NetBackup™ Appliance Upgrade Guide

Release 2.7.1

Models 5220, 5230, and 5330

Red Hat Enterprise Linux (RHEL) Operating System

✔Symantec™

NetBackup™ Appliance Upgrade Guide

Documentation version: Release 2.7.1

Legal Notice

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.veritas.com/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.veritas.com/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system

- Version and patch level

- Network topology

- Router, gateway, and IP address information

- Problem description:

  - Error messages and log files

  - Troubleshooting that was performed before contacting Technical Support

  - Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization

- Product registration updates, such as address or name changes

- General product information (features, language availability, local dealers)

- Latest information about product updates and upgrades

- Information about upgrade assurance and support contracts

- Advice about technical support options

- Nontechnical presales questions

- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

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

Contents

Introduction

This chapter includes the following topics:

- About upgrades to NetBackup appliance version 2.7.1 and the Red Hat Enterprise Linux operating system

About upgrades to NetBackup appliance version 2.7.1 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 NetBackup 5220, 5230, or 5330 appliances with software versions 2.6.1.2 and earlier that you currently use can be upgraded to version 2.7.1. In some situations, you may need to upgrade twice to get to version 2.7.1.

Note: The NetBackup 5200 Appliance is not supported for upgrades to version 2.7.1, due to Intel components that are not supported by RHEL version 6.6.

This topic covers the following information that you should review before an upgrade to version 2.7.1:

Supported upgrade paths

Pre-flight check before the upgrade

Third-party plug-ins for RHEL

Appliance behavior during upgrades

Changes during the upgrade process

Post upgrade tasks

Supported upgrade paths

The following describes the supported upgrade paths to version 2.7.1:

- Direct upgrade path
  Any NetBackup 5220, 5230, or 5330 appliances with version 2.6.1 through 2.6.1.2 can be upgraded directly to version 2.7.1.

- 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 2.7.1. It is recommended that these systems first be upgraded to version 2.6.1.2, then upgrade to version 2.7.1.

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 2.7.1.

Pre-flight check before the upgrade

When you attempt to upgrade to version 2.7.1, the upgrade script runs a pre-flight check that analyzes several system parameters to determine if the appliance is ready for the upgrade. The pre-flight check provides information about what was found and whether you can proceed with the upgrade. If the pre-flight 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 2.7.1 upgrades" on page 15.

Note: Upgrades to version 2.7.1 are not supported if you have installed Teradata binaries on the appliance. If the pre-flight check finds Teradata binaries on the appliance, the upgrade cannot begin. The Teradata binaries must be removed before you can upgrade to version 2.7.1.

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 require that these plug-ins get replaced with the appropriate RHEL versions. If the pre-flight upgrade script identifies any RHEL third-party plug-ins that are not found, the upgrade is not allowed to proceed.

Refer to the following topic for installation details:

See "Pre-upgrade tasks for NetBackup appliance version 2.7.1 upgrades" on page 15.

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
  ```

- 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 Symantec 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.

- 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 NetBackup 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:

- 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 2.7.1 upgrades" on page 32.

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 2.7.1 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

To help you determine the estimated time for an appliance upgrade, refer to Table 2-1 for the various upgrade scenarios.

Table 2-1   Upgrade scenarios and related time estimations

Model	Estimated base time	Additional time considerations
5220	3 - 3.5 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.
5230	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 Symantec Storage Shelf units, add 15 minutes.

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

Model	Estimated base time	Additional time considerations
5330	2.5 - 3.25 hours	For appliances with Expansion Storage Shelf units, add 15 minutes for each unit.
		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:

- Make sure that your appliance environment currently uses software version 2.6.1, 2.6.1.1, or 2.6.1.2. Only these versions support a direct upgrade to version 2.7.1.

- 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 2.7.1 upgrades" on page 15.

- 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. Upgrades cannot be performed simultaneously on multiple servers.

- 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 2.7.1, first upgrade the master server to
NetBackup version 7.7.1.

- 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 2.7.1 upgrades"
on page 15.

- 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 2.7.1 can only be used with an appliance server
  with version 2.7.1 or later. Client add-ons must also be the same as the client
  version.

Pre-upgrade tasks

This chapter includes the following topics:

- Pre-upgrade tasks for NetBackup appliance version 2.7.1 upgrades

Pre-upgrade tasks for NetBackup appliance version 2.7.1 upgrades

To prepare for an upgrade to version 2.7.1, 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

Stop all backup jobs and run a software self-test

The pre-flight 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 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 2.7.1, 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 pre-flight 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

The existing SUSE Linux Enterprise Server (SLES) third-party plug-ins must be replaced with the appropriate Red Hat Enterprise Linux (RHEL) versions. Otherwise, the pre-flight upgrade script does not allow the upgrade to start.

To install the 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
  http://www.symantec.com/business/theme.jsp?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 share `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 `Manage > OpenStorage > Share > Close`.

Note: 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

Performing the upgrade

This chapter includes the following topics:

- Methods for downloading appliance software release updates

- Installing the NetBackup appliance version 2.7.1 software update using the NetBackup Appliance Web Console

- Installing the NetBackup appliance version 2.7.1 software update using the NetBackup Appliance Shell Menu

- Post upgrade tasks for 2.7.1 upgrades

Methods for downloading appliance software release updates

NetBackup appliance software release updates are available from the Symantec 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

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

When downloading software updates directly onto an appliance, Internet access is required.

To use this method, the appliance requires Internet access to download the files or packages from the Symantec 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 Symantec 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-<version>-<release>.x86_64.rpm
    ```

    Where *<version>* is the version of software release and *<release>* is the software version release number.

- For a UNIX client package:

    ```
    Main_Menu > Manage > Software > Download
    SYMC_NBAPP_addon_nbclient_<platformname>-<version>-<release>.x86_64.rpm
    ```

    Where *<platformname>* is the client platform or operating system name, *<version>* is the version of the client package, and *<release>* is the software version release number.
    For example:

    ```
    Main_Menu > Manage > Software > Download
    SYMC_NBAPP_addon_nbclient_Solaris-7.6.0.2-SLES11.x86_64.rpm
    ```

- For a Windows client package:

    ```
    Main_Menu > Manage > Software > Download
    SYMC_NBAPP_addon_nbwin_<platformname>-<version>-<release>.x86_64.rpm
    ```

    Where *<platformname>* is the client platform or operating system name, *<version>* is the version of the client package, and *<release>* is the software version release number.
    For example:

    ```
    Main_Menu > Manage > Software > Download
    SYMC_NBAPP_addon_nbwin-7.6.0.2-SLES11.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 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 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 Symantec 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 systems	Map the following appliance CIFS share on your computer: **Note:** On Windows systems, you are prompted to provide the user name (`admin`) and its corresponding password.
UNIX systems	Mount the following appliance NFS share: ■ `mkdir -p /mount/<appliance-name>` ■ `mount <appliance-name>:/inst/patch/incoming /mount/<appliance-name>`

4   To download release updates, enter the following URL for the Symantec Support site where the release updates and the client packages are posted:

    http://www.symantec.com/business/support/index?page=landing&key=58991

5   Download and unzip or untar the release update or the client package as follows:

■   For release updates
    The release update `.rpm` file name may be split into multiple files with names. The following example demonstrates a software update file that is split into three files:

```
NB_Appliance_N_<version>-<release>.x86_64-tar-split.1of3
    NB_Appliance_N_<version>-<release>.x86_64-tar-split.2of3
    NB_Appliance_N_<version>-<release>.x86_64-tar-split.3of3
```

Where `<version>` is the version of software release and `<release>` is the software version release number.

To continue with release update downloading, go to step 6.

■ For client packages

Client packages are not split and use the following naming convention:

`SYMC_NBAPP_addon_nbwin_<version>.x86_64.rpm` or

`SYMC_NBAPP_addon_nbclient_<platform and version>.x86_64.rpm`

Where `<platform and version>` is the specific platform operating system and the NetBackup version of the client package. For example:

`SYMC_NBAPP_addon_nbclient_HP-UX-IA64-7.6.0.2-SLES11.x86_64.rpm`

To continue with client package downloading, go to step 8.

6   Use one of the following commands to join (and extract) the release update.rpm files:

■ For Windows, use a `copy /b` command similar to the following to join three split files:

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

Note: This command is one string. Make sure that it contains no spaces when you enter it. In addition, `<version>` is the version of software release and `<release>` is the software version release number.

Use Windows WinRAR utilities to uncompress the resulting `.tar` file, `NB_Appliance_N_<version>-<release>.tar`.

The resulting files are as follows:

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

`update.rpm.md5_checksum`

■ For UNIX, use a `cat` or similar command to join three split files as follows:

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

Where `<version>` is the version of software release and `<release>` is the software version release number.

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

The resulting files from the preceding command are as follows:

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

`update.rpm.md5_checksum`

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

`http://www.symantec.com/docs/TECH154080`

---

7   Compute the md5 checksum value for the
     `SYMC_NBAPP_update-<version>-<release>.x86_64.rpm` as follows:

- For Windows systems:
  To compute the md5 checksum, click on the following link for details:
  http://support.microsoft.com/kb/889768

- For UNIX systems, run the following command:
  `md5sum SYMC_NBAPP_update-<version>-<release>.x86_64.rpm`

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

8   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.

---

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

10   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: The release update or the client package cannot be verified and moved unless the Symantec Critical System Protection (SCSP) scanning is complete.

- `List Version`

- `List Details All`

- `List Details Base`

- `Share Open`

- `Share Close`

11 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 21.

Installing the NetBackup appliance version 2.7.1 software update using the NetBackup Appliance Web Console

After you have performed the items in the pre-upgrade checklist, use the following procedure to start the appliance upgrade.

To install a downloaded appliance 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 2.7.1 upgrades" on page 15.

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 21.
    See "Downloading software updates directly to a NetBackup appliance" on page 21.
    See "Downloading software updates to a NetBackup appliance using a client share" on page 22.

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, preinstallation check window appears.
    You must provide answers to the preinstallation questions. Then select **Finish** to close the preinstallation 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 pre-flight check.

9   Monitor the pre-flight 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 pre-flight 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 2.7.1 upgrades" on page 15.

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 Symantec 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, Symantec 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 the NetBackup appliance version 2.7.1 software update using the NetBackup Appliance Shell Menu

After you have performed the items in the pre-upgrade checklist, use the following
procedure to start the appliance upgrade.

To install a downloaded appliance 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 2.7.1 upgrades"
    on page 15.

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 pre-flight 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 pre-flight 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 2.7.1 upgrades" on page 15.

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: 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 Symantec 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, Symantec 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 for 2.7.1 upgrades

After the upgrade process has completed successfully, check the following parameters and make any necessary changes as described.

- SDCS mode
  After the upgrade, 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

Index