Veritas NetBackup™ Appliance Upgrade Guide

Release 5.1.1

VERITAS™

Veritas NetBackup™ Appliance Upgrade Guide

Last updated: 2023-07-18

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

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

Documentation feedback

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

APPL.docs@veritas.com

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

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

Chapter 1

Introduction

This chapter includes the following topics:

About upgrading to NetBackup appliance software version 5.1.1

Use an SSH session or the IPMI console to log in to the NetBackup Appliance Shell Menu to upgrade appliances. For upgrades from versions 3.1 and later, you may also use the **Appliance Management Console**. To upgrade the nodes in a high availability (HA) setup, you must use the NetBackup Appliance Shell Menu. The **Appliance Management Console** does not support upgrades for HA nodes.

Before you begin any upgrades, review the following topics:

See "Supported upgrade paths" on page 6.

See "About upgrades for NetBackup Appliance HA setups" on page 12.

See "About corresponding NetBackup software versions " on page 7.

See "About the Appliance Install Manager" on page 7.

Supported upgrade paths

- Direct upgrade paths
  - 5240, 5250, or 5340 appliances with versions 3.3.0.1, 4.0, 4.1 and 5.0
  - 5350 appliances with versions 4.0, 4.1 and 5.0
  - 5340 HA setups with versions 4.0, 4.1 and 5.0
- Two-step upgrade path

Appliance models 5240, 5250, and 5340 with versions 3.2 and earlier must be upgraded twice to get to version 5.1.1. It is recommended that these systems first be upgraded to the minimum supported version (3.3.0.1 or 4.0), and then upgraded to version 5.1.1.

About corresponding NetBackup software versions

NetBackup software version 10.1.1 is included with NetBackup appliance release 5.1.1. Table 1-1 lists the corresponding NetBackup versions for the currently supported NetBackup appliance software releases.

Table 1-1 Supported appliance software releases and the corresponding NetBackup software versions

Appliance software release	NetBackup software version
3.2	8.2
3.3.0.1	8.3.0.1
4.0	9.0
4.1	9.1
5.0	10.0
5.1.1	10.1.1

About the Appliance Install Manager

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

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

The **AIM** window appears as soon as you start the upgrade and provides the following view modes:

- **Main**
  This default view shows the main upgrade steps and task results.
- **Verbose**
  This view shows the detailed upgrade logs.

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

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

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

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

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

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

Chapter 2

Upgrade planning

This chapter includes the following topics:

Requirements and best practices for upgrading NetBackup appliances

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

- Make sure that your appliance environment currently uses software versions 3.3.0.1, 4.0, 4.1, or 5.0 and their associated maintenance releases. Only these versions support a direct upgrade to version 5.1.1.
- You can perform upgrades from the **Appliance Management Console**. After you review all upgrade guidelines and perform the required pre-upgrade tasks, refer to the *Veritas Appliance Management Guide* for the upgrade procedure.

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

- Always perform upgrades with the admin user account. Do not use a non-admin user account to upgrade appliances.
- Always perform a full disaster recovery (DR) backup before an upgrade.
  - Primary servers
    Make sure that you have a recent and complete NetBackup Catalog backup.
  - MSDP configurations

Make sure to configure your deduplication pool catalog backup policy and perform a successful backup. For details, refer to the following article: https://www.veritas.com/support/en_US/article.100046592

- Export and re-import the device certificates.
  If IPSec functionality is configured on any appliance that you plan to upgrade, it will be unconfigured after the upgrade and the device certificates may not be retained. To avoid this issue, you must export the device certificates before upgrading the appliance. Contact Veritas Technical Support to configure IPsec functionality on your appliance.
  Use the `Network > Security > Export` command to perform this task. The `Export` command copies two `.pfx` files (`serialnumber.pfx` and `.serialnumber.pfx`) to a location that you specify when you run the command.
  Export the device certificates before an upgrade as follows:
  - Log in to the NetBackup Appliance Shell Menu and navigate to the following view:
    `Network > Security > Export`
  - Enter the following export option details:
    `Export` *`[EnterPasswd] [PathValue]`*
    Where *[EnterPasswd]* is the field used to answer the question, "Do you want to enter a password?". You must enter **yes** or **no**.
    Where *[PathValue]* is the location where you want to place the exported certificates.
  - After the export has completed, back up both of the `.pfx` files to a non-appliance location.
    After the upgrade has completed, re-import the device certificates. Contact Veritas Support to configure IPsec functionality on your appliance.
    See "Post upgrade tasks" on page 25.
- Delete previously downloaded release updates, client packages, and client add-ons.
  To make sure that there is enough space in the `/inst` partition during the upgrade, first delete all previously downloaded release updates, client packages, and client add-ons from the appliance. As a best practice, always remove downloaded packages after all appliances and clients have been upgraded.
  If you do not delete the previously downloaded packages and the `/inst` directory on the appliance does not contain enough space, the preflight check and the Appliance Upgrade Readiness Analyzer tool prevent the upgrade. Even if enough space exists to allow the upgrade to start, the upgrade may fail if the old client add-ons are not removed. For downloaded packages on high availability (HA) nodes, you must remove the packages from both nodes.

NetBackup Appliance Web Console

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

NetBackup Appliance Shell Menu

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

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

- Follow the same upgrade order for appliances as for traditional NetBackup upgrades. If you use NetBackup OpsCenter, upgrade it first. Then upgrade appliances starting with the primary server appliance, followed by all media server appliances.
- If you have multiple media servers to upgrade, you must perform the upgrade process on each individual media server.
  Appliance media servers (nodes) in an HA setup are updated one at a time. Both nodes must use the same appliance software version. Once you have upgraded one node, you must upgrade the other node immediately.
  See "About upgrades for NetBackup Appliance HA setups" on page 12.
- If a traditional NetBackup primary server is used with an appliance media server, that primary server must have the same NetBackup version or later as the media server appliance. For example, before you upgrade a media server appliance to version 5.1.1, first upgrade the NetBackup primary server to version 10.1.1.
  See "About corresponding NetBackup software versions " on page 7.
- Make sure that the NetBackup primary 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 primary server and the media server.

- If you have enabled the STIG feature on an appliance and you need to upgrade it or install an EEB on it, do not plan such installations during the 4:00am - 4:30am time frame. By following this best practice, you can avoid interrupting the automatic update of the `AIDE` database and any monitored files, which can cause multiple alert messages from the appliance.
- NetBackup clients must use the same or an earlier software version as the appliance. Clients cannot run at a later version than the appliance. For example, a client with NetBackup version 10.1.1 can only be used with an appliance server with version 5.1.1 or later. Client add-ons must also be the same as the client version.
  See "About corresponding NetBackup software versions " on page 7.
- Upgrades to version 3.2 and later using the NetBackup Appliance Shell Menu or the Appliance Management Console (AMS) do not support ECA deployment during the upgrade. After a successful upgrade, you can enable the ECA for NetBackup. For details, see the *NetBackup Appliance Commands Reference Guide*. Additionally, you can configure the ECA to the appliance infrastructure services such as `mongodb`, `tomcat`, and `nginx`. For details, see the *NetBackup Appliance Security Guide*.
- Starting with appliance software version 4.0, Guest users and existing local users cannot access a Universal Share or CIFS shares. After an upgrade to versions 4.0 and later, you can grant access to these shares as follows:
  - Guest users: Replace a Guest user by creating a new local user.
  - Existing local users: Change the passwords for these users.
- Use a compatible version of the NetBackup Administration Console to manage the NetBackup services.
  The NetBackup Administration Console is backward-compatible. A patch release (x.x.x.x) console is compatible with a major (x.x) or minor NetBackup release (x.x.x) that shares the same first and second digits.
- The image within the SSD/ISO partition is refreshed after the upgrade.

About upgrades for NetBackup Appliance HA setups

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

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

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

- One or two nodes in the HA setup
  HA nodes must be upgraded from within the HA setup. If you remove a node from the HA setup, you cannot upgrade the remaining node. HA nodes must be upgraded from within an HA setup that contains both nodes.
- One node at a time
  Only one node can be upgraded at a time so that the workload can continue on the other node.
- One software version
  Both nodes must use the same appliance software version. Once you have upgraded one node, you must upgrade the other node immediately.
- Node upgrade order
  Start the upgrade process on the node where the MSDP service and the virtual IP service are offline, typically, the partner node.

  After the upgrade on the first node has completed, immediately perform the following tasks in the order as shown:
  - On the upgraded node, run the `Support > Test Software` command to verify the status of various appliance software components.
  - If the test passes, log in to the other node and upgrade it in the same manner as the first node.
- MSDP configuration
  Starting with release 4.0, HA nodes can be upgraded even if MSDP storage is not configured.
- Downloading packages from the NetBackup Appliance Shell Menu
  You only need to download rpm packages to one node. After you run the `Manage > Software > List Downloaded` command on the HA node with the downloaded package, run the command on the other node to make the package available on that node.

Upgrade time estimation

Appliance upgrades can take from 1 - 2 hours, depending on the hardware configuration and the current software version.

Note: The above time estimate is based on lab test results for upgrades from all supported direct upgrade paths. The actual upgrade time is dependent on the complexity of the configured environment and can vary.

Chapter 3

Performing the upgrade

This chapter includes the following topics:

Methods for downloading appliance software release updates

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

https://www.veritas.com/content/support/en_US/downloads

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

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

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

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.
     See "Installing a NetBackup appliance software update using the NetBackup Appliance Shell Menu" on page 19.
   - If the table does not contain a software update that you want to install, proceed to the next step.
4. In the **Online Software Updates** table on the page, select a software update and click **Download**.

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

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

See "Downloading software updates directly to a NetBackup appliance" on page 16.

See "Downloading software updates to a NetBackup appliance using a client share" on page 17.

Downloading software updates directly to a NetBackup appliance

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

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

To download software release updates directly onto the appliance

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

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

3. To download an available appliance software update, enter the following command:

   ```
   Main_Menu > Manage > Software > Download
   VRTS_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
   VRTS_NBAPP_update-5.1.1.x86_64.rpm
   ```

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

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

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

See "Requirements and best practices for upgrading NetBackup appliances" on page 9.

See "Downloading software updates to a NetBackup appliance using a client share" on page 17.

Downloading software updates to a NetBackup appliance using a client share

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

For high availability (HA) setups, you only need to download the package to one node. After you complete the package download on the first node, see step 7 for details to make the package available on the other node.

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

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

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

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

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

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

   - Windows CIFS share

     \\<*appliance-name*>\incoming_patches

   - UNIX NFS share

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

4. Copy the release update or client package to the mounted share.

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

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

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

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

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

- `Share Close`

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

`Main_Menu > Manage > Software > List Downloaded`

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

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

See "Requirements and best practices for upgrading NetBackup appliances" on page 9.

See "Downloading software updates directly to a NetBackup appliance" on page 16.

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

Use the following procedure to start the appliance upgrade.

Note: Always perform upgrades with the admin user account. Do not use a non-admin user account to upgrade appliances.

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

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

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

- All required pre-upgrade updates have been completed. For a complete list of required updates prior to 5.1.1 upgrades, refer to the following article: https://www.veritas.com/support/en_US/article.100046066
- All jobs have been stopped or suspended and all SLPs have been paused.

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

2 Log in to the NetBackup Appliance Shell Menu from the IPMI console.

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

---

3 Make sure that you have downloaded and have run the latest version of the Appliance Upgrade Readiness Analyzer tool. The analyzer tool must produce a `pass` result before you can continue to the next step.

4 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.

5 Monitor the preflight check and watch for any failure and warning messages.

- If no **Check failed** messages appear, you are prompted to continue to the next step to start the upgrade.
- If any **Check failed** messages appear, the upgrade is not allowed. You must resolve the reported failures, then launch the upgrade script again so that the preflight check can verify that the failures have been resolved.
- 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.
- If any warning messages appear, Veritas recommends that you read the message and try to resolve the issue before you continue the upgrade. A warning message does not prevent the upgrade from proceeding.

6 Starting with release 5.0, a Call Home settings test is performed. If Call Home is disabled, a prompt appears for you to enable the feature to ensure the Call Home test is performed. You can also enable a proxy server if the test fails. The following warning message is displayed:

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

You can ignore this warning and continue to the next step.

7 After all preflight check items have passed, and before the upgrade begins, you must first select how the upgrade process should respond if any errors occur during the upgrade. The following prompt appears:

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

immediately enforce an automatic rollback? [yes, no]
```

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

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

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

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

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

```
To continue with the upgrade, verify the following CA
certificate detail and enter "yes" to trust the CA certificate.
CA Certificate Details:
     Subject Name : /CN=nbatd/OU=root@abc.example.com/O=vx
       Start Date : Jul 14 12:59:18 2017 GMT
      Expiry Date : Jul 09 14:14:18 2037 GMT
 SHA1 Fingerprint : 31:E9:97:2E:50:11:51:7C:D6:25:7F:32:86:3D:
                    6B:D5:33:5C:11:E2

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

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

  ```
  >> Enter token:
  ```

  Note: If the appliance does not have a valid host-id certificate before the next upgrade to a later version, a reissue token is required for the next upgrade.

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

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

9 Primary server upgrades from software versions 3.1.1 and earlier require you to provide a Veritas Usage Insights registration key. To obtain the registration key, follow the onscreen instructions.

10 During the upgrade process, you can login using SSH and start the AIM window to check the upgrade status (except during the reboot process).

To check the upgrade status, you can:

- Login using an SSH session and start the AIM window to monitor the upgrade process. Enter the following command:
  Main_Menu > **Manage** > **Software** > **UpgradeStatus**.
- Login using the IPMI console and start the AIM window. Enter the following command:
  Main_Menu > **Manage** > **Software** > **UpgradeStatus**.
- Monitor the upgrade process using the IPMI console. When all the updates have been installed successfully, a login prompt appears.

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

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

- Press the **V** key to switch to the **Verbose** view to see the logs. If there are any Unique Message Identification (UMI) codes for the errors, search for them on the Veritas Support website to get more detailed information.
- Try to fix the problem that the **AIM** window reports.

If you need to use the shell menu, log on to the NetBackup Appliance Shell Menu through an SSH session. When the **AIM** window appears, press the **S** key to close it.

- Go back to the **AIM** window on the IPMI console.
  If you tried fixing the problem, press the **A** key to attempt the self-test again.
  If you cannot fix the problem, contact Veritas Support or press the **R** key to roll back the appliance to the previous software version.

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

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

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

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

13 For HA setups only:

After you have completed the upgrade on the first node, run the `Support > Test Software` command to verify the status of various appliance software components. If the test passes, log in to the other node and upgrade it in the same manner as the first node.

14 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, reboot those clients.

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

Note: Starting with NetBackup Appliance version 5.0, refer to the *NetBackup Appliance Security Guide* to run NetBackup commands as a NetBackupCLI user.

Chapter 4

Post upgrade tasks

This chapter includes the following topics:

Post upgrade tasks

After the upgrade process has completed successfully, refer to the following for any required or recommended tasks that you should perform:

https://www.veritas.com/support/en_US/article.100054698

Chapter 5

NetBackup client upgrades with VxUpdate

This chapter includes the following topics:

About VxUpdate

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

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

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

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

To successfully create and use deployment policies, Veritas recommends:

Table 5-1

Step	Action	Additional information
1	Populate the repository	See "VxUpdate repository management" on page 27.
2	Create the deployment policy	See "Deployment policy management" on page 30.
3	(Optional) Manually run the upgrade from the primary server or the client	See "Manually initiating upgrades from the primary server using VxUpdate" on page 34. See "Manually initiating upgrades from the client using VxUpdate" on page 39.

VxUpdate repository management

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

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

The package types you can load into the repository include:

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

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

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

VxUpdate formatted packages are available from the Veritas Support licensing portal. Emergency binaries and hotfixes are obtained from the standard locations. You should download the VxUpdate versions of these packages and place them in a location accessible to the primary server. Once they are accessible to your primary server, you can add them to the VxUpdate package repository.

Downloading Veritas approved NetBackup client packages

1. Go to the Veritas Support licensing portal.
2. Enter your user name and password.
3. Select **Licensing**.
4. Enter or select your account number.
5. Select **Apply Filters**
6. Select your account number from the resulting table.

   This action presents a listing of your entitlements. From here, you have the ability to download the associated software.
7. Select **Downloads**
8. Use the filter options to limit the results to the NetBackup product line and the appropriate product version.

   Add your filters and select **Apply Filters**.
9. Under **Actions**, select the download icon
10. In the resulting table, select the VxUpdate packages and then select **Download**.

    The client packages follow the naming convention shown:
    `vxupdate_nbclient_`*`version_operatingsystem_platform`*`.sja`
11. Download the files to a local machine, then upload the files to `/inst/patch/incoming` on the appliance. Next, upload the files to the appliance as follows:
    - On the machine with the downloaded files, log in to the NetBackup Appliance Web Console and navigate to **Manage > Software Updates**.

- Select the downloaded files and upload them to the appliance.

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

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

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

See the section called “Adding packages to the VxUpdate package repository” on page 29.

Adding packages to the VxUpdate package repository

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

To add packages to the repository

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

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

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

Example: `AddPkg vxupdate_nbclient_8.2_suse_ppc64le.sja`

3 To view the repository and verify that the package was added, run the `ListPkgs` option.

4 To see the package details, run the `ShowPkgDetails n` option, where *`n`* is the package ID number.

Deleting packages from the VxUpdate package repository

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

To delete packages from the repository

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

   `Main > Manage > Software > VxUpdate`

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

   Example: `DelPkg 1`

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

Deployment policy management

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

Creating a deployment policy

Note: You must add packages to the VxUpdate repository before you can create a working deployment policy. You can create deployment policies without packages in the repository, but those policies fail to run successfully.

For more information regarding adding packages, see the *Repository Management* section within the NetBackup Upgrade Guide.

---

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

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

- **Media server**: Specify the media server from drop-down. The media server that is specified is used to connect and transfer files to the hosts that are included in the policy. The media server also caches the files from the repository. The media server must be version 8.1.2 or later. Since the repository resides on the primary server, the primary server is the default value for the media server field.
- **Java GUI and JRE**: Specify if you want the Java GUI and the JRE upgraded on the target systems. The three options include:
  - INCLUDE: Install or upgrade the Java GUI and JRE components on the specified computers.
  - EXCLUDE: Exclude the Java GUI and JRE components from the specified computer. Any preexisting Java GUI and JRE packages are removed.
  - MATCH: Preserve the current state of the Java GUI and JRE components. The components are upgraded if they are present on the pre-upgraded system. The components are not installed if they are not present on the pre-upgraded system.
- (Conditional): Select the **Limit simultaneous jobs** option and specify a value for **jobs** to limit the total number of concurrent jobs that can run at a time. The minimum value is 1 and the maximum value is 999.
  If the check box is selected, the default value is 3. If you do not select the check box, no limit is enforced for the simultaneous upgrade jobs.
  You can set unlimited simultaneous upgrade jobs through command line interface by setting the value as 0.
- **Select hosts**: Select hosts from the **Available hosts** list and select **Add** to add hosts to the deployment policy. The list is generated from hosts in the host database and backup policies. Once you select **Add**, the hosts are shown under **Selected hosts**.

6 Select the **Schedules** tab in the **Change Deployment Policy** window.

You can see a summary of all schedules within that policy.

7 Select **New**.

8 Specify the information that is shown in the **Add Deployment Schedule** window.

- **Name**: Enter a name for the new schedule.
- **Type**: Specify the type of schedule you want created.

  Schedule types:

  - Precheck
    Performs the various precheck operations, including confirming there is sufficient space on the client for the update. The precheck schedule type does not exist for EEB packages.
  - Stage
    Moves the update package to the client, but does not install it. Also performs the precheck operation.
  - Install
    Installs the specified package. Also performs the precheck and the stage package operations. If you already performed the stage package operation, the install schedule does not move the package again.

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

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

9 A **Security** tab appears when you select a deployment package that contains support for external certificate authorities.

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

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

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

Deselecting this option does not allow the user to change the security configuration settings during the upgrade.

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

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

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

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

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

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

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

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

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

To change a deployment policy

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

Deleting a deployment policy

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

Manually initiating upgrades from the primary server using VxUpdate

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

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

See "Manually initiating upgrades from the client using VxUpdate" on page 39.

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

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

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

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

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

   - Specify the type of schedule you want to run from the **Type** drop-down.
   - Select the media server you want to use from the **Media server** drop-down.
   - Confirm that the host you want upgraded is listed under **Selected hosts**.

5 (Conditional) If present, click on the **Configure** button to configure external certificate authority information.

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

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

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

Deselecting this option does not allow the user to change the security configuration settings during the upgrade.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

   Windows: `install_path\netbackup\bin`

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

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

   ```
   nbinstallcmd -policy policy_name -schedule schedule
   [-master_server primary]
   ```

   Where *policy_name* is the name of the deployment policy, *schedule* is the name of the schedule, and *primary* is the name of the primary server.

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

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

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

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

---

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

   Windows: `install_path\netbackup\bin`

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

2. Use the `nbinstallcmd` command as shown:

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

   Where:

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

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

Commands Reference Guide

Manually initiating upgrades from the client using VxUpdate

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

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

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

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

See "Manually initiating upgrades from the primary server using VxUpdate" on page 34.

The `nbinstallcmd` version on a back-level host is not the current `nbinstallcmd` version when you initiate a non-policy based upgrade directly on the target client or media server. Refer to the Commands Reference Guide for the currently installed version of for the exact format of `nbinstallcmd` command.

Because of this older version of `nbinstallcmd`, exceptions to normal VxUpdate behavior include:

- If your primary server uses both certificate and an external certificate, and your target media server or client is at 8.1.2: Running a non-policy based upgrade directly on the target host is not supported. You must upgrade with one of the options shown:
  - Upgrade the client or the media server using VxUpdate from the primary server.
  - Create a policy on the primary server. Then run policy-based `nbinstallcmd` on the target client or media server.
  - Disable the external certificate on your primary server before starting the non-policy-based upgrade on the target host. You may turn on the external certificate after the upgrade completes successfully.

- If the client or the media server is at 8.2 or earlier, the `-components` flag is not available. This flag was introduced in 8.3 to enable optional installation of the Java GUI and JRE. When you run an ad-hoc `nbinstallcmd` on a client or a media server at 8.2 or earlier, the `-components javagui_jre` option defaults to `MATCH`. This value causes the upgrade to match the Java GUI and JRE status of the pre-upgrade host. If the pre-upgrade host had Java GUI and JRE installed, it remains installed after upgrade. If the pre-upgrade host did not have Java GUI and JRE installed, it is not installed after upgrade.

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

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

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

   Windows: *`install_path`*`\netbackup\bin`

2. Use the `nbinstallcmd` as shown:

   `nbinstallcmd -policy` *`policy`* `-schedule` *`schedule`* `-master_server` *`name`*

   Example: `nbinstallcmd -policy all_clients -schedule install812 -master_server primary1`

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

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

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

Commands Reference Guide

Deployment job status

Monitor and review deployment job status in the Activity Monitor in the Administration Console. The **Deployment** job type is the new type for VxUpdate policies. Deployment policy parent jobs that exit with a status code 0 (zero) indicate that all the child jobs successfully completed. Parent jobs that finish with a status code 1 indicate that one or more of the child jobs succeeded, but at least one failed. Any other status code indicates failure. Review the status of the child jobs to determine

why they failed. Otherwise, there are no differences between deployment jobs and other jobs.

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

Linux: `/usr/openv/netbackup/bin/admincmd`

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

Use the syntax shown:

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

Note: Staring with NetBackup Appliance version 5.0, refer to the *NetBackup Appliance Security Guide* to run NetBackup commands as a NetBackupCLI user.

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

Table 5-2 Deployment policy operating system and hardware

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

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

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

https://www.veritas.com/content/support/en_US/article.100039650

Your deployment job may receive a status code 7207. This error can occur if precheck or upgrade processes take longer than expected to finish or never finish. To configure the amount of time VxUpdate waits before jobs end with status 7207, you can define the following values in the configuration on the primary server.

`VXUPDATE_CLIENT_READ_TIMEOUT_SECONDS`

This value controls how long the precheck operations and the client upgrade operations are allowed to take, in seconds. The default value is 1800, or 30 minutes. It can be decreased to as little as 600, 10 minutes, or increased to as much as 3600, 60 minutes.

`VXUPDATE_SERVER_READ_TIMEOUT_SECONDS`

This value controls how long server upgrade operations are allowed to take, in seconds. The default value is 2700, or 45 minutes. It can be decreased to as little as 600, 10 minutes, or increased to as much as 5400, 90 minutes.

See the Commands Reference Guide for details on how to use the `bpsetconfig` command to add values to the configuration of a primary server.

Chapter 6

Troubleshooting

This chapter includes the following topics:

Troubleshooting upgrade issues

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

Index