Veritas NetBackup™ Upgrade Guide

Release 9.1

VERITAS™

Veritas NetBackup™ Upgrade Guide

Last updated: 2021-06-30

Legal Notice

Copyright © 2021 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
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://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

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 7

About the NetBackup 9.1 Upgrade Guide 7
Available NetBackup upgrade methods 8
About changes in NetBackup 9.1 10
Windows compiler and security requirements for NetBackup 9.1 and later installation and upgrade 10
Java GUI and JRE installation optional for some computers 11
Logging directory permissions require reset on rollback 11
Upgrades from NetBackup 7.6.0.4 and earlier are not supported 11
External certificate authority certificates supported in NetBackup 8.2 and later 12
About Veritas Usage Insights 12
Best practices for Veritas Usage Insights 13

Chapter 2 Planning for an upgrade 15

General upgrade planning information 15
About planning a NetBackup 9.1 upgrade 15
How to plan for an upgrade to NetBackup 9.1 16
Known catalog backup limitation 19
About security certificates for NetBackup hosts 19
About automatic file changes from an upgrade 20
Reduce the job database size before upgrade 21
Known SUSE Linux primary server upgrade issue 22
About upgrade tools 22
About Veritas Services and Operations Readiness Tools 22
Recommended SORT procedures for upgrades 23
About the NetBackup preinstall checker 27
Upgrade operational notes and limitations 28
Creating the user account to support the NetBackup web server 28
About NetBackup 9.1 support for Fibre Transport Media Server with RHEL 7.5 and later 29
MSDP changes in NetBackup 8.1 30
Potential required changes for NetApp clusters 30

Errors when Bare Metal Restore information is replicated using Auto Image Replication 30
Upgrade issue with pre-8.1 clients and 8.1 or later media servers 31

Chapter 3 Master server upgrade 32

About primary server upgrades 32
Preinstall procedure for upgrading to NetBackup 9.1 33
Performing local, remote, or clustered server upgrades on Windows systems 37
Performing silent upgrades on Windows systems 49
Upgrading UNIX and Linux server software to NetBackup 9.1 52
Post-install procedure for upgrading to NetBackup 9.1 57
About NetBackup startup and shutdown scripts 62
Completing your system update after an upgrade 63

Chapter 4 Media server upgrade 66

Upgrading NetBackup media servers to NetBackup 9.1 66
Silently upgrading NetBackup media server software on UNIX and Linux 69

Chapter 5 MSDP upgrade for NetBackup 76

MSDP upgrade considerations for NetBackup 8.1 76
About MSDP rolling data conversion 77
About MSDP fingerprinting algorithm changes 78

Chapter 6 Client upgrade 79

About client upgrades 79
Upgrading UNIX and Linux clients with the NetBackup upgrade script 80
Upgrade of the UNIX and Linux client binaries with native installers 82

Chapter 7 NetBackup Deployment Management with VxUpdate 96

About VxUpdate 96
Commands used in VxUpdate 97
Repository management 98
Deployment policy management 101

Manually initiating upgrades from the primary server using VxUpdate 105
Manually initiating upgrades from the media server or client using VxUpdate 110
Deployment job status 112

Appendix A Reference 114

NetBackup master server web server user and group creation 115
Generate a certificate on the inactive nodes of a clustered master server 117
About the NetBackup Java Runtime Environment 118
Add or Remove Java GUI and JRE after upgrade 120
About the NetBackup web user interface 121
About the NetBackup answer file 122
Persistent Java Virtual Machine options 141
About RBAC bootstrapping 142
About NetBackup software availability 143
Additional post-upgrade steps for NetApp clusters 144
Using NetApp disk arrays with Replication Director 146
About compatibility between NetBackup versions 150
Upgrade requirements for UNIX and Linux 151
Installation and upgrade requirements for Windows and Windows clusters 155
Requirements for Windows cluster installations and upgrades 162
Removing a clustered media server by migrating all data to a new media server 163
Disabling the connection between your OpsCenter server and your NetBackup Primary Server 164
Post upgrade procedures for Amazon cloud storage servers 165
Upgrading clients after servers are upgraded 166

Index 171

Chapter 1

Introduction

This chapter includes the following topics:

- About the NetBackup 9.1 Upgrade Guide
- Available NetBackup upgrade methods
- About changes in NetBackup 9.1
- About Veritas Usage Insights
- Best practices for Veritas Usage Insights

About the NetBackup 9.1 Upgrade Guide

The NetBackup 9.1 Upgrade Guide is provided to help assist you plan and accomplish your upgrade to NetBackup 9.1. This guide is updated periodically to provide you with the most up-to-date information. You can obtain the latest version of this guide on the NetBackup 9.1 Upgrade portal, at the following link:

http://www.veritas.com/docs/000115678

The Veritas Services and Operations Readiness Tools (SORT) is also a valuable resource for upgrade preparation. More information about SORT is available.

See “About Veritas Services and Operations Readiness Tools” on page 22.

Caution: The NetBackup 9.1 upgrade guide provides an upgrade path from NetBackup version 7.7.x and later to NetBackup 9.1. Information about required upgrade steps for older versions of NetBackup are removed from the NetBackup 8.1 and later upgrade guides. This change simplifies the upgrade procedure for customers with more current versions of NetBackup.

For a successful upgrade from older NetBackup versions directly to 9.1, you must:

Refer to the *NetBackup 8.0 Release Notes* to understand the changes to NetBackup.

Refer to the upgrade procedure that is listed in the *NetBackup 8.0 Upgrade Guide*.

Combine the upgrade steps in the NetBackup 8.0 procedure with the upgrade steps in the *NetBackup 9.1 Upgrade Guide*.

Veritas recommends that you refer to the *NetBackup Release Notes* and *NetBackup Upgrade Guide* for each release, not only NetBackup 8.0, for details about these earlier upgrades. These documents provide additional information about upgrade steps and the requirements that are helpful for a successful upgrade.

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

Available NetBackup upgrade methods

The table that is shown details the various ways you can upgrade NetBackup.

Table 1-1

Upgrade method and operating system	Server	Client
Interactive UNIX and Linux	Primary server See "Upgrading UNIX and Linux server software to NetBackup 9.1" on page 52. Media server See "Upgrading NetBackup media servers to NetBackup 9.1" on page 66.	Review the server information.

Table 1-1 *(continued)*

Upgrade method and operating system	Server	Client
Interactive Windows	Primary server See "Performing local, remote, or clustered server upgrades on Windows systems" on page 37. Media server See "Upgrading NetBackup media servers to NetBackup 9.1" on page 66.	Review the server information.
Silent UNIX and Linux	Not a valid upgrade method for primary servers. Media server See "Silently upgrading NetBackup media server software on UNIX and Linux" on page 69.	See "Upgrade of the UNIX and Linux client binaries with native installers" on page 82.
Silent Windows	Primary and media server See "Performing silent upgrades on Windows systems" on page 49.	Review the server information.
Remote UNIX and Linux	Not a valid upgrade method.	Remote UNIX and Linux client upgrades See "Upgrading clients after servers are upgraded" on page 166. Chef and SCCM templates https://sort.veritas.com/utility/netbackup/deployment
Remote Windows	Primary server See "Performing local, remote, or clustered server upgrades on Windows systems" on page 37. Media server See "Upgrading NetBackup media servers to NetBackup 9.1" on page 66.	Chef and SCCM templates https://sort.veritas.com/utility/netbackup/deployment

About changes in NetBackup 9.1

The following describes some important changes to NetBackup version 9.1. For complete details, see the *NetBackup Release Notes* for version 9.1.

Windows compiler and security requirements for NetBackup 9.1 and later installation and upgrade

NetBackup 9.1 and later for Windows uses the Visual Studio 2019 compiler and the Windows 10 Software Development Kit (SDK). The installation and the upgrade process use Microsoft redistributable utilities to install Visual Studio 2019 C++ run-time libraries on Windows hosts where they are not already installed. These utilities can fail or behave unexpectedly on hosts without all the security updates in place. Windows hosts must have all security updates in place before you install or upgrade to NetBackup 9.1 or later.

More information on the Microsoft redistributable utilities is available: https://visualstudio.microsoft.com/downloads/

Failures and unexpected behaviors include:

- NetBackup's installation or upgrade process fails shortly after start with a message about inability to deploy Visual Studio 2019 C++ run-time libraries.
- The `nbcertcmdtool` application failing unexpectedly when executed by the NetBackup installation or upgrade process. This failure is difficult to distinguish from `nbcertcmdtool` failures that result from invalid or insufficient security configuration.
- MSDP applications fail unexpectedly near the conclusion of the NetBackup installation or upgrade process.

To prevent this problem, apply all Windows security updates before any install or any upgrade attempts.

For Windows Server 2012 R2 and Windows 8.1, the list of required security updates includes KB 2919355 (https://support.microsoft.com/en-us/topic/windows-rt-8-1-windows-8-1-and-windows-server-2012-r2-update-april-2014-3c9d820b-7079-359d-8660-21de648fa31d).

For Windows Server 2012 R2, 2008 Service Pack 2, Windows 8.1, and all other earlier supported versions, you must install the Universal C run-time in Windows update. This update lets NetBackup run correctly. Microsoft KB 3118401 is the minimum patch level to ensure the appropriate C++ run-time binaries are present. Other later patches should contain this fix.

More information about this requirement is available:
https://support.microsoft.com/en-us/topic/update-for-universal-c-runtime-in-windows-322bf30f-4735-bb94-3949-49f5c49f4732

Java GUI and JRE installation optional for some computers

Starting with NetBackup 8.3, the Java GUI and the JRE packages are optional for UNIX, Linux, and Windows media servers and UNIX and Linux clients.

As with previous releases, the Java GUI and JRE packages are installed automatically on all master servers because they are required. The Java GUI and the JRE are not part of the default installation on Windows clients. Install the Java Remote Administration Console if you require this functionality on your Windows clients.

The various NetBackup installation methods allow the user the choice to install or not install the Java GUI and JRE packages. More information about installing the Java GUI and the JRE after install or upgrade is available.

See "Add or Remove Java GUI and JRE after upgrade" on page 120.

Logging directory permissions require reset on rollback

If the NetBackup 8.3 Windows upgrade fails and you need to rollback to an earlier version, you must use the `mklogdir` command to reset the log folder permissions. The NetBackup 8.3 upgrade modifies the permissions on the logging folders and those permissions are incompatible with early versions of NetBackup. After you roll back NetBackup, run `mklogdir.bat -fixFolderPerm` to revert the permissions on the logging folders to the pre-8.3 permissions. This requirement is only applicable to the Windows platform. For additional information on the `mklogdir` command, refer to the NetBackup Commands Reference Guide.

Upgrades from NetBackup 7.6.0.4 and earlier are not supported

Substantial logic is required to upgrade NetBackup from release to release. In the interest of efficiency, upgrade logic specific to NetBackup 7.6.0.4 and earlier is retired. These releases of NetBackup are end of support life and are unsupported. If you attempt to upgrade NetBackup 7.6.0.4 or earlier to 9.1, the preinstallation check fails and the upgrade cannot continue.

If you are running one of these versions of NetBackup and want to upgrade to NetBackup 9.1, use an intermediate release as a stepping stone. More information is available about supported versions of NetBackup

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

External certificate authority certificates supported in NetBackup 8.2 and later

NetBackup introduced support for external certificate authority certificates in NetBackup 8.2. This change provides an alternative to the NetBackup Certificate Authority for providing host verification and security. It supports certificates in PEM, DER, and P7B formats.

For information on external CA support in NetBackup and external CA-signd certificates, see the NetBackup Security and Encryption Guide.

External certificate authority limitations in NetBackup 8.2

- **External certificate authority specifications containing UNC paths or mapped network drives fail for Windows hosts that use a remote installation method**

  You cannot use UNC paths and mapped network drives for external CA certificate specifications on Windows hosts performing remote installations. Remote installation methods include VxUpdate and the setup wizard push installation option. If you attempt to use a UNC path or mapped network drive, the precheck and the installation operations fail due to inaccessible paths.

About Veritas Usage Insights

Veritas Usage Insights helps you manage your NetBackup deployment more efficiently, spot trends, and plan for the future. With accurate, near real-time reporting, it reveals the total amount of data that is backed up. Usage Insights alerts you if you are close to exceeding your licensed capacity limits. Usage Insights requires Veritas NetBackup 8.1.2 and later.

Usage Insights provides:

- Accurate, near real-time reporting of terabytes protected
- Usage trends that are shown in a graphical display
- Consumption assessments to alert before licensed capacity is exceeded
- Easy capacity planning and budgeting
- Identification of growth spikes or potential gaps in coverage

For customers who use capacity licensing (NDMP, Limited Edition, or Complete), Usage Insights helps accurately measure capacity usage. This measurement gives total visibility into how each of the protected workloads consumes storage and enables efficient capacity planning. Furthermore, Usage Insights eliminates the need for these customers to provide manual uploads of telemetry data to Veritas by automatically providing the necessary telemetry.

The following URL provides additional answers to frequently asked questions.

https://help.veritas.com/vxhelp6/#/?context=veritas_usage_insights_netbackup&token=vui_nbu_faqs

Caution: Usage Insights is compatible with Google Chrome and Mozilla Firefox. Veritas does not recommend using Microsoft Edge or Microsoft Internet Explorer, as they do not render all information correctly.

See "Best practices for Veritas Usage Insights" on page 13.

Best practices for Veritas Usage Insights

Veritas suggests certain best practices for use of the Usage Insights tool.

- Usage Insights is compatible with Google Chrome and Mozilla Firefox. Veritas does not recommend using Microsoft Edge or Microsoft Internet Explorer, as they do not render all information correctly.
- Confirm your site's ability to transmit secure web traffic.
  Usage Insights uses `HTTPS` to send relevant information. Your master server must allow outbound `HTTPS` traffic to take advantage of the automatic upload feature. Manual uploads require `HTTPS` traffic from the upload location.
- Your customer registration key is not a license key.
  The registration key is required for Usage Insights to work, but it is not your NetBackup license key. The customer registration key is downloaded from the Usage Insights website and is specific to Usage Insights.
- If you have multiple account IDs, when you download your customer registration key, you may have an aggregate registration key. This aggregate registration key includes all of your account IDs. You can use the aggregate key on all of your master servers. NetBackup does, however, prompt you to assign the specific key with a specific account ID to a specific master server. If you want, you can use this aggregate key for all your master servers.
- During install and upgrade to NetBackup 8.1.2, 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.
- Be aware that NetBackup does not support the short file name format (8.3 format) for the customer registration key file name.
- For answers to frequently asked questions, visit the URL shown:

https://help.veritas.com/vxhelp6/#/?context=veritas_usage_insights_netbackup&token=vui_nbu_faqs

To download the customer registration key

1. Log into Veritas NetInsights Console with Google Chrome or Mozilla Firefox.

   https://netinsights.veritas.com

2. Navigate to the **Veritas Usage Insights** page.
3. Download the appropriate customer registration key for your master server.

Chapter 2

Planning for an upgrade

This chapter includes the following topics:

- General upgrade planning information
- About upgrade tools
- Upgrade operational notes and limitations

General upgrade planning information

Review this section for the details that are related to planning for an upgrade.

About planning a NetBackup 9.1 upgrade

The currently installed version of NetBackup affects the upgrade process for the NetBackup 9.1 upgrade. Upgrades from any version of NetBackup must plan for the NBDB database rebuild and the MSDP rolling conversion. Table 2-1 has additional information about what tasks you must perform for the upgrade.

Table 2-1 Required upgrade tasks based on currently installed version

Upgrade task	Versions that must perform the task
NBDB database rebuild	All versions must perform the NBDB database rebuild.
MSDP conversion	All versions that use MSDP must perform the MSDP rolling conversion. See "MSDP upgrade considerations for NetBackup 8.1" on page 76.

Before you begin an upgrade, Veritas recommends that you review the *NetBackup Release Notes* document that is included with your media kit or the electronic

product image files. This document describes important changes in NetBackup 9.1 that you should be familiar with before you upgrade.

Caution: To help ensure a successful upgrade to NetBackup 9.1, you should visit the SORT page and the NetBackup Upgrade Portal and for complete upgrade details:

SORT page:

https://sort.veritas.com/netbackup

See "About Veritas Services and Operations Readiness Tools" on page 22.

NetBackup Upgrade Portal:

http://www.veritas.com/docs/000115678

See "How to plan for an upgrade to NetBackup 9.1" on page 16.

How to plan for an upgrade to NetBackup 9.1

Several factors must be considered when you prepare for an upgrade to NetBackup 9.1.

Starting NetBackup daemons and services as non-administrative user

New to NetBackup 9.1, you can start most of the NetBackup daemons and services as a non-root user. Veritas recommends that you start the NetBackup services as a non-root user. If you decide to use a less privileged user, you must plan accordingly. Ensure that the user account has access to the paths of disaster recovery files, external certificate authority (ECA) files, and temporary files.

On UNIX and Linux, you see a new prompt during the upgrade. The new prompt asks you to provide a service user, preferably a non-root user. You must create this user in advance and the user must have `nbwebgrp` as the secondary group.

On Windows, you can use the Local Service built-in account as the service account. This option is available in the **Custom** upgrade path.

Media Server Deduplication Pool rolling conversion

The NetBackup 8.1 upgrade includes a rolling conversion of the Media Server Deduplication Pool (MSDP).

By default, the rolling conversion is performed when the system is not busy. In other words, the conversion runs when backups, restores, CRQP, CRC checks, compaction, etc. are not active. This conversion is not expected to affect normal system operations. After the rolling conversion is finished, there is no difference

between the converted system and a new installation. More information about the rolling conversion is available.

See “MSDP upgrade considerations for NetBackup 8.1” on page 76.

See “About MSDP rolling data conversion” on page 77.

Specify security administrator for RBAC

If you plan to use role-based access control (RBAC), you must designate a security administrator. More information is available:

See “About the NetBackup web user interface” on page 121.

See NetBackup Web UI Administrator's Guide.

Addition of web service account for NetBackup installation and upgrade

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 “NetBackup master server web server user and group creation” on page 115.

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.

Caution: 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

Upgrades of UNIX clustered NetBackup 8.2 with NAT enabled

Upgrades of NetBackup 8.2 UNIX clusters with NAT enabled incorrectly identify the NAT state. As a result, NAT is disabled after the upgrade to 9.1. After you complete the NetBackup 9.1 upgrade, you must turn NAT on again. More information is included in the post-upgrade procedure.

See “Post-install procedure for upgrading to NetBackup 9.1” on page 57.

Move the NetBackup database from any `btrfs` file systems

It is not supported the installation or upgrade of the NetBackup database on a `btrfs` file system. If the NetBackup database resides on a `btrfs` file system, move the database to a supported file system (such as `ext4` or `xfs`) before you start the upgrade. The database files reside on the primary server in the directories under `/usr/openv/db`. More information about moving the database before an upgrade is available. See "Preinstall procedure for upgrading to NetBackup 9.1" on page 33.

Java GUI and JRE changes

Starting with NetBackup 8.3, the Java GUI and the JRE packages are optional for UNIX, Linux, and Windows media servers and UNIX and Linux clients.

As with previous releases, the Java GUI and JRE packages are installed automatically on all primary servers because they are required. The Java GUI and the JRE are not part of the default installation on Windows clients. Install the Java Remote Administration Console if you require this functionality on your Windows clients.

The various NetBackup upgrade methods allow the user the choice to upgrade or uninstall the Java GUI and JRE packages. More information about installing or removing the Java GUI and the JRE after upgrade is available.

See "Add or Remove Java GUI and JRE after upgrade" on page 120.

Environment variable for certificate key size

NetBackup uses security certificates to authenticate NetBackup hosts for secure communication. The security certificates conform to the X.509 Public Key Infrastructure (PKI) standard. A NetBackup primary server acts as the certificate authority (CA) and issues digital certificates to hosts. NetBackup now supports the following certificate key sizes: 2048 bits, 4096 bits, 8192 bits, and 16384 bits.

With a NetBackup 9.1 upgrade, new root CA with 2048 bit key strength is deployed. To use a certificate key size larger than 2048 bits, set the `NB_KEYSIZE` environment variable on the primary server before you start the installation.

For example:

```
NB_KEYSIZE = 4096
```

The `NB_KEYSIZE` can only have the following values: 2048, 4096, 8192, and 16384.

For more information about CA migration and certificate key sizes, see the NetBackup Security and Encryption Guide.

Table 2-2 shows the overview of the upgrade procedure.

Table 2-2 Overview of the upgrade process

Step	Details	More information
1	Review operating system requirements and confirm the computer meets all requirements.	See "Upgrade requirements for UNIX and Linux" on page 151. See "Installation and upgrade requirements for Windows and Windows clusters" on page 155. See "Requirements for Windows cluster installations and upgrades" on page 162.
2	Confirm that the web server user account and group account are created and enabled.	More information is available: See "NetBackup master server web server user and group creation" on page 115.
3	Begin the upgrade process	See "About primary server upgrades" on page 32.

Known catalog backup limitation

Veritas supports mixed versions of NetBackup in the backup environment. Limitations exist, however, when you back up the NetBackup catalog.

If the primary server performs catalog backups to a separate media server, that media server must use the same version of NetBackup as the primary server. Since the NetBackup catalog resides on the primary server, the primary server is considered to be the client for a catalog backup.

As such, the media server must have the same version of NetBackup as the primary server.

Failure to use the same version of NetBackup on the media server results in improperly protected catalog data.

More information on mixed version support is available.

See "About compatibility between NetBackup versions" on page 150.

About security certificates for NetBackup hosts

NetBackup uses security certificates for authentication of NetBackup hosts. The NetBackup security certificates conform to the X.509 Public Key Infrastructure (PKI) standard. A master server acts as the NetBackup Certificate Authority (CA) and issues NetBackup certificates to hosts.

NetBackup provides two types of NetBackup host security certificates: Host ID-based certificates and host name-based certificates. Host ID-based certificates are based

on Universally Unique Identifiers (UUID) that are assigned to each NetBackup host. The NetBackup master server assigns these identifiers to the hosts.

Any security certificates that were generated before NetBackup 8.0 are now referred to as host name-based certificates. NetBackup is in the process of replacing these older certificates with newer host ID-based certificates. The transition will be completed in future releases and the use of host name-based certificates will be eliminated. However, the transition is ongoing and the current NetBackup version continues to require the older host name-based certificates for certain operations.

More information about the post-installation process is available: https://www.veritas.com/support/en_US/article.100044300

For information on external CA support in NetBackup and external CA-signed certificates, see the NetBackup Security and Encryption Guide.

About automatic file changes from an upgrade

When you upgrade from an earlier NetBackup version, certain customizable scripts are overwritten. Before NetBackup overwrites these scripts, it saves copies of them so that any modifications are preserved.

For UNIX and Linux

Table 2-3 Protected paths and files for UNIX and Linux

Protected path or file	Action
`/usr/openv/netbackup/bin/initbpdbm` `/usr/openv/netbackup/bin/initbprd`	The current NetBackup version number is appended to the file name. Example: `initbpdbm.`*`version`*
`/usr/openv/netbackup/nblog.conf`	A suffix is added to the file during upgrade. Review the contents of the `/usr/openv/netbackup` directory after the upgrade completes for details.

`/usr/openv/msg/C`
`/usr/openv/netbackup/bin/goodies`
`/usr/openv/netbackup/bin/help`
`/usr/openv/volmgr/help`
	The entire directory is moved to the directory name plus the current version number.
	Example:
	`/usr/openv/netbackup/bin/goodies.`*`version`*

For Windows

Table 2-4 Protected paths and files for Windows

Protected path or file	Action
install_path\NetBackup\nblog.conf	The file is copied to the *install_path*\NetBackup.*release* directory. The *release* value is the current version of NetBackup. Example: *install_path*\NetBackup.*version*
install_path\NetBackup\bin\goodies\netbackup.adm *install_path*\NetBackup\bin\goodies\help_script.cmd *install_path*\NetBackup\bin\goodies\available_media.cmd *install_path*\NetBackup\bin\goodies\check_coverage.cmd *install_path*\NetBackup\bin\goodies\cleanstats.cmd *install_path*\NetBackup\bin\goodies\duplicate_images.cmd *install_path*\NetBackup\bin\goodies\verify_images.cmd *install_path*\NetBackup\bin\goodies\bpstart_notify *install_path*\NetBackup\bin\goodies\bpend_notify	The files are copied to the *install_path*\NetBackup\bin\goodies.*release* directory. The *release* value is the current version of NetBackup. Example: *install_path*\NetBackup\bin\goodies.*version*\netbackup.adm

Reduce the job database size before upgrade

The job database is now cached in memory in web services. Following an upgrade, existing VMware and Red Hat Virtualization (RHV) jobs are assigned an asset namespace to enable access control at an asset level. This process may take some time. You should reduce the size of the jobs database before upgrade to minimize the amount of processing required to perform the association and minimize the effect on web services performance. Very large job databases may see an alert regarding high heap space usage. For details on reducing the size of the job database or increasing the maximum heap size for web services, see the following article.

http://www.veritas.com/docs/100049809

Known SUSE Linux primary server upgrade issue

In some rare cases, the preinstall checker for SUSE Linux primary servers reports that the `webservice` user or `webservice` group does not exist.

Please validate that the user and group exist as expected and rerun the upgrade.

If the problem persists, set an environment variable to override the preinstall checker failure and rerun the operation.

```
NBPREINSTALL_CRITICAL_OVERRIDE=YES
```

About upgrade tools

Review this section for the upgrade details that are related to tools, including Services and Operations Readiness Tools (SORT).

About Veritas Services and Operations Readiness Tools

Veritas Services and Operations Readiness Tools (SORT) is a robust set of standalone and web-based tools that support Veritas enterprise products. For NetBackup, SORT provides the ability to collect, analyze, and report on host configurations across UNIX/Linux or Windows environments. This data is invaluable when you want to assess if your systems are ready for an initial NetBackup installation or for an upgrade.

Access SORT from the following webpage:

https://sort.veritas.com/netbackup

Once you get to the SORT page, more information is available as follows:

- **Installation and Upgrade Checklist**
  Use this tool to create a checklist to see if your system is ready for a NetBackup installation or an upgrade. This report contains all the software and the hardware compatibility information specific to the information provided. The report also includes product installation or upgrade instructions, as well as links to other references.
- **Hot fix and EEB Release Auditor**
  Use this tool to find out whether a release that you plan to install contains the hot fixes that you need.
- **Custom Reports**
  Use this tool to get recommendations for your system and Veritas enterprise products.
- **NetBackup Future Platform and Feature Plans**

Use this tool to get information about what items Veritas intends to replace with newer and improved functionality. The tool also provides insight about what items Veritas intends to discontinue without replacement. Some of these items include certain NetBackup features, functionality, 3rd-party product integration, Veritas product integration, applications, databases, and the OS platforms.

Help for the SORT tools is available. Click **Help** in the upper right corner of the SORT home page. You have the option to:

- Page through the contents of the help similar to a book
- Look for topics in the index
- Search the help with the search option

Recommended SORT procedures for upgrades

Veritas recommends current NetBackup users perform the four procedures that are listed for an initial introduction to SORT. The tool has many other features and functions, but these serve as a good introduction to SORT for users who already use NetBackup. In addition, the procedures provide a helpful base of knowledge for other SORT functionality.

Table 2-5

Procedure	Details
Create a Veritas Account on the SORT webpage	See "To create a Veritas Account on the SORT page" on page 23.
Create system-specific installation reports	See "To create a system-specific installation report for Windows" on page 24. See "To create a system-specific installation report for UNIX or Linux" on page 25.
Review the future platform and feature plans.	See "To review future platform changes and feature plans" on page 26.
Review the hot fix and emergency engineering binary release auditor information.	See "To review hot fix and emergency engineering binary information" on page 26.

To create a Veritas Account on the SORT page

1. In your web browser, navigate to:

   https://sort.veritas.com/netbackup

2. In the upper right corner, click **Login**, then click **Register now**.

3 Enter the requested login and contact information:

Email address	Enter and verify your email address
Password	Enter and verify your password
First name	Enter your first name
Last name	Enter your last name
Company name	Enter your company name
Country	Enter your country
Preferred language	Select your preferred language
CAPTCHA text	Enter the displayed CAPTCHA text. If necessary, refresh the image.

4 Click **Submit**.

5 When you receive your login information, you can log into SORT and begin uploading your customized information.

To create a system-specific installation report for Windows

1 Go to the SORT website:

https://sort.veritas.com/netbackup

2 In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.

3 Select the **Data Collectors** tab

4 Select the radio button for **Graphical user interface** and download the correct data collector for your platform.

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.

5 Launch the data collector after it finishes downloading.

6 On the **Welcome** screen, select **NetBackup** from the product family section and click **Next**.

7 On the **System Selection** screen, add all computers you want analyzed. Click **Browse** to see a list of computers you can add to the analysis. Veritas recommends starting the tool with an administrator or a root account.

8 When all systems are selected, review the **System names** section and click **Next**.

9 In the **Validation Options** screen, under **Validation options**, select the version to which you plan to upgrade.

10 Click **Next** to continue

11 The utility performs the requested checks and displays the results. You can upload the report to My SORT, print the results, or save them. Veritas recommends that you upload the results to the My SORT website for ease of centralized analysis. Click **Upload** and enter your My SORT login information to upload the data to My SORT.

12 When you are finished, click **Finish** to close the utility.

To create a system-specific installation report for UNIX or Linux

1 Go to the SORT website:

https://sort.veritas.com/netbackup

2 In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.

3 Select the **Data Collector** tab.

4 Download the appropriate data collector for your platform.

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.

5 Change to directory that contains downloaded utility.

6 Run `./sortdc`

The utility performs checks to confirm the latest version of the utility is installed. In addition, the utility checks to see it has the latest data. The utility then lists the location of the log file for this session.

7 If requested, press **Enter** to continue.

8 Select the **NetBackup Family** at the **Main Menu**.

9 Select **Installation/Upgrade report** when prompted **What task do you want to accomplish?**

You can select multiple options by separating your response with commas.

10 Specify the system or systems you want included in the report.

If you previously ran a report on the specified system, you may be prompted to run the report again. Select **Yes** to re-run the report.

The utility again lists the location of the log files for the session.

The progress of the utility is displayed to the screen.

11 Specify **NetBackup** when prompted for the product you want installation or upgrade reports.

12 Enter the number that corresponds to the version of NetBackup you want to install.

The utility again lists the location of the log files for the session.

The progress of the utility is displayed to the screen.

13 The utility prompts you to upload the report to the SORT website if you want to review the report online. The online report provides more detailed information than the text-based on-system report.

14 When your tasks are finished, you can exit the utility. You have the option to provide feedback on the tool, which Veritas uses to make improvements to the tool.

To review future platform changes and feature plans

1 In your web browser, navigate to:

https://sort.veritas.com/netbackup

2 Find and select the **NetBackup Future Platform and Feature Plans** widget.

3 Select **Display Information**.

4 Review the information provided

5 Optional - sign in to create notification - Click **Sign in and create notification**.

To review hot fix and emergency engineering binary information

1 In your web browser, navigate to:

https://sort.veritas.com/netbackup

2 Find and select the **NetBackup Hot Fix and EEB Release Auditor** widget.

3 Enter the hot fix or emergency engineering binary (EEB) information.

4 Click **Search**.

5 The new page shows a table with the following columns:

Hot fix of EEB Identifier	Shows the hot fix or EEB number that was entered on the previous screen.
Description	Displays a description of the problem that is associated with the hot fix or EEB.
Resolved in Versions	Provides the version of NetBackup where this issue is resolved.

About the NetBackup preinstall checker

The server installer for both the UNIX/Linux and the Windows platforms includes a preinstall checker. This feature helps to determine if your server is ready for a successful installation or upgrade.

The check runs automatically when you start an installation or upgrade on a master or a media server. The results of the check are shown at the following point:

- UNIX/Linux upgrade script
  After you answer the question “Is this host the master server”.
- Windows installation wizard
  On the **Ready to Install the Program** screen, where the **Installation Summary** appears.

NetBackup uses a preinstallation program that does a check at the beginning of installations or upgrades. The check looks for any known problems that you can eliminate so the operation can succeed. The checks that are performed are developed from customer input on the previous problems that were encountered during installations and upgrades. Veritas can update the checker whenever new customer feedback is received. Refreshes are not dependent on a NetBackup release. If your server can connect to telemetry.veritas.com, NetBackup automatically updates the checker with the latest version when the installation or the upgrade starts.

One of the tests that is performed is a comparison of the locally installed Emergency Engineering Binary (EEB) updates with the fixes included with the version of NetBackup being installed. If any of the preinstall tests fail, a message appears to indicate what type of action is required.

Some test failures are considered minor and let you continue with the installation or the upgrade. Critical test failures prevent the installation or the upgrade from happening. The output informs you that other action must be taken before you can proceed safely with the installation or the upgrade.

The preinstall check results are stored in the following locations:

- UNIX
  In the installation trace file in the following path:
  `/usr/openv/tmp`
- Windows
  In the following directory:
  `%ALLUSERSPROFILE%\Veritas\NetBackup\InstallSummary\`

See “About Veritas Services and Operations Readiness Tools” on page 22.

Upgrade operational notes and limitations

Review this section for the upgrade details that are related to operational notes, limitations, and requirements.

Creating the user account to support the NetBackup web server

Beginning with NetBackup 8.0, the NetBackup primary server includes a configured 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).

You can use numerous procedures to create users and groups in operating systems. Some specific approaches are shown but other methods may accomplish the same goal. The home directory path, user name, and group names are not hard-coded, and can be changed. The default local user name is **nbwebsvc**, and the default local group name is **nbwebgrp**.

Note: For UNIX and Linux platforms, the UID must be the same for each local account in a clustered environment. Be sure that the local accounts are defined consistently on all cluster nodes.

To create the user account and the user group on UNIX or Linux

1. Create the local group with the command shown:

   Command: `# groupadd group_name`

   Example: `# groupadd nbwebgrp`

2. Create the local user account with the command shown:

   Command: `# useradd -g group_name -c comment -d /usr/openv/wmc user_name`

   Example: `# useradd -g nbwebgrp -c 'NetBackup Web Services application account' -d /usr/openv/wmc nbwebsvc`

To create the user account and the user group on Windows

Note: You must use domain accounts in clustered environments on Windows.

Note: Web service user account names are limited to 20 characters.

---

1. Create the local user account with the command shown:

   Command: `C:\>net user user_name StrongPassword /add` (where *StrongPassword* is a strong password to associate with the account)

   Example: `C:\>net user nbwebsvc 1U*s7lQ# /add`

2. Create the local group with the command shown:

   Command: `C:\>net localgroup group_name /add`

   Example: `C:\>net localgroup nbwebgrp /add`

3. Make the new user a member of the new group with the command shown:

   Command: `C:\>net localgroup group_name user_name /add`

   Example: `C:\>net localgroup nbwebgrp nbwebsvc /add`

4. Grant the **Log On As a Service** right to the new user as follows:

   - Go to **Control Panel > Administrative Tools > Local Security Policy**.
   - Under **Security Settings**, click **Local Policies** and then **User Rights Assignment**.
   - Right-click on **Log on as a service** and select **Properties**.
   - Add the local user.
   - Save your changes and close the **Log on as a service** properties dialog.

Installation of the NetBackup primary server fails if any of these requirements are not met. On Windows, you are asked to provide the password for the user account as part of the installation process.

About NetBackup 9.1 support for Fibre Transport Media Server with RHEL 7.5 and later

If you plan to use Fibre Transport Media Server (FTMS) with RHEL 7.5 and later, ensure that you upgrade NetBackup to 8.1.2 or later. You can also use a new RHEL 7.5 or later release system that has NetBackup 8.1.2 or later.

Before you upgrade RHEL to 7.5 or later release, complete the following steps:

1. Disable FTMS.
2. Upgrade NetBackup to 8.1.2 or later.
3. Upgrade RHEL to 7.5 or later release and then reconfigure FTMS.

For more information about reconfiguring FTMS, see the NetBackup SAN Client and Fibre Transport Guide.

MSDP changes in NetBackup 8.1

The NetBackup 7.7.x or 8.0 to 8.1 upgrade includes a rolling Media Server Deduplication Pool (MSDP) data conversion. This conversion works in the background to convert all existing data containers to the AES encryption and the SHA-2 fingerprint algorithm. You can manage and monitor the rolling data conversion with the `crcontrol` command. More information about the use of the `crcontrol` command is available. See the rolling data conversion sections in the NetBackup Deduplication Guide. Additionally, refer to the `crcontrol` command in the NetBackup Commands Reference Guide.

The rolling conversion is performed when the system is not busy. In other words, the conversion runs when backups, restores, CRQP, CRC checks, compaction, etc. are not active. This conversion is not expected to affect normal system operations. After the rolling conversion is finished, there is no difference between the converted system and a new installation.

No explicit steps are required for conversion process during the upgrade of NetBackup. After upgrade, the rolling conversion begins to work in the background. Once the rolling conversion is started, is not possible return to the original NetBackup version. More information about the rolling conversion is available. See the rolling data conversion sections in the NetBackup Deduplication Guide.

Potential required changes for NetApp clusters

As part of the 9.1 upgrade, review the settings of any NetApp clusters. If the cluster mode is set to Node scope mode, both Veritas and NetApp recommend that you change to Vserver aware mode. If you plan to move to Vserver aware mode as part of the upgrade, create a detailed image report for each of your filers. Use the `bpimagelist` command to generate this list. Depending on the size of your environment, this activity can take some time. More information is available.

See “Additional post-upgrade steps for NetApp clusters ” on page 144.

Errors when Bare Metal Restore information is replicated using Auto Image Replication

Successful Auto Image Replication (AIR) of Bare Metal Restore (BMR) information requires two things. First, the primary server in the target domain must have BMR enabled. Second, the primary server in the target domain must be at the same or higher version of NetBackup than any clients that send BMR information. For example, if the primary server in the target domain is NetBackup 9.1 and the client in the originating domain is 7.7.3, AIR works correctly.

If the client in the originating domain is NetBackup 9.1 and the primary in the target domain is 7.7.3, the BMR information fails to replicate. All other information is successfully sent, only the BMR information is not replicated. You can restore the contents of the client, but you cannot use BMR.

More information about this topic is available.

http://www.veritas.com/docs/TECH211267

Upgrade issue with pre-8.1 clients and 8.1 or later media servers

With the NetBackup 8.1 upgrade, the fingerprinting algorithm was upgraded from MD5 to SHA2 to provide improved protection against security vulnerabilities. Veritas introduced two conversion methods to convert existing MD5 fingerprint data to SHA2: rolling conversion and inline conversion. Problems occur under the conditions shown:

- Client is pre-8.1 NetBackup.
- Client uses Client Direct, which performs deduplication at the client.
- Client is backed up by a NetBackup 8.1 or later media server.

Under these conditions, the fingerprint conversion happens inline. As a result, backup performance is negatively effected and the CPU processing load on the media server increases. The media server has to rehash the MD5 information and create a SHA2 fingerprint.

To prevent this issue:

- For pre-8.1 clients, change their backup to use media server deduplication (MSDP) with a media server that is at NetBackup 8.1 or later. This action avoids the backup performing the inline conversion.
- Do not use Client Direct on pre-8.1 clients that are backed up by 8.1 and later media servers.

Chapter 3

Master server upgrade

This chapter includes the following topics:

- About primary server upgrades
- Preinstall procedure for upgrading to NetBackup 9.1
- Performing local, remote, or clustered server upgrades on Windows systems
- Performing silent upgrades on Windows systems
- Upgrading UNIX and Linux server software to NetBackup 9.1
- Post-install procedure for upgrading to NetBackup 9.1
- About NetBackup startup and shutdown scripts
- Completing your system update after an upgrade

About primary server upgrades

Upgrade NetBackup on the primary server before you upgrade NetBackup on any other computers in your environment. Once the primary server upgrade is finished, you can upgrade media servers, and then clients. NetBackup supports a mixed version environment. More information about this topic is available.

See “About compatibility between NetBackup versions” on page 150.

Note: Remember to update OpsCenter before you update your NetBackup primary servers. You must also disable OpsCenter data collection. See the *OpsCenter Administrator's Guide* for complete information.

NetBackup includes an administration console for all the supported versions of NetBackup. More information about supported versions of NetBackup is available.

https://sort.veritas.com/eosl

Note: It is recommended that after you install or upgrade NetBackup server software, you uninstall older versions of the Remote Administration Console (Windows and Java) present on the host. If the native NetBackup Administration Console for Windows is present, it is automatically uninstalled when you install or upgrade the NetBackup server software.

See "About compatibility between NetBackup versions" on page 150.

Proceed with the upgrade.

See "Preinstall procedure for upgrading to NetBackup 9.1" on page 33.

Preinstall procedure for upgrading to NetBackup 9.1

Use the following procedure to upgrade your environment to NetBackup 9.1.

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 "About NetBackup 9.1 support for Fibre Transport Media Server with RHEL 7.5 and later" on page 29.

Note: Remember to update OpsCenter to version 9.1 before you update your NetBackup primary servers to version 9.1. You must also disable OpsCenter data collection. See the OpsCenter Administrator's Guide for complete information.

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

Be aware there is a known issue for OpsCenter upgrades on 64-bit Windows platforms. If language packs or Maintenance Packs are installed, the upgrade can fail. More information about this issue is available.

http://www.veritas.com/docs/TECH211070

You can disable the OpsCenter data collection for a specific primary server. If you disable data collection, you can upgrade your primary server before your OpsCenter server. Disabling data collection results in known issues. More information about disabling data collection and the risks is available.

See "Disabling the connection between your OpsCenter server and your NetBackup Primary Server" on page 164.

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

Preinstall steps to upgrade to NetBackup 9.1 and complete the image metadata migration

1. Perform environment checks with the SORT tool.

   See "Recommended SORT procedures for upgrades" on page 23.

2. Download the Customer Registration Key for Veritas Usage Insights. More information about Veritas Usage Insights is available.

   See "About Veritas Usage Insights" on page 12.

   During install and upgrade to NetBackup 9.1, 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 UNIX, 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/openv/db`.

To move the NetBackup database files on UNIX:

- Perform a catalog backup.
- Shut down all NetBackup daemons:
  `/usr/openv/netbackup/bin/bp.kill_all`
- Start the SQL Anywhere daemon:
  `/usr/openv/netbackup/bin/nbdbms_start_stop start`
- Move the existing data, index, and transaction log files:
  `/usr/openv/db/bin/nbdb_move -data` *`data_directory`* `-index` *`index_directory`* `-tlog` *`log_directory`*
  If you use mirrored transaction log, use the command shown:
  `/usr/openv/db/bin/nbdb_move -data` *`data_directory`* `-index` *`index_directory`* `-tlog` *`log_directory`* `-mlog` *`log_mirror_directory`*
- Start all NetBackup daemons:
  `/usr/openv/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 "Windows compiler and security requirements for NetBackup 9.1 and later installation and upgrade" on page 10.

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 OpsCenter data collection for this primary server.
- 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 "Reduce the job database size before upgrade" on page 21.

- 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:

    ```
    hagrp -freeze NetBackup_service_group -persistent
    ```

  Refer to the *Veritas 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 "NetBackup master server web server user and group creation" on page 115.

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 "Persistent Java Virtual Machine options" on page 141.

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/openv/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, based on your platform. More information is available about this topic.

- See "Performing local, remote, or clustered server upgrades on Windows systems" on page 37.
- See "Performing silent upgrades on Windows systems" on page 49.
- See "Upgrading UNIX and Linux server software to NetBackup 9.1" on page 52.

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

Use the following procedure to upgrade to NetBackup 9.1 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 9.1 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 9.1 to its original state on the local host.
   - Select **Remove** to remove NetBackup 9.1 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.

- 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.

10 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 "About Veritas Usage Insights" on page 12.

During install and upgrade to NetBackup 9.1, 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.

---

11 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 acccounts 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 "Installation and upgrade requirements for Windows and Windows clusters" on page 155.

12 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.
  - **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**.

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**.

13 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.
OpsCenter Server Name (Optional)	OpsCenter is a web-based administration and management tool for NetBackup. If you have an OpsCenter server or plan to install one, enter the server name or the IP address for that server here. For a clustered server, do not use the virtual name. Instead, use the actual host name of the cluster node.

Click **Next**.

14 (**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.

15 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:

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**.

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**.

16 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**.

17 (**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

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

If the ECA heath 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.

19 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.

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

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

Add Licenses

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.

22 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.

23 The binaries are successfully installed. Proceed to the post-installation procedure.

More information is available.

See "Post-install procedure for upgrading to NetBackup 9.1" on page 57.

Performing silent upgrades on Windows systems

A silent upgrade avoids the need for interactive input in the same manner as performing a remote upgrade. Silent NetBackup installations are not supported if you want to run the NetBackup services as a specific user rather than the local system.

To perform a silent upgrade, you must first modify the appropriate NetBackup script. After script modification, you can run the script to initiate the silent upgrade.

The script shuts down all NetBackup services so that the upgrade can be initiated. If the script detects that other system processes still maintain a handle on any NetBackup files, the upgrade fails. To identify which NetBackup processes are still running, check the `NetBackup Install` log file at the following location:

`%ALLUSERSPROFILE%\Veritas\NetBackup\InstallLogs`

After you have manually stopped each of the identified processes, you can run the upgrade script again.

Note: For Windows 2012/2012 R2/2016 Server Core systems, you can only upgrade NetBackup with this procedure.

To upgrade NetBackup server software silently

1. Log on as administrator to the system where you want to upgrade NetBackup.
2. Navigate to the location where the ESD images (downloaded files) reside.
3. Open Windows Explorer and copy the contents of the `X64` directory to a temporary directory on your hard drive. Choose the directory that is associated with the platform type that you want to install.
4. Since the source files are read-only, you must change the permissions for the copied files to allow the installation or the update.
5. In the temporary directory where the copied files reside, select the appropriate script to modify:
   - To upgrade a primary server, edit `silentprimary.cmd`
   - To upgrade a media server, edit `silentmedia.cmd`
   - To upgrade a NetBackup Remote Administration Console, edit `silentadmin.cmd`
6. Edit the following lines as needed for your installation:
   - `SET ADDITIONALSERVERS=media1,media2,media3`

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

If no other servers are to communicate with this host, remove this line from the script.

- `SET ABORT_REBOOT_INSTALL=0`

  This line lets you determine how you want the upgrade to continue if a restart is required. Select from the following settings:

0 (default)	By default, a silent upgrade does not abort if it is determined that a restart is required. If you leave this setting at 0, select one of the following tasks: ■ After the upgrade is complete, check the installation log to see if a restart is required. If the string **in use** appears anywhere in the log, you must restart the system manually. ■ Force an automatic restart after the upgrade is complete. To force an automatic restart, before you run the script, remove the following option from the silent installation command script (`silent*.cmd`): `REBOOT="ReallySuppress"` **Warning:** A forced restart occurs with no warning to the user. It does not cancel the upgrade or roll back the system to its original state.
1	Select this setting to abort the upgrade if it is determined that a restart is required. If a restart is needed, this setting cancels the upgrade and the system is rolled back to its original state.

- `SET USAGE_INSIGHTS_FILE_PATH=`*`path`*

  For primary servers only, you must specify the path to the Veritas Usage Insights customer registration key. More information is available. See “About Veritas Usage Insights” on page 12.

- `SET ALLOW_PRE_90_UPGRADE=`*`value`*

  This field is for primary servers only. This value determines if the upgrade from releases earlier than NetBackup 9.0 can proceed. Specify `1` to allow the upgrade to continue. The upgrade includes the infinite expiration conversion process. If you specify `0`, then you cannot upgrade the primary server.

NetBackup 9.0 and later versions support the expiration dates 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 article that is shown for more information:
https://www.veritas.com/content/support/en_US/article.100048600

- `SET ECA_CERT_STORE=`*`cert_store_string`*
  This field is for media servers only. Use this field to specify the external certificate location in a Windows certificate store. This field is specified in the form *`store_name\issuer_DN\subject`*. This field is required to use an external certificate from the Windows certificate store.
- `SET ECA_CERT_PATH=`*`path`*
  This field is for media servers only. Use this field to specify the path and the file name of the external certificate file. This field is required to set up an external certificate from a file.
- `SET ECA_TRUST_STORE_PATH=`*`path`*
  This field is for media servers only. Use this field to specify the path and the file name of the file representing the trust store location. This field is required to set up an external certificate from a file.
- `SET ECA_PRIVATE_KEY_PATH=`*`path`*
  Use this field to specify the path and the file name of the file representing the private key. This field is required to set up an external certificate from a file.
- `SET ECA_CRL_CHECK_LEVEL=`*`value`*
  This field is for media servers only. Use this field to specify the CRL mode. This field is required. Supported values are:
  - `USE_CDP`: Use the CRL defined in the certificate.
  - `USE_PATH`: Use the CRL at the path that is specified in `ECA_CRL_PATH`.
  - `DISABLED`: Do not use a CRL.
- `SET ECA_CRL_PATH=`*`path`*
  This field is for media servers only. Use this field to specify the path and the file name of the CRL associated with the external CA certificate. This field is required only when `ECA_CRL_CHECK_LEVEL` is set to `USE_PATH`. If not applicable, leave this field empty.
- `SET ECA_KEY_PASSPHRASEFILE=`*`path`*

This field is for media servers only. Use this field to specify the path and the file name of the file that contains the passphrase to access the keystore. This field is optional and applies only when setting up an external certificate from a file.

- `SET INCLUDE_JAVA_GUI_AND_JRE=value`
  Installation of the NetBackup Java GUI and JRE packages is optional for NetBackup Windows media server installation. This option specifies if the Java GUI and the JRE packages should be installed, upgraded, or removed. Supported values for this option are:
  - INCLUDE: Include the Java GUI and JRE when installing or upgrading NetBackup.
  - EXCLUDE: Exclude the Java GUI and JRE when installing or upgrading NetBackup. Any preexisting NetBackup Java GUI and JRE packages are removed.
  - MATCH: Match the existing configuration on the host. Hosts that already have the Java GUI and JRE components are updated with the latest versions. The components are excluded for all other hosts.

7 Save the script and run it.

8 Examine the installation log at the following location:

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

This log includes information about the optional installation of the Java GUI and the JRE.

Search the installation log for the following error indications:

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

9 The binaries are successfully installed. Proceed to the post-installation procedure. More information is available.

See "Post-install procedure for upgrading to NetBackup 9.1" on page 57.

Upgrading UNIX and Linux server software to NetBackup 9.1

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 UNIX and Linux server software to 9.1

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. For Solaris systems, all of the NetBackup scripts that you may have modified are removed when you run the upgrade script.

   For non-Solaris systems, 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 “About automatic file changes from an upgrade” on page 20.

   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

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/openv` 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.

More information is available.

See "Post-install procedure for upgrading to NetBackup 9.1" on page 57.

Post-install procedure for upgrading to NetBackup 9.1

Post-installation steps to upgrade to NetBackup 9.1 describes the post-installation steps to upgrade NetBackup and complete the image metadata migration.

Post-installation steps to upgrade to NetBackup 9.1

1. Check for an available NetBackup 9.1 maintenance release. Maintenance releases include very important fixes that are released after NetBackup 9.1. Veritas encourages you to install the latest available maintenance release during upgrade activities.

   To access the latest NetBackup 9.1 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.
     UNIX/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/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/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 "About the NetBackup web user interface" on page 121.

   See NetBackup Web UI 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. If you have a clustered primary server, generate a certificate on the inactive nodes for secure communications. More information is available.

   See "Generate a certificate on the inactive nodes of a clustered master server" on page 117.

6. (Conditional) This step applies only to cluster installations. If this computer is not a clustered primary server upgrade, proceed to the next step.

   Update the other nodes in the cluster. You can update the other primary servers nodes in the cluster to NetBackup 9.1 by following standard cluster upgrade process. For complete details, see the *Veritas 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

   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 9.1, 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 "About security certificates for NetBackup hosts" on page 19.

More information about this topic is available.

See "Upgrading NetBackup media servers to NetBackup 9.1" on page 66.

9 Reactivate the following in the order as shown:

- All disk staging storage units.
- All NetBackup policies.
- All storage lifecycle policies (SLPs).
- OpsCenter data collection for this primary server.

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

See "Post upgrade procedures for Amazon cloud storage servers" on page 165.

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

See "Additional post-upgrade steps for NetApp clusters " on page 144.

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 "Upgrading NetBackup media servers to NetBackup 9.1" on page 66.

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 UNIX 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 "Completing your system update after an upgrade" on page 63.

About NetBackup startup and shutdown scripts

When you install NetBackup, the installation script also performs configuration of startup and shutdown scripts. Startup scripts allow the NetBackup daemons to start automatically when the system boots. Shutdown scripts automatically terminate the startup scripts at system shutdown.

The installation process copies the NetBackup startup and shutdown scripts to the appropriate operating system location.

For non-cluster upgrades, any existing NetBackup related startup and shutdown scripts are saved, and the newly released versions of those scripts are installed.

Table 3-1 lists the links for the startup and the shutdown scripts for the various platforms that are installed during NetBackup installation.

Table 3-1 NetBackup startup and shutdown script links by platform

Platform	Links

AIX	`/etc/rc.netbackup.aix`
	■ The NetBackup installation script edited the `/etc/inittab` file and added the following entry to ensure that the script is called during a level-two boot:
	`netbackup:2:wait:/etc/rc.netbackup.aix`
	■ To shut down, add the following line to the `/etc/rc.shutdown` file:
	`/etc/rc.netbackup.aix stop`

HP-UX	`/sbin/rc1.d/K001netbackup ->/sbin/init.d/netbackup` `/sbin/rc2.d/S777netbackup ->/sbin/init.d/netbackup`

Linux Debian	`/etc/rc0.d/K01netbackup ->/etc/init.d/netbackup`
	`/etc/rc1.d/K01netbackup ->/etc/init.d/netbackup`
	`/etc/rc2.d/S95netbackup ->/etc/init.d/netbackup`

Table 3-1 NetBackup startup and shutdown script links by platform *(continued)*

Platform	Links
Linux Red Hat	/etc/rc.d/rc0.d/K01netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc1.d/K01netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc2.d/S77netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc3.d/S77netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc5.d/S77netbackup ->/etc/rc.d/init.d/netbackup /etc/rc.d/rc6.d/K01netbackup ->/etc/rc.d/init.d/netbackup
Linux SUSE	/etc/init.d/rc0.d/K01netbackup ->/etc/init.d/netbackup /etc/init.d/rc2.d/S77netbackup ->/etc/init.d/netbackup /etc/init.d/rc3.d/S77netbackup ->/etc/init.d/netbackup /etc/init.d/rc5.d/S77netbackup ->/etc/init.d/netbackup /etc/init.d/rc6.d/K01netbackup ->/etc/init.d/netbackup
Solaris	/etc/rc0.d/K01netbackup ->/etc/init.d/netbackup /etc/rc1.d/K01netbackup ->/etc/init.d/netbackup /etc/rc2.d/S77netbackup ->/etc/init.d/netbackup

Completing your system update after an upgrade

After you have upgraded servers and clients, you may need to perform additional tasks to complete the update of your NetBackup environment.

Perform any of the following that apply to your NetBackup environment:

Primary server privileges	If you upgraded a primary server that allowed nonroot users to administer NetBackup, you must reconfigure the permissions and the group. The default permissions and group on the newly installed files allow only a root user to perform NetBackup administration.
Update the trust relationship between remote primary servers for targeted auto image replication (AIR)	After you upgrade both your source and your target primary server from 8.0 or earlier to 8.1 or later, you must update the trust relationship. Upgrading from NetBackup 8.1 to a later version does not require you to reestablish the trust relationship. Run the command that is shown on both the source and the target primary servers to reestablish the trust relationship: `nbseccmd -setuptrustedprimary -update` More information is available. See the NetBackup Commands Reference Guide.
Add-on products	Upgrade any add-on products (such as NetBackup language packages) on all upgraded clients. All add-on products should be at the same version as the NetBackup client.
NetBackup scripts	If you made changes to NetBackup scripts before the upgrade, apply those changes to the new, upgraded versions of the scripts.
External certificate authority	Configure your external certificate authority. If you opted to skip the security configuration or if your environment uses ECA, you may need to configure an ECA. More information about configuring ECAs is available: 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.

Update storage servers	NetBackup does not update objects such as storage servers and disk pools every time the storage changes. Storage changes can result from NetBackup MSDP changes and 3rd party OST vendor software upgrades. Additionally, changes to the storage-defined replication topologies that SLP replication uses as well as import operations require an update. The user must proactively confirm these changes through the use of the `updatests` and `updatedp` commands. A NetBackup upgrade may introduce new functionality you want to use in your environment. Veritas recommends that you run the `updatests` and `updatedp` commands on the storage servers and disk pools where you want to use this new functionality. For more information about the `updatests` and `updatedp` commands, see the NetBackup Commands Reference Guide
NetBackup Access Control or Enhanced Auditing	If NetBackup Access Control or Enhanced Auditing is enabled in your environment, you must run the `bpnbat -login` command after the primary server upgrade.

Chapter 4

Media server upgrade

This chapter includes the following topics:

- Upgrading NetBackup media servers to NetBackup 9.1
- Silently upgrading NetBackup media server software on UNIX and Linux

Upgrading NetBackup media servers to NetBackup 9.1

There are three media server upgrade methods available for customers: the NetBackup upgrade script, the native UNIX and Linux installers, and VxUpdate. The NetBackup upgrade script is the standard upgrade method and is recommended for new users. The native UNIX and Linux installers are potentially more difficult and require additional steps. VxUpdate provides remote installation capabilities as well as the ability to upgrade on a user-defined schedule.

Upgrades of media servers with MSDP include a rolling data conversion. The rolling conversion is performed when the system is not busy. In other words, the conversion runs when backups, restores, CRQP, CRC checks, compaction, etc. are not active. This conversion is not expected to affect normal system operations. After the rolling conversion is finished, there is no difference between the converted system and a new installation.

NetBackup also requires that media servers have a security certificate so that they function correctly. More information about this topic is available.

See “About security certificates for NetBackup hosts” on page 19.

NetBackup includes an administration console for all the supported versions of NetBackup. More information about supported versions of NetBackup is available.

https://sort.veritas.com/eosl

Additional steps are required if the NetBackup 8.1.2 upgrade includes an upgrade to RHEL 7.5 and you use Fibre Transport Media Server (FTMS). More information is available.

See "About NetBackup 9.1 support for Fibre Transport Media Server with RHEL 7.5 and later" on page 29.

Table 4-1 Media server migration procedure

Step	Task	Completed
1	If your media server upgrade is part of the primary server upgrade, you can proceed to the next step. If not, deactivate the media server.	
2	Stop all NetBackup services. ■ On UNIX systems: `/usr/openv/netbackup/bin/bp.kill_all` ■ On Windows systems: *`install_path`*`\NetBackup\bin\bpdown -f`	
3	Upgrade the NetBackup binaries. More information is available about this topic. ■ See "Performing local, remote, or clustered server upgrades on Windows systems" on page 37. ■ See "Performing silent upgrades on Windows systems" on page 49. ■ See "Upgrading UNIX and Linux server software to NetBackup 9.1" on page 52. ■ See "Silently upgrading NetBackup media server software on UNIX and Linux" on page 69. ■ See "About VxUpdate" on page 96.	
4	If you did not get a security certificate, generate the certificate. More information about this topic is available. See "About security certificates for NetBackup hosts" on page 19.	

Table 4-1 Media server migration procedure *(continued)*

Step	Task	Completed
5	Check for an available NetBackup 9.1 maintenance release. Maintenance releases include very important fixes that are released after NetBackup 9.1. It is recommended that you install the latest available maintenance release during upgrade activities. To access the latest NetBackup 9.1 maintenance release: **1** Go to the Veritas SORT website. https://sort.veritas.com/netbackup **2** 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**. **3** Under **Upgrade Information**, there is a ***version_number* Download Links** hyperlink. Click that hyperlink for the latest maintenance release. **4** If no maintenance release is available, proceed to step 6. **5** If you find a maintenance release is available, download it now. **6** Prepare for the install by stopping all NetBackup processes and services. Use the command shown: UNIX/Linux: `/usr/openv/netbackup/bin/bp.kill_all` Windows: *`install_path`*`\NetBackup\bin\bpdown -f` **7** Install the maintenance release. **8** Restart NetBackup with the commands shown: UNIX/Linux systems: `/usr/openv/netbackup/bin/bp.start_all` Windows systems: *`install_path`*`\NetBackup\bin\bpup -f`	
6	(Conditional) If the media server upgrade is part of a primary server upgrade, skip this step. Reactivate the media server.	
7	(Conditional) If the media server upgrade is part of a primary server upgrade, resume the primary server upgrade procedure.	

Silently upgrading NetBackup media server software on UNIX and Linux

You can upgrade NetBackup UNIX and Linux media servers with native installers. You can use either the NetBackup install script or your preferred installer method.

- For Linux: `rpm`, `yum`, etc.
- For Solaris: `pkginfo`, `pkgadd`

A successful installation or upgrade is recorded in the `/usr/openv/pack/install.history` file.

Caution: You must remove the NetBackup Nutanix plug-in package before you upgrade NetBackup Red Hat and SUSE Linux with the native installers. Both the Nutanix plug-in and NetBackup install the same libraries to the same location, which results in a failure to upgrade. The upgrade fails with an `install of` *`package_name`* `conflicts with file from package` *`package_name`* error message.

Use the command that is shown to uninstall the plug-in before attempting the NetBackup upgrade.

```
rpm -e VRTSnbntnxahv*
```

To upgrade the UNIX or Linux media server binaries using native installers:

1. Please create the NetBackup installation answer file (`NBInstallAnswer.conf`) in the media server `/tmp` directory. More information about the answer file and its contents is available.

   See "About the NetBackup answer file" on page 122.

2. (Conditional) If your environment uses a NetBackup Certificate Authority, and the media server is already configured for NetBackup Certificate Authority, proceed to 4. Otherwise, populate `NBInstallAnswer.conf` with the following required information:

   `CA_CERTIFICATE_FINGERPRINT=`*`fingerprint`*

   Example (the fingerprint value is wrapped for readability):

   ```
   CA_CERTIFICATE_FINGERPRINT=01:23:45:67:89:AB:CD:EF:01:23:45:67:
   89:AB:CD:EF:01:23:45:67
   ```

   Depending on the security configuration in your NetBackup environment, you may need to add the `AUTHORIZATION_TOKEN` option to the answer file. Additional information about the `AUTHORIZATION_TOKEN` option is available.

   See "About the NetBackup answer file" on page 122.

3. (Conditional) If your environment uses an external certificate authority, and the media server is already configured for external certificate authority, proceed to 4. Otherwise, populate `NBInstallAnswer.conf` with the following required information:

   - `ECA_CERT_PATH`

     Use this field to specify the path and the file name of the external certificate file. This field is required to set up an external certificate from a file.

   - `ECA_TRUST_STORE_PATH`

     Use this field to specify the path and the file name of the file representing the trust store location. This field is required to set up an external certificate from a file.

   - `ECA_PRIVATE_KEY_PATH`

     Use this field to specify the path and the file name of the file representing the private key. This field is required to set up an external certificate from a file.

   - `ECA_KEY_PASSPHRASEFILE`

     Use this field to specify the path and the file name of the file that contains the passphrase to access the keystore. This field is optional and applies only when setting up an external certificate from a file.

- ECA_CRL_CHECK_LEVEL

  Use this field to specify the CRL mode. This field is required. Supported values are:

  - USE_CDP: Use the CRL defined in the certificate.
  - USE_PATH: Use the CRL at the path that is specified in ECA_CRL_PATH.
  - DISABLED: Do not use a CRL.
  - SKIP: Used to skip setting up the certificate authority. To skip the ECA configuration, you must set all required ECA_ values to SKIP. Be aware that if you continue with the installation without a certificate authority, the backups and restores fail.

- ECA_CRL_PATH

  Use this field to specify the path to the CRL associated with the external CA certificate. This field is required only when ECA_CRL_CHECK_LEVEL is set to USE_PATH. If not applicable, leave this field empty.

4 Additionally, you can add the optional parameters shown to the NBInstallAnswer.conf file.

- Additional LICENSE entries
- Additional SERVER entries

More information about each option is available.

See "About the NetBackup answer file" on page 122.

5 Download the server package that matches your server platform to a system with sufficient space. Then extract the required server package.

Extract the contents of the server package file. Example:

- For Linux Red Hat:

  ```
  tar -xzvf NetBackup_9.1_LinuxR_x86_64.tar.gz
  ```

- For Linux SuSE:

  ```
  tar -xzvf NetBackup_9.1_LinuxS_x86_64.tar.gz
  ```

- For Solaris SPARC:

  ```
  tar -xzvf NetBackup_9.1_Solaris_Sparc64.tar.gz
  ```

- For Solaris x86:

  ```
  tar -xzvf NetBackup_9.1_Solaris_x86.tar.gz
  ```

6 Change to the directory for your desired operating system and copy server files to the media server.

Operating system directory:

- For Linux Red Hat:

  `NetBackup_9.1_LinuxR_x86_64/linuxR_x86/anb`

- For Linux SuSE:

  `NetBackup_9.1_LinuxS_x86_64/linuxS_x86/anb`

- For Solaris SPARC:

  `NetBackup_9.1_Solaris_Sparc64/solaris/anb`

- For Solaris x86

  `NetBackup_9.1_Solaris_x86/solaris_x86/anb`

Copy server files to the computer to be installed

- Linux: `VRTSnetbp.rpm` and `VRTSpddes.rpm`
- Linux Red Hat: `VRTSpddei.rpm`
- Solaris: `VRTSnetbp.pkg` and `VRTSpddes.pkg`

7 Extract the client binaries and copy them to the media server:

Extract the client binaries:

```
tar -xzvf client_dist.tar.gz
```

Change directory to your desired operating system:

- Red Hat: `openv/netbackup/client/Linux/RedHat2.6.32`
- SuSE: `openv/netbackup/client/Linux/SuSE3.0.76`
- SPARC: `openv/netbackup/client/Solaris/Solaris10`
- Solaris_x86: `openv/netbackup/client/Solaris/Solaris_x86`

Copy the files that are shown to the media server.

Note: The upgrade of the Java GUI and the JRE is optional. If you do not want them upgraded, omit the copy and the install of the `VRTSnbjava` and `VRTSnbjre` packages.

Veritas recommends the removal of the old Java GUI and JRE packages if you decide not to upgrade them.

See "Add or Remove Java GUI and JRE after upgrade" on page 120.

Linux
```
VRTSnbpck.rpm
VRTSpbx.rpm
VRTSnbclt.rpm
VRTSnbjre.rpm
VRTSnbjava.rpm
VRTSpddea.rpm
VRTSnbcfg.rpm
```

Solaris
```
.pkg_defaults
VRTSnbpck.pkg.gz
VRTSpbx.pkg.gz
VRTSnbclt.pkg.gz
VRTSnbjre.pkg.gz
VRTSnbjava.pkg.gz
VRTSpddea.pkg.gz
VRTSnbcfg.pkg.gz
```

Note: The Solaris client binaries include a hidden administration file called `.pkg_defaults`. This administration file contains default installation actions.

8 (Conditional) For Solaris, extract the compressed package files with the command shown:

```
gunzip VRTS*.*
```

This action extracts all the package files as shown:

```
VRTSnbpck.pkg
VRTSpbx.pkg
VRTSnbclt.pkg
VRTSnbjre.pkg
VRTSnbjava.pkg
VRTSpddea.pkg
VRTSnbcfg.pkg
```

9 Install the Veritas precheck package.

- Linux: `rpm –U VRTSnbpck.rpm`
- Solaris: `pkgadd -a .pkg_defaults -d VRTSnbpck.pkg VRTSnbpck`

10 (Conditional) If you are upgrading from pre-NetBackup 8.0, remove the old `SYMC*` packages. The example shown indicates the commands used to remove the `SYMC` RPM packages. This process preserves your NetBackup configuration.

```
rpm -e SYMCnbjava
rpm -e SYMCpddea
rpm -e SYMCnbclt
rpm -e SYMCnbjre
rpm -e SYMCpddes
rpm -e SYMCnetbp
```

11 Install the files in the order that is shown with the commands shown:

Note: The upgrade of the Java GUI and the JRE is optional. If you do not want them upgraded, omit the copy and the install of the `VRTSnbjava` and `VRTSnbjre` packages.

Veritas recommends the removal of the old Java GUI and JRE packages if you decide not to upgrade them.

See "Add or Remove Java GUI and JRE after upgrade" on page 120.

Linux

```
rpm –U VRTSpbx.rpm
rpm –U VRTSnbclt.rpm
rpm –U VRTSnbjre.rpm
rpm –U VRTSnbjava.rpm
rpm –U VRTSpddea.rpm
rpm –U VRTSpddes.rpm
rpm –U VRTSpddei.rpm
rpm –U VRTSnbcfg.rpm
rpm –U VRTSnetbp.rpm
```

Note that `VRTSpddei.rpm` is for Linux Red Hat only.

Solaris

Use the `pkgadd -a admin -d device [pkgid]` command as shown to install the files:

```
pkgadd -a .pkg_defaults -d VRTSpbx.pkg VRTSpbx
pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt
pkgadd -a .pkg_defaults -d VRTSnbjre.pkg VRTSnbjre
pkgadd -a .pkg_defaults -d VRTSnbjava.pkg VRTSnbjava
pkgadd -a .pkg_defaults -d VRTSpddea.pkg VRTSpddea
pkgadd -a .pkg_defaults -d VRTSpddes.pkg VRTSpddes
pkgadd -a .pkg_defaults -d VRTSnbcfg.pkg VRTSnbcfg
pkgadd -a .pkg_defaults -d VVRTSnetbp.pkg VRTSnetbp
```

- The `-a` option defines a specific admin (`.pkg_defaults`) to use in place of the default administration file. The admin file contains default installation actions.
- The `-d` device option specifies the source of the software packages. A device can be the path to a device, a directory, or a spool directory.
- Use the `pkgid` parameter to specify a name for the package being installed. This parameter is optional.

12 You can remove the old versions of the Java GUI and the JRE if you no longer plan to use them.

- Linux:

  ```
  rpm -e VRTSnbjava.rpm
  rpm -e VRTSnbjre.rpm
  ```

- Solaris:

  ```
  pkgrm VRTSnbjava
  pkgrm VRTSnbjre
  ```

Chapter 5

MSDP upgrade for NetBackup

This chapter includes the following topics:

- MSDP upgrade considerations for NetBackup 8.1
- About MSDP rolling data conversion
- About MSDP fingerprinting algorithm changes

MSDP upgrade considerations for NetBackup 8.1

Because of the changes in the fingerprint algorithm for MSDP in NetBackup 8.1, consider your MSDP environment as you plan your upgrade path. Any NetBackup 8.0 and older host cannot access the NetBackup 8.1 MSDP because of the new fingerprint algorithm. Failed NetBackup jobs can result from a failure to plan for this condition.

If the media servers list for an 8.1 MSDP storage server contains 8.0 or older servers, you can experience failures because of the new algorithm. If the common media server between an 8.1 server and an 8.0 server is the 8.0 server, jobs can fail. If you use client direct, the client must be upgraded to 8.1 or you can experience client direct restore errors. These failures are because the 8.0 and older hosts cannot access the 8.1 server.

As you plan your upgrade, if you have multiple media servers as part of an MSDP environment, consider the options shown:

- Upgrade all MSDP media servers that share access rights to each other together. Upgrade all clients that use client direct to these MSDP disk pools.
  This option insures there are no interruptions in your environment.

- Upgrade MSDP media servers and clients using client direct as your environment allows and make no configuration changes.

  If the selected common media server is not a NetBackup 8.1 server, the risk is restores, verifies, imports, and optimized duplication may fail. If client direct is used on older clients, you can experience client direct restore errors. This failure is because of the algorithm change.

- Upgrade MSDP media servers and clients using client direct as your environment allows. Modify your list of credentialed media servers for the upgraded storage servers to only include NetBackup 8.1 servers.

  This action effectively revokes access rights for the non-upgraded servers to the upgraded servers. The risk is previously configured operations may stop working because of the access change. If you choose this option, you should make detailed notes about the configuration changes so you can revert those changes once all media servers are upgraded.

  If duplication jobs copy from an 8.1 MSDP to an 8.0 or older MSDP, then create a storage unit for the older MSDP. Restrict the **Media Servers** list on that new storage unit to the 8.1 host. You must change any storage lifecycle policy (SLP) controlled duplication jobs if they copy from an 8.0 or older MSDP host to an 8.1 MSDP host. Set the **Alternate Read Server** on the duplication stage to the 8.1 media server.

About MSDP rolling data conversion

NetBackup 8.0 introduced the AES encryption algorithm to replace the existing Blowfish algorithm. NetBackup 8.1 introduces the SHA-2 fingerprint algorithm to replace the existing MD5-like algorithm. The upgrades to both the encryption and the fingerprint algorithms are designed to enhance data security.

The environments that are upgraded to NetBackup 8.1 may include Blowfish encrypted data and the MD5-like fingerprints that need to be converted to the new format. To handle the conversion and secure the data, a new internal task converts the current data container to the AES encryption and the SHA-2 fingerprint algorithm. This new task is referred to as the rolling data conversion.

Rolling data conversion traverses all existing data containers. If the data is encrypted with the Blowfish algorithm, the data is re-encrypted with the AES algorithm. Then a new SHA-2 fingerprint is generated. After the conversion, the data container has a new file with a `.map` extension, in addition to the `.bhd` and `.bin` files. The `.map` file contains the mapping between the SHA-2 and the MD5-like fingerprints. The `.bhd` file includes the SHA-2 fingerprints.

In a new installation of NetBackup 8.1, the rolling data conversion is marked as **Finished** and doesn't start in the future. For an upgrade to NetBackup 8.1, the

rolling data conversion is enabled by default and works in the background after the MSDP conversion completes. Only the data that existed before upgrade is converted. All new data uses the new SHA-2 fingerprint and does not need conversion.

You can manage and monitor the rolling data conversion using the `crcontrol` command. More information about its use is available.

See the NetBackup Deduplication Guide and the NetBackup Commands Reference Guide.

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

About MSDP fingerprinting algorithm changes

With NetBackup 8.1, Media Server Deduplication Pool (MSDP) introduces a more secure fingerprint algorithm. The SHA-2 algorithm replaces the existing MD5-like algorithm. NetBackup 8 .1 can handle both fingerprint types, and the new server is compatible with old clients and old servers. Conversion happens during the interaction between old clients and old servers and the new server. The fingerprint conversion requires additional computation time. The interaction between old clients and old servers and new server is slower than if both the client and the server are new.

If you have a mixed media server environment that uses both the MD5-like algorithm and the SHA-2 algorithm, the initial backup may lose deduplication ratio. It is recommended that you split the media servers by algorithm and create different storage units for each of them.

More information is available.

NetBackup Deduplication Guide

Chapter 6

Client upgrade

This chapter includes the following topics:

- About client upgrades
- Upgrading UNIX and Linux clients with the NetBackup upgrade script
- Upgrade of the UNIX and Linux client binaries with native installers

About client upgrades

Once the primary and the media servers for a client computer are upgraded, you can upgrade the client computer. Do not upgrade a client computer before the associated primary and media server are upgraded.

From a Veritas perspective, client computer upgrades present minimal concerns. The client computers have minimal NetBackup binaries and no NetBackup databases. From the customer perspective, however, the client computers may host mission critical databases or unique business-specific applications. As such, review your client computers and determine where you need to engage additional resources to ensure uninterrupted access to important databases and applications.

Veritas supports three client upgrade methods:

- NetBackup upgrade script. The NetBackup upgrade script is the standard upgrade method and is recommended for new users. More information is available.
  See “Performing local, remote, or clustered server upgrades on Windows systems” on page 37.
  See “Upgrading UNIX and Linux clients with the NetBackup upgrade script” on page 80.
- Native UNIX and Linux installers. The native UNIX and Linux installers are potentially more difficult and require additional steps. More information is available.

See "Upgrade of the UNIX and Linux client binaries with native installers" on page 82.

- VxUpdate. VxUpdate is the replacement for LiveUpdate and allows you to schedule the client upgrade for your client computers. More information is available.
See "About VxUpdate" on page 96.

Upgrading UNIX and Linux clients with the NetBackup upgrade script

Use the following procedure to upgrade to NetBackup 9.1 on UNIX and Linux clients:

To upgrade UNIX and Linux clients with the NetBackup upgrade script:

1. Log in to the client as root.
2. Navigate to where the ESD images (downloaded files) reside and enter the command shown:

```
./install
```

3. When the following message appears press `Enter` to continue:

```
Veritas Installation Script
Copyright (c) 2019 Veritas Technologies LLC. All rights reserved.


                Installing NetBackup Client Software


Please review the VERITAS SOFTWARE LICENSE AGREEMENT located on
the installation media before proceeding. The agreement includes
details on the NetBackup Product Improvement Program.

For NetBackup installation and upgrade information specific to your
platform and to find out if your installed EEBs or hot fixes are
contained in this release, check the Installation and Upgrade checklists
and the Hot Fix and EEB Release Auditor, both available on the Veritas
Services and Operations Readiness Tools (SORT) page:
https://sort.veritas.com/netbackup.

Do you wish to continue? [y,n] (y)
```

4 After NetBackup checks for required system conditions, press `Enter` to continue.

```
Do you want to install the NetBackup client software for this
client? [y,n] (y)
```

5 (Conditional) If your environment uses NetBackup Certificate Authority, the installer retrieves certificate details and prompts you to confirm the information. After you confirm the certificate authority information, you are prompted for authorization token information.

6 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.

7 When prompted, indicate how the upgrade should handle the Java GUI and the 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 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.

8 If there are no problems, the installer exits without error.

Upgrade of the UNIX and Linux client binaries with native installers

You can upgrade NetBackup UNIX and Linux clients with native installers. You can use either the NetBackup install script or your preferred installer method. This change does not include those clients that use the Debian package. Those clients must be upgraded with the NetBackup install script.

- For AIX: `lslpp`, `installp`
- For HP-UX: `swlist`, `swinstall`
- For Linux: `rpm`, `yum`, etc.
- For Solaris: `pkginfo`, `pkgadd`

A successful installation or upgrade is recorded in the `/usr/openv/pack/install.history` file.

Caution: You must remove the NetBackup Nutanix plug-in package before you upgrade NetBackup Red Hat and SUSE Linux with the native installers. Both the Nutanix plug-in and NetBackup install the same libraries to the same location, which results in a failure to upgrade. The upgrade fails with an `install of` *`package_name`* `conflicts with file from package` *`package_name`* error message.

Use the command that is shown to uninstall the plug-in before attempting the NetBackup upgrade.

```
rpm -e VRTSnbntnxahv*
```

To upgrade the UNIX or Linux client binaries using native installers:

1. Please create the NetBackup installation answer file (`NBInstallAnswer.conf`) in the client `/tmp` directory. More information about the answer file and its contents is available.

   See "About the NetBackup answer file" on page 122.

2. (Conditional) If your environment uses a NetBackup Certificate Authority, and the client is already configured for NetBackup Certificate Authority, proceed to 5. Otherwise, populate `NBInstallAnswer.conf` with the following required information:

   `CA_CERTIFICATE_FINGERPRINT=`*`fingerprint`*

   Example (the fingerprint value is wrapped for readability):

   ```
   CA_CERTIFICATE_FINGERPRINT=01:23:45:67:89:AB:CD:EF:01:23:45:67:
   89:AB:CD:EF:01:23:45:67
   ```

   Depending on the security configuration in your NetBackup environment, you may need to add the `AUTHORIZATION_TOKEN` option to the answer file. Additional information about the `AUTHORIZATION_TOKEN` option is available.

   See "About the NetBackup answer file" on page 122.

3. (Conditional) If your environment uses an external certificate authority, and the client is already configured for external certificate authority, proceed to 5. Otherwise, populate `NBInstallAnswer.conf` with the following required information:

   - `SET ECA_CERT_PATH=`*`path`*

     Use this field to specify the path and the file name of the external certificate file. This field is required to set up an external certificate from a file.

   - `SET ECA_TRUST_STORE_PATH=`*`path`*

     Use this field to specify the path and the file name of the file representing the trust store location. This field is required to set up an external certificate from a file.

   - `SET ECA_PRIVATE_KEY_PATH=`*`path`*

     Use this field to specify the path and the file name of the file representing the private key. This field is required to set up an external certificate from a file.

   - `SET ECA_KEY_PASSPHRASEFILE=`*`path`*

     Use this field to specify the path and the file name of the file that contains the passphrase to access the keystore. This field is optional and applies only when setting up an external certificate from a file.

- SET ECA_CRL_CHECK_LEVEL=*value*

  Use this field to specify the CRL mode. This field is required. Supported values are:

  - USE_CDP: Use the CRL defined in the certificate.
  - USE_PATH: Use the CRL at the path that is specified in ECA_CRL_PATH.
  - DISABLED: Do not use a CRL.
  - SKIP: Used to skip setting up the certificate authority. To skip the ECA configuration, you must set all required ECA_ values to SKIP. Be aware that if you continue with the installation without a certificate authority, the backups and restores fail.

- SET ECA_CRL_PATH=*path*

  Use this field to specify the path to the CRL associated with the external CA certificate. This field is required only when ECA_CRL_CHECK_LEVEL is set to USE_PATH. If not applicable, leave this field empty.

4 (Conditional) If the NetBackup primary server is configured to support network address translation (NAT) clients, populate NBInstallAnswer.conf with the following required information:

```
ACCEPT_REVERSE_CONNECTION=TRUE
```

More information is available. See "About the NetBackup answer file" on page 122.

5 Additionally, you can add the optional parameter shown to the NBInstallAnswer.conf file.

- SERVICES=no
- MERGE_SERVER_LIST=*value*

More information about each option is available.

See "About the NetBackup answer file" on page 122.

6 Extract the required client files from the appropriate client package and copy them to the client computer.

- Download the CLIENTS1 package for UNIX clients to a system with sufficient space.
- Download the CLIENTS2 package for Linux clients to a system with sufficient space.
- Extract the contents of the CLIENTS1 or the CLIENTS2 file.
  Example:

AIX	`gunzip NetBackup_9.1_CLIENTS1.tar.gz; tar -xvf NetBackup_9.1_CLIENTS1.tar`
HP-UX	`gunzip -dc NetBackup_9.1_CLIENTS1.tar.gz | tar -xvf`
Linux	`tar -xzvf NetBackup_9.1_CLIENTS2.tar.gz`
Solaris	`tar -xzvf NetBackup_9.1_CLIENTS1.tar.gz`

- Change to the directory for your desired operating system. Example:

AIX	`CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/RS6000/AIX6/`
HP-UX	`CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/HP-UX-IA64/HP-UX11.31/`

Linux	For Linux Red Hat:
	`CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux/RedHat2.6.18/`
	For Linux SuSE:
	`CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux/SuSE3.0.76`

Linux - s390x	For Linux-s390x Red Hat:
	`CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux-s390x/IBMzSeriesRedHat2.6.18/`
	For Linux-s390x SuSE:
	`CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux-s390x/IBMzSeriesSuSE3.0.76`

Linux - ppc64le	For Linux-ppc64le Red Hat:
	`CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux-ppc64le/IBMpSeriesRedHat3.10.0/`
	For Linux-ppc64le SuSE:
	`CLIENTS2/NBClients/anb/Clients/usr/openv/netbackup/client/Linux-ppc64le/IBMpSeriesSuSE4.4.21`

Solaris	For Solaris SPARC:
	`CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/Solaris/Solaris10/`
	For Solaris x86
	`CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/Solaris/Solaris_x86_10_64/`

- Copy the files that are shown to the client computer.

Note: The upgrade of the Java GUI and the JRE is optional. If you do not want them upgraded, omit the copy and the install of the `VRTSnbjava` and `VRTSnbjre` packages.

It is recommended to remove the old Java GUI and JRE packages if you decide not to upgrade them.

See "Add or Remove Java GUI and JRE after upgrade" on page 120.

AIX

```
VRTSnbpck.image
VRTSpbx.image.gz
VRTSnbclt.image.gz
VRTSnbjre.image.gz
VRTSnbjava.image.gz
VRTSpddea.image.gz
VRTSnbcfg.image.gz
```

HP-UX

```
VRTSnbpck.depot
VRTSpbx.depot.gz
VRTSnbclt.depot.gz
VRTSnbjre.depot.gz
VRTSnbjava.depot.gz
VRTSpddea.depot.gz
VRTSnbcfg.depot.gz
```

Linux

```
VRTSnbpck.rpm
VRTSpbx.rpm
VRTSnbclt.rpm
VRTSnbjre.rpm
VRTSnbjava.rpm
VRTSpddea.rpm
VRTSnbcfg.rpm
```

Note: Please be aware the `VRTSnbjre.rpm`, `VRTSnbjava.rpm`, and `VRTSpddea.rpm` files are not supported on the IBM pSeries clients.

Solaris

```
.pkg_defaults
VRTSnbpck.pkg.gz
VRTSpbx.pkg.gz
VRTSnbclt.pkg.gz
VRTSnbjre.pkg.gz
VRTSnbjava.pkg.gz
VRTSpddea.pkg.gz
VRTSnbcfg.pkg.gz
```

Note: The Solaris client binaries include a hidden administration file called `.pkg_defaults`. This administration file contains default installation actions.

Note: Be aware there is no `VRTSpddea.rpm` for the **z/Architecture** client.

Note: Please be aware the `VRTSnbjre.rpm`, `VRTSnbjava.rpm`, and `VRTSpddea.rpm` files are not supported on the IBM pSeries clients.

---

7 (Conditional) For Solaris, HP-UX, and AIX, extract the compressed package files with the command shown:

```
gunzip VRTS*.*
```

This action extracts all the package files as shown:

```
VRTSnbpck.pkg
VRTSpbx.pkg
VRTSnbclt.pkg
VRTSnbjre.pkg
VRTSnbjava.pkg
VRTSpddea.pkg
VRTSnbcfg.pkg
```

8 Install the Veritas precheck package.

- AIX: `installp -ad VRTSnbpck.image all`
- HP-UX: `swinstall -s VRTSnbpck.depot \*`
- Linux: `rpm -U VRTSnbpck.rpm`
- Solaris: `pkgadd -a .pkg_defaults -d VRTSnbpck.pkg VRTSnbpck`

9 (Conditional) If you are upgrading from pre-NetBackup 8.0, remove the old `SYMC*` packages. The example shown indicates the commands used to remove the `SYMC` RPM packages. This process preserves your NetBackup configuration.

```
rpm -e SYMCnbjava
rpm -e SYMCpddea
rpm -e SYMCnbclt
rpm -e SYMCnbjre
```

10 Install the files in the order that is shown with the command shown:

Note: The upgrade of the Java GUI and JRE is optional. If you do not want them upgraded, omit the copy and the install of the `VRTSnbjava` and `VRTSnbjre` packages.

It is recommended to remove the old Java GUI and JRE packages if you decide not to upgrade them.

See "Add or Remove Java GUI and JRE after upgrade" on page 120.

AIX

```
installp -ad VRTSpbx.image all
installp -ad VRTSnbclt.image all
installp -ad VRTSnbjre.image all
installp -ad VRTSnbjava.image all
installp -ad VRTSpddea.image all
installp -ad VRTSnbcfg.image all
```

Alternatively use a single command to install all packages:

```
installp -ad folder_name all
```

HP-UX

```
swinstall -s VRTSpbx.depot \*
swinstall -s VRTSnbclt.depot \*
swinstall -s VRTSnbjre.depot \*
swinstall -s VRTSnbjava.depot \*
swinstall -s VRTSpddea.depot \*
swinstall -s VRTSnbcfg.depot \*
```

Alternatively use a single command to install all packages:

```
swinstall -s ./VRTSnbpck.depot \*;swinstall -s
./VRTSpbx.depot \*;swinstall -s ./VRTSnbclt.depot
\*;swinstall -s ./VRTSnbjre.depot \*;swinstall -s
./VRTSnbjava.depot \*;swinstall -s ./VRTSpddea.depot
\*;swinstall -s ./VRTSnbcfg.depot \*
```

Linux

```
rpm –U VRTSpbx.rpm
rpm –U VRTSnbclt.rpm
rpm –U VRTSnbjre.rpm
rpm –U VRTSnbjava.rpm
rpm –U VRTSpddea.rpm
rpm –U VRTSnbcfg.rpm
```

Note: Please be aware the `VRTSnbjre.rpm`, `VRTSnbjava.rpm`, and `VRTSpddea.rpm` files are not supported on the IBM pSeries clients.

Solaris

Use the `pkgadd -a admin -d device [pkgid]` command as shown to install the files:

```
pkgadd -a .pkg_defaults -d VRTSpbx.pkg VRTSpbx
pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt
pkgadd -a .pkg_defaults -d VRTSnbjre.pkg VRTSnbjre
pkgadd -a .pkg_defaults -d VRTSnbjava.pkg VRTSnbjava
pkgadd -a .pkg_defaults -d VRTSpddea.pkg VRTSpddea
pkgadd -a .pkg_defaults -d VRTSnbcfg.pkg VRTSnbcfg
```

- The `-a` option defines a specific admin (`.pkg_defaults`) to use in place of the default administration file. The admin file contains default installation actions.
- The `-d` device option specifies the source of the software packages. A device can be the path to a device, a directory, or a spool directory.
- Use the `pkgid` parameter to specify a name for the package being installed. This parameter is optional.

11 (Conditional) If you do not have the answer file in place or you do not populate it correctly, you receive the error message shown:

```
WARNING: There is no answer file present and no valid bp.conf.
Therefore, security configuration is not complete. Manual steps
are required before backups and restores can occur. For more
information:
https://www.veritas.com/support/en_US/article.000127129
```

Change to the `/usr/openv/netbackup/bin/private` directory and run the `nb_init_cfg` command to configure the `bp.conf` file. You can also manually configure `bp.conf` file. You may have to set up the security and the certificate configuration manually. More information is available.

https://www.veritas.com/support/en_US/article.000127129

12 You can remove the old versions of the Java GUI and the JRE if you no longer plan to use them.

- Linux:

  ```
  rpm -e VRTSnbjava.rpm
  rpm -e VRTSnbjre.rpm
  ```

- Solaris:

  ```
  pkgrm VRTSnbjava
  pkgrm VRTSnbjre
  ```

- HP-UX

  ```
  swremove VRTSnbjava
  swremove VRTSnbjre
  ```

- AIX

  ```
  installp -u VRTSnbjre
  installp -u VRTSnbjava
  ```

Customers who use the NetBackup installation script for their UNIX and Linux clients only see a single change to the installation behavior. The NetBackup installation script no longer copies the installation package into the `/usr/openv/pack/` directory on the client. A successful installation or upgrade is recorded in the `/usr/openv/pack/install.history` file.

Installation error messages on UNIX and Linux, their causes, and their solutions

Installation attempts that vary from the procedure that is shown may generate error messages. Table 6-1 shows some of the actions and the message that is generated.

Table 6-1 Installation error messages and solutions

Install action	Error message	Solution
For AIX		
User attempts to install the binaries on top of the same version of the binaries.	`# installp -ad VRTSnbpck.image all` `package VRTSnbpck.image is already installed`	Use the `lslpp -L` *`package_name`* command to determine the name of the installed package. Uninstall this package and then retry the operation.

User attempts to install the binaries in the incorrect order.	`# installp -ad VRTSnbcfg.image all`
	`error: Failed dependencies:`
	`VRTSnbclt >= 8.1.0.0 is needed by VRTSnbcfg-version-platform`
		Refer to the documentation for the correct image package installation order. More information is also available in the error which lists the dependent packages.
		See "To upgrade the UNIX or Linux client binaries using native installers:" on page 83.

Table 6-1 Installation error messages and solutions *(continued)*

Install action	Error message	Solution

User attempts to install an older version of a binary over the top of a newer version of the binary.	`# installp -d VRTSnbclt.image all`
	`WARNING:`
	`file /usr/openv/lib/java/nbvmwaretags.jar from install of VRTSnbclt-version-platform conflicts with file from package VRTSnbclt-version-platform`
		Use the `lslpp -L` *`package_name`* command to determine the name of the installed package. Uninstall this package and then retry the operation.

For HP-UX		
User attempts to install the binaries on top of the same version of the binaries.	`# swinstall -s ./VRTSnbpck.depot` `1 filesets have the selected revision already installed.`	Use the `swlist` command to determine the name of the installed package. Uninstall this package and then retry the operation.
User attempts to install the binaries in the incorrect order.	`# swinstall -s ./VRTSnbcfg.depot` `ERROR: "`*`hostname`*`:/": The software dependencies for 1 products or filesets cannot be resolved.`	Refer to the documentation for the correct depot package installation order. More information is also available in the error which lists the dependent packages. See "To upgrade the UNIX or Linux client binaries using native installers:" on page 83.
User attempts to install an older version of a binary over the top of a newer version of the binary.	`# swinstall -s ./VRTSnbclt.depot` `WARNING: "`*`hostname`*`:/": 1 filesets have a version with a higher revision number already installed.`	Use the `swlist` command to determine the name of the installed package. Uninstall this package and then retry the operation.
For Linux		
User attempts to install the binaries on top of the same version of the binaries.	`# rpm -U VRTSnbpck.rpm` `package VRTSnbpck.rpm-`*`version-platform`*` is already installed`	Use the `rpm` command to determine the name of the installed package. Uninstall this package and then retry the operation.

User attempts to install the binaries in the incorrect order.	`# rpm -U VRTSnbcfg.rpm`
	`error: Failed dependencies:`
	`VRTSnbclt >= 8.1.0.0 is needed by VRTSnbcfg-`*`version-platform`*
		Refer to the documentation for the correct RPM installation order. More information is available.
		See "To upgrade the UNIX or Linux client binaries using native installers:" on page 83.

Table 6-1 Installation error messages and solutions *(continued)*

Install action	Error message	Solution
User attempts to install an older version of a binary over the top of a newer version of the binary.	`# rpm -U VRTSnbclt.rpm` `file /usr/openv/lib/java/nbvmwaretags.jar from install of VRTSnbclt-`*`version-platform`* `conflicts with file from package VRTSnbclt-`*`version-platform`*	Use the `rpm` command to determine the name of the installed package. Uninstall this package and then retry the operation.
For Solaris		

Table 6-1 Installation error messages and solutions *(continued)*

Install action	Error message	Solution
User attempts to install the binaries on top of the same version of the binaries		Use the `pkginfo` command to determine the name of the package that is currently installed. Uninstall this package and then retry the operation. Alternatively, use the admin file that is provided with the package to reinstall the package.

Table 6-1 Installation error messages and solutions *(continued)*

Install action	Error message	Solution
	pkgadd -a .pkg_defaults -d VRTSnbpck.pkg VRTSnbpck Processing package instance <VRTSnbpck> from </root/packages/Solaris/ Solaris_x86_10_64/VRTSnbpck.pkg> NetBackup Pre-Check(i386) 8.1.0.0 This appears to be an attempt to install the same architecture and version of a package which is already installed. This installation will attempt to overwrite this package. Copyright 2017 Veritas Technologies LLC. All rights reserved. ## Executing checkinstall script. Using </> as the package base directory. ## Processing package information. ## Processing system information. 6 package pathnames are already properly installed. ## Verifying disk space requirements. Installing NetBackup Pre-Check as <VRTSnbpck> ## Executing preinstall script. Wednesday, May 10, 2017 03:15:44 PM IST: Installing package VRTSnbpck.	

Table 6-1 Installation error messages and solutions *(continued)*

Install action	Error message	Solution

	`Installing NB-Pck.`
	
	`## Installing part 1 of 1.`
	
	`[ verifying class <NBclass> ]`
	
	`## Executing postinstall script.`
	
	`Wednesday, May 10, 2017 03:15:45 PM IST: Install of package VRTSnbpck was successful.`	

User attempts to install the binaries in the incorrect order.	`# pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt`
	
	`ERROR: VRTSnbpck >=8.1.0.0 is required by VRTSnbclt. checkinstall script suspends`
		Refer to the documentation for the correct package installation order. More information is available.
		
		See "To upgrade the UNIX or Linux client binaries using native installers:" on page 83.

User attempts to install an older version of a binary over the top of a newer version of the binary.	`# pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt`
	
	`Processing package instance <VRTSnbclt> from </root/80packages/Solaris/Solaris_x86_10_64/VRTSnbclt.pkg>`
	
	`NetBackup Client(i386) 8.0.0.0`
	
	`The following instance(s) of the <VRTSnbclt> package are already installed on this machine:`
	
	`1 VRTSnbclt NetBackup Client`
	
	`(i386) 8.1.0.0`
	
	`Do you want to overwrite this installed instance [y,n,?,q]`
		Use the `pkginfo` command to determine the name of the package that is currently installed. Uninstall this package and then retry the operation.

Chapter 7

NetBackup Deployment Management with VxUpdate

This chapter includes the following topics:

- About VxUpdate
- Commands used in VxUpdate
- Repository management
- Deployment policy management
- Manually initiating upgrades from the primary server using VxUpdate
- Manually initiating upgrades from the media server or client using VxUpdate
- Deployment job status

About VxUpdate

VxUpdate provides a policy-based upgrade tool for media servers and clients. By using the policy format, Veritas provides a simplified tool for media server and 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.

The deployment policy lets you configure and run deployment activities on a schedule or enable the client host owners to upgrade at their convenience. Furthermore, you can split deployment activities into smaller, discrete tasks. You can schedule pre-check, staging, and installation tasks as separate activities with different schedules, each with their own specific deployment windows.

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 NetBackup Administrative Console. Deployment policies are located in the NetBackup Administration Console under **Deployment Management > Deployment Policies**.

To successfully create and use deployment policies, Veritas recommends:

Table 7-1

Step	Action	Additional information
1	Populate the NetBackup repository	See "Repository management" on page 98.
2	Create the deployment policy	See "Deployment policy management" on page 101.
3	(Optional) Manually run the upgrade from the primary server, media server, or the client	See "Manually initiating upgrades from the primary server using VxUpdate" on page 105. See "Manually initiating upgrades from the media server or client using VxUpdate" on page 110.

Commands used in VxUpdate

NetBackup uses two commands to let you modify the NetBackup package repository as well as initiate policies from the command line. Command-line policy initiation is useful in environments where scripting is in use. The commands are:

- `nbrepo`

  Use the `nbrepo` command to manage the NetBackup package repository. You can add, validate, and delete packages, as well as obtain package identifier and other information on packages in the repository. This command is only located on the primary server.

- `nbinstallcmd`

Use the `nbinstallcmd` command to initiate the deployment policies from the command line. You can also use the command to initiate on-demand deployment jobs. This command is located on all hosts in the NetBackup environment.

More information about these and other related commands is available.

NetBackup Commands Reference Guide

Repository management

VxUpdate uses a repository that resides on the primary server. The repository contains all packages that you can deploy to media servers and clients. Your repository can contain upgrade packages, engineering binaries, and hotfixes. With VxUpdate, the `nbrepo` command controls the package repository management. Do not attempt to manually modify or update the repository without the use of the `nbrepo` command. Depending on the packages added, the repository can grow large. Confirm that you have sufficient space on your primary server for all packages that are required for your environment. Monitor the repository directory on the primary server and remove unnecessary packages from the repository. For UNIX, the repository is in `/usr/openv/var/global/repo`. For Widows, the repository is in *`install_path`*`\NetBackup\var\global\repo`.

The `nbrepo` command verifies and populates the repository with NetBackup packages. Veritas signs the VxUpdate packages. Attempts to populate the repository with unofficial or unsigned NetBackup packages fails. These packages are referenced in the deployment policies that install NetBackup on target hosts. When you use the `nbrepo` command 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 media server and client packages
  You can upgrade NetBackup media servers and clients to a newer version of NetBackup with VxUpdate. These packages are slightly different from standard NetBackup media server and 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 media servers and 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 media server or client hotfixes that Veritas creates for NetBackup 8.1.2 and later releases include VxUpdate formatted fixes.

Downloading Veritas NetBackup approved media server and client packages

VxUpdate formatted packages are available from the myveritas.com 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 NetBackup package repository.

1. Go to the myveritas.com 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**.

    Packages that contain both media server and client binaries follow the naming convention shown: `vxupdate_nb_`*`version_operatingsystem_platform`*`.sja`
11. Download and extract the files to a temporary location on your computer.

When you finish downloading and extracting all the relevant packages to your computer, add the packages to the NetBackup package repository. More information about this topic is available.

See "Adding packages to the NetBackup package repository" on page 99.

Adding packages to the NetBackup package repository

VxUpdate can only use the Veritas signed packages that you added to the NetBackup package repository. Use the `nbrepo` command to add packages to the repository. This command adds metadata to the EMM database and places the packages in the repository directory structure on the file system. You can use the `nbrepo` command to list the contents of the package repository as well as the details about individual packages.

1. Navigate to the `admincmd` directory from a command prompt.

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

   Windows: *`install_path`*`\NetBackup\bin\admincmd\`

2. Use the `nbrepo` command with the `-a` option:

   `nbrepo -a` *`package_path`*

   Example: `nbrepo -a C:\temp\nbclient_8.1.2_windows_x64.sja`

3. After successfully verifying and adding the package to the repository, the command returns a success message.

4. More information about the `nbrepo` command is available.

   NetBackup Commands Reference Guide

5. When there are packages in the repository that are no longer used, remove the packages. More information is available.

   See "Removing packages from the NetBackup package repository" on page 100.

Removing packages from the NetBackup package repository

You can remove packages from the repository either when they are no longer needed or to conserve disk space. For example, remove the NetBackup 8.1.2 packages once all of the clients are upgraded to that version. Use the `nbrepo` command to remove packages. Use of the `-pkgDetails` option shows the package details, including the file system path and other package attributes. To verify that a package is removed, use the `nbrepo` command to list all packages. You can confirm that the package is no longer in the repository. You can also verify that the package is no longer located at the file system path.

1. Navigate to the `admincmd` directory from a command prompt.

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

   Windows: *`install_path`*`\NetBackup\bin\admincmd\`

2. Use the `nbrepo` command with the `-l` option to list all the packages and their identifiers.

   `nbrepo -l`

3. Use the `nbrepo` command with the `-d` option to delete any unused packages.

   `nbrepo -d` *`package_identifier`*

   Example: `nbrepo -d 6`

4. More information about the `nbrepo` command is available.

   NetBackup 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. More information about the management of the VxUpdate repository is available.

See "Repository management" on page 98.

---

1. In the NetBackup 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 NetBackup hosts that are included in the policy. The media server also caches the files from the NetBackup repository. The media server must be version NetBackup 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.
     When you upgrade media servers, the **Media server** drop-down is automatically set to the primary server and cannot be changed.
   - **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 NetBackup 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**.
  Deployment policies can contain either media servers or clients but not both. When you select the package you want installed, the list of available hosts is filtered to media servers or clients.

Note: To upgrade a 7.7.x or 8.0 media server, the media server must be in a backup policy. The policy does not need to be active and you do not need to run the policy. Once the media server is upgraded to post NetBackup 8.1 version, you can remove the policy. The policy only needs to have the media server in the client list. You do not need to specify a file list, schedule, or any other policy attributes.

If the media server is not in a policy, the operating system for the media server is listed as **Unknown**. A tool tip suggests this issue is a missing package. **Package for the selected host's operating system is missing. Add the required missing packages to the repository using the nbrepo command line.** While it may be true the package is not in the repository, you should also add the media server to a backup policy. If the tool tip persists after the media server is added to a policy, you probably need to add the required package.

---

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 NetBackup to use the existing NetBackup 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 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:

- **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 media servers and 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 media server or client with the command line. More information is available.

See "Manually initiating upgrades from the media server or client using VxUpdate" on page 110.

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

1. In the NetBackup 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 host in a policy from the administration console

1. Select **NetBackup Management > Host Properties > Media Servers** or **NetBackup Management > Host Properties > Clients** in the NetBackup 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. When you upgrade media servers, the **Media server** drop-down is automatically set to the primary server and cannot be changed.
   - 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 NetBackup to use the existing NetBackup 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 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:

- **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 a client upgrade job from the **Policies** section of the NetBackup Administrative Console. Select **NetBackup Management > Policies** in the NetBackup 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. This procedure is only applicable to clients, not media servers.

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

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

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

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

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

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

To manually initiate an upgrade from the command line for all media servers or 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 media servers or clients to upgrade.
   - *client1*, *client2*, *clientN* is a list of media servers or 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.

NetBackup Commands Reference Guide

Manually initiating upgrades from the media server or client using VxUpdate

Manually initiate deployment jobs when you are logged into the media server or 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 NetBackup version or for other upgrades such as emergency binaries.

Among the reasons for a media server or 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 media server or client. You cannot use the `nbinstallcmd` command on a media server or client to launch jobs on other media servers or clients. If you want to launch updates on other media servers and 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 105.

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 NetBackup Commands Reference Guide for the currently installed version of NetBackup 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 NetBackup certificate and an external certificate, and your target media server or client is at NetBackup 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 NetBackup 8.2 or earlier, the `-components` flag is not available. This flag was introduced in NetBackup 8.3 to enable optional installation of the NetBackup Java GUI and JRE. When you run an ad-hoc `nbinstallcmd` on a client or a media server at NetBackup 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 media server or 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.

   Note: When you initiate a media server upgrade with the `nbinstallcmd` command, you must include both the `-master_server` and the `-media_server` options. In this case, the value for both these options must be the same.

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

You can start a media server or client initiated deployment job without an associated policy from the command line. The options that are required for the `nbinstallcmd` command vary depending on your security configuration and the NetBackup version

on the computer you want to upgrade. Refer to the `nbinstallcmd` command documentation for a list of all possible options and examples of command usage.

NetBackup Commands Reference Guide

Deployment job status

Monitor and review deployment job status in the Activity Monitor in the NetBackup 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 NetBackup 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:

UNIX or 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`*

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

Table 7-2 Deployment policy operating system and hardware

Operating system	Hardware
`hpux`	`ia64`
`debian`	`x64`
`redhat`	`x64`
`suse`	`x64`
`redhat`	`ppc64le`
`suse`	`ppc64le`

Table 7-2 Deployment policy operating system and hardware *(continued)*

Operating system	Hardware
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 **NetBackup Global Security Settings** in the NetBackup 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 NetBackup 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 NetBackup 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 NetBackup Commands Reference Guide for details on how to use the `bpsetconfig` command to add values to the NetBackup configuration of a primary server.

Appendix A

Reference

This appendix includes the following topics:

- NetBackup master server web server user and group creation
- Generate a certificate on the inactive nodes of a clustered master server
- About the NetBackup Java Runtime Environment
- Add or Remove Java GUI and JRE after upgrade
- About the NetBackup web user interface
- About the NetBackup answer file
- Persistent Java Virtual Machine options
- About RBAC bootstrapping
- About NetBackup software availability
- Additional post-upgrade steps for NetApp clusters
- Using NetApp disk arrays with Replication Director
- About compatibility between NetBackup versions
- Upgrade requirements for UNIX and Linux
- Installation and upgrade requirements for Windows and Windows clusters
- Requirements for Windows cluster installations and upgrades
- Removing a clustered media server by migrating all data to a new media server
- Disabling the connection between your OpsCenter server and your NetBackup Primary Server
- Post upgrade procedures for Amazon cloud storage servers

- Upgrading clients after servers are upgraded

NetBackup master server web server user and group creation

Beginning with NetBackup 8.0, the NetBackup master server includes a configured 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 master server (or each node of a clustered master server).

Note: For security purposes, do not create web server users or groups with administrator or superuser privileges.

You can use numerous procedures to create users and groups in operating systems. Some specific approaches are shown, but other methods may accomplish the same goal. The home directory path, user name, and group names are not hard-coded, and can be changed. The default local user name is `nbwebsvc`, and the default local group name is `nbwebgrp`. The user and group must have sufficient permissions to run daemons.

More information about this topic is available.

See "Upgrade requirements for UNIX and Linux" on page 151.

Please be aware of the operating system-specific account and group requirements:

- In UNIX and Linux clustered environments, make sure that the local accounts are defined consistently on all cluster nodes. The UID must be the same for each local account. You can use LDAP accounts on UNIX.
- For Windows clustered master servers, you must use a domain account. You can use a domain account for non-clustered environments, but it is not required.
- For Windows clustered master servers, you must use a domain group.

The NetBackup Master Server installation fails if any of these requirements are not met. On Windows, you are asked to provide the password for the user account as part of the installation process.

Note: If the password associated with the web server account expires after initial configuration, NetBackup provides no notification the password has expired. This behavior is normal and expected, as the operating system manages the account and the password.

As long as the web server remains active, the account and the web server continue to operate normally.

When the web server is restarted, or if you attempt to restart the `nbwmc` service, the service fails to start, due to the expired password. Navigate to the appropriate area in the operating system, supply the correct password, and restart the service.

More information about the web services account and group is available. See the Veritas NetBackup Security and Encryption Guide and the section on the web services account.

To create the local user account and the local group:

1. Create a local group.
   - **Linux and UNIX:** `# groupadd nbwebgrp`
   - **Windows:** `C:\>net localgroup nbwebgrp /add`
2. Create a local user.
   - **Linux and UNIX:** `# useradd -g nbwebgrp -c 'NetBackup Web Services account' -d /usr/openv/wmc nbwebsvc`
   - **Windows:** `C:\>net user nbwebsvc` *`strong_password`* `/add`
3. (Conditional) For Windows only, make the user a member of the group:

   `C:\>net localgroup nbwebgrp nbwebsvc /add`
4. (Conditional) For Windows only, grant the **Log on as a service** right to the user:
   - Go to **Control Panel > Administrative Tools > Local Security Policy**.
   - Under **Security Settings**, click **Local Policies > User Rights Assignment**.
   - Right-click on **Log on as a service** and select **Properties**
   - Add the local user. The default local user name is `nbwebsvc`.
   - Save your changes and close the **Properties** dialog for **Log on as a service**.

Generate a certificate on the inactive nodes of a clustered master server

After finishing a clustered master server installation or upgrade, you must generate a certificate on all inactive nodes. This procedure is required for backups and restores of the inactive node of the cluster to succeed.

Generating the certificate on the inactive nodes in a clustered master server

---

Note: Unless otherwise indicated, all commands are issued from the inactive node

---

1. (Conditional) Add all inactive nodes to the cluster.

   If all the nodes of the cluster are not currently part of the cluster, start by adding them to the cluster. Please consult with your operating system cluster instructions for assistance with this process.

2. Run the `nbcertcmd` command to store the Certificate Authority certificate on the inactive node.

   UNIX: `/usr/openv/netbackup/bin/nbcertcmd -getCACertificate`

   Windows: *`install_path`*`\NetBackup\bin\nbcertcmd -getCACertificate`

3. Run the `nbcertcmd` command to generate the host certificate on the inactive node.

   ```
   nbcertcmd -getCertificate
   ```

4. (Conditional) If the `nbcertcmd -getCertificate` command fails with an error message indicating that a token is needed, you need a token from the Certificate Authority. Use the steps that are shown to get and correctly use the token.

   - On the active node, use the `bpnbat` command as shown to authorize the necessary changes. When you are prompted for the authentication broker, enter the virtual server name, not the local node name.

     ```
     bpnbat -login -loginType WEB
     ```

   - On the active node, use the `nbcertcmd` command to create a token.

     ```
     nbcertcmd -createToken -name token_name
     ```

     The token name is not important to this procedure. When the command runs, it displays the token string value. Note this value as it is necessary for the next command.

   - On the inactive node, use the authorization token with the `nbcertcmd` command to store the host certificate.

     ```
     nbcertcmd -getCertificate -token
     ```

This command prompts you for the token string value. Enter the token string from the `nbcertcmd -createToken` command.

Additional information about certificates is available. Please see the section on deploying certificates on master server nodes in the *Veritas NetBackup Security and Encryption Guide*.

About the NetBackup Java Runtime Environment

Veritas installs a customized version of the Java Runtime Environment (JRE) when you install any of the products shown. The customized version of JRE does not include all the directories that a standard JRE installation includes, such as `man` and `plugin`.

Products that install the JRE:

- NetBackup master server, media server, or UNIX and Linux client software
- NetBackup Java Remote Administration Console
- OpsCenter Server or View Builder

Starting with NetBackup 8.3, the Java GUI and the JRE packages are optional for UNIX, Linux, and Windows media servers and UNIX and Linux clients.

As with previous releases, the Java GUI and JRE packages are installed automatically on all master servers because they are required. The Java GUI and the JRE are not part of the default installation on Windows clients. Install the Java Remote Administration Console if you require this functionality on your Windows clients.

The various NetBackup installation methods allow the user the choice to install or not install the Java GUI and JRE packages. More information about installing or removing the Java GUI and the JRE after install or upgrade is available.

See “Add or Remove Java GUI and JRE after upgrade” on page 120.

Previously, the JRE package that is installed with NetBackup or OpsCenter was only updated when you upgraded to a later release of either software. You can use the `nbcomponentupdate` utility to update the JRE to a supported version for the products shown:

- NetBackup master server, media server, or UNIX and Linux client software
- NetBackup Java Remote Administration Console
- OpsCenter Server or View Builder

Note: You cannot use this utility to update the JRE for the NetBackup Plug-in for VMware vCenter.

If your system is running NetBackup 8.0 or later, use Table A-1 to determine the location of the `nbcomponentupdate` utility.

Table A-1 Location of JRE update utility

Product	Operating system	Path
NetBackup	Windows	*install_path*\netbackup\java\nbcomponentupdate.exe
	UNIX or Linux	/usr/openv/java/nbcomponentupdate
OpsCenter Server	Windows	*install_path*\server\bin\nbcomponentupdate.exe
	UNIX or Linux	SYMCOpsCenterServer/bin/nbcomponentupdate
OpsCenter View Builder	Windows	*install_path*\viewbuilder\bin\nbcomponentupdate.exe
NetBackup Java Remote Administration Console	Windows	*install_path*\java\nbcomponentupdate.exe

If you have a NetBackup 7.7.x or earlier, download the `nbcomponentupdate` utility from the location shown:

https://www.veritas.com/support/en_US/article.000115043

More information about the `nbcomponentupdate` command and its parameters is available.

NetBackup Commands Reference Guide

The NetBackup installed version of the JRE is the supported major version for that NetBackup release. Use this utility to update to a minor version of the supported major JRE version. For example, if NetBackup 8.0 installed JRE 1.8.0.31, the supported major version is 1.8. Use this utility to update to JRE 1.8.0.92.

Veritas recommends that you update to another major JRE version only if the JRE vendor declares an end-of-life for the installed JRE version. If the JRE vendor declares an end-of-life for JRE 1.8, which is also the installed JRE version in your environment, update to JRE 1.9.

Close the product, such as NetBackup, before you attempt to update the JRE. If the product is active when you attempt the update, the utility exits with an error message that requests you to close the product.

Caution: Do not stop the utility while the JRE update is in progress. This action can cause the product that uses the JRE, such as NetBackup, to become unstable.

If there are additional versions of the JRE installed on your system for other applications, the NetBackup JRE does not interfere with them. The NetBackup JRE does not provide integration with web browsers and does not allow Java Applets or Web Start to run. For that reason, the NetBackup JRE cannot be used in a browser-based attack that uses Java Applet or Web Start vulnerabilities.

More information about NetBackup JRE alerts is available.

http://www.veritas.com/docs/TECH50711

Add or Remove Java GUI and JRE after upgrade

You can add or remove the Java GUI and the JRE packages after the upgrade operation completes.

Add Java GUI and JRE

To add the packages, use one of the options shown:

- Create and run a VxUpdate policy (or ad hoc operation) and specify that the Java GUI and JRE packages should be included.
- On UNIX, access the upgrade media and run the commands shown:

Linux	`rpm -U VRTSnbjre.rpm` `rpm -U VRTSnbjava.rpm`
Solaris	`pkgadd -a .pkg_defaults -d VRTSnbjre.pkg VRTSnbjre` `pkgadd -a .pkg_defaults -d VRTSnbjava.pkg VRTSnbjava`
HP-UX	`swinstall -s VRTSnbjre.depot \*` `swinstall -s VRTSnbjava.depot \*`
AIX	`installp -ad VRTSnbjre.image all` `installp -ad VRTSnbjava.image all`
Debian	Re-run the Debian install script and specify the correct value to add the Java GUI and the JRE packages.

- On Windows, access the installation media, and run the packages shown:
  - `Veritas NetBackup JRE.msi`
  - `Veritas NetBackup Java GUI.msi`

Remove Java GUI and JRE

To remove the packages, use one of the options shown:

- Create and run a VxUpdate policy (or ad hoc operation) and specify that the Java GUI and JRE packages should be excluded.
- On UNIX, run the commands shown:

Linux	`rpm -e VRTSnbjava.rpm` `rpm -e VRTSnbjre.rpm`
Solaris	`pkgrm VRTSnbjava` `pkgrm VRTSnbjre`
HP-UX	`swremove VRTSnbjava` `swremove VRTSnbjre`
AIX	`installp -u VRTSnbjre` `installp -u VRTSnbjava`
Debian	Re-run the Debian install script and specify the correct value to remove the Java GUI and the JRE packages.

- On Windows
  - Select **Start > Settings > Control Panel**.
  - In the **Control Panel** window, select the appropriate utility for installed programs and applications.
  - From the **Currently Installed Programs** list, select **Veritas NetBackup Java** and click **Remove**.
  - From the **Currently Installed Programs** list, select **Veritas NetBackup JRE** and click **Remove**.

About the NetBackup web user interface

In version 8.1.2, Veritas introduces a new web user interface for use with NetBackup. The new interface is designed to improve the ease of use and functionality. At this

time, not all functionality of the NetBackup Administration Console is present in the new interface.

NetBackup uses the Transport Layer Security (TLS) protocol to encrypt the communication for the new interface. You need a TLS certificate that identifies the NetBackup host to enable TLS on the NetBackup web server. NetBackup uses self-signed certificates for client and host validation. A self-signed certificate is automatically generated during install for enabling TLS communications between the web browser and the NetBackup web server. You can create and implement third-party certificates to use in place of the self-signed certificates to support the NetBackup Web Service. The certificates are used for TLS encryption and authentication. See the NetBackup Web UI Administrator's Guide for more information.

First-time sign in to a NetBackup master server from the NetBackup web UI

After the installation of NetBackup, a root user or an administrator must sign into the NetBackup web UI from a web browser and create RBAC roles for users. A role gives a user permissions and access to the NetBackup environment through the web UI, based on the user's role in your organization. Some users have access to the web UI by default.

See the NetBackup Web UI Administrator's Guide for details on authorized users, creating roles, and signing in and out of the web UI.

About the NetBackup answer file

NetBackup provides a way to perform unattended, silent installation, and upgrades with a predefined set of configuration options. These options allow the user to:

- Override some default values.
- Avoid answering some questions during interactive installation.

On UNIX and Linux, templates for media and clients are available at the top level of the NetBackup installation image that is downloaded from Veritas. These templates should be modified as needed and placed in `/tmp/NBInstallAnswer.conf` for use during installs and upgrades.

On Windows, templates for master, media, and client are in the `windows_x64` directory at the top level of the NetBackup installation image that is downloaded from Veritas. These templates are called `silentmaster.cmd`, `silentmedia.cmd`, and `silentclient.cmd`.

Templates for media and clients are available at the top level of the NetBackup installation image downloaded from Veritas.

Populate the NetBackup answer file on the target host before you run the installation script. Create the file if it does not exist. The supported entries are shown along with any relevant information.

Table A-2 All template options and required computers

Option	NetBackup role	Platform	Required for upgrade?
ABORT_REBOOT_INSTALL	Master, media, and client	Windows	No
ACCEPT_REVERSE_CONNECTION	Client	All	No
ADDITIONALSERVERS	Master, media, and client	Windows	No
ALLOW_PRE_90_UPGRADE	Master	All	See the option for details.
AUTHORIZATION_TOKEN	Media and client	All	Review About security configuration considerations for details.
CA_CERTIFICATE_FINGERPRINT	Media and client	All	Review About security configuration considerations for details.
CLIENT	Client	Windows	Yes
CLIENT_NAME	Media and client	UNIX and Linux	No
ECA_CERT_PATH	Media and client	All	Review About security configuration considerations for details.
ECA_CERT_STORE	Media and client	Windows	Review About security configuration considerations for details.
ECA_CRL_CHECK_LEVEL	Media and client	All	Review About security configuration considerations for details.
ECA_CRL_PATH	Media and client	All	Only when ECA_CRL_CHECK_LEVEL=USE_PATH is specified.
ECA_KEY_PASSPHRASEFILE	Media and client	All	No
ECA_PRIVATE_KEY_PATH	Media and client	All	Review About security configuration considerations for details.
ECA_TRUST_STORE_PATH	Media and client	All	Review About security configuration considerations for details.

Table A-2 All template options and required computers *(continued)*

Option	NetBackup role	Platform	Required for upgrade?
INCLUDE_JAVA_GUI_AND_JRE	Media and clients	All	UNIX and Linux media servers and clients: No Windows media servers: Yes
INSTALL_PATH	Media and client	All	No
INSTALLDIR	Master, media, and client	Windows	No
LICENSE	Media	UNIX and Linux	No
LICENSEKEY	Master and media	Windows	No
MACHINE_ROLE	Media and client	UNIX and Linux	No
MASTERSERVER	Master, media, and client	Windows	Yes
MEDIA_SERVER	Client	UNIX and Linux	No
MEDIASERVER	Media	Windows	No
MERGE_SERVERS_LIST	Client	UNIX and Linux	No
OPSCENTER_SERVER_NAME	Master	Windows	No
RBAC_DOMAIN_NAME	Master	UNIX and Linux	No
RBAC_DOMAIN_TYPE	Master	UNIX and Linux	No
RBAC_PRINCIPAL_NAME	Master	UNIX and Linux	No
RBAC_PRINCIPAL_TYPE	Master	UNIX and Linux	No
SERVER	Media and client	UNIX and Linux	No
SERVICES	Client	UNIX and Linux	No
SERVICESTARTTYPE	Master, media, and client	Windows	No
SERVICE_USER	Master	UNIX and Linux	Yes
STOP_NBU_PROCESSES	Master, media, and client	Windows	No
USAGE_INSIGHTS_FILE_PATH	Master	Windows	Possibly

Table A-2 All template options and required computers *(continued)*

Option	NetBackup role	Platform	Required for upgrade?
VNETD_PORT	Master, media, and client	Windows	No
WEBSVC_DOMAIN	Master	Windows	Yes
WEBSVC_GROUP	Master	All	Unix and Linux: No Windows: Yes
WEBSVC_PASSWORD_PLAIN	Master	Windows	Yes
WEBSVC_USER	Master	All	Unix and Linux: No Windows: Yes

About security configuration considerations

The version of NetBackup and the operation that is performed determines what security parameters are required in the template file.

Security configuration considerations for initial installation or pre-8.1 upgrade

If this operation is an initial installation or an upgrade from pre-8.1, at least one set of security configuration parameters must be provided.

To use the NetBackup master server as your Certificate Authority, the CA_CERTIFICATE_FINGERPRINT of the master server must be provided. The AUTHORIZATION_TOKEN option may be required depending on either the security level of the master server or if this computer is already configured on the master server. More information is available: https://www.veritas.com/support/en_US/article.000127129.

To use an external certificate authority on UNIX and Linux, the ECA_CERT_PATH, ECA_CRL_CHECK_LEVEL, ECA_PRIVATE_KEY_PATH, and ECA_TRUST_STORE_PATH values are required. More information is available: 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.

To use an external certificate authority on Windows: either provide the ECA_CERT_STORE and ECA_CRL_CHECK_LEVEL values or all values previously specified for UNIX and Linux.

The ECA_CRL_PATH and ECA_KEY_PASSPHRASEFILE values are optional. More information is available: 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.

Security configuration considerations for upgrades of NetBackup 8.1 or newer

When you upgrade NetBackup from a version that already has secure communications configured (NetBackup 8.1 or newer), the `CA_CERTIFICATE_FINGERPRINT` and `AUTHORIZATION_TOKEN` values are ignored.

Security configuration considerations for upgrades of NetBackup 8.2 or newer

When you upgrade NetBackup from a version that already has ECA configured (NetBackup 8.2 or newer), all the `ECA*` parameters are ignored.

About skipping the external certificate authority configuration

To continue the installation or upgrade without configuring the certificate authority, specify `SKIP` for all the required `ECA_` options. Be aware the installation or upgrade fails if you don't set all the `ECA_` values to `SKIP`. If you continue the installation or the upgrade without the required certificate authority components, backups and restores fail.

`ABORT_REBOOT_INSTALL`

- Description: This option halts the installation or upgrade if a restart is required. Valid values are 0, don't halt and 1, halt.
- Applicable platforms: Windows only.
- Default value: `0`
- Required: No.
- `ABORT_REBOOT_INSTALL 0 | 1`
- Return to Table A-2.

`ACCEPT_REVERSE_CONNECTION`

- Description: Use this option to identify how a NAT client connects with a NetBackup host. Accepted values are `TRUE` and `FALSE`. Set this option to `TRUE` if NetBackup needs to support NAT, otherwise set it to `FALSE`. Set `ACCEPT_REVERSE_CONNECTION=FALSE` if:
  - You do not want NetBackup to support NAT clients.
  - The NetBackup clients are not behind the firewall.

- Applicable platforms: Both UNIX and Windows.
- Default value: `FALSE`
- `ACCEPT_REVERSE_CONNECTION=TRUE | FALSE`
- Return to Table A-2.

ADDITIONALSERVERS

- Description: Use this option to Include NetBackup media servers that are used to proxy security requests to the master server. List only the servers that were added since the last installation of this host. The install process combines the existing set of servers with the new ones. The use of IP addresses is not supported. Valid input values are a comma-separated list of fully qualified computer names.
- Applicable platforms: Windows only.
- Default value: None.
- Required: No.
- `ADDITIONALSERVERS` *`server1,server2,servern`*
- Return to Table A-2.

ALLOW_PRE_90_UPGRADE

- Description: This field is for master servers only. This value determines if the upgrade from pre-NetBackup 9.0 releases to NetBackup 9.0 and later can proceed. The upgrade includes the infinite expiration conversion process. This conversion only takes place when you upgrade from pre-NetBackup 9.0 to NetBackup 9.0 or later. The upgrade behavior and need for this option depend on your master server platform.
  - **Windows**
    This value is required for silent upgrades of Windows master servers. Specify `1` to allow the upgrade to continue, specify `0` to prevent the upgrade. This value is ignored during an interactive Windows master server upgrade. Depending on the size of the NetBackup catalog and the required conversion time, you may be asked if you want to continue the upgrade.
  - **UNIX**
    For UNIX and Linux master servers, specify `yes` or `no` to eliminate user prompts. If the infinite expiration conversion is expected to add length to the upgrade process, a value of `yes` means the upgrade proceeds. A value of `no` means the upgrade stops. If this value is not specified, NetBackup prompts you if you want to continue with the upgrade.

NetBackup 9.0 and later versions support the expiration dates 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 article that is shown for more information: https://www.veritas.com/content/support/en_US/article.100048600

- Applicable platforms: Both UNIX and Windows.
- Default value: None
- Required: Platform and upgrade method dependent.
- `ALLOW_PRE_90_UPGRADE=yes|no` (UNIX)
  `ALLOW_PRE_90_UPGRADE=1|0` (Windows)
- Return to Table A-2.

AUTHORIZATION_TOKEN

- Description: This option specifies that NetBackup should automatically use an authorization or a reissue token when it retrieves the host certificate. The `AUTHORIZATION_TOKEN` is 16 upper case letters. Some environments require an authorization token for backups and restores to work correctly. If this information is required and is not provided in the answer file, the installation fails. If `SKIP` is specified, the installer attempts to retrieve a host certificate without including a token. In some environments this choice may result in additional manual steps following the installation.
  Be aware that `AUTHORIZATION_TOKEN` is ignored under either of these conditions:
  - ECA is in use on the master server.
  - The master server's security level is set lower than `High`.
- Applicable platforms: Both UNIX and Windows.
- Default value: None.
- Required: Review About security configuration considerations for details.
- `AUTHORIZATION_TOKEN=`*`ABCDEFGHIJKLMNOP`* `| SKIP`
- Return to Table A-2.

CA_CERTIFICATE_FINGERPRINT

- Description: This option specifies the Certificate Authority (CA) Certificate Fingerprint. Both SHA-1 and SHA-256 fingerprints are supported. The Certificate Fingerprint is retrieved from the CA during installation or upgrade. The fingerprint format is 59 or 95 characters and is a combination of the digits 0-9, the letters

A-F, and colons. For example, `01:23:45:67:89:AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23:45:67`. The fingerprint value must match the fingerprint for the server value that is specified in the first `SERVER=server_name` option. To continue the installation or upgrade without configuring security, specify `CA_CERTIFICATE_FINGERPRINT=SKIP`.
Be aware that `CA_CERTIFICATE_FINGERPRINT` is ignored under either of these conditions:

- ECA is in use on the master server.
- The master server's security level is set lower than `High`.

- Applicable platforms: Both UNIX and Windows.
- Default value: None.
- Required: Review About security configuration considerations for details.
- `CA_CERTIFICATE_FINGERPRINT=fingerprint | SKIP`
- Return to Table A-2.

`CLIENT`

- Description: This option specifies the name that NetBackup uses to identify this client host. The `%COMPUTERNAME%` value lets the local host provide the computer name. If this value is used, it may be possible to use the same answer file on all computers within a single master server domain. The use of IP addresses is not supported.
- Applicable platforms: Windows only.
- Default value: None.
- Required: Yes.
- `CLIENT=client_name | %COMPUTERNAME%`
- Return to Table A-2.

`CLIENT_NAME`

- Description: This option specifies the name that NetBackup uses to identify this computer. The `XLOCALHOSTX` value lets the local host provide the computer name. If this value is used, it may be possible to use the same answer file on all computers within a single master server domain. This value is added to the `bp.conf` file.

  If `CLIENT_NAME` is specified on upgrade, a check is made to validate that the name that is provided in the answer file matches the value that is configured in the `bp.conf` file.

- Applicable platforms: Unix and Linux only.
- Default value: None.
- Required: No
- `CLIENT_NAME=`*`name`* `|` `XLOCALHOSTX`
- Return to Table A-2.

ECA_CERT_PATH

- Description: This option specifies the path and the file name of the external certificate file.
  To skip setting up the certificate authority, set all required `ECA_` values to `SKIP`. Be aware that if you continue with the installation without a certificate authority, the backups and restores fail.
  The `ECA_CERT_PATH` option is ignored on upgrade if ECA is already configured on the host or if NBCA only is in use on the master server.
- Applicable platforms: All.
- Default value: None.
- Required: Review About security configuration considerations for details.
- `ECA_CERT_PATH=`*`path_and_file_name`*
- Return to Table A-2.

ECA_CERT_STORE

- Description: This option specifies the external certificate location in a Windows certificate store. The option is required to set up an external certificate from the Windows certificate store.
- Applicable platforms: Windows only.
- Default value: None.
- Required: Review About security configuration considerations for details.
- `ECA_CERT_STORE=`*`store_name\issuer_distinguished_name\subject`*
- Return to Table A-2.

ECA_CRL_CHECK_LEVEL

- Description: This option specifies the CRL mode. Supported values are:
  - `USE_CDP`: Use the CRL defined in the certificate.
  - `USE_PATH`: Use the CRL at the path that is specified in `ECA_CRL_PATH`.

- DISABLED: Do not use a CRL.
- SKIP: Used to skip setting up the certificate authority. To skip the ECA configuration, you must set all required ECA_ values to SKIP. Be aware that if you continue with the installation without a certificate authority, the backups and restores fail.
  The ECA_CERT_PATH option is ignored on upgrade if ECA is already configured on the host or if NBCA only is in use on the master server.

- Applicable platforms: All.
- Default value: None.
- Required: Review About security configuration considerations for details.
- ECA_CRL_CHECK_LEVEL=*value*
- Return to Table A-2.

ECA_CRL_PATH

- Description: This option specifies the path and the file name of the CRL associated with the external CA certificate.
  To skip setting up the certificate authority, set all required ECA_ values to SKIP. Be aware that if you continue with the installation without a certificate authority, the backups and restores fail.
  The ECA_CERT_PATH option is ignored on upgrade if ECA is already configured on the host or if NBCA only is in use on the master server.
- Applicable platforms: All.
- Default value: None.
- Required: Only when ECA_CRL_CHECK_LEVEL=USE_PATH is specified.
- ECA_CRL_PATH=*path*
- Return to Table A-2.

ECA_KEY_PASSPHRASEFILE

- Description: This option specifies the path and the file name of the file that contains the passphrase to access the keystore.
  The ECA_CERT_PATH option is ignored on upgrade if ECA is already configured on the host or if NBCA only is in use on the master server.
- Applicable platforms: All.
- Default value: None.
- Required: No

- ECA_KEY_PASSPHRASEFILE=*path/filename*
- Return to Table A-2.

ECA_PRIVATE_KEY_PATH

- Description: This option specifies the path and the file name of the file representing the private key.
  To skip setting up the certificate authority, set all required ECA_ values to SKIP. Be aware that if you continue with the installation without a certificate authority, the backups and restores fail.
  The ECA_CERT_PATH option is ignored on upgrade if ECA is already configured on the host or if NBCA only is in use on the master server.
- Applicable platforms: All.
- Default value: None.
- Required: Review About security configuration considerations for details.
- ECA_PRIVATE_KEY_PATH=*path/filename*
- Return to Table A-2.

ECA_TRUST_STORE_PATH

- Description: This option specifies the path and the file name of the file representing the trust store location.
  To skip setting up the certificate authority, set all required ECA_ values to SKIP. Be aware that if you continue with the installation without a certificate authority, the backups and restores fail.
  The ECA_CERT_PATH option is ignored on upgrade if ECA is already configured on the host or if NBCA only is in use on the master server.
- Applicable platforms: All.
- Default value: None.
- Required: Review About security configuration considerations for details.
- ECA_TRUST_STORE_PATH=*path/filename*
- Return to Table A-2.

INCLUDE_JAVA_GUI_AND_JRE

- Description: Used to determine how to handle the optional Java and JRE components during install or upgrade. Supported values are:
  - INCLUDE: Include the Java GUI and JRE as part of the installation or upgrade.

- EXCLUDE: Exclude the Java GUI and JRE. This option also removes all previous versions of the Java GUI and the JRE if they are present on the host.
- MATCH: Match the existing configuration on the host. If you specify this option on an initial installation, the components are not installed.

- Applicable platforms: All.
- Default value: None
- Required: UNIX and Linux, no. Windows media servers, yes.
- Return to Table A-2.

INSTALL_PATH

- Description: This option specifies the location to install the NetBackup binaries. Only the absolute path to a base directory is required for this option. The installer automatically appends /openv. This option cannot be used to change the location of NetBackup during an upgrade.
  Be aware that the INSTALL_PATH option is ignored on upgrade.
- Applicable platforms: Unix and Linux only.
- Default value: /usr
- Required: No
- INSTALL_PATH = *path*
- Return to Table A-2.

INSTALLDIR

- Description: This option specifies the location to install NetBackup. The fully qualified path to the base directory is required.
- Applicable platforms: Windows only.
- Default value: None.
- Required: Yes
- INSTALLDIR=C:\Program Files\Veritas
- Return to Table A-2.

LICENSE

- Description: This option specifies the license key string to apply to the server. Additional LICENSE = *key_string* lines may be added if more licenses are to be applied. This option only adds additional keys - no existing keys are removed.

- Applicable platforms: Unix and Linux only.
- Default value: None.
- Required: No.
- `LICENSE = key_string`
- Return to Table A-2.

LICENSEKEY

- Description: This option specifies the NetBackup license key for the installation.
- Applicable platforms: Windows only.
- Default value: None.
- Required: Yes for master and media servers. Not required for clients.
- `LICENSEKEY=NetBackup_license_key`
- Return to Table A-2.

MACHINE_ROLE

- Description: This option specifies the NetBackup role to install and configure on this computer. For upgrades, this value must match the configured role on the computer.
- Default value: None. Supported values are `MASTER`, `MEDIA`, and `CLIENT`.
- Applicable platforms: Unix and Linux only.
- Required: No.
- `MACHINE_ROLE = MASTER | MEDIA | CLIENT`
- Return to Table A-2.

MASTERSERVER

- Description: This option specifies the server name this computer recognizes as the current NetBackup master server. If this host is the master server, `%COMPUTERNAME%` can be used for the value. The use of IP addresses is not supported. Additional master servers can be specified with the `ADDITIONALSERVERS` option.
- Applicable platforms: Windows only.
- Default value: None.
- Required: Yes.
- `MASTERSERVER=master_server_name`

- Return to Table A-2.

MEDIA_SERVER

- Description: This option specifies that NetBackup may use the named host to tunnel secure web requests for this client. A tunnel is required when communication between the client and the NetBackup Web Service on the master server is blocked. This communication is required to obtain a host certificate during the NetBackup installation or upgrade. Multiple `MEDIA_SERVER` entries may exist in the answer file. Each one is used as a candidate to tunnel https requests. These entries are added to the `bp.conf` file.
- Applicable platforms: Unix and Linux only.
- Default value: None.
- Required: No.
- `MEDIA_SERVER=`*`media_server_name`*
- Return to Table A-2.

MEDIASERVER

- Description: This option specifies the name of the host this computer recognizes as its media server. The use of IP addresses is not supported.
- Applicable platforms: Windows only.
- Default value: None.
- Required: No.
- `MEDIASERVER=`*`media_server_name`*
- Return to Table A-2.

MERGE_SERVERS_LIST

- Description: Merge the servers present in `bp.conf` on the master with the server list contained in this client's `bp.conf`.
- Applicable platforms: Unix and Linux only.
- Default value: `NO`
- Required: No.
- `MERGE_SERVERS_LIST = yes | no`
- Return to Table A-2.

OPSCENTER_SERVER_NAME

- Description: This option specifies the name of the server that runs the OpsCenter. Leave this option empty if you don't use OpsCenter. You can also configure OpsCenter after install.
- Applicable platforms: Windows only.
- Default value: None.
- Required: No.
- `OPSCENTER_SERVER_NAME=`*`OpsCenter_server_name`*
- Return to Table A-2.

RBAC_DOMAIN_NAME

- Description: This option specifies the domain name of the principal that is configured to have the role-based access control (RBAC) permissions for the Administrator role.
- Default value: None.
- Applicable platforms: Unix and Linux only.
- Required: No
- `RBAC_DOMAIN_NAME = `*`domain_name`*
- Return to Table A-2.

RBAC_DOMAIN_TYPE

- Description: This option specifies the domain type of the principal that is configured to have the role-based access control (RBAC) permissions for the Administrator role.
- Applicable platforms: Unix and Linux only.
- Default value: None.
- Required: No
- `RBAC_DOMAIN_TYPE = `*`domain_type`*
- Return to Table A-2.

RBAC_PRINCIPAL_NAME

- Description: This option specifies the name of the principal that is configured to have the role-based access control (RBAC) permissions for the Administrator role. This user or the user group must already exist on the system.

- Applicable platforms: Unix and Linux only.
- Default value: None.
- Required: No
- `RBAC_PRINCIPAL_NAME = principal_name`
- Return to Table A-2.

RBAC_PRINCIPAL_TYPE

- Description: This option specifies the type of the principal that is configured to have the role-based access control (RBAC) permissions for the Administrator role.
- Applicable platforms: Unix and Linux only.
- Default value: None.
- Required: No
- `RBAC_PRINCIPAL_TYPE = USER | USERGROUP`
- Return to Table A-2.

SERVER

- Description: This option specifies the server name this computer recognizes as the current NetBackup master server. Additional `SERVER=` lines may be added if there are other servers that should be recognized. In the case where multiple `SERVER=` lines are present, the first occurrence is the master server. These entries are added to the `bp.conf` file.
- Applicable platforms: Unix and Linux only.
- Default value: None.
- Required: No.
- `SERVER=master_server_name`
- Return to Table A-2.

SERVICES

- Description: This option specifies whether NetBackup services should be started upon completion of the client installation or upgrade. If no is specified, the NetBackup services are not started. Additional manual configuration steps may be performed after the install or upgrade but before the NetBackup services are started.
- Applicable platforms: Unix and Linux only.

- Default value: `YES`
- Required: No.
- `SERVICES=no`
- Return to Table A-2.

SERVICESTARTTYPE

- Description: This option specifies if the NetBackup services are restarted after the host server reboots.
- Applicable platforms: Windows only.
- Default value: `Automatic`
- Required: No.
- `SERVICESTARTTYPE=Automatic | Manual`
- Return to Table A-2.

SERVICE_USER

- Description: This option specifies the service user account is used to start most of the NetBackup services or daemons on the master server. Be aware of the items shown:
  - Veritas recommends you do not use the root user as the service user.
  - Veritas recommends you do not use the `nbwebsvc` user as the service user.
  - The `nbwebgrp` group must be a secondary group of the service user.
  - Ownership of the `/usr/openv` directory changes to the new service user account that you specify with this option.
  - Use the `nbserviceusercmd --changeUser` command to change this user after installation.
  - For cluster servers, the service user and the service user ID must be same on all cluster nodes.
  - More information about the service user account is available: https://www.veritas.com/docs/100048220
- Applicable platforms: UNIX and Linux only.
- Default value: None.
- Required: Yes.
- `SERVICE_USER=`*`name`*

- Return to Table A-2.

STOP_NBU_PROCESSES

- Description: This option specifies if the install process should stop any active NetBackup processes automatically if detected. Be sure to confirm there are no active NetBackup jobs and that all NetBackup databases are shut down before installation or upgrade. Valid input values are 0 for don't stop, and 1 for stop.
- Applicable platforms: Windows only.
- Default value: `0`
- Required: No.
- `STOP_NBU_PROCESSES = 0 | 1`
- Return to Table A-2.

USAGE_INSIGHTS_FILE_PATH

- Description: This option specifies the path and the file name of the Usage Insights customer registration key file.
- Applicable platforms: Windows only.
- Default value: None.
- Required: Upgrades from pre-NetBackup 8.1.2 require this option. Upgrades from 8.1.2 and later do not require this option.
- `USAGE_INSIGHTS_FILE_PATH = path_and_file_name`
- Return to Table A-2.

VNETD_PORT

- Description: This option specifies the port NetBackup's `vnetd` process uses.
- Applicable platforms: Windows only.
- Default value: `13724`
- Required: No.
- `VNETD_PORT=port_number`
- Return to Table A-2.

WEBSVC_DOMAIN

- Description: Use this option to associate the web server with Domain (Active Directory) accounts. Provide the domain name in this field. If you plan to associate the web server with local accounts, leave this field blank.

- Applicable platforms: Windows only.
- Default value: None.
- Required: No.
- `WEBSVC_DOMAIN=`*`domain_name`*
- Return to Table A-2.

WEBSVC_GROUP

- Description: This option specifies the group name of the account that the NetBackup web server uses. This group must already exist on the system.
- Applicable platforms: All.
- Default value: `nbwebgrp`
- Required: UNIX and Linux master servers, no. Windows master servers, yes.
- `WEBSVC_GROUP=`*`custom_group_account_name`*
- Return to Table A-2.

WEBSVC_PASSWORD_PLAIN

- Description: This option specifies the password for the Windows `WEBSVC_USER` account. If your `websvc` password contains any special characters `(% ^ & < > | ' ` , ; = ( ) ! " \ [ ] . * ?)`, add the appropriate escape characters to the password. For example if the `websvc` password is `abc%` you must enter `abc%%`.

  Caution: This option places the password for this account in clear text and can potentially be a security concern.

- Applicable platforms: Windows only.
- Default value: None.
- `WEBSVC_PASSWORD_PLAIN=`*`password`*
- Return to Table A-2.

WEBSVC_USER

- Description: This option specifies the user name of the account that the NetBackup web server uses. This user must already exist on the system.
- Applicable platforms: All.

- Default value: `nbwebsvc`
- Required: UNIX and Linux master servers, no. Windows master servers, yes.
- `WEBSVC_USER=`*`custom_user_account_name`*
- Return to Table A-2.

Persistent Java Virtual Machine options

Before NetBackup 9.0, any web service Java Virtual Machine (JVM) tuning values (such as memory allocation) are overwritten during NetBackup upgrades. In NetBackup 9.0, Veritas has defined a set of web server JVM tuning options that persist across upgrades. These options are defined as environment variables in an executable shell script that is stored on the local host. The script's contents override the out of the box JVM tuning options. The script only runs when the NetBackup 9.0 or later web service starts. You can configure the options for which you want to override the default values. You can define this script at any time. Once the values are defined, you do not need to redefine them in any future upgrades.

To define the persistent JVM tuning options:

1. Create the `wmcConfig` script in the appropriate NetBackup configuration directory:

   Windows:
   `install_path``\Veritas\NetBackup\var\global\wsl\config\wmcConfig.bat`

   UNIX and Linux: `/usr/openv/var/global/wsl/config/wmcConfig.sh`

2. Edit the script to include the desired variables from the supported variables list. Each value must be on its own line. Supported variables are:

   ```
   WMC_HEAP
   WMC_METASPACE
   WMC_NEW_RATIO
   WMC_SURVIVOR_RATIO
   WMC_GC_CONFIG
   WMC_HEAP_DUMP_CONFIG
   ```

   Refer to the JVM documentation from Oracle for more information on the variables and their appropriate ranges.

3. Restart the web service to apply the configuration changes.

About RBAC bootstrapping

RBAC Bootstrapping lets you assign role-based access control (RBAC) permissions to a user or a user group during NetBackup installation or upgrade on UNIX platforms. The UNIX installer uses the `bpnbaz -AddRBACPrincipal` command to grant the Administrator role permissions to the user or the user group that you specify in the `/tmp/NBInstallAnswer.conf` file.

Note: RBAC bootstrapping provides access to all objects for the specified user or user group, even if previously the user or the user group had restricted access to certain objects. For example, the existing user Tester1 was assigned the Default VMware Administrator role. If Tester 1 is specified for RBAC bootstrapping, Tester1 is assigned the Administrator role.

After installation or upgrade, you can run the `bpnbaz -AddRBACPrincipal` command standalone on both Windows and UNIX platforms to assign RBAC permissions. The command is available only on the master server. For more information about this command, see the *NetBackup Command Reference Guide*.

RBAC Bootstrapping during installation and upgrades on UNIX platforms:

Use the answer file template `NBInstallAnswer-master.template` available in the install package to create the `/tmp/NBInstallAnswer.conf` file. In that file, add the following entries before you run the installation or upgrade:

`RBAC_DOMAIN_TYPE = domain_type`

`RBAC_DOMAIN_NAME = domain_name`

`RBAC_PRINCIPAL_TYPE = USER | USERGROUP`

`RBAC_PRINCIPAL_NAME = principal_name`

Be aware that `RBAC_DOMAIN_TYPE` supports the values shown: `NT, VX, UNIXPWD, LDAP`.

Note: Additional information about the `RBAC_*` options is available.

See "About the NetBackup answer file" on page 122.

RBAC bootstrapping is not performed if all the entries are empty or missing. In this case, the message `Answer file did not contain any RBAC entries` is posted in the install trace file. The install process always continues whether the RBAC

bootstrapping is successful or not. The audit records are created under the `SEC_CONFIG` category.

If RBAC bootstrapping is successful, the installer displays the following message:

`Successfully configured the RBAC permissions for` *`principal_name`*`.`

The installer also displays this message if the user or the user group already exists with the Administrator RBAC role.

If one or more RBAC entries exist in the answer file, but a required answer file entry is missing, the installer displays the following message:

```
Warning: Unable to configure the RBAC permissions. One or more
required fields are missing in /tmp/NBInstallAnswer.conf.
```

If there are other issues with the RBAC Bootstrapping, the installer displays the following message:

```
Warning: Failed to configure the RBAC permissions for principal_name.
Refer to logs in /usr/openv/netbackup/logs/admin for more information.
```

If RBAC bootstrapping is successful but auditing fails, the install displays the following message:

```
Successfully configured the RBAC permissions for
user_or_usergroup_name.
WARNING: Auditing of this operation failed.
Refer to logs in /usr/openv/netbackup/logs/admin for more information.
```

After the installation or upgrade completes, the specified user or user group is assigned the Administrator role with its corresponding RBAC access permissions. The user can then access APIs and the Web UI.

About NetBackup software availability

NetBackup 9.1 is available as ESD images for download from the **MyVeritas** webpage. The images adhere to a 1.8G size limitation.

To ensure the accuracy of the ESD download, some of the product images have been split into smaller, more manageable files. Before you uncompress any file, you must first join the split image files that you can identify as `1 of 2` and `2 of 2`. A `Download Readme.txt` file on **MyVeritas** describes how to join the files together.

Additional post-upgrade steps for NetApp clusters

After a NetBackup upgrade, review your NetApp cluster configuration as additional steps may be required to insure everything continues to work as expected. Table A-3 lists the various configurations and how to proceed.

Caution: If at any time after the upgrade the mode changes from Node scope to Vserver aware, you must perform the additional steps. Failure to perform the additional steps places your data at risk.

Table A-3 Additional required NetApp cluster changes

NetApp cluster mode at time of upgrade	Changes to NetApp cluster mode after upgrade	More information
Node scope mode	No changes	Veritas and NetApp both recommend that you change to Vserver aware mode at your earliest convenience.
Node scope mode	Change to Vserver aware mode	Additional steps required. See "Additional changes for Node scope mode to Vserver aware mode" on page 145.
Vserver aware mode	Not applicable	Additional steps required. See "Additional changes required for NetApp clusters in Vserver aware mode" on page 146.

Note: Once a media server detects Vserver aware mode, no further backup activities are performed on any other media server running any earlier releases of NetBackup.

If you change from Node scope mode to Vserver aware mode, you must do the following:

Additional changes for Node scope mode to Vserver aware mode

1. Enable the Vserver aware mode on the cluster by disabling node-scope-mode.
2. If there are tape devices attached to the cluster nodes, you must reconfigure them. Configure the tape devices to use the cluster-management logical interface (LIF) as the NDMP host for the device configuration. NetBackup does not support use of node name for device configuration.

   See the *Veritas NetBackup for NDMP Administrator's Guide* for additional information.
3. Credential all the LIF that are used for backups.

   This activity includes the Cluster Management LIF as well as any Vserver Data LIFs that are used for backup policies.

   See the *Veritas NetBackup for NDMP Administrator's Guide* for additional information.
4. Update the database for all existing NDMP hosts in your environment. Use the command that is shown to update the database.

   ```
   tpautoconf –verify NDMP_host_name
   ```
5. Update or replace any storage units that use the node names of the cluster to use the cluster LIF.
6. Update or replace any existing policies that back up the cluster.

   You must use either the Data LIF or the Cluster-management LIF as the client name. NetBackup does not support the use of the node name for the client name. The backup selections may also need to be modified.
7. Add an intercluster management LIF for each node that does not host a cluster management LIF.

   The NetApp cluster requires this activity to perform NDMP 3 way or NDMP Remote backups. Without these LIFs, all 3 way or remote backups from the volumes that are not hosted on the same node as the cluster management LIF fail.
8. To restore, verify, or duplicate the old images, you may have to use alternate read host.

Additional changes required for NetApp clusters in Vserver aware mode

1. Run `tpautoconf` command on each Vserver. This command must be run from the media servers that have credentials to the Vserver.

   ```
   tpautoconf -verify ndmp_host
   ```

   Once the command runs successfully, the output of the `nbemmcmd` should look similar to the following:

   ```
   servername1@/>nbemmcmd -listsettings -machinename machinename123 -
   machinetype ndmp
   NBEMMCMD, Version: 7.7
   The following configuration settings were found:
   NAS_OS_VERSION="NetApp Release 8.2P3 Cluster-Mode"
   NAS_CDOT_BACKUP="1"
   Command completed successfully.

   NAS_OS_VERSION displays the NetApp Version.
   NAS_CDOT_BACKUP tells us if NetBackup uses the new cDOT capabilities.
   ```

   The `tpautoconf -verify ndmp_host` command is not required when a new Vserver is added.

2. Add devices to the NDMP cluster as necessary and access them using the cluster management LIF. As you add devices, you must discover the devices.
3. Add storage units for the newly discovered devices.
4. Update any existing policies that back up the cluster.

   You must use either the Data LIF or the Cluster-management LIF as the client name. NetBackup does not support the use of the node name for the client name. The backup selections may also need to be modified.

Using NetApp disk arrays with Replication Director

Replication Director can replicate snapshots on a NetApp disk array in two different situations:

- In non-cluster mode: 7-mode is used to replicate snapshots on NAS and SAN. The plug-in must be installed on the OnCommand Unified Manager (OCUM) server (Figure A-1).
- In cluster-mode: Clustered Data ONTAP (cDOT) is used to replicate snapshots between storage virtual machines (SVMs or vServers). Support is for NAS only.

The plug-in must be installed on either a Windows or a Linux computer other than the OCUM server, the master server, or any media servers (Figure A-2).

Both modes support the same topologies.

Table A-4 describes the association between NetBackup versions and the NetApp plug-ins.

Table A-4 Version compatibility

NetBackup version	NetApp plug-in version	Description	Ratio of master server to OCUM server	Supported policy types
7.7 and later	1.1	Provides 7-mode support for all NetBackup Replication Director features.	One master server supports many OCUM servers. The plug-in must be installed on the OnCommand Unified Manager (OCUM) server.	MS-Windows, Standard, NDMP, VMware, Oracle
	1.1 P1	Provides 7-mode support for all NetBackup Replication Director features.	One master server supports many OCUM servers.	MS-Windows, Standard, NDMP, VMware, Oracle
	2.0	Provides cDOT support.	One master server supports many OCUM servers. The plug-in must be installed on either a Windows or a Linux computer other than the OCUM server, the master server, or any media servers.	MS-Windows, Standard, NDMP, VMware, Oracle

Note: You must upgrade the entire NetBackup environment before upgrading the plug-in. Upgrade all master servers, media servers, clients, and any hosts which communicate with the plug-in.

Figure A-1 Communication between NetBackup and the NBUPlugin for 7-mode

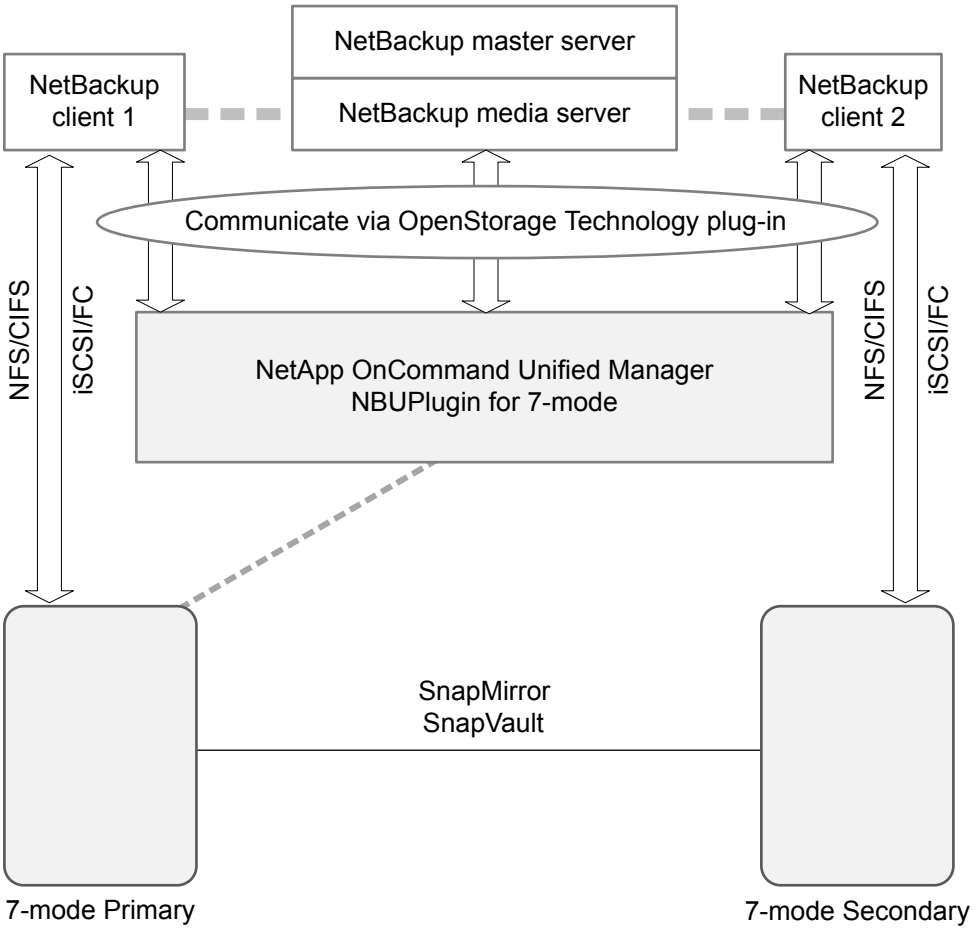
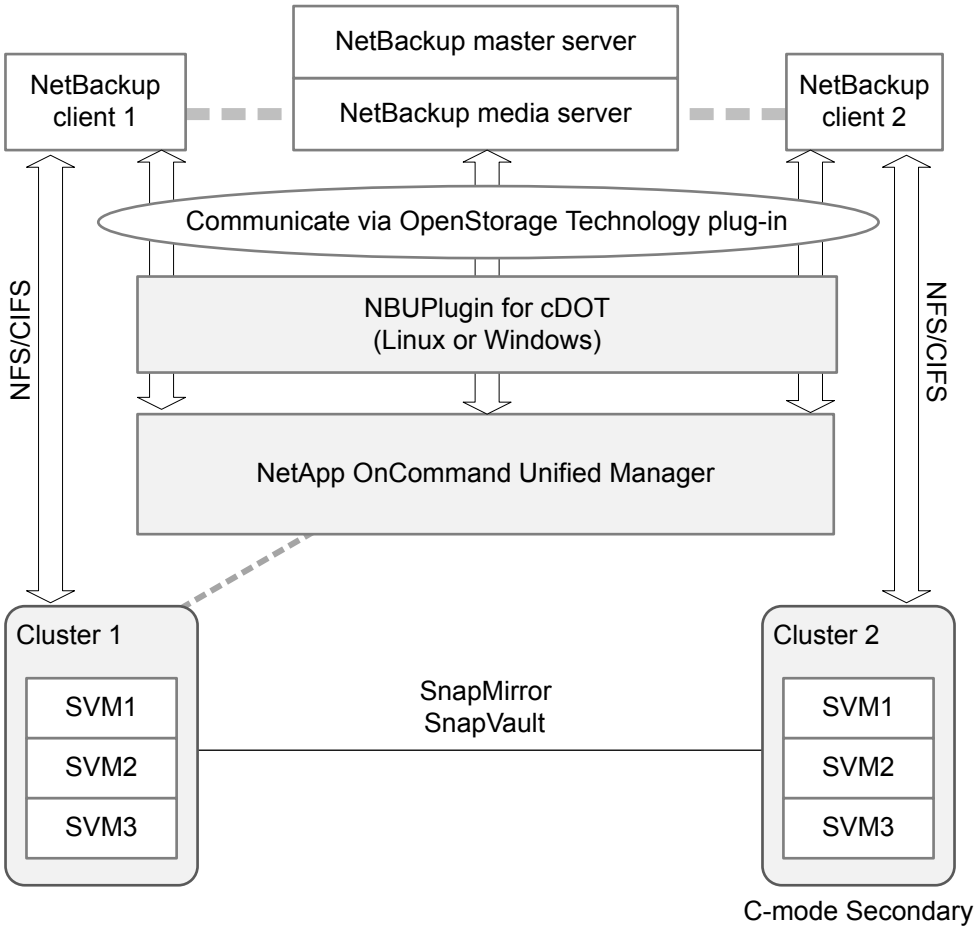


Figure A-2 Communication between NetBackup and the NBUPlugin for Clustered Data ONTAP



Determining the version of the plug-in

To determine the NBUPlugin version, look for the following version file on the system where the NBUPlugin is installed:

On Windows: *Install_path*\Program Files\Netapp\NBUPlugin\version.txt

On UNIX: /usr/NetApp/NBUPlugin/version.txt

The contents of the file lists the product name, the build date, and the NBUPlugin version. If more than one plug-in is installed, both are listed.

Upgrading the plug-in

If upgrading the NetApp Plug-in for Veritas NetBackup, make sure that all storage lifecycle policy jobs that use the old plug-in are complete before upgrading.

To determine whether all of the jobs that are associated with a storage lifecycle policy are complete, in process, or not started, use the following command:

On Windows: `install_path\NetBackup\bin\admincmd>nbstlutil.exe stlilist -U`

On UNIX: `/usr/openv/netbackup/bin/admincmd/nbstlutil stlilist -U`

About compatibility between NetBackup versions

You can run mixed versions of NetBackup between master servers, media servers, and clients. This back-level support lets you upgrade NetBackup one server at a time, which minimizes the effect on overall system performance.

Veritas supports only certain combinations of servers and clients. In mixed version environments, certain computers must be the highest version. Specifically, the version order is: OpsCenter server, master server, media server, and then clients. For example, the scenario that is shown is supported: 9.0 OpsCenter server > 8.3.0.1 master server > 8.3 media server > 8.0 client.

All NetBackup versions are four digits long. The NetBackup 9.0 release is the 9.0.0.0 release. Likewise, the NetBackup 8.3 release is the NetBackup 8.3.0.0 release. For the purposes of supportability, the fourth digit is ignored. An 8.3 master server supports an 8.3.0.1 media server. Likewise, an 8.3.0.1 master supports an 8.3 OpsCenter server. An example of what is not supported is an 8.3 OpsCenter server with a 9.0 master server.

The NetBackup catalog resides on the master server. Therefore, the master server is considered to be the client for a catalog backup. If your NetBackup configuration includes a media server, it must use the same NetBackup version as the master server to perform a catalog backup.

At NetBackup 8.1, it is critical to follow the longstanding requirement that the master server is upgraded first. Then upgrade all media servers that are required to support any 8.1 clients. Veritas recommends that you upgrade all your media servers before upgrading any clients. After all master and all media servers are at NetBackup 8.1, begin to upgrade your clients to 8.1. Pre-8.1 media servers are not able to backup or restore NetBackup 8.1 clients.

For complete information about compatibility between NetBackup versions, refer to the Veritas SORT website.

https://sort.veritas.com/

Veritas recommends that you review the End of Support Life information available online.

https://sort.veritas.com/eosl

Upgrade requirements for UNIX and Linux

Table A-5 describes the requirements to prepare your UNIX and Linux systems for NetBackup upgrade. Use this table as a checklist to address each item.

For the most up-to-date information about installation requirements, Veritas recommends use of the SORT website. More information about SORT is available.

See "About Veritas Services and Operations Readiness Tools" on page 22.

Table A-5 NetBackup requirements for UNIX and Linux

Check	Requirement	Details
	Operating System	■ For a complete list of compatible UNIX and Linux operating systems, refer to the *Software Compatibility List (SCL)* at the following website: http://www.netbackup.com/compatibility https://sort.veritas.com/netbackup
	Memory	■ Master servers in a production environment with several database agents enabled should have a minimum of 16 GB of memory and four cores each. NetBackup does not enforce minimum memory requirements. Veritas does, however, recommend using at least the minimum recommended memory. Failure to use the minimum recommended memory amounts can result in unacceptable performance. ■ Media servers in a production environment with several database agents enabled should have a minimum of 4 GB of memory each.

Table A-5 NetBackup requirements for UNIX and Linux *(continued)*

Check	Requirement	Details
	Disk space	■ The exact amount of space that is required depends on the hardware platform. More information about this topic is available. NetBackup Release Notes for 9.1 ■ NetBackup catalogs contain information about your backups that become larger as you use the product. The disk space that the catalogs require depends primarily on the following aspects of your backup configuration: ■ The number of files that are backed up. ■ The frequency of your backups. ■ The amount of time that you set to retain your backup data. If space is an issue, you can install NetBackup on an alternate file system. The installation lets you select an alternate install location, and creates the appropriate link from `/usr/openv`. **Note:** The value for disk space is for initial installation only. The NetBackup catalog requires considerably more space once the master server is placed in a production environment.
	General requirements	■ Ensure that the `gzip` and the `gunzip` commands are installed on the local system. The directories where these commands are installed must be part of the root user's path environment variable setting. ■ All NetBackup installation ESD images, appropriate licenses, and the root password for all servers. ■ A server of a supported hardware type that runs a supported version of its operating system (with applicable patches), adequate disk space, and supported peripherals. For details on these requirements, refer to the NetBackup Release Notes for 9.1. ■ All NetBackup servers must recognize and be recognizable by their client systems. In some environments, this means that each must be defined in the other's `/etc/hosts` file. Other environments may use the Network Information Service (NIS) or Domain Name Service (DNS). ■ The minimum screen resolution configuration is 1024x768, 256 colors.

Table A-5 NetBackup requirements for UNIX and Linux *(continued)*

Check	Requirement	Details
	Clustered systems	■ Ensure that each node in the NetBackup cluster can run the `ssh` command or its equivalent. The root user must be able to perform a remote logon to each node in the cluster without entering a password. This remote logon is necessary for installation and configuration of the NetBackup server and any NetBackup agents and options. After installation and configuration are complete, it is no longer required. ■ You must install, configure, and start the cluster framework before you install NetBackup. ■ You must have defined a virtual name using DNS, NIS, or the `/etc/hosts` file. The IP address is defined at the same time. (The virtual name is a label for the IP address.) ■ Begin the upgrade from the active node, and then upgrade the inactive nodes. More information about cluster requirements is available. NetBackup Clustered Master Server Administrator's Guide
	NFS compatibility	Veritas does not support installation of NetBackup in an NFS-mounted directory. File locking in NFS-mounted file systems can be unreliable.
	Kernel reconfiguration	For some peripherals and platforms, kernel reconfiguration is required. For more details, see the NetBackup Device Configuration Guide.
	Linux	Before NetBackup installation, confirm the system libraries that are shown are present. If any library is not present, install the one provided by your operating system. ■ `libnsl.so.1` ■ `insserv-compat` ■ `libXtst`
	Red Hat Linux	For Red Hat Linux, NetBackup requires server networking.
	Other backup software	Veritas recommends that you remove any other vendor backup software currently configured on your system before you install this product. Other vendor backup software can negatively affect how NetBackup installs and functions.

Table A-5 NetBackup requirements for UNIX and Linux *(continued)*

Check	Requirement	Details
	Web Services	Beginning with NetBackup 8.0, the NetBackup master 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 master server (or each node of a clustered master server). You must create these required account elements before installation. More information is available: See "NetBackup master server web server user and group creation" on page 115. **Note:** Veritas recommends that you save the details of the user account that you use for the NetBackup Web Services. A master 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 By default, the UNIX installation script attempts to associate the web server with user account `nbwebsvc` and group account `nbwebgrp`. You can override these default values with the NetBackup installation answer file. You must populate the NetBackup installation answer file on the target host before you start the UNIX installation script. Populate the NetBackup installation answer file with custom web server account names as shown. **1** Log in to the server as root. **2** Open the file /tmp/NBInstallAnswer.conf with your preferred text editor. Create the file if it does not exist. **3** Override the default web server user account name by adding the line shown: `WEBSVC_USER=`*`custom_user_account_name`* **4** Override the default web server group account name by adding the line shown: `WEBSVC_GROUP=`*`custom_group_account_name`* **5** Save and close the file.

Table A-5 NetBackup requirements for UNIX and Linux *(continued)*

Check	Requirement	Details
	Customer Registration Key for Veritas Usage Insights	Beginning with NetBackup 8.1.2, you must specify a Customer Registration Key for Veritas Usage Insights. More information about Veritas Usage Insights is available: See "About Veritas Usage Insights" on page 12. During install and upgrade to NetBackup 8.1.2, 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.

Installation and upgrade requirements for Windows and Windows clusters

Table A-6 describes the requirements to prepare your Windows systems for NetBackup installation. Use this table as a checklist to address each item.

For the most up-to-date information about installation requirements, Veritas recommends use of the SORT website. More information about SORT is available.

See "About Veritas Services and Operations Readiness Tools" on page 22.

Caution: Veritas supports moving the NetBackup catalog with the `nbdb_move` command to a non-default location on a Windows cluster after installation or upgrade. Before any upgrades, however, you must move the NetBackup catalog back to the default location for the upgrade to succeed. Do not attempt a NetBackup upgrade if the catalog is not in the default location. You master server is rendered unusable if you fail to move the database back to the default location before upgrade. More information about the nbdb_move is available.

NetBackup Commands Reference Guide

Table A-6 NetBackup installation and upgrade requirements for Windows and Windows clusters

Check	Requirement	Details
	Operating system	■ Make sure that you have applied the most current operating system patches and updates, including any security updates. If you are not certain that your operating system is current, contact your operating system vendor and request the latest patches and upgrades. ■ For a complete list of compatible Windows operating systems, refer to the *Software Compatibility List (SCL)* at the following website: http://www.netbackup.com/compatibility
	Memory	■ NetBackup does not enforce minimum memory requirements. Veritas does, however, recommend using at least the minimum recommended memory. Failure to use the minimum recommended memory amounts can result in unacceptable performance. ■ Media servers in a production environment with several database agents enabled should have a minimum of 4 GB of memory each.
	Disk space	■ An NTFS partition. ■ The exact amount of space that is required to accommodate the server software and the NetBackup catalogs depends on the hardware platform. More information about this topic is available. NetBackup Release Notes for 9.1 ■ Upgrades require additional space on the primary drive, even if NetBackup is installed to an alterative location. The primary drive is the drive where Windows is installed. ■ For server upgrades Veritas requires 2.8 GB of free space on the primary Windows drive when you install NetBackup to an alternative drive location. ■ For client upgrades Veritas requires 1.7 GB of free space on the primary Windows drive when you install NetBackup to an alternative drive location. ■ NetBackup catalogs contain information about your backups that become larger as you use the product. The disk space that the catalogs require depends primarily on the following aspects of your backup configuration: ■ The number of files that are backed up. ■ The frequency of your backups. ■ The amount of time that you set to retain your backup data. ■ Veritas recommends that you have a minimum available disk space of 5% in any Disk Storage Unit volume or file system. **Note:** The value for disk space is for initial installation only. The NetBackup catalog requires considerably more space once the master server is placed in a production environment.

Table A-6 NetBackup installation and upgrade requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	General requirements	Make sure that you have all of the following items: ■ NetBackup installation ESD images ■ Appropriate license keys ■ Administrator account and password for all servers ■ Screen resolution configured for at least 1024x768, 256 colors. **Note:** To install NetBackup on Windows 2012 R2, Windows 2012 UAC-enabled, and Windows Server 2016 environments, you must log on as the official administrator. Users that are assigned to the Administrators Group and are not the official administrator cannot install NetBackup in UAC-enabled environments. To allow users in the Administrators Group to install NetBackup, disable UAC.

Table A-6 NetBackup installation and upgrade requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	Remote and cluster installations	

Table A-6 NetBackup installation and upgrade requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
		In addition to all previously stated installation requirements, the following guidelines apply to remote installations and cluster installations: ■ All nodes in the cluster must run the same operating system version, service pack level, and NetBackup version. You cannot mix versions of server operating systems. ■ The installation account must have administrator privileges on all remote systems or on all nodes in the cluster. ■ The source system (or primary node) must run Windows 2012/2012 R2/Windows 2016. ■ The destination PC (or clustered nodes) must have Windows 2012/2012 R2/Windows 2016. ■ The Remote Registry service must be started on the remote system. The NetBackup installer can enable and start the Remote Registry service on the remote system. If the Remote Registry service is not started, the installation receives the following error message: `Attempting to connect to server server_name failed with the following error: Unable to connect to the remote system. One possible cause for this is the absence of the Remote Registry service. Please ensure this service is started on the remote host and try again.` ■ NetBackup virtual name and IP address Have the virtual name and IP address for NetBackup available. You must provide this information during installation. ■ Cluster support changes for media servers You cannot perform a new installation of a clustered media server. ■ Windows Server Failover Clusters (WSFC) ■ The shared disk that the NetBackup Group uses must already be configured in the cluster and online on the active node. ■ Install NetBackup from the node with the shared disk (that is, the active node). ■ Computer or host names cannot be longer than 15 characters. ■ Cluster server (VCS) clusters: All NetBackup disk resources must be configured in Veritas Enterprise Administrator (VEA) before you install NetBackup. ■ Cluster node device configuration and upgrades When you upgrade clusters, the `ltid` and the robotic daemons retrieve the device configuration for a particular cluster node from the EMM database. The cluster node name (provided by `gethostname`) stores or retrieves the device configuration in the EMM database. The cluster node name is used when any updates are made to the device configuration, including when `ltid` updates the drive status. The cluster node name is only used to indicate where a device is connected. The NetBackup virtual

Table A-6 NetBackup installation and upgrade requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
		name is employed for other uses, such as the robot control host. More information about cluster requirements is available. NetBackup Clustered Master Server Administrator's Guide
	Remote Administration Console host names	You must provide the names of the Remote Administration Console hosts during master server installation.
	NetBackup communication	Make sure that your network configuration allows all servers and clients to recognize and communicate with one another. Generally, if you can reach the clients from a server by using the ping command, the setup works with NetBackup. ■ NetBackup services and port numbers must be the same across the network. ■ Veritas suggests that you use the default port settings for NetBackup services and Internet service ports. If you modify the port numbers, they must be the same for all master servers, media servers, and clients. The port entries are in the following file: `%SYSTEMROOT%\system32\drivers\etc\services`. To change the default settings, you must perform a custom installation of NetBackup or manually edit the `services` file.
	CIFS-mounted file systems	Veritas does not support installation of NetBackup in a CIFS-mounted directory. File locking in CIFS-mounted file systems can be unreliable.
	Storage devices	Devices such as robots and standalone tape drives must be installed according to the manufacturers' instructions and recognized by the Windows software.
	Server names	When you are prompted for server names, always enter the appropriate host names. Do not enter IP addresses.
	Mixed versions	Make sure to install NetBackup servers with a release level that is at least equal to the latest client version that you plan to use. Earlier versions of server software can encounter problems with later versions of client software. See "About compatibility between NetBackup versions" on page 150.
	Installations on Windows 2012/2012 R2 Server Core/Windows 2016	You can only install NetBackup on these computers with the silent installation method. See "Performing silent upgrades on Windows systems" on page 49.

Table A-6 NetBackup installation and upgrade requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	Other backup software	Remove any other vendor's backup software currently configured on your system. The backup software of another vendor can negatively affect how NetBackup installs and functions.
	Web Services	Beginning with NetBackup 8.0, the NetBackup master 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 master server (or each node of a clustered master server). More information is available: See "NetBackup master server web server user and group creation" on page 115. **Note:** Veritas recommends that you save the details of the user account that you use for the NetBackup Web Services. A master 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
	CA Certificate fingerprint	(Conditional) For media servers and clients only: If you use a NetBackup Certificate Authority, you must know the CA Certificate fingerprint of the master server at time of installation. This requirement only applies if you use a NetBackup Certificate Authority. More information is available about the details on the CA Certificate fingerprint and its role in generation of security certificates. https://www.veritas.com/support/en_US/article.000127129
	Authorization Token	(Conditional) For media servers and clients only: In some cases, the installer requires an authorization token to successfully deploy security certificates. More information is available about the details on authorization tokens and their role in generation of security certificates. In some cases, if you use a NetBackup Certificate Authority, the installer requires an authorization token to successfully deploy security certificates. More information is available about the details on authorization tokens and their role in generation of security certificates. https://www.veritas.com/support/en_US/article.000127129

Table A-6 NetBackup installation and upgrade requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	External certificate authority	For master servers (including cluster): The configuration of an external certificate authority is a post-installation activity. For media servers and clients: You can configure the ECA during the install procedure or after the installation completes. More information about post-installation configuration is available: 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.
	Customer Registration Key for Veritas Usage Insights	Beginning with NetBackup 8.1.2, you must specify a Customer Registration Key for Veritas Usage Insights. More information about Veritas Usage Insights is available: See "About Veritas Usage Insights" on page 12. During install and upgrade to NetBackup 8.1.2, 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.

See "Upgrade requirements for UNIX and Linux" on page 151.

Requirements for Windows cluster installations and upgrades

In addition to the normal server requirements, NetBackup cluster installations require special considerations.

The following describes the guidelines for NetBackup cluster installations and upgrades on Windows systems:

Table A-7 Windows cluster requirements for installation and upgrade

Item	Requirement
Server operating system	

Table A-7 Windows cluster requirements for installation and upgrade *(continued)*

Item	Requirement
Privileges	To perform clustered installations, you must have administrator privileges on all of the remote nodes in the cluster. Veritas recommends that you keep a record of all nodes in the cluster and what software exists on each node.
NetBackup virtual name and IP address	Have the virtual name and IP address for NetBackup available. You must provide this information during installation.
Operating system on nodes	All clustered nodes must use the same operating system version, service pack level, and NetBackup version. You cannot run mixed server versions in a clustered environment.
Cluster support changes for media servers	Clustered media servers are not supported.
Windows Server Failover Clusters (WSFC)	
Cluster Server (VCS) clusters	■ All NetBackup disk resources must be configured in Veritas Enterprise Administrator (VEA) before you install NetBackup.
Cluster node device configuration and upgrades	When you upgrade clusters, the `ltid` and the robotic daemons retrieve the device configuration for a particular cluster node from the EMM database. The cluster node name (provided by `gethostname`) stores or retrieves the device configuration in the EMM database. The cluster node name is used when any updates are made to the device configuration, including when `ltid` updates the drive status. The cluster node name is only used to indicate where a device is connected. The NetBackup virtual name is employed for other uses, such as the robot control host.

Removing a clustered media server by migrating all data to a new media server

You can remove clustered media servers from the NetBackup environment. You must migrate all data from the cluster to a new standalone server, and then decommission the old clustered server.

The steps required to migrate all NetBackup resources and decommission a media server is covered in depth in the NetBackup Administrator's Guide, Volume I. Please see the **About decommissioning a media server** topic in the NetBackup Administrator's Guide, Volume I.

Disabling the connection between your OpsCenter server and your NetBackup Primary Server

If you need to upgrade your NetBackup Primary Server before you upgrade your OpsCenter server, you can disable the relationship between your primary and OpsCenter servers.

Please be aware of the limitations and potential data loss concerns related to disabling data collection:

- It is not supported to collect data from the NetBackup primary server that is at a higher version than the OpsCenter server. The OpsCenter server must be at the same version or higher than the NetBackup primary server.
- After the OpsCenter Data Collection is disabled for the primary server, OpsCenter does not receive any alerts or new data in the OpsCenter reports. Data that was collected before data collection was disabled is still available in the OpsCenter reports.
- After you upgrade OpsCenter and enable data collection, OpsCenter receives any new alerts for the primary server and new data in the reports. OpsCenter collects data for the time when data collection was disabled only if the data is still available on the primary server. Reporting data and alerts are lost if the primary server job retention level is shorter than the time that the data collection is disabled.

To disable the connection between the primary server and the OpsCenter server

1. Disable data collection in OpsCenter.

   Settings > Configuration > NetBackup > *NetBackup Primary Server to be upgraded* > Disable Data Collection

2. Upgrade the NetBackup Primary Server.

   You can now operate both NetBackup and OpsCenter, but OpsCenter does not have complete data.

To enable the connection between the primary server and the OpsCenter server

1. Upgrade OpsCenter.
2. Enable data collection on OpsCenter once the OpsCenter upgrade completes successfully.

   Settings > Configuration > NetBackup > *NetBackup Primary Server to be upgraded* > Enable Data Collection

Post upgrade procedures for Amazon cloud storage servers

Starting with NetBackup 8.1, the object size for Amazon (S3) and Amazon GovCloud storage servers has changed. This change affects the valid range for read and write buffer size for these cloud storage servers. You must update the read and write buffer size values for pre-NetBackup 8.1 servers using the NetBackup Administration Console on the primary server. Update these settings for each cloud storage server that is associated with a media server.

For the valid range, review the `READ_BUFFER_SIZE` and `WRITE_BUFFER_SIZE` information in the *NetBackup Cloud Administrator's Guide*.

To update the Amazon (S3) and Amazon GovCloud read and write buffer size in the NetBackup Administrators Console

1. Open the NetBackup Administration Console.
2. Go to **Media and Device Manager > Credentials > Storage Server**.
3. For your Amazon (S3) and Amazon GovCloud storage servers:
   - Double click the storage server in the right pane to open the **Change Storage Server** dialog box.
   - In the **Change Storage Server** dialog box, click the **Properties** tab.
   - Update the value of the parameters shown. Enter these values in bytes:

     ```
     READ_BUFFER_SIZE
     WRITE_BUFFER_SIZE
     ```

4. Click **Save**.

Use the commands shown to update the read and write buffer size from the command line

1. `nbdevconfig -getconfig -stype` *`storage_server_type`* `-storage_server` *`storage_server_name`* `-configlist` *`filename`*
2. Update the value of the parameters shown. Enter these values in bytes:

   ```
   READ_BUFFER_SIZE
   WRITE_BUFFER_SIZE
   ```

3. `nbdevconfig -setconfig -stype` *`storage_server_type`* `-storage_server` *`storage_server_name`* `-configlist` *`filename`*

Upgrading clients after servers are upgraded

The `update_clients` installation script lets you push client software to clients. It does not let you push client software to a remote client that is also a NetBackup media or primary server. You cannot push software this way because the server software and client binaries must be of the same version on a single host.

Note: Be aware you cannot use the `update_clients` installation script to push NetBackup 8.2 or later clients. You must use VxUpdate.

The `update_clients` installation script can determine the full client list that is configured on the server. When it is run without any parameters, it attempts to update all clients (as determined by `/usr/openv/netbackup/bin/admincmd/bpplclients`). If you do not want to upgrade all clients, you can specify a subset of clients. Use the hardware type and operating system parameters or use the `-ClientList` parameter.

You can run `update_clients` from a media server. The `-ClientList` parameter is required in this situation. The script lets you maintain a media server and a set of clients at an earlier release level than the primary server. Doing so requires the informed use of the `update_clients -ClientList` command on a primary server and a media server to avoid unwanted client upgrades.

For clustered environments, you can push client software only from the active node.

Note: Additional steps are required to deploy clients in a secure environment where the clients do not have direct connectivity to the primary server. More information on this topic is available. See the topic on deploying certificates on clients without connectivity to the primary server in the NetBackup Security and Encryption Guide.

During a client upgrade, the new client files are written to a directory in `/tmp` on the client. This directory must have sufficient space to temporarily store the new client files to ensure a successful upgrade. If sufficient space is not available, a status message informs you that the upgrade script could not write to the location in the `/tmp` directory. To resolve this issue, allocate more space to the `/tmp` directory and perform the upgrade procedure again. The temporary directory is removed when the upgrade is complete.

To upgrade clients after you have upgraded servers

1 Use one of the following methods to start the installation script:

ESD images (downloaded files)	■ Navigate to the location where the installation images reside. ■ Enter the following command: `./install`
Native install tools	NetBackup supports the install and upgrade of the UNIX and Linux client binaries with native installers. More information is available. See "Upgrade of the UNIX and Linux client binaries with native installers" on page 82.

2 When the following message appears, press **Enter** to continue:

```
Installing NetBackup Client Software.
Do you wish to continue? (y/n) [y]
```

The client binaries represent the operating system versions where the binaries were compiled. The binaries typically function perfectly on later versions of the operating system. For example, Solaris 10 binaries are also used on the Solaris 11 level of the operating system.

3 Select the client type that you want to load and follow the prompts to load that client type. Repeat as necessary until all desired client types have been loaded.

Make sure that you load the software for all of the UNIX client types that you intend to push to from this server. Otherwise, you cannot add these client types to the NetBackup policy configuration.

4 As a root user on the NetBackup primary server, enter the following command to see whether bprd is running:

```
/usr/openv/netbackup/bin/bpps
```

If bprd is running, stop it with the following command:

```
/usr/openv/netbackup/bin/admincmd/bprdreq -terminate
```

5 Enter the following command to make sure that backups or restores are not in progress:

```
/usr/openv/netbackup/bin/admincmd/bpdbjobs
```

6 Update UNIX client software by running the update_clients script. Specify the host names of the individual nodes (not virtual names) in the list of clients.

Use one of the following commands:

If you do not use a -ClientList file:	/usr/openv/netbackup/bin/update_clients
If you use a -ClientList file:	/usr/openv/netbackup/bin/update_clients -ClientList *filename*

The -ClientList parameter is required on a media server.

For more than 30 clients, you can divide the list into multiple files and run update_clients for each file.

To create a client list file, perform the following steps:

- Change to the NetBackup admincmd directory, as follows:

```
cd /usr/openv/netbackup/bin/admincmd
```

- Use the bpplclients command to create a file that contains a list of clients currently configured in the NetBackup database. The options to use on this command differ depending on whether you push from a primary server or from a media server, as follows:

If you push from the primary server:	./bpplclients -allunique -noheader > *file*
If you push from a media server:	./bpplclients -allunique -noheader -M \ *m_server_name* > *file*

The option descriptions are as follows:

`m_server_name`	Name of the NetBackup primary server in this environment.
`file`	Name of the file to contain the list of unique clients. If no clients have been configured in the NetBackup database, the file is empty.

The `bpplclients` command writes output to `file` in the following format:

```
hardware os client
```

`hardware`	The hardware name. For example, run the `ls` command in directory `/usr/openv/netbackup/client`.
`os`	The operating system name. For example, run the `ls` command in directory `/usr/openv/netbackup/client/`*`hardware`*`.`
`client`	The name of the client.

The contents of `file` might look like the following example:

```
Solaris Solaris9 curry
```

- (Optional) Edit `file`.
  Perform this step to change the contents of `file`. Edit `file` to contain only those clients you want to update with NetBackup client software. The host names of the clients must be the clients' individual node names. They cannot be virtual names. The `hostname` command and the `domainname` command return the correct values for the individual node names. The format can be either `hostname` or `hostname.domainname`.

7 The `update_clients` script requests primary server information from you.

```
Starting update_clients script.
There are N clients to upgrade.
Do you want the bp.conf file on the clients updated to list this
server as the primary server? (y/n) [y]
```

Type either **`y`** or **`n`**.

Press **`Enter`**.

8 Enter the number of updates you want to occur simultaneously.

```
Enter the number of simultaneous updates you wish to take
place. [1 - 30] (default: 15):
```

9 The installer attempts to retrieve the certificate authority certificate details.

```
Getting CA certificate details.
Depending on the network, this action may take a few minutes. To
continue without setting up secure communication, press Ctrl+C.
```

Be aware if you press `Ctrl+C`, this action requires you to rerun the installation or continue with the installation without the required security components. If these security components are absent, backups and restores fail.

If a certificate authority certificate is found, you receive the message shown:

```
Using CA Certificate fingerprint from primary server:
01:23:45:67:89:AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23:45:67
If clients need an authorization token for installation, please
specify one here. Token (leave blank for no authorization token):
```

If you leave the authorization token blank, you receive the message shown:

```
WARNING: Authorization Token was not specified.
Manual steps may be required before backups and restores can occur.
```

10 Type either **`y`** or **`n`** in response to the question.

```
The upgrade will likely take Y to Z minutes.
Do you want to upgrade clients now? (y/n) [y]
```

11 After all servers and clients are updated, start the `bprd` daemon as the root user on the primary server by entering the following command:

```
/usr/openv/netbackup/bin/initbprd
```

Index

A

about
    preinstall checker 27
    startup and shutdown scripts 62
    UNIX and Linux upgrade requirements 151
    Veritas Services and Operations Readiness Tools 22
authentication certificates. *See* security certificates
Auto Image Replication
    Bare Metal Restore
        errors 30
automatic file changes
    after upgrade 20

B

Bare Metal Restore
    Auto Image Replication
        errors 30
bpplclients command 169
    create client list 168

C

catalog backup
    limitation 19
certificates. *See* security certificates
changes
    in NetBackup 9.1 10
clients
    upgrading after server upgrades 166
cluster
    private network 46
cluster installation and upgrade
    requirements 162
commands
    bpplclients 169
complete system update
    after upgrade 63
create client list
    bpplclients command 168

D

Domain Name Service (DNS) 152

H

hosts file 152

I

installation requirements
    Windows systems 155

L

limitation
    catalog backup 19
local, remote, clustered upgrade
    Windows systems 37

M

media server
    upgrade 66
mixed version support 150

N

NBUPlugin
    determining the version 149
    upgrading 150
NetBackup 9.1
    changes 10
NetBackup Electronic Software Distribution (ESD) images 143
NetBackup scripts
    startup and shutdown 62
    UNIX 62
Network Information Service (NIS) 152

P

plug-ins
    NetApp 147
    upgrading from NetApp 150

preinstall checker
about 27
primary server
upgrade 32
private network
cluster 46

R

recommended upgrade procedures
Veritas Operations Readiness Tools 23
required changes
after upgrade 63
requirements
cluster installation and upgrade 162
requirements for server installation
Linux 153
Red Hat Linux 153

S

security certificates
for NetBackup hosts 19
server installation
requirements for Linux 153
requirements for Red Hat Linux 153
servers
silent upgrade on Windows 49
silent upgrade on Windows
servers 49
SORT
Veritas Operations Readiness Tools 23
Veritas Services and Operations Readiness Tools 22
startup and shutdown
NetBackup scripts 62
startup and shutdown scripts
about 62

U

UNIX
NetBackup scripts 62
UNIX and Linux systems
upgrade requirements 151
UNIX and Linux upgrade requirements
about 151
upgrade
automatic file changes after 20
complete system update after 63
media server 66
upgrade *(continued)*
plan 16
planning 15
primary server 32
required changes after 63
upgrade clients
after upgrading servers 166
upgrade method 33, 57
upgrade requirements
UNIX and Linux systems 151
upgrade server software
server software 52
user account
web server 28

V

Veritas Operations Readiness Tools (SORT)
recommended upgrade procedures 23
Veritas Services and Operations Readiness Tools (SORT)
about 22
versions, determining NetApp NBUPlugin 147

W

web server
user account 28
Windows systems
cluster installation and upgrade requirements 162
installation requirements 155
local, remote, clustered upgrade 37