Veritas NetBackup™ Appliance Upgrade Guide

Release 3.0

NetBackup 52xx and 5330

Red Hat Enterprise Linux (RHEL) Operating System

VERITAS™

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

Release 3.0

Legal Notice

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

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

APPL.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Introduction

This chapter includes the following topics:

- About upgrades to NetBackup Appliance software version 3.0 and the Red Hat Enterprise Linux operating system

About upgrades to NetBackup Appliance software version 3.0 and the Red Hat Enterprise Linux operating system

Starting with NetBackup Appliance software version 2.7.1, Red Hat Enterprise Linux (RHEL) replaces the SUSE Linux Enterprise Server (SLES) operating system. Any existing 5220, 5230, 5240 or 5330 appliances that currently use earlier software versions can be upgraded to version 3.0. In some situations, you may need to upgrade twice to get to version 3.0.

Note: The NetBackup 5200 appliance is not supported for upgrades to versions 2.7.1 and later, due to Intel components that are not supported by RHEL version 6.6 or later.

This topic covers the following information that you should review before an upgrade to version 3.0:

Supported upgrade paths

Preflight check before the upgrade

Third-party plug-ins for RHEL

Appliance behavior during upgrades

Changes during the upgrade process

About corresponding NetBackup software version

Post upgrade tasks

Supported upgrade paths

The following describes the supported upgrade paths to version 3.0:

- Direct upgrade path
  The following appliances can be upgraded directly to version 3.0:

  - Any NetBackup 5220, 5230, or 5330 appliances with version 2.6.1, 2.6.1.x and 2.7.x

  - NetBackup 5240 appliance with version 2.7.3

- 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 3.0. It is recommended that these systems first be upgraded to version 2.6.1.2, then upgraded to version 3.0.

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 3.0.

Preflight check before the upgrade

When you attempt to upgrade to version 3.0, the upgrade script runs a preflight check that analyzes several system parameters to determine if the appliance is ready for the upgrade. The preflight check provides information about what was found and whether you can proceed with the upgrade. 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 you can upgrade.

Refer to the following topic for more information:

See "Pre-upgrade tasks for NetBackup Appliance version 3.0 upgrades" on page 13.

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. If the preflight check finds Teradata binaries on the appliance, the upgrade is not allowed to proceed.

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 that these plug-ins
be replaced with the appropriate RHEL versions. If the preflight upgrade script
identifies any required RHEL third-party plug-ins that are not found, the upgrade is
not allowed to proceed.

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 NetBackup Appliance version 3.0 upgrades" on page 13.

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 if there are any active NetBackup jobs. The upgrade process only
  proceeds if it is determined that no active jobs are detected.
  Only after the required criteria are met, the appliance software is upgraded, and
  the version number is updated to the appropriate release.

- Web services are unavailable during most of the upgrade process, which
  prevents access to the NetBackup Appliance Web Console. To view the upgrade
  progress during this time, run the following command from the NetBackup
  Appliance Shell Menu:

  `Main > Manage > Software > UpgradeStatus`

- For upgrades from 2.6.1 or 2.6.1.x to 2.7.x and later, the appliance restarts four
  times while the upgrade is in progress. The following describes what takes place
  at each restart:

    - First restart - installs the Red Hat Enterprise Linux (RHEL) operating system.

- Second restart - initializes the appliance using the new RHEL operating system.

- Third restart - restores the appliance configuration.

- Fourth restart - initializes the restored appliance configuration with the RHEL operating system.
  After the first restart, the NetBackup Appliance Web Console and any SSH-based connections to the server are unavailable until all restarts have 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 restart the appliance during this time. You can use the Veritas Remote Management interface (or IPMI) to view the system restart 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.

- For upgrades from 2.7.1 and later, the appliance restarts twice while the upgrade is in progress. The following describes what takes place at each restart:

  - First restart - updates the operating system and appliance software.

  - Second restart - initializes the restored appliance configuration.

- Before the upgrade has completed, a self-test is performed automatically. If the self-test fails, you are prompted to either retry the self-test or to roll back to the previous version.

- After a successful appliance upgrade, the Fibre Transport Media Server (FTMS) is restarted 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 the upgrade process

During the upgrade, the following change occurs:

- For upgrades from 2.6.1 or 2.6.1.x to 2.7.x or later, the Symantec Critical System Protection (SCSP) feature is updated to version 6.5 and renamed as Symantec Data Center Security (SDCS). For more information, refer to the following topic:
  See "Post upgrade tasks for 3.0 upgrades" on page 32.

About corresponding NetBackup software version

NetBackup software version 8.0 is included with NetBackup Appliance release 3.0. Table 1-1 lists the corresponding NetBackup version for recent NetBackup Appliance software releases.

Table 1-1   Appliance software releases and the corresponding NetBackup software version

Appliance software release	NetBackup software version
2.7.3	7.7.3
3.0	8.0

Post upgrade tasks

After the upgrade has completed successfully, some options or configuration settings may change.

Refer to the following topic for a list of items to check after the upgrade:

See "Post upgrade tasks for 3.0 upgrades" on page 32.

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 -> 3.0 2.6.1.x -> 3.0	2.5 - 3 hours	■ For master server upgrades, add 30 minutes. ■ For appliances that were previously upgraded from versions 2.0.x, 2.5.x, or 2.6.0.1, add 30 minutes.
	2.7.x -> 3.0	1.5 - 2 hours	

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

Model	Upgrade path	Estimated base time	Additional time considerations
5230	2.6.1 -> 3.0 2.6.1.x -> 3.0	2.5 - 3 hours	■ For master server upgrades, add 15 minutes. ■ For appliances that were previously upgraded from versions 2.5.4 or 2.6.0.1, add 30 minutes. ■ For appliances with more than two Veritas Storage Shelf units, add 15 minutes.
	2.7.x -> 3.0	1.5 - 2 hours	
5330	2.6.1 -> 3.0 2.6.1.x -> 3.0	2 - 2.5 hours	For appliances with Expansion Storage Shelf units, add 15 minutes for each unit.
	2.7.x -> 3.0	1.5 - 2 hours	
5240	2.7.3 -> 3.0	1.5 - 2 hours	
			For all upgrade scenarios, include the following as necessary: ■ For every 350,000 jobs on the master server, add 10 minutes. For example, add 30 minutes for a master server with a job list of 1 million records. ■ For every 250 VLANs that you have configured, add 5 minutes.

Upgrade guidelines

Review the following guidelines before you begin the upgrade:

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

■ To make sure that there is enough space for the new software update, 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, a different method is required for client package removal.

See "Pre-upgrade tasks for NetBackup Appliance version 3.0 upgrades" on page 13.

- 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 3.0, first upgrade the master server to NetBackup version 8.0.
  See About corresponding NetBackup software version on page 8.

- 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 NetBackup Appliance version 3.0 upgrades" on page 13.

- 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 8.0 can only be used with an appliance server with version 3.0 or later. Client add-ons must also be the same as the client version.
  See About corresponding NetBackup software version on page 8.

Pre-upgrade tasks

This chapter includes the following topics:

■ Pre-upgrade tasks for NetBackup Appliance version 3.0 upgrades

Pre-upgrade tasks for NetBackup Appliance version 3.0 upgrades

To prepare for an upgrade to version 3.0, 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

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, do 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 3.0, 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

- On the appliance to be upgraded, log on using the NetBackup Appliance Web Console. - 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**.	- On the appliance to be upgraded, log on using the NetBackup Appliance Shell Menu. - To see a list of all downloaded release updates and client packages, enter 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: Do not include the `.rpm` extension when you enter the client add-on file name.

For appliances that once used version 2.6.0.1

If the appliance that you want to upgrade has ever had appliance version 2.6.0.1 installed, 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.

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.

Increase configuration volume size

During the upgrade to 3.0, if the configuration volume does not have enough space, the preflight check prevents the upgrade attempt. To avoid this problem, do the following to increase the configuration volume size before the upgrade or when the preflight check prompts you to increase it:

- Log on to the appliance from the NetBackup Appliance Shell Menu.

- Enter `Main_Menu > Manage > Storage`, then run the following command:

  `Resize Configuration 100GB`.

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

■ 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

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 Web Console

- 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:

- See "Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console" on page 20.

- See "Downloading software updates directly to a NetBackup appliance" on page 20.

- See "Downloading software updates to a NetBackup appliance using a client share" on page 21.

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.

   Proceed to software installation as described in the previous step.

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 > List Downloaded
```

See "Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console" on page 20.

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: 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 the package file names for the release update packages and the client packages. After reviewing the names, continue with the remaining steps to download the files.

- Release updates

  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

  Where <release> is the software release number and <version> is the version number of the software release. For example: 2.7.x-1.

  To verify that the downloaded release update packages have the same MD5 or SHA1 checksums as those posted on the Veritas Support web site, do the following:

  - Enter the following URL for the Veritas Support site where the release updates and the client packages are posted:
    https://www.veritas.com/content/support/en_US/58991.html

  - In the **How to...** section, click the download link for the posted software update.

  - On the README page, in the right column, click **Attachments**.

  - Verify that the checksums shown in the pop-up window match the downloaded file checksums.

- Client packages

  `SYMC_NBAPP_addon_nbwin_<`*`release`*`>-<`*`date`*`>.x86_64.rpm` or

  `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:

  `SYMC_NBAPP_addon_nbclient_HP-UX-IA64-7.7.1-20150910.x86_64.rpm`

5 Use one of 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 version 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* is the software release number and *version* is the version number of the software release. For example: 2.7.x-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.

- 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 20.

Installing a NetBackup Appliance software update using the NetBackup Appliance Web Console

Use the following procedure to start the appliance upgrade.

To install a downloaded release update using the NetBackup Appliance Web Console

1 Check to make sure that the following pre-upgrade tasks have been performed:

- All jobs have been stopped or suspended and all SLPs have been paused.

- The `Support > Test Software` command has been run and returned a **Pass** result.

- All of the necessary RHEL plug-in packages have been copied into the appropriate location.

See "Pre-upgrade tasks for NetBackup Appliance version 3.0 upgrades" on page 13.

2 Open a web browser and log on to the appliance using the NetBackup Appliance Web Console.

3 Select **Manage > Software Updates**.

4 From the **Software Updates** page, locate the appropriate software update in the **Downloaded Software Updates** table.

- If the table contains the software update that you want to install, proceed to the next step.

- If the table does not contain a software update that you want to install, refer to the following topics:
  See "Downloading software updates to a NetBackup appliance using the NetBackup Appliance Web Console" on page 20.
  See "Downloading software updates directly to a NetBackup appliance" on page 20.
  See "Downloading software updates to a NetBackup appliance using a client share" on page 21.

5 Select the check box that is associated with the software update that you want to install and click **Install**.

The following events occur after you click **Install**:

- The **Software Updates** page refreshes and presents a table that displays the server (master or media) that is to be upgraded. The table also shows the name and version of the software update.

  Note: If you plan to upgrade more than one media server, you must run this upgrade procedure on each media server.

- An interactive, pre-installation check window appears.
  You must provide answers to the pre-installation questions. Then select **Finish** to close the pre-installation check window.

6 On the **Downloaded Software Updates** table, click **Next**.

7 The **Confirm** pop-up window displays the server (master or media) that you are about to upgrade.

If this information is correct, click **Next**. If the information is not correct, click **Cancel**.

8 Click **Next** to open a **Confirmation Required** pop-up window. An administrator must enter a user name and a password as a final step before the software installation or the upgrade begins. After you enter these credentials, click **Confirm**. If you want to stop or exit the installation, click **Cancel**.

The **Software Updates** page refreshes and updates the information that is displayed in the **Downloaded Software Updates** table. This table displays the progress of the upgrade, starting with the preflight check.

9 Monitor the preflight check and watch for any **Check failed** messages. Proceed as follows:

- If no **Check failed** messages appear, you are prompted to start the upgrade. Proceed to the next step.

- 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.

- 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 NetBackup Appliance version 3.0 upgrades" on page 13.

10 The system may restart several times during the upgrade process. After the first restart, the NetBackup Appliance Web Console and any SSH-based connections to the server are unavailable until the restart 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 restart the appliance during this time. You can use the Veritas Remote Management interface (IPMI) to view the system restart 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.

11 After the status of the server reaches 100%, the information in the title line of the table indicates whether the upgrade was successful. The following status can occur depending on whether the upgrade was successful:

- **The appliance version is <*the target version*> and not in upgrade state.** If the target (or new) version appears, the upgrade was successful. Click **Finish** to complete the process.

- **The appliance version is <*the original version*> and not in upgrade state.** If the original (or pre-upgrade) version appears, the upgrade has failed, and an automatic rollback has taken place. The rollback returns the server back to the original version.

- **Failed to create the PRE_UPGRADE checkpoint, please resolve this issue first**
  A checkpoint creation process is performed automatically before the upgrade operation begins. This checkpoint is used to enable the server to roll back to it, if the upgrade fails. If the failure message appears, it indicates that the creation of the checkpoint failed, and the upgrade operations were not performed. You must determine what caused the issue and resolve it before you can attempt the upgrade again.

- **Self-Test failed on <*nodename*>, please resolve the issue first.** The self-test operation is executed automatically before the upgrade completes. If the self-test fails, you are prompted to either roll back or retry the self-test after you have investigated the problem using the NetBackup Appliance Shell Menu.

12 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 rescan 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/openv/netbackup/bin/bp.kill_all
  /usr/openv/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, you must manually initiate a SCSI device refresh at the OS level. The method to accomplish the refresh action depends on the operating system that the client is running. 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 any SLES 10 or SLES 11 SAN clients that still do not
> work, Veritas recommends that you upgrade 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.

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 returned a
        Pass result.

    ■   All of the necessary RHEL plug-in packages have been copied into the
        appropriate location.

    See "Pre-upgrade tasks for NetBackup Appliance version 3.0 upgrades"
    on page 13.

2   Open an SSH session and log on to the appliance using the NetBackup
    Appliance Shell Menu.

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. 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.

- 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 NetBackup Appliance version 3.0 upgrades" on page 13.

5 Watch the onscreen progress of the upgrade to see an estimated completion time. To see the current status of the upgrade, enter the following command:

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

6 The upgrade may force the appliance to restart several times.

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.

Note: For upgrades from 2.6.1 or 2.6.1.x, the system may restart several times during the upgrade process. After the first restart, the NetBackup Appliance Web Console and any SSH-based connections to the server are unavailable until the restart 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 restart the appliance during this time. You can use the Veritas Remote Management interface (IPMI) to view the system restart 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.

---

7 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/openv/netbackup/bin/bp.kill_all`

  `/usr/openv/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 3.0 upgrades

Post upgrade tasks for 3.0 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 as Symantec Data Center Security (SDCS). This feature is set automatically to the un-managed mode (default). If the SCSP feature was set to the managed mode before the upgrade, you must change SDCS to the managed mode to continue receiving centralized alerts and reports. Setting this feature to the managed mode requires that you connect the appliance to the SDCS server. 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, use the following list to help resolve the issues.

Rollback after upgrade failure causes inactive media server

Warning dialog appears with the message **Error processing drive**

Preflight checkpoint creation failure prevents upgrade from starting

Self-test failure during an upgrade

AdvancedDisk storage pool error occurs after upgrade to 2.7.x or later and re-image

Old checkpoints remain after interrupting an upgrade or rollback

Rollback after upgrade failure causes inactive media server

During an upgrade to 2.7.x or later, if a canceled replication operation is restarted right after the checkpoint is created, the upgrade fails and the system rolls back automatically. After rollback, you can not start a backup because the media server is no longer active.

To ensure a successful backup, use the following steps to activate the media server manually:

1   Log on to the NetBackup Administration Console as administrator.

2   On the left panel, navigate to **Media and Device Management > Devices > Media Servers**.

3   On the right panel, right-click the media server you need and select **activate** from the shortcut menu.

For further assistance, contact Veritas Technical Support.

Warning dialog appears with the message Error processing drive

If backup jobs are in progress during the upgrade, the following warning dialog appears:
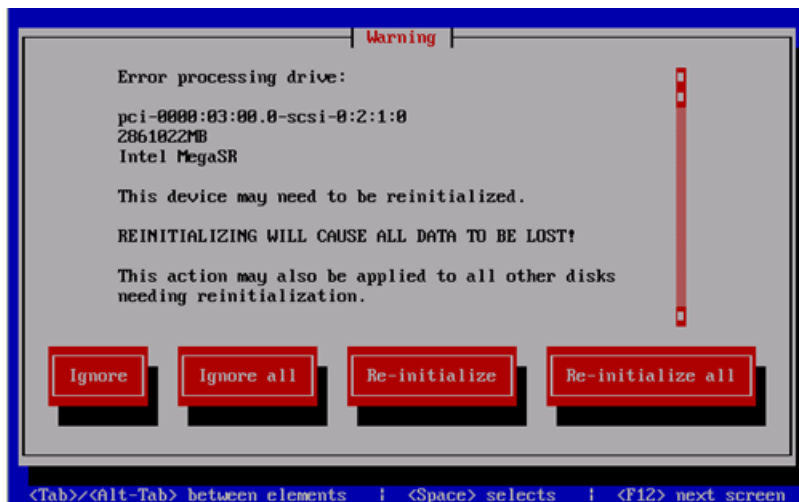
If this dialog appears, select **Ignore** or **Ignore all** to continue with the upgrade. This action does not reinitialize the disk and allows the upgrade to complete.

Note: To prevent this issue, before you upgrade any servers, make sure to stop all backup jobs.

Before you upgrade a master server, pause all jobs and any Storage Lifecycle Policies (SLPs).

Before you upgrade a media server, stop all jobs that are currently running and suspend the jobs that may be scheduled to start during the upgrade.

For further assistance, contact Veritas Technical Support.

Preflight checkpoint creation failure prevents upgrade from starting

If there is not enough free space on the `/repository` partition, a pre-upgrade checkpoint cannot be created, and the upgrade cannot proceed. The upgrade requires at least 40 GB of free space in `/repository` to proceed.

To resolve this issue:

Contact Veritas Technical Support and ask the representative to refer to TechNote 000095753.

Self-test failure during an upgrade

To verify that the upgrade is successful, the upgrade process performs an automatic self-test of a backup and a restore to and from the `/tmp` directory. If the `/tmp` for the appliance you are upgrading is on the NetBackup exclude list, the self-test fails.

To resolve this issue:

Log on to the NetBackup Administration Console to remove the `/tmp` directory from the NetBackup exclude list.

AdvancedDisk storage pool error occurs after upgrade to 2.7.x or later and re-image

When you upgrade to version 2.7.x or later and then re-image to that version without resetting the storage, the following error message may appear:

[Error] Cannot create NetBackup objects for 'AdvancedDisk' storage pool. One of the disk volumes is not configured. Restart the Appliance and retry. Contact Veritas Technical Support if the issue persists.

This issue is caused by an AdvancedDisk diskpool path redirection.

To resolve this issue:

Contact Veritas Technical Support and ask the representative to refer to TechNote 000095808.

Old checkpoints remain after interrupting an upgrade or rollback

If you interrupt an upgrade or a rollback process, old checkpoints from the previous version may still remain in the new file system. These checkpoints can cause a constant output of information after you configure storage, followed by entering the `Manage > Storage > Show` command.

The following shows an example of the command output.

```
Use of uninitialized value $storage_key in hash element at
/opt/NBUAppliance/scripts/nbapp_storage_core.pm line 3471.

Use of uninitialized value $storage_key in hash element at
 /opt/NBUAppliance/scripts/nbapp_storage_core.pm line 3475.

Use of uninitialized value $storage_key in hash element at
 /opt/NBUAppliance/scripts/nbapp_storage_core.pm line 3476.
```

This problem does not adversely affect the appliance functions.

To remove the old checkpoints, contact Veritas Technical Support and ask the representative to refer to TechNote 000115860.

Warning: To avoid erratic, unexpected, or undesired appliance operation, do not interrupt an upgrade or a rollback process.

Index