance upgrade to 2.7.x or later and re-image](#)
- [Old checkpoints remain after interrupting a NetBackup appliance upgrade or rollback](#)

# Index

## A

- appliance behavior during upgrades 8
- Appliance Install Manager (AIM) 10
- appliance server or client package
  - download directly 23
- appliance upgrades
  - guidelines and best practices 12

## C

- changes during upgrade 10
- client share
  - download software updates 24

## D

- disk drive firmware 20
- download directly
  - appliance server or client package 23
- download methods
  - release updates 22
- download software updates
  - from NetBackup Appliance Web Console 22
  - using client share 24

## G

- guidelines and best practices
  - appliance upgrades 12

## I

- install update from NetBackup Appliance Shell Menu
  - version 3.1 28

## P

- post upgrade tasks
  - SDCS mode 33
- pre-upgrade tasks
  - delete previously downloaded packages 17
  - deleting version 2.6.0.1 client packages 18
  - obtain RHEL third-party plug-ins 19
  - stop backups and run self-test 16

- pre-upgrade tasks (*continued*)

- update firewall rules 20
  - version 3.1 upgrades 16

- preflight check
  - before upgrade 7

## S

- SDCS mode
  - post upgrade tasks 33
- software updates
  - download from NetBackup Appliance Web Console 22

## T

- troubleshoot upgrade issues 35

## U

- update disk drive firmware 20
- upgrade
  - pre-upgrade tasks 16
  - version 3.1 with RHEL operating system 6
- upgrade guidelines 13
- upgrade time estimation 12
- upgrades
  - supported upgrade paths 7

## V

- version 2.7.x upgrades
  - RHEL third-party plugins 8
- version 3.1
  - install update from NetBackup Appliance Shell Menu 28
- version 3.1 upgrades
  - RHEL operating system 6