

# NetBackup™ Upgrade Quick Start Guide

Release 10.1

**VERITAS™**

# NetBackup™ Upgrade Quick Start Guide

Last updated: 2022-08-30

## Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC  
2625 Augustine Drive  
Santa Clara, CA 95054

<http://www.veritas.com>

## Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

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

Japan

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

## Documentation

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

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

## Documentation feedback

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

[NB.docs@veritas.com](mailto:NB.docs@veritas.com)

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

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

## Veritas Services and Operations Readiness Tools (SORT)

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

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

# Contents

<b>Chapter 1</b>	<b>About the NetBackup Quick-Start Upgrade Guide</b>	<b>5</b>
	.....	5
	About the NetBackup Quick-Start Upgrade Guide .....	5
<b>Chapter 2</b>	<b>Windows Upgrade Quick Start Guide</b>	<b>7</b>
	Preinstall procedure for upgrading to NetBackup 10.1 .....	27
	Performing local, remote, or clustered server upgrades on Windows systems .....	11
	Post-install procedure for upgrading to NetBackup 10.1 .....	35
<b>Chapter 3</b>	<b>UNIX/Linux Upgrade Quick Start Guide</b>	<b>27</b>
	Preinstall procedure for upgrading to NetBackup 10.1 .....	27
	Upgrading Linux server software to NetBackup 10.1 .....	31
	Post-install procedure for upgrading to NetBackup 10.1 .....	35

# About the NetBackup Quick-Start Upgrade Guide

This chapter includes the following topics:

- [About the NetBackup Quick-Start Upgrade Guide](#)

## About the NetBackup Quick-Start Upgrade Guide

This manual is designed as a supplement to the *NetBackup Upgrade Guide* for the experienced user. Use of this manual by novice or inexperienced NetBackup administrators is not recommended. These administrators should use the *NetBackup Upgrade Guide*.

---

**Note:** All information in this manual is duplicate information from the *NetBackup Upgrade Guide*. Veritas presents this information in a different format for ease of use by the more experienced users. If you like the format of the *NetBackup Upgrade Guide*, there is no need to consult this manual.

---

The information in this manual assumes that you have already read and understand the upgrade prerequisites. It assumes that you have already performed any of the necessary planning procedures and are aware how long upgrades take. It assumes that you are aware of all the changes that are outlined in the *NetBackup Release Notes*.

---

**Caution:** If at any time while using this manual, you are unsure of a step, a procedure, or have questions, refer to the *NetBackup Upgrade Guide* for additional information. The *NetBackup Upgrade Guide* has greater detail on all areas of the upgrade process.

<http://www.veritas.com/docs/DOC5332>

---

# Windows Upgrade Quick Start Guide

This chapter includes the following topics:

- [Preinstall procedure for upgrading to NetBackup 10.1](#)
- [Performing local, remote, or clustered server upgrades on Windows systems](#)
- [Post-install procedure for upgrading to NetBackup 10.1](#)

## Preinstall procedure for upgrading to NetBackup 10.1

Use the following procedure to upgrade your environment to NetBackup 10.1.

Several tools are available to help you perform the extra step that is required for the guided method. For more details, contact your Business Critical Services (BCS) representative.

Additional steps are required if the NetBackup upgrade includes an upgrade to RHEL 7.5 and you use Fibre Transport Media Server (FTMS). More information is available.

See the [NetBackup Upgrade Guide](#).

---

**Note:** For NetBackup installations that include globally clustered primary servers using the Global Cluster Option (GCO), follow the upgrade planning guidelines in this guide. Then, refer to the following document for the specific steps to upgrade these servers: [https://www.veritas.com/support/en\\_US/article.100041191](https://www.veritas.com/support/en_US/article.100041191)

---

## Preinstall steps to upgrade to NetBackup 10.1 and complete the image metadata migration

- 1 Perform environment checks with the SORT tool.  
See the [NetBackup Upgrade Guide](#).
- 2 Download the Customer Registration Key for Veritas Usage Insights. More information about Veritas Usage Insights is available.  
See the [NetBackup Upgrade Guide](#).

During install and upgrade to NetBackup 10.1, please allow the installer to copy the `veritas_customer_registration_key.json` file to its final destination. NetBackup can set the file permission and ownership correctly through this process. If you place the file onto your systems outside of the install or the upgrade process, the process may not work correctly.

- 3 (Conditional) On Linux, if the NetBackup database files reside on `btrfs` file system, move it to a supported file system (such as `ext4` or `xfs`) before you upgrade. It is not supported to reside the NetBackup database on a `btrfs` file system. The database files reside on the primary server in the directories under `/usr/opensv/db`.

To move the NetBackup database files on Linux:

- Perform a catalog backup.
- Shut down all NetBackup daemons:  

```
/usr/opensv/netbackup/bin/bp.kill_all
```
- Start the SQL Anywhere daemon:  

```
/usr/opensv/netbackup/bin/nbdbms_start_stop start
```
- Move the existing data, index, and transaction log files:  

```
/usr/opensv/db/bin/nbdb_move -data data_directory -index  
index_directory -tlog log_directory
```

If you use mirrored transaction log, use the command shown:

```
/usr/opensv/db/bin/nbdb_move -data data_directory -index  
index_directory -tlog log_directory -mlog log_mirror_directory
```
- Start all NetBackup daemons:  

```
/usr/opensv/netbackup/bin/bp.start_all
```
- Perform a catalog backup.

- 4 (Conditional) On Windows, be sure that all operating system and security updates are applied. More information is available.  
See the [NetBackup Upgrade Guide](#).



- 5 Perform any pre-upgrade tasks that you would normally do in regard to your NetBackup environment. For example:
  - Stop all customized or third-party scripts.
  - Perform any cluster-specific tasks.
  - Run a hot catalog backup.
  - Disable all storage lifecycle policies (SLPs).
  - Deactivate all NetBackup policies.
  - Deactivate all disk staging storage units for all pre-NetBackup 7.5.x environments.
  - For VMware and Red Hat Virtualization (RHV) environments, reduce the size of the job database before upgrade. Following an upgrade, existing VMware and RHV jobs are assigned an asset namespace to enable access control at an asset level. This process may take some time. More information about this process is available:  
See the [NetBackup Upgrade Guide](#).
  - For clustered systems only, take the following NetBackup resources offline:
    - Windows Server Failover Clusters (WSFC): Take all of the NetBackup group resources offline except for the disk, the virtual name, and the virtual IP address. Refer to the Microsoft Cluster Administration documentation to determine how to take the NetBackup group resources offline through the cluster administrator interface.
    - Cluster Server (VCS) clusters: Take the NetBackup resource offline. Freeze the NetBackup group with the `-persist` option using the command shown:

```
hagrpl -freeze NetBackup_service_group -persistent
```

Refer to the *NetBackup Clustered Primary Server Administrator's Guide* for the commands to take these resources offline.
- 6 (Conditional) If you plan to change your NetApp cluster to Vserver mode from node scope mode, create a detailed image report for each filer. You can generate this report with the `bpimagelist` command. The example that is shown is one possible option. Use whatever options are necessary for your environment.

```
bpimagelist -client ndmp_host_name
```

- 7 Beginning with NetBackup 8.0, the NetBackup primary server includes a configured Tomcat web server to support critical backup operations. This web server operates under user account elements with limited privileges. These user account elements must be available on each primary server (or each node of a clustered primary server). More information is available:

See the [NetBackup Upgrade Guide](#).

---

**Note:** It is recommended that you save the details of the user account that you use for the NetBackup Web Services. A primary server recovery requires the same NetBackup Web Services user account and credentials that were used when the NetBackup catalog was backed up.

---

**Note:** If the NetBackup PBX is running in secure mode, please add the web service user as authorized user in PBX. More information about determining PBX mode and how to correctly add users is available.

<http://www.veritas.com/docs/000115774>

---

- 8 (Conditional) If you have customized the settings for your Tomcat web server, determine if those settings persist across upgrades. More information is available:

See the [NetBackup Upgrade Guide](#).

- 9 Stop any applications on the system that interact with NetBackup. This step includes any databases or system components being backed up. Failure to stop these applications may result in unexpected behavior. Observed behavior includes aborted upgrades and application failures.

For Oracle users, ensure that no backups are running. Stop the RMAN processes before you install NetBackup. If you use AIX, you should run `/usr/bin/slibclean` as the root user after you stop the RMAN processes.

If you cannot stop your Oracle database, a procedure is available that may let you install NetBackup with the Oracle database active. More information on this topic is available.

<http://www.veritas.com/docs/TECH158276>

- 10 Stop all NetBackup services.

- On UNIX systems: `/usr/opensv/netbackup/bin/bp.kill_all`
- On Windows systems: `install_path\NetBackup\bin\bpdown -f`

The preinstall procedure is completed. Proceed to upgrade the NetBackup binaries.

# Performing local, remote, or clustered server upgrades on Windows systems

Use the following procedure to upgrade to NetBackup 10.1 on a local, a remote, or a clustered computer.

## To upgrade the NetBackup binaries for a local, remote, or clustered server on Windows

- 1 Log on to the system where you want to initiate the NetBackup upgrade. Be sure to log on with administrator privileges.
  - To upgrade local Windows systems, log on to the computer directly at the console.
  - To upgrade remote Windows systems, log on to a system with network access to all of the hosts where you want to install NetBackup.
  - To upgrade clustered Windows systems, log on to the active node (the node with the shared disk).
- 2 Navigate to the directory where the ESD images (downloaded files) reside and run `Browser.exe` to start the NetBackup Installation Wizard.
- 3 On the initial browser screen (**Home**), click **Installation**.
- 4 On the **Installation** screen, click **Server Software Installation**.
- 5 On the **Welcome** screen, review the content and click **Next**.
- 6 (Conditional) If you previously installed NetBackup 10.1 on this host, you see the **Program Maintenance** dialog.
  - Select **Modify** to change installation settings for the local host, or to use the local host as a platform to perform push installation to remote hosts.
  - Select **Repair** to restore NetBackup 10.1 to its original state on the local host.
  - Select **Remove** to remove NetBackup 10.1 from the local host.
- 7 On the **License Agreement** screen, do the following:
  - **I agree to and accept the terms of the license agreement.**  
You must select this item to upgrade the software.
  - Click **Next**.

- 8 On the **Veritas NetBackup Installation Type** screen, provide the following information:

**Where to install**

For a local upgrade, select **Install to this computer only**.

For a remote upgrade, select **Install to multiple computers on your network**.

For a clustered upgrade, the only option is **Install a clustered primary server**.

**Typical**

Select this option to upgrade NetBackup with the default settings.

**Media server only:** By default the typical option looks at the media server's configuration and only upgrades the Java GUI and the JRE packages if they are currently present. Choose **Custom** if you want to force a state other than what is currently on the media server. If you select to exclude the Java GUI and the JRE, any previous versions are removed.

**Custom**

Select this option to override the default NetBackup settings.

Click **Next**.

- 9 On the **NetBackup License and Server Type** screen, provide the following information:

■ **License**

For upgrades, the license for the existing installation type determines which components you can select.

---

**Note:** For remote upgrades, the license that you enter here gets pushed to the other nodes. Your license may enable add-on products. If you push NetBackup to nodes that have an add-on product already installed, your license works for the add-on product(s).

---

For remote or for clustered upgrades, the following occurs during the upgrade process to verify that you have the proper credentials to perform the upgrade:

- When you select a clustered system for upgrade, NetBackup determines if you have proper administrator credentials on all nodes in the cluster. If you do not have the proper credentials, the system is not added to the list.

**Performing local, remote, or clustered server upgrades on Windows systems**

- If you have the proper credentials, NetBackup performs a second check to determine if a license is needed. If a license is needed and one was not entered, the system cannot be added to the list. You must enter a valid license to upgrade on that node. If you enter an invalid license, this screen remains visible until a valid license is entered.
- Click **NetBackup Primary Server** to proceed to upgrade the primary server software.
- Click **NetBackup Media Server** to proceed to upgrade the media server software. Note that the media server upgrade does not require a license.

**10** (Conditional) Remote upgrades see the **FIPS Compliance in NetBackup** dialog.

NetBackup does not support changing the FIPS mode during upgrade. Enable FIPS mode before the upgrade if the existing NetBackup version supports FIPS. Otherwise, enable it after the upgrade.

Enabling or disabling FIPS mode during Windows remote upgrade does not change the existing FIPS mode value in the NetBackup configuration on remote hosts.

For more information about FIPS please check the *NetBackup Security and Encryption Guide*.

**11** On the **Customer Registration Key** screen, enter the location of the customer registration key. You download this file from the Veritas Usage Insights site and place the file on the appropriate primary server. More information about Veritas Usage Insights is available.

See the [NetBackup Upgrade Guide](#).

During install and upgrade to NetBackup 10.1, please allow the installer to copy the `veritas_customer_registration_key.json` file to its final destination. NetBackup can set the file permission and ownership correctly through this process. If you place the file onto your systems outside of the install or the upgrade process, the process may not work correctly.

---

**Note:** Be aware that NetBackup does not support the short file name format (8.3 format) for the customer registration key file name.

---

**12** On the **NetBackup Web Services** screen, enter the **Web Services Password**.

This password is the password for the NetBackup web services user account. You must create this account before you install the primary server. More information is available.

On the **NetBackup Web Services** screen, specify the account type and the account details.

**What types of accounts should we use?** Select either **Local** or **Domain (Active Directory)**.

Select **Local** if you want to associate the web server with a user and a group account that exist on the local host.

Select **Domain (Active Directory)** if you want to associate the web server with a user and a group account that exist on a trusted Windows domain.

**What are the existing account details** Specify the information as shown:

- **Domain** - If you chose the **Domain (Active Directory)** account type, specify the name of the domain to which the user and the group accounts belong.
- **Group** - Specify the name of the group account to associate with the web server.
- **User** - Specify the name of the user account to associate with the web server. For security reasons, do not specify a user account that has administrative privileges on the host.
- **Password** - Specify the password of the user account in the **User** field.

More information is available.

See the [NetBackup Upgrade Guide](#).

**13** This step applies only to **Custom** upgrades. For **Typical** installations, skip to the next step.

This step describes how to select and configure the **NetBackup Features**, **NetBackup Port Numbers**, and the **NetBackup Services**.

- **Java GUI and JRE Options**  
(Conditional: Media server only) Depending on your upgrade, the options you see include:
  - **Include Java GUI and JRE:** Install or upgrade the Java GUI and the JRE on the specified computer.
  - **Exclude Java GUI and JRE:** Exclude the Java GUI and the JRE components from the specified computer. Any preexisting Java GUI and JRE components are removed.

**Performing local, remote, or clustered server upgrades on Windows systems**

- **Match Existing Configuration:** Preserve the current state of the Java GUI and JRE components. The components are upgraded if they are present on the pre-upgraded systems. The components are not installed if they are not present on the pre-upgraded systems.
- **NetBackup Port Numbers**  
 On this screen, you can change port numbers, if it is necessary in your configuration.  
 You may need to change a port number if you encounter conflicts when NetBackup and another industry product try to share the same port. Another example is if a port conflict occurs with a firewall, which may cause security issues.  
 To change a port number, select the port number that you want to replace and type the new number.  
 Click **Next**.
- **NetBackup Services**  
 On this screen, provide the following startup account and startup type information for NetBackup services:

**Privileged Account Details** Specify either **Local System account** or **Custom account**.

By default, the **Local System account** is selected, so that NetBackup uses the built-in system account. When this option is selected, the fields below it are disabled.

To specify a different system account:

- Select **Custom account**.
- Enter the account information in the following fields:
  - Domain**
  - Username**
  - Password**

**Non-Privileged Account Details** Specify either **Same as the Privileged Account specified above** or **Local Service account**.

Using a local service account involves a one-time conversion that may significantly increase the upgrade time based on your catalog size.

For more information for the non-privileged service user account, refer to: <https://www.veritas.com/docs/100048220>

This information is only applicable to primary server upgrades.

**Startup Type** This option determines whether NetBackup services start automatically if you need to restart the NetBackup host. The default is **Automatic**.

To start NetBackup services manually after a restart, select **Manual**.

**Performing local, remote, or clustered server upgrades on Windows systems****Start job-related NetBackup services following installation**

By default, job-related services are set to start automatically after the upgrade has completed.

To prevent job-related services from starting automatically, click on the box to clear the check mark.

**Safe Abort Option**

This option determines how the upgrade proceeds if a restart is required as part of the upgrade.

If you select this option and the upgrade process determines that a restart is required, the upgrade stops. The system is then rolled back to its original state.

If you do not select this option, the upgrade proceeds even if the upgrade process determines that a restart is required.

Click **Next**.

**14** On the **NetBackup System Names** screen, provide the following information:**Primary Server Name**

For primary server installations, enter the name of the local computer.

For media server installations, you must change the name to the primary server name to which the media server is configured.

**Note:** For clustered servers, this field is **NetBackup Virtual Host Name**. Veritas strongly recommends that you not change this value.

**Additional Servers**

Enter the names of any additional NetBackup primary servers and media servers that you want to communicate with this server. Include the names of computers where you plan to install NetBackup later.

To enter more than one name, separate each name with a comma or press **Enter** after each name.

**Media Server Name**

This field appears only for NetBackup Enterprise media server installations.

When you install media server software, this field defaults to the local server name.

Click **Next**.

**15 (Conditional: For media servers only)** If your environment uses an external certificate authority, you receive the **External Certificate** screen. On the **External Certificate** screen, select one of the three radio buttons based on how you want to configure the external certificate authority (ECA). Depending on which one you select, you must complete different information:

- **Use Windows certificate store**

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



---

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

---

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

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

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

- **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.
- **Do not use a CRL.**
- **Use certificate from a file**

After you select this option, specify the following:

  - **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.
  - **CRL option:** Specify the correct CRL option for your environment:
    - **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.
    - **Do not use a CRL.**
- **Proceed without security**

You receive a warning message listing potential issues. Depending on the state of the current security configuration, NetBackup may be unable to

perform backups or restores until an external CA certificate has been configured.

Click **Next** to continue.

**16** For remote upgrades only, on the **Veritas NetBackup Remote Hosts** screen, specify the hosts where you want NetBackup installed.

- **Windows Destination Systems**

Right-click **Windows Destination Computers** and select from the drop-down menu, or use the following methods:

**Performing local, remote, or clustered server upgrades on Windows systems****Browse**

Click here to search the network for the hosts where you want to upgrade NetBackup.

- On the **Available Systems** dialog box, select the computer to add and click **Next**.
- On the **Remote Computer Login Credentials** dialog box, enter the user name, the password, and the domain of the account for NetBackup to use on the remote computers.
- If you plan to upgrade multiple remote computers, click the box next to **Remember User Name and Password**. Selecting this option prevents the need to enter this information for each remote computer.

When you provide credentials, you select host nodes and add them to the **Windows Destination Systems** list. These are the nodes on which you remotely upgrade NetBackup. Make sure that you select your local host when you select systems to install.

Each time you choose a system, NetBackup performs system and license checks. For example, it verifies the system for a server upgrade that matches the type that you selected, as follows:

- NetBackup not installed: Considers the remote to be verified.
- NetBackup already installed: Compares the upgrade type on that system to the upgrade type that you request.
- Invalid combination: Notifies you of the problem and disallows the choice. One example of an invalid combination is to try to install a Remote Administration Console on a remote system that is already a primary server.
- Remote system not a supported platform or level: Notifies you of the problem and disallows the choice.

The upgrade procedure also verifies that you have proper administrator credentials on the remote system. If you do not have administrator credentials, the **Enter Network Password** screen appears, and prompts you to enter the administrator's user name and password.

Click **OK** and continue selecting destination systems.

This process repeats for each node that you select. You can elect to retain the user name and password. In that case, you are prompted only when the user name or password is not valid.

Note the following about the push-install process in a clustered environment:

- You can upgrade NetBackup on any number of nodes. However, the clustering service sets the limit for the number of nodes in a cluster, not NetBackup.
- Language packages and other NetBackup add-on products cannot be upgraded with the push method. Add-on products must be upgraded on each individual node in the cluster group. For instructions on how to upgrade these products, refer to the NetBackup documentation that supports each product.

**Browse (cont.)**

*(continued)*

- NetBackup pushes to the other nodes only the license you enter at the beginning of the upgrade. Your license may enable add-on products. If you push NetBackup to nodes that have an add-on product already installed, your license works for that product.
- Click **OK**.

**Performing local, remote, or clustered server upgrades on Windows systems****Import**

Click here to import a text file that contains a list of host names. When you create the text file, the host names must be defined in the following format:

```
Domain\ComputerName
```

**Add**

Click here to add a host manually.

- On the **Manual Remote Computer Selection** dialog box appears, enter the **Domain** and the **Computer Name**, then click **OK**.
- On the **Remote Computer Login Credentials** dialog box, enter the **User Name** and the **Password** of the account to be used to perform the upgrade on the remote computers.
 

If you plan to add and upgrade multiple remote computers, click the box next to **Remember User Name and Password**. Selecting this option prevents the need to enter this information for each remote computer.
- Click **OK**.

**Remove**

To remove a host from the **Destination Systems** list, select the host and click here.

**Change**

Click here to change the destination for NetBackup file installation on the selected remote host.

- Click **Next**.

- 17** For cluster upgrades only, on the **Cluster Settings** screen, review the information displayed. All information except the **Public Network** is displayed for informational purposes and cannot be changed. If you need to change the public network, select the correct public network from the drop-down.

---

**Warning:** You must not select a private network that is assigned to this cluster.

---

Click **Cluster Configuration**. When the successful cluster configuration message appears, click **Next**.

- 18 (Conditional: For primary servers only)** Depending on the size of your catalog, you may be prompted to proceed with the **Infinite retention conversion**.

Upgrades from pre-NetBackup 9.0 to NetBackup 9.0 and later include the infinite expiration conversion. This conversion supports expiration dates beyond 2038. This conversion may extend the time that is required to complete the upgrade. Review the article that is shown for more information:

[https://www.veritas.com/content/support/en\\_US/article.100048600](https://www.veritas.com/content/support/en_US/article.100048600)

- 19** On the **Ready to Install the Program** screen, review the **Installation Summary** that shows your selections from the previous steps.

If the ECA health check utility indicates the Cryptographic Service Provider (CSP) or the Key Storage Provider (KSP) doesn't support the security descriptors, the upgrade cannot proceed.

This flag indicates that the provider cannot be used when NetBackup services are run in the local service user account context. Use a provider that supports security descriptors or use an administrator account to run all NetBackup services.

For more details on the service user account, see the *Limitations of Windows Certificate Store support when NetBackup services are running in Local Service account context* information in the [NetBackup Security and Encryption Guide](#).

- 20** Select one of the following options:

- Click **Install** to start the installation.
- Click **Back** to view the previous screens and make any changes, then return to this screen and click **Install**.
- Click **Cancel** to cancel the upgrade.

After you click **Install**, the upgrade process begins and a screen appears that shows you the upgrade progress. This process may take several minutes.

For remote or for cluster upgrades only, right-click on a system in the dialog box to see the upgrade status. Up to five upgrades occur simultaneously. When an upgrade is completed, another one begins so that a maximum of five upgrades are in progress.

- 21** For remote upgrades only, when all remote upgrades have completed, click **Finish**.

- 22** On the **Installation Complete** screen, select from the following options:

## Add Licenses

**Add Licenses** is only applicable to primary servers.

Veritas recommends that you enter additional licenses now for any other NetBackup products you plan to install.

- To enter additional licenses, click **Add Keys**.
- When the list of **Current License Keys** appears, click **Add Key** to enter a new license key, then click **Add**.
- After all license keys are entered, close the **Current License Keys** window.

**View installation log file**

An upgrade log file provides detailed installation information and shows whether any errors occurred. This log includes information about the optional installation of the Java GUI and the JRE.

Examine the upgrade log at the following location:

```
%ALLUSERSPROFILE%\Veritas\NetBackup\InstallLogs\
```

**Note:** When you perform a remote upgrade to multiple computers, this option only lets you view the log for the local computer. Each computer that you selected for upgrade contains its own upgrade log file. To view the log file of a remote computer, open a Windows Explorer window and enter \\<COMPUTERNAME>.

Search the upgrade log for the following error indications:

- Strings that include `Return Value 3`.
- Important log messages that are color coded as follows:  
Yellow = warning.  
Red = error.

**Finish**

Select one of the following to complete the upgrade:

- If you are done upgrading software on all servers, click the box next to **Launch NetBackup Administration Console now** and click **Finish**.  
The NetBackup Administration Console starts a Configuration Wizard so that you can configure your NetBackup environment.
- If you have more server software to upgrade, click **Finish**.  
You can move on to the next computer and upgrade the necessary server software.

- 23 If any NetBackup cluster configuration is modified manually or by any external script, make sure that the change is reflected correctly in NetBackup cluster registry. Contact Veritas Enterprise technical support if you have questions.
- 24 The binaries are successfully installed. Proceed to the post-installation procedure.

## Post-install procedure for upgrading to NetBackup 10.1

[Post-installation steps to upgrade to NetBackup 10.1](#) describes the post-installation steps to upgrade NetBackup and complete the image metadata migration.

### Post-installation steps to upgrade to NetBackup 10.1

- 1 Check for an available NetBackup 10.1 maintenance release. Maintenance releases include very important fixes that are released after NetBackup 10.1.

Veritas encourages you to install the latest available maintenance release during upgrade activities.

To access the latest NetBackup 10.1 maintenance release:

- Go to the NetBackup SORT website.  
<https://sort.veritas.com/netbackup>
  - In the **Installation and Upgrade Checklist** section:
    - Under **Product**, select the correct product (NetBackup Enterprise Server or NetBackup Server)
    - Under **Product version you are installing or upgrading to** specify the latest version of NetBackup
    - Under **Platform** select the platform of the server you want to upgrade.
    - Under **Processor** specify the processor of your server.
    - Under **Product version you are upgrading from (Optional)** select the current version of NetBackup on the server you want to upgrade.
    - Click **Generate Checklist**.
  - Under **Upgrade Information**, there is a **version\_number Download Links** hyperlink. Click that hyperlink for the latest maintenance release.
  - If no maintenance release is available, restart `bprd` if you terminated it. Proceed once `bprd` is restarted.  
Linux: `/usr/openv/netbackup/bin/bprd`  
Windows: `install_path\NetBackup\bin\bprd`
  - If you find a maintenance release is available, download it now.
  - Prepare for the install by stopping all NetBackup processes and services. Use the command shown:  
UNIX and Linux: `/usr/openv/netbackup/bin/bp.kill_all`  
Windows: `install_path\NetBackup\bin\bpdown -f`
  - Install the maintenance release.
  - Restart NetBackup with the commands shown:  
UNIX and Linux systems: `/usr/openv/netbackup/bin/bp.start_all`  
Windows systems: `install_path\NetBackup\bin\bpup -f`
- 2 Set a passphrase for the disaster recovery package. If you do not set a passphrase, the catalog backups fail. More information is available. Please see the information about passphrases in the [NetBackup Troubleshooting Guide](#).

- 3 If you plan to use role-based access control (RBAC), you must designate a security administrator. More information is available:  
  
See the [NetBackup Web UI Security Administrator's Guide](#).
- 4 Start any applications on the system that interact with NetBackup. This step includes any databases or system components being backed up.
- 5 (Conditional) If you have a clustered primary server, generate a certificate on the inactive nodes for secure communications. More information is available.  
  
See the [NetBackup Upgrade Guide](#).
- 6 (Conditional) If this server is a clustered server, update the other nodes in the cluster. You can update the other primary servers nodes in the cluster to NetBackup 10.1 by following standard cluster upgrade process. For complete details, see the [NetBackup Clustered Primary Server Administrator's Guide](#).  
  
If the NetBackup resource is not online, bring that resource online.  
  
<http://www.veritas.com/docs/DOC5332>
- 7 (Conditional) For a primary server that uses external certificate authority (ECA) or for a media server that skipped ECA configuration, configure the ECA now. More information is available:  
  
[https://www.veritas.com/support/en\\_US/article.100044300](https://www.veritas.com/support/en_US/article.100044300)  
  
For more information, see the [NetBackup Security and Encryption Guide](#) and refer to the chapter on external CA and external certificates.
- 8 If you have any media servers that you intend to upgrade to NetBackup 10.1, you may upgrade them now. If you start any media server upgrades, do not continue with this procedure until the media server upgrades are complete.

---

**Note:** NetBackup requires that media servers have a security certificate to function correctly in certain use cases. More information about this topic is available.

See the [NetBackup Upgrade Guide](#).

---

More information about this topic is available.

See the [NetBackup Upgrade Guide](#).

- 9 Reactivate the following in the order as shown:
  - All disk staging storage units.
  - All NetBackup policies.
  - All storage lifecycle policies (SLPs).



- 10** (Conditional) If your environment uses cloud storage, you need to update the read and write buffer sizes. More information is available.

See the [NetBackup Upgrade Guide](#).
- 11** (Conditional) If you have a NetApp cluster, additional steps may be required. More information is available.

See the [NetBackup Upgrade Guide](#).
- 12** (Conditional) For the cloud and the storage servers with SSL enabled, the CRL validation is enabled by default. Verify if the storage servers are running and the CRL functionality works correctly. More information is available.

See the [NetBackup Cloud Administrator's Guide](#).
- 13** (Conditional) For Amazon configurations, after you upgrade NetBackup and CloudPoint to the latest version, you must update the credentials. Run the `tpconfig -update` command. After the upgrade, the credentials are updated to only support the AWS IAM role. More information is available.

See the [NetBackup Cloud Web UI Administrator's Guide](#).
- 14** Monitor your backup environment to verify that normal NetBackup operation has resumed.

- 15** Upgrade any media servers and clients not already upgraded as time and backup windows permit. Be sure to upgrade the media servers before you upgrade the clients. You cannot back up or restore a NetBackup 8.1 client to a pre-8.1 media server.

See the [NetBackup Upgrade Guide](#).

A client upgrade is the same as a client installation. See the *NetBackup Installation Guide - UNIX and Windows* manual for help with the installation.

<http://www.veritas.com/docs/DOC5332>

---

**Note:** All scripts must be stored and run locally. One recommendation is that scripts should not be world-writable. Scripts are not allowed to be run from network or remote locations. Any script that is created and saved in the NetBackup `db_ext` (UNIX) or `dbext` (Windows) location needs to be protected during a NetBackup uninstall.

For more information about registering authorized locations and scripts, review the knowledge base article:

<http://www.veritas.com/docs/000126002>

For more information about your specific database agent, review the documentation for that agent:

<http://www.veritas.com/docs/DOC5332>

---

- 16** (Conditional) For upgrades of NetBackup 8.2 Linux clusters with NAT enabled to the latest version, the upgrade disables NAT. To turn on NAT and allow the cluster to monitor the `nbmqbroker` service that is added to a NetBackup cluster group, run the command shown:

- To configure with default ports:

```
configureMQ -enableCluster -defaultPorts
```

- To configure with specific ports:

```
configureMQ -enableCluster -externalPort port1 -internalPorts  
port2 port3 port4
```

- 17** Perform any additional upgrade steps. More information about this topic is available.

See the [NetBackup Upgrade Guide](#).

# UNIX/Linux Upgrade Quick Start Guide

This chapter includes the following topics:

- [Preinstall procedure for upgrading to NetBackup 10.1](#)
- [Upgrading Linux server software to NetBackup 10.1](#)
- [Post-install procedure for upgrading to NetBackup 10.1](#)

## Preinstall procedure for upgrading to NetBackup 10.1

Use the following procedure to upgrade your environment to NetBackup 10.1.

Several tools are available to help you perform the extra step that is required for the guided method. For more details, contact your Business Critical Services (BCS) representative.

Additional steps are required if the NetBackup upgrade includes an upgrade to RHEL 7.5 and you use Fibre Transport Media Server (FTMS). More information is available.

See the [NetBackup Upgrade Guide](#).

---

**Note:** For NetBackup installations that include globally clustered primary servers using the Global Cluster Option (GCO), follow the upgrade planning guidelines in this guide. Then, refer to the following document for the specific steps to upgrade these servers: [https://www.veritas.com/support/en\\_US/article.100041191](https://www.veritas.com/support/en_US/article.100041191)

---

### Preinstall steps to upgrade to NetBackup 10.1 and complete the image metadata migration

- 1 Perform environment checks with the SORT tool.  
See the [NetBackup Upgrade Guide](#).
- 2 Download the Customer Registration Key for Veritas Usage Insights. More information about Veritas Usage Insights is available.  
See the [NetBackup Upgrade Guide](#).

During install and upgrade to NetBackup 10.1, please allow the installer to copy the `veritas_customer_registration_key.json` file to its final destination. NetBackup can set the file permission and ownership correctly through this process. If you place the file onto your systems outside of the install or the upgrade process, the process may not work correctly.

- 3 (Conditional) On Linux, if the NetBackup database files reside on `btrfs` file system, move it to a supported file system (such as `ext4` or `xfs`) before you upgrade. It is not supported to reside the NetBackup database on a `btrfs` file system. The database files reside on the primary server in the directories under `/usr/opensv/db`.

To move the NetBackup database files on Linux:

- Perform a catalog backup.
- Shut down all NetBackup daemons:  
`/usr/opensv/netbackup/bin/bp.kill_all`
- Start the SQL Anywhere daemon:  
`/usr/opensv/netbackup/bin/nbdbms_start_stop start`
- Move the existing data, index, and transaction log files:  
`/usr/opensv/db/bin/nbdb_move -data data_directory -index index_directory -tlog log_directory`  
If you use mirrored transaction log, use the command shown:  
`/usr/opensv/db/bin/nbdb_move -data data_directory -index index_directory -tlog log_directory -mlog log_mirror_directory`
- Start all NetBackup daemons:  
`/usr/opensv/netbackup/bin/bp.start_all`
- Perform a catalog backup.

- 4 (Conditional) On Windows, be sure that all operating system and security updates are applied. More information is available.  
See the [NetBackup Upgrade Guide](#).

- 5 Perform any pre-upgrade tasks that you would normally do in regard to your NetBackup environment. For example:
  - Stop all customized or third-party scripts.
  - Perform any cluster-specific tasks.
  - Run a hot catalog backup.
  - Disable all storage lifecycle policies (SLPs).
  - Deactivate all NetBackup policies.
  - Deactivate all disk staging storage units for all pre-NetBackup 7.5.x environments.
  - For VMware and Red Hat Virtualization (RHV) environments, reduce the size of the job database before upgrade. Following an upgrade, existing VMware and RHV jobs are assigned an asset namespace to enable access control at an asset level. This process may take some time. More information about this process is available:  
 See the [NetBackup Upgrade Guide](#).
  - For clustered systems only, take the following NetBackup resources offline:
    - Windows Server Failover Clusters (WSFC): Take all of the NetBackup group resources offline except for the disk, the virtual name, and the virtual IP address. Refer to the Microsoft Cluster Administration documentation to determine how to take the NetBackup group resources offline through the cluster administrator interface.
    - Cluster Server (VCS) clusters: Take the NetBackup resource offline. Freeze the NetBackup group with the `-persist` option using the command shown:  

```
hagrpl -freeze NetBackup_service_group -persistent
```

 Refer to the *NetBackup Clustered Primary Server Administrator's Guide* for the commands to take these resources offline.
- 6 (Conditional) If you plan to change your NetApp cluster to Vserver mode from node scope mode, create a detailed image report for each filer. You can generate this report with the `bpimagelist` command. The example that is shown is one possible option. Use whatever options are necessary for your environment.

```
bpimagelist -client ndmp_host_name
```

- 7** Beginning with NetBackup 8.0, the NetBackup primary server includes a configured Tomcat web server to support critical backup operations. This web server operates under user account elements with limited privileges. These user account elements must be available on each primary server (or each node of a clustered primary server). More information is available:

See the [NetBackup Upgrade Guide](#).

---

**Note:** It is recommended that you save the details of the user account that you use for the NetBackup Web Services. A primary server recovery requires the same NetBackup Web Services user account and credentials that were used when the NetBackup catalog was backed up.

---

**Note:** If the NetBackup PBX is running in secure mode, please add the web service user as authorized user in PBX. More information about determining PBX mode and how to correctly add users is available.

<http://www.veritas.com/docs/000115774>

---

- 8** (Conditional) If you have customized the settings for your Tomcat web server, determine if those settings persist across upgrades. More information is available:

See the [NetBackup Upgrade Guide](#).

- 9** Stop any applications on the system that interact with NetBackup. This step includes any databases or system components being backed up. Failure to stop these applications may result in unexpected behavior. Observed behavior includes aborted upgrades and application failures.

For Oracle users, ensure that no backups are running. Stop the RMAN processes before you install NetBackup. If you use AIX, you should run `/usr/bin/slibclean` as the root user after you stop the RMAN processes.

If you cannot stop your Oracle database, a procedure is available that may let you install NetBackup with the Oracle database active. More information on this topic is available.

<http://www.veritas.com/docs/TECH158276>

- 10** Stop all NetBackup services.

- On UNIX systems: `/usr/opensv/netbackup/bin/bp.kill_all`
- On Windows systems: `install_path\NetBackup\bin\bpdown -f`

The preinstall procedure is completed. Proceed to upgrade the NetBackup binaries.

# Upgrading Linux server software to NetBackup 10.1

You should schedule your upgrade and reconfiguration for a time when backups do not run. However, the upgrade procedure instructs you to deactivate all policies to ensure that backups do not interfere with the upgrade. You can also temporarily modify policies so that backups do not run while you upgrade and reconfigure NetBackup.

## To upgrade Linux server software to 10.1

- 1 Log on as the root user on the server.
- 2 If the NetBackup Administration Console is open, you must close it now.
- 3 (Conditional) For clustered environments, perform the following tasks:
  - If necessary, edit the `bp.conf` and the `vm.conf` files as follows:  
If a `REQUIRED_INTERFACE` entry exists, replace it with a `CLUSTER_NAME` entry. Otherwise, add a new `CLUSTER_NAME` entry. This entry should be defined as the virtual server name.  
For a primary server, make sure that the first `SERVER` entry matches the `CLUSTER_NAME` entry for the `bp.conf` file.
  - Take the NetBackup Server Resource (*ServerResource*) offline. Use the command shown:  

```
/opt/VRTSvcs/bin/hares -offline ServerResource -sys $nodename
```
  - Freeze the NetBackup Group so that migrations do not occur while the inactive nodes are upgraded. Use the command shown:  

```
/opt/VRTSvcs/bin/hagrp -freeze group -persistent
```
  - If you have a VCS cluster configured, you can freeze the NetBackup Group by using the Cluster Manager interface or the command line.
  - Before you proceed with a cluster upgrade, refer to the *NetBackup Clustered Primary Server Administrator's Guide* for other cluster upgrade requirements.  
<http://www.veritas.com/docs/DOC5332>
- 4 NetBackup scripts that are not covered in Chapter 1 that you modified are removed when you run the upgrade script. More information about this topic is available.

See the [NetBackup Upgrade Guide](#).

Save any files that you have modified and want to keep.

- 5** Navigate to the location where the installation images reside. Enter the command that is shown to start the upgrade script:

```
./install
```

- 6** Follow the prompts in the installation script to install the NetBackup server binaries.
- 7 (Conditional: For primary servers only)** If prompted, reply to the question regarding the infinite expiration conversion:

NetBackup 9.0 and later versions support the retention periods that extend beyond the year 2038. To ensure compatibility with previous NetBackup versions, all items with an infinite expiration date are updated to reflect the new infinite expiration date value. This conversion may extend the time that is required to complete the upgrade. Review the following article for more information:

[https://www.veritas.com/content/support/en\\_US/article.100048600](https://www.veritas.com/content/support/en_US/article.100048600)

```
Date of collection: date_time
NetBackup state: online|offline
Records found: records
Conversion time estimate: time (hh:mm)
```

Please see the linked article to obtain a more accurate estimate of how long the conversion may take.

Would you like to continue with the upgrade? [y,n]

- 8 (Conditional: For primary server only)** If prompted, provide the name of the service user account you want to use to start most of the daemons. This prompt is only shown if the installer cannot retrieve the service user value from the bp.conf file.

Enter the name of the service user account to be used to start most of the daemons

Please note:

- The service username cannot exceed 32 characters and can only contain English characters.
- Veritas does not recommend that you use the root user as the service user.
- You cannot use the `nbwebsvc` user as the service user.
- The `nbwebgrp` group must be a secondary group of the service user.



- Ownership of the `/usr/opensv` directory changes to the new service user account that you specified here.
- Using a service account involves a one-time conversion that may significantly increase the upgrade time based on your catalog size.
- If you want to change the service user account after the installation, use the `nbserviceusercmd --changeUser` command.

For more details on the service user account, see:  
<https://www.veritas.com/docs/100048220>

**9 (Conditional: For media servers only)** If your environment uses an external certificate authority, provide the external certificate authority information at the prompts shown:

```
Enter the certificate file path or q to skip security configuration:
/usr/eca/cert_chain.pem
```

```
Enter the trust store location or q to skip security configuration:
/usr/eca/trusted/cacerts.pem
```

```
Enter the private key path or q to skip security configuration:
/usr/eca/private/key.pem
```

```
Enter the passphrase file path or q to skip security configuration
(default: NONE): /usr/eca/private/passphrase.txt
```

---

**Note:** Be aware the passphrase file path is optional.

---

**10 (Conditional: For media servers only)** When prompted, provide the required information for the CRL configuration:

```
Should a CRL be honored for the external certificate?
1) Use the CRL defined in the certificate.
2) Use the CRL from a file path.
3) Do not use a CRL.
q) skip security configuration
CRL option (1):
```

**11 (Conditional: For media servers only)** If you specified **Use the CRL from a file path**, you must enter the path to the CRL location:

```
Enter the CRL location path or q to skip security configuration:
/usr/eca/crl
```

**12 (Conditional: For media servers only)** The installer echoes the configuration information you entered and attempts to retrieve details for the external certificate:

```
External CA values entered:
Certificate file path: /usr/eca/cert_chain.pem
Trust store file path: /usr/eca/trusted/cacerts.pem
Private key file path: /usr/eca/private/key.pem
Passphrase file path: /usr/eca/private/passphrase.txt
    CRL check level: Use the CRL from a file path.
    CRL location path: /usr/eca/crl
```

Getting external CA certificate details

```
    Issued By : CN=IITFRMNUSINT,O=Veritas,OU=iitf
    Subject Name : CN=cuomovm04,O=Veritas,OU=iitf
    Expiry Date : Oct 31 17:25:59 2019 GMT
    SHA1 Fingerprint : 62:B2:C3:31:D5:95:15:85:9D:C9:AE:C6:EA:C2:
                        DF:DF:6D:4B:92:5B
    Serial Number : 0x6c7fa2743072ec3eaae4fd60085d468464319a
    Certificate Path : /usr/eca/cert_chain.pem
```

Validating host ECA certificate.

NOTE: Depending on the network, this action may take a few minutes.  
 To continue without setting up secure communication, press Ctrl+C.

**13 (Conditional: For media servers only)** If the external certificate enrollment pre-check finishes successfully, select **1** and press **Enter** to continue.

The external certificate enrollment pre-check is successful.

The external certificate is valid for use with primary server *name*  
 How do you want to proceed?

- 1) Continue the installation using this certificate.
- 2) Modify the external CA values entered.
- 3) Abort the installation.

Default option (1):

- 14 (Conditional: For media servers only)** If the external certificate enrollment pre-check fails, select from the choices shown. The default is **2**.

The external certificate enrollment pre-check failed.

The external certificate is not valid for use with primary server *name*  
 How do you want to proceed?

- 1) Continue the installation and set up external certificates later.
- 2) Modify the external CA values entered.
- 3) Abort the installation.

Default option (2):

- 15 (Conditional: For media servers only)** When prompted, indicate how the upgrade should handle the Java GUI and JRE binaries.

The Java GUI and JRE packages are currently *install\_state* on this host.

The Java GUI and JRE can be optionally included with NetBackup. The Java GUI and JRE enable the NetBackup Administration Console and the Backup, Archive and Restore (BAR) GUI. Choose an option from the list below.

- 1) Update the Java GUI and JRE.
- 2) Remove the Java GUI and JRE.

If you specify **1**, the Java and JRE binaries are installed or upgraded, based on the status of the server. If you specify **2**, the Java and JRE binaries are removed or excluded, based on the status of the server.

- 16** When the script finishes, the binaries are successfully installed.

Proceed to the post-installation procedure.

## Post-install procedure for upgrading to NetBackup 10.1

[Post-installation steps to upgrade to NetBackup 10.1](#) describes the post-installation steps to upgrade NetBackup and complete the image metadata migration.

### Post-installation steps to upgrade to NetBackup 10.1

- 1** Check for an available NetBackup 10.1 maintenance release. Maintenance releases include very important fixes that are released after NetBackup 10.1. Veritas encourages you to install the latest available maintenance release during upgrade activities.

To access the latest NetBackup 10.1 maintenance release:

- Go to the NetBackup SORT website.  
<https://sort.veritas.com/netbackup>
  - In the **Installation and Upgrade Checklist** section:
    - Under **Product**, select the correct product (NetBackup Enterprise Server or NetBackup Server)
    - Under **Product version you are installing or upgrading to** specify the latest version of NetBackup
    - Under **Platform** select the platform of the server you want to upgrade.
    - Under **Processor** specify the processor of your server.
    - Under **Product version you are upgrading from (Optional)** select the current version of NetBackup on the server you want to upgrade.
    - Click **Generate Checklist**.
  - Under **Upgrade Information**, there is a **version\_number Download Links** hyperlink. Click that hyperlink for the latest maintenance release.
  - If no maintenance release is available, restart `bprd` if you terminated it. Proceed once `bprd` is restarted.  
 Linux: `/usr/opensv/netbackup/bin/bprd`  
 Windows: `install_path\NetBackup\bin\bprd`
  - If you find a maintenance release is available, download it now.
  - Prepare for the install by stopping all NetBackup processes and services. Use the command shown:  
 UNIX and Linux: `/usr/opensv/netbackup/bin/bp.kill_all`  
 Windows: `install_path\NetBackup\bin\bpdown -f`
  - Install the maintenance release.
  - Restart NetBackup with the commands shown:  
 UNIX and Linux systems: `/usr/opensv/netbackup/bin/bp.start_all`  
 Windows systems: `install_path\NetBackup\bin\bpup -f`
- 2** Set a passphrase for the disaster recovery package. If you do not set a passphrase, the catalog backups fail. More information is available. Please see the information about passphrases in the [NetBackup Troubleshooting Guide](#).
- 3** If you plan to use role-based access control (RBAC), you must designate a security administrator. More information is available:  
 See the [NetBackup Web UI Security Administrator's Guide](#).

- 4 Start any applications on the system that interact with NetBackup. This step includes any databases or system components being backed up.
- 5 (Conditional) If you have a clustered primary server, generate a certificate on the inactive nodes for secure communications. More information is available. See the [NetBackup Upgrade Guide](#).
- 6 (Conditional) If this server is a clustered server, update the other nodes in the cluster. You can update the other primary servers nodes in the cluster to NetBackup 10.1 by following standard cluster upgrade process. For complete details, see the [NetBackup Clustered Primary Server Administrator's Guide](#).  
If the NetBackup resource is not online, bring that resource online.  
<http://www.veritas.com/docs/DOC5332>
- 7 (Conditional) For a primary server that uses external certificate authority (ECA) or for a media server that skipped ECA configuration, configure the ECA now. More information is available:  
[https://www.veritas.com/support/en\\_US/article.100044300](https://www.veritas.com/support/en_US/article.100044300)  
For more information, see the [NetBackup Security and Encryption Guide](#) and refer to the chapter on external CA and external certificates.
- 8 If you have any media servers that you intend to upgrade to NetBackup 10.1, you may upgrade them now. If you start any media server upgrades, do not continue with this procedure until the media server upgrades are complete.

---

**Note:** NetBackup requires that media servers have a security certificate to function correctly in certain use cases. More information about this topic is available.

See the [NetBackup Upgrade Guide](#).

---

More information about this topic is available.

See the [NetBackup Upgrade Guide](#).

- 9 Reactivate the following in the order as shown:
  - All disk staging storage units.
  - All NetBackup policies.
  - All storage lifecycle policies (SLPs).
- 10 (Conditional) If your environment uses cloud storage, you need to update the read and write buffer sizes. More information is available.  
See the [NetBackup Upgrade Guide](#).

- 11** (Conditional) If you have a NetApp cluster, additional steps may be required. More information is available.

See the [NetBackup Upgrade Guide](#).

- 12** (Conditional) For the cloud and the storage servers with SSL enabled, the CRL validation is enabled by default. Verify if the storage servers are running and the CRL functionality works correctly. More information is available.

See the [NetBackup Cloud Administrator's Guide](#).

- 13** (Conditional) For Amazon configurations, after you upgrade NetBackup and CloudPoint to the latest version, you must update the credentials. Run the `tpconfig -update` command. After the upgrade, the credentials are updated to only support the AWS IAM role. More information is available.

See the [NetBackup Cloud Web UI Administrator's Guide](#).

- 14** Monitor your backup environment to verify that normal NetBackup operation has resumed.

- 15** Upgrade any media servers and clients not already upgraded as time and backup windows permit. Be sure to upgrade the media servers before you upgrade the clients. You cannot back up or restore a NetBackup 8.1 client to a pre-8.1 media server.

See the [NetBackup Upgrade Guide](#).

A client upgrade is the same as a client installation. See the *NetBackup Installation Guide - UNIX and Windows* manual for help with the installation.

<http://www.veritas.com/docs/DOC5332>

**Note:** All scripts must be stored and run locally. One recommendation is that scripts should not be world-writable. Scripts are not allowed to be run from network or remote locations. Any script that is created and saved in the NetBackup `db_ext` (UNIX) or `dbext` (Windows) location needs to be protected during a NetBackup uninstall.

For more information about registering authorized locations and scripts, review the knowledge base article:

<http://www.veritas.com/docs/000126002>

For more information about your specific database agent, review the documentation for that agent:

<http://www.veritas.com/docs/DOC5332>

**16** (Conditional) For upgrades of NetBackup 8.2 Linux clusters with NAT enabled to the latest version, the upgrade disables NAT. To turn on NAT and allow the cluster to monitor the `nbmqbroker` service that is added to a NetBackup cluster group, run the command shown:

- To configure with default ports:

```
configureMQ -enableCluster -defaultPorts
```

- To configure with specific ports:

```
configureMQ -enableCluster -externalPort port1 -internalPorts  
port2 port3 port4
```

**17** Perform any additional upgrade steps. More information about this topic is available.

See the [NetBackup Upgrade Guide](#).