NetBackup™ Installation Guide

UNIX and Windows

Release 10.4

VERITAS™

NetBackup™ Installation Guide

Last updated: 2024-03-25

Legal Notice

Copyright © 2024 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, Veritas Alta, 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 Preparing for installation 8

General installation information 8
Available NetBackup installation methods 8
About compatibility between NetBackup versions 10
About NetBackup software availability 10
Required libraries missing from some Linux distributions 11
How to install NetBackup 11
Creating the user account to support the NetBackup web server 13
About storage device configuration 15
About security certificates for NetBackup hosts 16
Environment variable for certificate key size 17
Restrictions on the NetBackup installation directory 17
NetBackup database is not supported on the `btrfs` file system 18
Installation operational notes and limitations 18
Windows compiler and security requirements for NetBackup 10.4 and later installation 18
Java GUI and JRE installation optional for some computers 19
Enable 8dot3 name file setting for the NetBackup primary servers 19
NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952 20
Host ID-based certificate is not deployed during installation on 8.1 media server or client host with dual stack configuration 20
External certificate authority certificates supported in NetBackup 8.2 and later 20
SCCM and Chef deployment tools and documentation now available 21
Known SUSE Linux primary server install issue 21
Performance and tuning considerations 21
SORT information 22
About Veritas Services and Operations Readiness Tools 22
Recommended SORT procedures for new installations 23
Veritas NetInsights Console information 27
About Veritas Usage Insights 27

Best practices for Veritas Usage Insights 28

Chapter 2 NetBackup licenses 29

About NetBackup license requirements 29
About license entry 30
Frequently asked questions about licenses 30

Chapter 3 Installing server software on UNIX systems 34

Installation requirements for UNIX and Linux 34
Do not mix non-English versions of Windows and UNIX platforms unless primary and media servers are NetBackup appliances 37
NetBackup installations on environments that run different versions of UNIX-based operating systems 38
Special installation guidelines for Solaris systems 38
Special installation guidelines for Linux clustered environments 38
How the installation script works 38
Installing NetBackup primary server software on Linux 40
Silently installing NetBackup primary server software on Linux 47
Continuing with NetBackup software installation 51
Installing NetBackup media server software on Linux 52
Silently installing NetBackup media server software on Linux 60
About pushing client software from a primary server to clients 64
Installing client type software on a primary server 65

Chapter 4 Installing server software on Windows systems 67

Installation requirements for Windows and Windows clusters 67
Requirements for Windows cluster installations 74
Performing local, remote, or clustered server installation on Windows systems 75
Post-installation tasks for NetBackup cluster environments 92
Verifying Windows cluster installations or upgrades 93
Installing NetBackup servers silently on Windows systems 94

Chapter 5 About the administrative interfaces 98

About the NetBackup web user interface 98
About the NetBackup Administration Console 99
Installing the NetBackup Administration Console 99
Installing multiple versions of the NetBackup Administration Console on Windows 100
Removing earlier versions of the NetBackup Administration Console on Windows 101
About the NetBackup Remote Administration Console 101
Installing the NetBackup Remote Administration Console 102

Chapter 6 Installing NetBackup client software 103

About NetBackup client installation 103
About NetBackup client installation on Windows 104
About Windows client installation methods and requirements 105
Installing NetBackup Windows clients locally or remotely 107
Installing NetBackup Windows clients silently 116
How to configure NetBackup clients 117
About NetBackup client installation on UNIX and Linux 118
About UNIX and Linux client installation methods 119
Installing UNIX clients locally 120
Install of the UNIX and Linux client binaries with native installers 126
About remote installation methods for UNIX and Linux clients 138
Adding a UNIX/Linux client after initial server installation 141

Chapter 7 Configuring NetBackup 143

About NetBackup startup and shutdown scripts 143
About NetBackup server configuration 145
Starting the NetBackup Administration Console 146
About the Device Configuration Wizard 148
About the Volume Configuration Wizard 150
About the Catalog Backup Wizard 151
About the Backup Policy Configuration Wizard 152

Chapter 8 Removing NetBackup server and client software 154

About NetBackup server software removal on Linux systems 154
About NetBackup client software removal on UNIX and Linux systems 155
Removing NetBackup from UNIX and Linux servers and clients 156
About NetBackup server software removal on Windows systems 170
Removing NetBackup server and client software from Windows servers, clusters, and clients 171
About removal of the Java Console state data from Windows servers and Windows clients 174
Removing a clustered media server by migrating all data to a new media server 174

Chapter 9 Reference 175

Generate a certificate on the inactive nodes of a clustered primary server 176
NetBackup database user 177
About the NetBackup answer file 178
About the NetBackup IT Analytics Data Collector 206
Manually install or uninstall NetBackup IT Analytics Data Collector binaries 207
Manually configure the NetBackup IT Analytics Data Collector 208
Persistent Java Virtual Machine options 211
About RBAC bootstrapping 212
NetBackup primary server web server user and group creation 214
About the NetBackup Java Runtime Environment 216
Add or Remove Java GUI and JRE after install 218
Using NetApp disk arrays with Replication Director 219
Security updates to the NetBackup database 223
Size guidance for the NetBackup primary server and domain 223

Chapter 1

Preparing for installation

This chapter includes the following topics:

- General installation information
- Installation operational notes and limitations
- Performance and tuning considerations
- SORT information
- Veritas NetInsights Console information

General installation information

This guide is for new installations of NetBackup. Review this section for the general installation information that is related to NetBackup.

To upgrade NetBackup, see the *NetBackup Upgrade Guide*.

Available NetBackup installation methods

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

Table 1-1 Installation options

Installation type and operating system	Server	Client
Interactive UNIX and Linux	Primary server See "Installing NetBackup primary server software on Linux" on page 40. Media server See "Installing NetBackup media server software on Linux" on page 52.	See "Installing UNIX clients locally" on page 120.
Interactive Windows	Primary and media server See "Performing local, remote, or clustered server installation on Windows systems" on page 75.	See "Installing NetBackup Windows clients locally or remotely" on page 107.
Silent UNIX and Linux	Primary server See "Silently installing NetBackup primary server software on Linux" on page 47. Media server See "Silently installing NetBackup media server software on Linux" on page 60.	See "Install of the UNIX and Linux client binaries with native installers" on page 126.
Silent Windows	Primary and media server See "Installing NetBackup servers silently on Windows systems" on page 94.	See "Installing NetBackup Windows clients silently" on page 116.
Remote UNIX and Linux	Not a valid installation method.	SSH See "Installing client software with the ssh method" on page 139. SFTP See "Installing client software with the sftp method" on page 140.

Table 1-1 Installation options *(continued)*

Installation type and operating system	Server	Client
Remote Windows	Primary and media server See "Performing local, remote, or clustered server installation on Windows systems" on page 75.	See "Installing NetBackup Windows clients locally or remotely" on page 107.

About compatibility between NetBackup versions

You can run mixed versions of NetBackup between primary 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: NetBackup Snapshot Manager computer, primary server, media server, and then clients. For example, the scenario that is shown is supported: 10.2 NetBackup Snapshot Manager > 10.0 primary server > 9.0 media server > 8.3.0.1 client.

All NetBackup versions are four digits long. The NetBackup 10.0 release is the 10.0.0.0 release. Likewise, the NetBackup 9.1 release is the NetBackup 9.1.0.0 release. For the purposes of supportability, the fourth digit is ignored. A 9.1 primary server supports a 9.1.0.1 media server. An example of what is not supported is a 9.1 primary server with a 10.0 media server.

The NetBackup catalog resides on the primary server. Therefore, the primary 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 primary server to perform a catalog backup.

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

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

About NetBackup software availability

NetBackup 10.4 is available as ESD images for download from the **MyVeritas** webpage (https://my.veritas.com/). 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.

Required libraries missing from some Linux distributions

NetBackup runs prechecks at installation and upgrade to determine if certain required operating system libraries are present. To run that precheck, the `libnsl.so.1` and `libcrypt.so.1` libraries must be present. Before you attempt an installation or upgrade, Veritas recommends that you search your Linux computer for these libraries.

NetBackup requires other operating system libraries for NetBackup to run correctly. Some distributions of Linux have removed these libraries from their core distribution. The NetBackup precheck successfully determines if any of these libraries are not present and informs you at install or upgrade time.

How to install NetBackup

For new NetBackup installations, install the software in the following order:

Step 1	Install primary server software.
Step 2	
Step 3	Install the NetBackup Remote Administration Console (optional).
Step 4	Install client software.
Step 5	Install any NetBackup add-on products (such as language packages).

Before you proceed with any installation procedure, be sure to review the installation requirements.

See “Installation requirements for UNIX and Linux” on page 34.

See “Installation requirements for Windows and Windows clusters” on page 67.

About the NetBackup preinstall checker

The NetBackup installer includes a preinstall checker. This feature helps to determine if your computer is ready for a successful installation or upgrade.

The check runs automatically when you start an installation. The results of the check are shown at the following point:

- UNIX or Linux install script

After you accept the end user license agreement but before the installation starts.

- Windows installation wizard
  On the **Ready to Install the Program** screen, where the **Installation Summary** appears.

Additionally, you can run the preinstall checker through VxUpdate. See NetBackup Upgrade Guide for more information on using VxUpdate to run the check.

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:

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

About the NetBackup Product Improvement Program

The NetBackup Product Improvement Program captures installation deployment and product usage information.

During the NetBackup installation, you are enrolled in the NetBackup Product Improvement Program and send this information automatically and securely to Veritas. The information that Veritas receives becomes part of a continuous quality

improvement program that helps understand how customers configure, deploy, and use the NetBackup product. This information is then used to help Veritas identify improvements in product features, testing, technical support, and future requirements.

To learn more about the NetBackup Product Improvement Program, refer to the NetBackup license agreement section 17.18 Data Collection; Data Protection Regulations. The following describes where to find the license agreement:

- UNIX
  In the downloaded media images from **MyVeritas** (https://my.veritas.com/), see the file `LICENSE`.
- Windows
  From the downloaded media images from **MyVeritas**, start the installation wizard (`Browser.exe`). On the **Home** page, click **Installation**. On the **Installation** page, select either **Server Software Installation** or **Client Software Installation**. On the **Welcome** page, click **Next** to advance to the **License Agreement** page.

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 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 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 storage device configuration

Reliable use of NetBackup depends on the proper configuration of your storage devices. To ensure reliable backups and restores, you must first install and configure devices to work with the operating system.

Before you install NetBackup, use the following guidelines to configure storage devices to work with the operating system:

New installations	Before you install NetBackup, Veritas recommends that you install and configure your devices with the latest version of drivers.
Connections and settings	To prepare and connect new devices, perform the following tasks: ■ Set the SCSI ID (target). Make sure that it is set it to an available SCSI ID. ■ Physically attach your device to a compatible host bus adapter where that SCSI ID is available. Compatible means that both the device and the host bus adapter are of the same type. For example, single-ended, high-voltage differential, low voltage differential, or Fibre Channel.
Configuration	To configure storage devices to work with the operating system, refer to the following documentation: ■ The instructions from the device and the operating system vendors. ■ See the chapter in the NetBackup Device Configuration Guide that is appropriate for your operating system.
NetBackup installation	After all storage devices are installed, configured, and verified to work with the operating system, you can install NetBackup.

Warning: An improperly configured device can lead to backup failures, data loss, or both.

See “Installation requirements for UNIX and Linux” on page 34.

See “Installation requirements for Windows and Windows clusters” on page 67.

Locating supported robot types

You can find a list of the supported robot types in the *NetBackup Hardware and Cloud Storage Compatibility List (HCCL)*.

For your convenience, Veritas periodically updates this document on the Veritas support website

To find the latest robot types that this release supports

- Click on the following link to access the *NetBackup Hardware and Cloud Storage Compatibility List (HCCL)*:

  http://www.netbackup.com/compatibility

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 primary 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 primary 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.

NetBackup uses the certificates that are issued from either a NetBackup Certificate Authority or an external certificate authority for host authentication. If you intend to use external certificates on your primary server, you configure the certificates in a post-installation process. The media servers and the clients that use external certificates can either configure external certificates during the installation or upgrade, or after the installation or upgrade.

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.

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 supports the following certificate key sizes: 2048 bits, 4096 bits, and 8192 bits.

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, and 8192.

Caution: You should carefully choose the key size for your environment. Choosing a large key size may reduce performance. You should consider all factors to determine the correct key size for your environment.

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

Restrictions on the NetBackup installation directory

Each NetBackup supported file system defines restrictions on file and folder names for the installation folder. Consult the file system vendor provided documentation for more details on the file and the folder name restrictions.

Additionally, NetBackup supports only certain characters for the installation folder name. Use of non-supported characters can produce unexpected results and possibly result in lost data. The NetBackup supported characters for the installation folder are:

- UNIX and Linux
  The POSIX fully portable file name characters (`A-Z a-z 0-9 . _ -`)
- Windows
  The printable characters within the ASCII 7-bit range

Note: On Traditional Chinese and Korean versions of Windows, if the NetBackup client is installed to a path that contains a space, restore operations may fail. Paths such as `C:\Program Files` contain a space. Make sure to install the NetBackup client software to a path that does not contain a space on these versions of Windows.

Be aware that for Windows primary servers, if you install NetBackup into a directory name with two periods, some restore operations fail. Directory names such as `..foldername` or `folder..name` are examples of directories where a restore can fail.

The database user must own the NetBackup database directory. The user that owns the database directory must not change. The directory name itself must also not change. For Linux, the database folder is `/usr/openv/db/data`. For Windows, it is *`install_path`*`\NetBackupDB\data`.

NetBackup database is not supported on the `btrfs` file system

Veritas does not support the installation of the NetBackup database on a `btrfs` file system. Do not attempt to install the NetBackup database onto a `btrfs` file system. The database files reside on the primary server in the directories under `/usr/openv/db`. Before you attempt a NetBackup upgrade, move the database to a supported file system (such as `ext4` or `xfs`) before you start the upgrade. More information about moving the database before an upgrade is available in the NetBackup Upgrade Guide.

Installation operational notes and limitations

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

Windows compiler and security requirements for NetBackup 10.4 and later installation

NetBackup 10.4 and later for Windows uses the Visual Studio 2022 compiler and the Windows 11 Software Development Kit (SDK). To run NetBackup 10.4, Windows computers require Visual C++ run-time libraries version 14.36.32532 or later. Microsoft makes available the redistributable utilities that install these libraries. More information on these redistributable utilities is available.

https://visualstudio.microsoft.com/downloads

These utilities from Microsoft can alter Windows hosts such that a restart is required. The restart requirement can occur if the Visual C++ run-time libraries are in use by one or more processes on the system. Before you install NetBackup 10.4 or later, Veritas recommends that you install Visual Studio 2022 C++ run-time libraries on Windows computers. The installation of these libraries should take place within a maintenance window where you can safely restart the computer.

On Windows computers that do not have compatible Visual C++ run-time libraries present, the NetBackup installation process may offer to do it for you. You are required to acknowledge the risks and opt-in. More information about the risks and the opt-in process is available.

https://www.veritas.com/content/support/en_US/article.100062924

The redistributable utilities can fail or behave unexpectedly on hosts without all security updates in place. If a Windows host is not current with security updates, the following behaviors can occur:

- NetBackup's installation process fails shortly after start with a message about inability to deploy Visual Studio 2022 C++ run-time libraries.
- The `nbcertcmdtool` application fails unexpectedly when run 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.

Java GUI and JRE installation optional for some computers

Starting with NetBackup 8.3, the Java GUI and the JRE packages are optional for 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 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 install” on page 218.

Enable 8dot3 name file setting for the NetBackup primary servers

For primary servers only: To use the NetBackup Messaging Broker service you must enable the 8dot3 name file setting for the volume where NetBackup is installed. Use the Microsoft `fsutil` command to modify or confirm this setting.

NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952

All NetBackup server names must use a host name that is complaint with RFC 1123 ("Requirements for Internet Hosts - Application and Support") and RFC 952 ("DOD Internet Host Table Specification") standards. These standards include the supported and unsupported characters that can be used in a host name. For example, the underscore character (_) is not a supported character for host names.

More information is available about these standards and about this issue:

RFC 1123: http://www.ietf.org/rfc/rfc1123.txt

RFC 952: http://www.ietf.org/rfc/rfc952.txt

NetBackup Status Code 130 System Error Occurred: http://www.veritas.com/docs/000125019

Host ID-based certificate is not deployed during installation on 8.1 media server or client host with dual stack configuration

In the environment shown, the host ID-based certificate is not deployed:

- The NetBackup primary server is 8.1 or later with IPv6-only configuration.
- NetBackup 8.1 software is installed on a media server or a client host with dual stack configuration.

The host ID-based certificate is not deployed because the web service connection between the host and the primary server was not established.

Workaround: Manually deploy the host ID-based certificate to the 8.1 host after the installation. Refer to the article shown:

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

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.

SCCM and Chef deployment tools and documentation now available

With the NetBackup 8.1 release, Veritas now supports the use of System Center Configuration Manager (SCCM) and Chef for NetBackup deployment. Veritas has tested and validated several different deployment paths. Documentation and templates for both SCCM and Chef are available. See SORT for additional details around the support and use of SCCM and Chef.

Known SUSE Linux primary server install 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 installation.

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

```
NBPREINSTALL_CRITICAL_OVERRIDE=YES
```

Performance and tuning considerations

The *NetBackup Backup Planning and Performance Tuning Guide* provides environmental recommendations based on field experience. Your specific environment may require different considerations.

Administrators should use the guide to analyze, evaluate, and tune NetBackup performance in their specific NetBackup environment. Use the information that is presented to determine:

- Size requirements for the NetBackup primary server.
- The number of CPUs, disk drives, and tape drives required.
- How best to optimize of NetBackup for various workloads.
- Tuning parameters for maximum backup performance.

- Appropriate strategies for improved recovery time.
- Available tools to understand how NetBackup handles data.

For additional information, see the NetBackup Backup Planning and Performance Tuning Guide.

SORT information

Review this section for the details that are related to 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 new installations

Veritas recommends new NetBackup users perform the three 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. In addition, the procedures provide a helpful base of knowledge for other SORT functionality.

Table 1-2

Procedure	Details
Create a Veritas Account on the SORT webpage	See "To create a Veritas Account on the SORT page" on page 23.
Create generic installation reports	See "To create a generic installation checklist" on page 24.
Create system-specific installation reports	See "To create a system-specific installation report for Windows" on page 25. See "To create a system-specific installation report for UNIX or Linux" 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 generic installation checklist

1 In your web browser, navigate to:

https://sort.veritas.com/netbackup

2 Find and select the **Installation and Upgrade Checklist** widget.

3 Specify the requested information

Product	Select the appropriate product from the drop-down menu. For NetBackup select **NetBackup Enterprise Server** or **NetBackup Server**.
Product version you are installing or upgraded to	Select the correct version of NetBackup. The most current version is always shown at the top of the list.
Platform	Select the operating system that corresponds to the checklist you want generated.
Processor	Select the correct processor type for your checklist.
Product version you are upgrading from (optional)	For new installations, do not make any selections. For upgrades, you can select the currently installed version of NetBackup.

4 Click **Generate Checklist**.

5 A checklist corresponding to your choices is created. You can modify your selections from this screen, and click **Generate Checklist** to create a new checklist.

You can save the resulting information as a PDF. Numerous options are available for NetBackup and many of them are covered in the generated checklist. Please spend time reviewing each section to determine if it applies to your environment.

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 or Linux computers, you need the UNIX or Linux 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 or Linux computers, you need the UNIX or Linux 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.

Veritas NetInsights Console information

Veritas NetInsights Console is a new SaaS-based unified platform with Veritas products and features. It helps you manage your usage and your license entitlements as well as leverages product telemetry and support data to offer software and appliance insights.

The NetInsights Console delivers a cohesive experience and eliminates the need to switch between multiple products.

To connect to Veritas NetInsights Console, use the following URL:

https://netinsights.veritas.com

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, Complete, Enterprise, Enterprise Cloud or Data Mover Edition), 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.

For details on frequently asked questions, see the *Veritas Usage Insights for NetBackup Getting Started Guide*.

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 28.

For additional information about Veritas Usage Insights, see the Veritas Usage Insights for NetBackup Getting Started Guide

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 primary server must allow outbound `HTTPS` traffic to take advantage of the automatic upload feature. Manual uploads require `HTTPS` traffic from the upload location.

Chapter 2

NetBackup licenses

This chapter includes the following topics:

- About NetBackup license requirements
- About license entry
- Frequently asked questions about licenses

About NetBackup license requirements

To install NetBackup primary server software, you must enter a NetBackup product license.

Use the process that is shown to download NetBackup license files:

To download the NetBackup license file

1. Log on to your Veritas Support account (Veritas Support) with your username and password.
2. Select **Licensing**. This option takes you to the Veritas Entitlement Management System (VEMS).
3. Select **Entitlements** on the **VEMS** main menu.
4. Search the **Entitlements** page for the entitlement that you want to use to generate a license key.
5. Once you have located the entitlement, select the associated **Generate License** option.
6. Use the **Select Version** filter to view the list of license key options for the version of the product that you want to deploy.

7 Select the license key option in the table, specify the required information, and select **Generate**.

8 Select **Download File** to save the new license to your computer.

Note: More information about how to download license files is available: https://www.veritas.com/content/support/en_US/article.100048764

More information about licenses is available:
https://www.veritas.com/support/en_US/article.100058779

For detailed information on how to administer NetBackup licenses, refer to the *NetBackup Web UI Administrator's Guide*.

About license entry

Licenses for all purchased NetBackup SKUs must be entered on the primary server.

Enter licenses by using one of the following methods:

- During NetBackup primary server installation (recommended).
  The installer prompts you to enter the licenses for all NetBackup products that you plan to install.
- NetBackup web UI
  After NetBackup primary server installation, open the console and select **Settings > License Management**.
- Command-line interface (UNIX only)
  After NetBackup primary server installation, use the following command:

  ```
  /usr/openv/netbackup/bin/admincmd/get_license_key
  ```

Note: Veritas recommends the use of a browser and the NetBackup web UI to manage licenses remotely.

Frequently asked questions about licenses

Veritas customers have asked the following questions about how to manage licenses.

Table 2-1

Question	Answer
Is the license system for NetBackup the same as the license system in other Veritas products?	NetBackup uses a common license system that other Veritas products also use. Please remember, however, that the common license system provides flexibility in the license features that each product implements. For example, NetBackup does not have a node-locked license system, but some other products do.
What does the license file look like? What information does it contain?	The file is an `slf` file. The file contains information on the following: ■ Which report, Capacity or Traditional, is generated ■ The validity of the license, if it is evaluation or subscription ■ Service contract information ■ Customer account information ■ Whether the file is a perpetual file or an subscription file ■ Information about when the file was generated
Is the license file serialized?	No, it is an `slf` file with all relevant details.
Can I see reports on what licenses I have?	Yes. Information about licenses is stored on the primary server. To access the information, open the NetBackup web UI and select **Settings > License management**. On UNIX servers, you can also run the following command: `/usr/openv/netbackup/bin/admincmd/get_license_key` For more information on how to view reports, refer to the *NetBackup Web UI Administrator's Guide*.
How do I enable options and agents?	When you install NetBackup, you are prompted to enter the license files for all options and agents. If you purchase an agent or other add-on product at a later date, you can enter its license file manually. Open the NetBackup web UI and select **Settings > License management**. On UNIX servers, you can also run the following command: `/usr/openv/netbackup/bin/admincmd/get_license_key`
Should I save the license files after they have been entered?	It is unnecessary to save the license files. They are always available to view and download on the VEMS **License Keys** page. For more details refer them to the VEMS user's guide: https://www.veritas.com/content/support/en_US/article.100048764

Table 2-1 *(continued)*

Question	Answer
What should I do if I have lost my license information?	Veritas has a record of all license files that are issued to customers. You can view these files on the VEMS **License Keys** page. More information is available: https://www.veritas.com/content/support/en_US/article.100048764 If you have purchased NetBackup from a Veritas partner, you need to contact that partner for information on your license.
Do I need a license to enable NetBackup Remote Administration Consoles?	No. NetBackup Remote Administration Consoles do not require special licenses. You can install them on any computer with access to the primary server.
Can a license be used multiple times?	Yes. You can use your licenses multiple times. You are, however, legally bound to install and use only the entitled capacity FETB or the number of NetBackup servers, clients, agents, and options for which you purchase licenses.
How do existing customers get licenses?	More information about how to download license keys is available. See “About NetBackup license requirements” on page 29. You can also review the website shown: https://www.veritas.com/support/en_US/article.100058779 If your maintenance is through a Veritas partner, you upgrade through the partner. Contact the partner for more details.
What if I do not get the right licenses?	Contact Customer Care at the website that is shown: https://www.veritas.com/content/support/en_US/contact-us
What does an evaluation license enable?	The evaluation license enables unrestricted use of NetBackup, its agents, and its options for a predetermined period of time.
Am I notified when an evaluation is about to expire?	To find out when a license expires, open the NetBackup web UI and select **Settings > License management**. You also receive a pop-up notification that evaluation license is about to expire. On UNIX servers, you can also run the following command: `/usr/openv/netbackup/bin/admincmd/get_license_key`

Table 2-1 *(continued)*

Question	Answer
What happens when an evaluation license expires?	The NetBackup services or daemons are shut down. When you attempt to use the product you are informed that its evaluation period has expired.
Does NetBackup save the backup configuration and catalog information when evaluation license expire?	Yes. Customers who add a perpetual or subscription license to an evaluation version of NetBackup have immediate access to their catalog information and configuration information.
How do I upgrade from an evaluation license to a perpetual or subscription license?	It is easy. When you purchase a perpetual or subscription license, you add that license to NetBackup. All the configuration information and catalog data from your evaluation version is retained. To enter your perpetual or subscription license, open the NetBackup web UI and select **Settings > License management**. If your evaluation license is expired, you must use the `bpminlicense` command to add licenses. Refer to the *NetBackup Commands Reference Guide* for more details. On UNIX servers, you can also run the following command: `/usr/openv/netbackup/bin/admincmd/get_license_key`

Chapter 3

Installing server software on UNIX systems

This chapter includes the following topics:

- Installation requirements for UNIX and Linux
- How the installation script works
- Installing NetBackup primary server software on Linux
- Installing NetBackup media server software on Linux
- About pushing client software from a primary server to clients

Installation requirements for UNIX and Linux

Table 3-1 describes the requirements to prepare your UNIX and Linux 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.

Table 3-1 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

Table 3-1 NetBackup requirements for UNIX and Linux *(continued)*

Check	Requirement	Details
	Memory	Use the information that is shown to correctly size your server: ■ The SORT website. See "About Veritas Services and Operations Readiness Tools" on page 22. ■ General details on how to size your NetBackup environment. See "Size guidance for the NetBackup primary server and domain" on page 223. ■ Detailed information about planning and tuning your NetBackup environment are available. These details are found in the *NetBackup Backup Planning and Performance Tuning Guide*.
	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 10.4 ■ 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 primary 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 10.4. ■ 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 3-1 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 Primary 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 files that are shown are present and installed if necessary. If any file is not present, install the one provided by your operating system. ■ `libnsl.so.1` ■ `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 3-1 NetBackup requirements for UNIX and Linux *(continued)*

Check	Requirement	Details
	Web Services	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). You must create these required account elements before installation. More information is available: See "NetBackup primary server web server user and group creation" on page 214. **Note:** Veritas recommends 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 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.

Do not mix non-English versions of Windows and UNIX platforms unless primary and media servers are NetBackup appliances

Do not mix non-English versions of Windows and UNIX platforms unless your primary servers and media servers are NetBackup appliances. If you mix non-English versions of Windows and UNIX platforms, differences in operating system architecture and encodings may cause non-ASCII file names and folder names to display incorrectly within the user interface. This issue may cause functional failures.

NetBackup installations on environments that run different versions of UNIX-based operating systems

NetBackup can be installed in environments that run different versions of UNIX-based operating systems as long as the system locales are identical. The use of different locales across UNIX platforms may cause non-ASCII file names and folder names to display incorrectly within the user interface. This issue may cause functional failures.

Special installation guidelines for Solaris systems

Several kernel-tunable parameters, such as Message Queue, Semaphore, and Shared Memory Parameters, can affect NetBackup performance. If you adjust these values, you may prevent your system performance from slowing down or even reaching a deadlock state.

More information about tunable parameters is available online.

- Recommended NetBackup *NIX semaphore tuning values (Linux and Solaris)
  http://www.veritas.com/docs/000081309
- Tuning Solaris 10 for NetBackup
  http://www.veritas.com/docs/000035120

Special installation guidelines for Linux clustered environments

Use the following guidelines when you install NetBackup in clustered systems:

- Ensure that each node in the NetBackup cluster can run the `ssh` command. The root user must be able to perform a remote login to each node in the cluster without entering a password. This remote login is necessary for installation and configuration of the NetBackup server and any NetBackup options. After installation and configuration are completed, it is no longer required.
- You must install, configure, and start the cluster framework before you install NetBackup. For additional installation prerequisites and installation notes, see the NetBackup Clustered Primary Server Administrator's Guide.
- You must have defined a virtual name using DNS, NIS, or `/etc/hosts`. The IP address is defined at the same time. (The virtual name is a label for the IP address.) Use this virtual name and IP address only for the NetBackup resource.

How the installation script works

When you install NetBackup server software, client software is also installed.

When you install NetBackup 10.4, the following options are also installed if the platform supports them:

- BMR Primary Server
- NDMP
- Veritas Product Authentication and Authorization (NetBackup Access Control)
- Vault
- BMR Boot Server
- DB2
- Encryption
- Informix
- VxUpdate agent
- Lotus Notes
- Oracle
- SAP
- Snapshot Client
- Sybase

Each option must also be configured as needed.

In addition to server software and options, the installation script performs the following tasks:

Host names	Places the host name in the `/usr/openv/netbackup/bp.conf` file on the server. For clustered environments, the script places the virtual host name in the `/usr/openv/netbackup/bp.conf` file on the server.
Automatic startup and shutdown scripts	Adds the automatic startup and shutdown scripts to the appropriate directories on the various supported platforms.

PBX	If the computer where you install NetBackup does not already have PBX and the platform supports it, the installation script installs PBX. If PBX already exists on the computer, the installation script performs one of the following tasks: ■ Updates the existing version if it is older than the version that is included with 10.4. ■ Does not update PBX if the existing version is the same or later than the version that is included with 10.4.

Installing NetBackup primary server software on Linux

The primary server manages backups, archives, and restores. The primary server is where the NetBackup catalog resides which includes the internal databases that contain information about NetBackup configuration and backups.

Veritas supports two primary server installation methods: either the NetBackup installation script or the native Linux installers. The NetBackup installation script is the standard installation method and is recommended for new users. The native Linux installers are potentially more difficult and require additional steps.

Customers who use the NetBackup installation script for their Linux primary servers 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.

Use the following guidelines for a new primary server installation:

Designate primary server	Designate the computer that you want to be the primary server and install the primary server software on that computer first.

Licenses	You must add either a NetBackup license file or an evaluation license during primary server installation. More information is available: https://www.veritas.com/support/en_US/article.100058779 If you do not have the license downloaded, you can use the evaluation license that is valid for 60 days from the date of installation. Services stop working after that period is over. You can use this license by answering **Yes** when prompted to install the evaluation license. For more information on how to administer NetBackup licenses, see the *NetBackup Web UI Administrator's Guide*.
Installation method	Available installation methods include: ■ NetBackup installation script See "To install NetBackup primary server software" on page 41. ■ Native Linux installers See "Silently installing NetBackup primary server software on Linux" on page 47.

To install NetBackup primary server software

1. Log in to the server 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 1993 - 2016 Veritas Corporation, All Rights Reserved.


        Installing NetBackup Server 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 out the Veritas Services and
Operations Readiness Tools (SORT) Installation and Upgrade Checklist
and Hot fix and EEB Release Auditor, respectively, at
https://sort.veritas.com/netbackup.

ATTENTION!  To help ensure a successful upgrade to NetBackup 10.4,
please visit the NetBackup 8.x Upgrade Portal:
http://www.veritas.com/docs/000115678.

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

4 When the following message appears press **Enter** to continue:

```
Is this host a primary server? [y/n] (y)
```

5 If you need to perform a disaster recovery of your primary server, select **y** when prompted. Press **Enter** for the default **N**.

```
Are you currently performing a disaster recovery of a primary
server? [y/n] (n)
```

The disaster recovery process requires additional steps and information that is not covered in this manual. More information is available.

NetBackup Troubleshooting Guide

6 When this message appears, provide the name of the service user account to be used to start most of the daemons.

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

Be aware of the following:

- You cannot use the root user as the service user.
- The `nbwebsvc` user should not be used as the service user.
- `nbwebgrp` 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 here during installation.
- If you want to change the service user account after the installation, use the `nbserviceusercmd --changeUser` command.
- The service user and service user ID must be same on all nodes of cluster.

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

If you enter root as the service user, you see the message shown:

```
ATTENTION! The NetBackup services currently use a root system
account, which is not recommended.
NetBackup is unable to use this account for the new scale-out
database server process.
Provide an alternative account name that meets the following
criteria:
- Root accounts are not allowed.
- The username must be 1-31 characters.
- The username must contain only English characters.
- The nbwebsvc user should not be used as the scale-out database
user.
For more details, see the article: https://www.veritas.com/docs/100053091

Enter the name of the system account which will own the
scale-out database server process:
```

7 For the NetBackup installation location, enter the appropriate platform information as follows:

- When the following question appears, press **Enter** to accept the default (**y**).

```
The NetBackup and Media Manager software is built
for use on <platform> hardware. Do you want to install
NetBackup and Media Manager files? [y,n] (y)
```

- When the following question appears, select where to install NetBackup and Media Manager software:

```
NetBackup and Media Manager are normally
installed in /usr/openv.
Is it OK to install in /usr/openv? [y,n] (y)
```

To accept the default (**y**), press **Enter**.
To change the installation location, type **n** and press **Enter**. Then enter the appropriate destination.
Additional information about installation folder restrictions is available.
See "Restrictions on the NetBackup installation directory" on page 17.

8 Enter the NetBackup Enterprise server license.

Provide an answer to `Are the license files downloaded from the Veritas licensing portal? (y/n):` when prompted.

- If you reply `y`, you are prompted to provide the file path to the license file.

```
Enter the license file name including the path (for example -
/usr/openv/slic.slf):
```

After you provide the license file path, reply `y` to add this license file:

```
Do you want to add this license? (y/n):
```

If you reply `n`, you are prompted if you want to use an evaluation license.
If you answer `y`, an evaluation license valid for 60 days is installed. More information is available:
https://www.veritas.com/support/en_US/article.100058779.
If you answer `n`, the installer cannot proceed without a license and it exits gracefully.

9 Provide an answer when prompted to add additional license files.

```
All additional licenses should be added at this time.

Do you want to add additional licenses now? [y,n] (y)
```

- If you answer `y`, provide the required license file information, and then enter `q` to quit the utility and proceed with the installation.
- If you answer `n`, the installer provides information about how to add license information from the command line and proceeds.

10 Verify or enter the correct computer name when prompted by the following message:

```
Installing NetBackup Enterprise Server version: 10.4
If this machine will be using a different network interface than
```

```
the default (name), the name of the preferred interface
should be used as the configured server name. If this machine
will be part of a cluster, the virtual name should be used as the
configured server name.
The domainname of your server appears to be "domain". You
may choose to use this domainname in your configured NetBackup
server name, or simply use "name" as the configured
NetBackup server name.
Would you like to use "name.domain" as the configured NetBackup server
name of this machine? [y, n] (y)
```

Note: Incorrect information for the domain name results in failures during the configuration of Authentication Broker and NetBackup Access Controls. To correct this problem, use the `bpnbaz -configureauth` command to configure Authentication Broker. More information about the `bpnbaz -configureauth` command is available.

NetBackup Commands Reference Guide

- To accept the displayed (default) name, press **`Enter`**.
- To change the displayed (default) name, type **`n`** and enter the name that you want.
- For a clustered NetBackup server, enter the virtual name for the NetBackup server and not the actual local host name.

11 Identify or verify the primary server by answering the following question when it appears:

```
Is <name> the primary server? [y, n] (y)
```

- To accept the displayed name (which is the name that you identified in the previous step), press **`Enter`**.
- If you entered a virtual name for the server in the previous step, the installation script presents the following question:

  ```
  Is this server part of a cluster installation?
  ```

  If the answer is yes, press **`y`** and answer the series of cluster configuration questions that appear.
  If the answer is no, press **`n`**.

12 Identify whether there are any media servers for this primary server by answering the following question when it appears:

```
Do you want to add any media servers now? [y, n] (n)
```

- If there are no media servers for this primary server, press **Enter** and proceed to the next step.
- If there are media servers for this primary server, type **y** and enter the name of each media server.
  When you enter the media server names, you must enter the computer name and the domain name. For example:

  alpha.domain.com

  Where `alpha` is the computer name and `domain.com` is the domain name.
  The media server names that you enter here are added to the `bp.conf` file on the primary server, automatically. After you install the media server software later, the primary server can then communicate with the media servers immediately.
- To add a media server to an existing and an operational NetBackup environment, you cannot use the procedures in this guide. For complete details on how to add a media server to an existing and an operational NetBackup environment, see the NetBackup Administrator's Guide, Volume I.

13 When the following message appears, press **Enter** and accept the default name of the EMM server. You must configure EMM on the primary server. All primary servers must have their own EMM configuration. Remote EMM or shared EMM is no longer supported.

```
NetBackup maintains a centralized catalog (separate from the
image catalog) for data related to media and device
configuration, device management, storage units, hosts and host
aliases, media server status, NDMP credentials, and other
information. This is managed by the Enterprise Media Manager
server.
Enter the name of the Enterprise Media Manager (default: <name>)
```

14 Answer the following question when it appears:

```
Do you want to start the NetBackup job-related processes so backups and
restores can be initiated? [y, n] (y)
```

- If you have (or want to have) a clustered NetBackup server, type **n**.
- For non-clustered installations, press **Enter** to accept the default answer (**y**) and start the NetBackup processes and the EMM server.

You must start these processes now because the EMM server must be running when you install any media servers later.

15 For a clustered NetBackup primary server, repeat these steps on every node on which you want to run NetBackup.

16 (Conditional) On a clustered NetBackup primary server, you must obtain the Certificate Authority certificate and the host certificate for each inactive node. More information is available:

See "Generate a certificate on the inactive nodes of a clustered primary server" on page 176.

17 After your initial installation is complete, you can install any other NetBackup add-on products (such as language packages).

18 (Conditional) If you use an external certificate authority (ECA) in your environment, 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.

19 (Conditional) If you plan to configure customized settings for your Tomcat web server, determine if those settings can persist across upgrades. More information is available:

See "Persistent Java Virtual Machine options" on page 211.

20 Complete the NetBackup installation as indicated.

See "Continuing with NetBackup software installation" on page 51.

Silently installing NetBackup primary server software on Linux

This section describes how to install a new NetBackup primary server. Veritas supports two primary server installation methods: either the NetBackup installation script or the native Linux installers. The NetBackup installation script is the standard installation method and is recommended for new users. The native Linux installers are potentially more difficult and require additional steps. You must still use the NetBackup installation script for cluster servers and disaster recoveries.

- For Linux: `rpm`, `yum`, etc.

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

To install the Linux primary server binaries using native installers:

1. Please create the NetBackup installation answer file (`NBInstallAnswer.conf`) in the primary server's temporary directory. That directory is usually the `/tmp` directory. More information about the answer file and its contents is available.

   See "About the NetBackup answer file" on page 178.

2. Populate `NBInstallAnswer.conf` with the following required information:

   ```
   SERVER=primary_server_name
   CLIENT_NAME=primary_server_name
   MACHINE_ROLE=PRIMARY
   LICENSE=EVALUATION | license_file_path
   SERVICE_USER=service_user
   ```

   Note: If the `SERVICE_USER` account is root, you must include the `DATABASE_USER=database_user` keyword, and provide a non-root account.

   For primary servers, the name that is specified in the `CLIENT_NAME=` line should match the first `SERVER=` line.

   To enter multiple licenses, provide a separate `LICENSE=license_file_path` for each license.

3. You can add optional parameters to the `NBInstallAnswer.conf` file. The parameters that are shown are examples of some of the parameters you can add. Veritas recommends that you review the NetBackup answer file section that is included in this documentation:

   - `INSTALL_PATH`
   - Additional `LICENSE` entries
   - Additional `SERVER` entries
   - `WEBSVC_GROUP`
   - `WEBSVC_USER`
   - `DATABASE_USER`
   - `VXDBMS_POSTGRESQL_POOLER_ODBC_PORT`

   See "About the NetBackup answer file" on page 178.

4. (Conditional) If you want to assign RBAC security and backup administration roles to a user or a user group, populate `NBInstallAnswer.conf` with the following required information:

   - `RBAC_DOMAIN_TYPE`

Use this field to specify the domain type to which the user or the user group belongs. The following `RBAC_DOMAIN_TYPE` values are supported: `NT, VX, UNIXPWD, LDAP`.

- `RBAC_DOMAIN_NAME`
  Use this field to specify the name of the domain to which the user or the user group belongs.
- `RBAC_PRINCIPAL_TYPE`
  Use this field to specify `USER` or `USERGROUP`.
- `RBAC_PRINCIPAL_NAME`
  Use this field to specify the user name or the user group.

More information about the `RBAC_*` options is available.

See "About RBAC bootstrapping" on page 212.

See "About the NetBackup answer file" on page 178.

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

Extract the contents of the server package file. Example:

- For Linux RedHat:
  ```
  tar -xzvf NetBackup_10.4_LinuxR_x86_64.tar.gz
  ```
- For Linux SuSE:
  ```
  tar -xzvf NetBackup_10.4_LinuxS_x86_64.tar.gz
  ```

6 Change to the directory for your desired operating system and copy server files to computer to be installed.

Operating system directory:

- For Linux RedHat:
  ```
  NetBackup_10.4_LinuxR_x86_64/linuxR_x86/anb
  ```
- For Linux SuSE:
  ```
  NetBackup_10.4_LinuxS_x86_64/linuxS_x86/anb
  ```

Copy server files to machine to be installed:

Linux

- `VRTSnbmqbrkr.rpm`
- `VRTSnbprimary.rpm`
- `VRTSnbslibs.rpm`
- `VRTSnbweb.rpm`

- VRTSnetbp.rpm
- VRTSpddei.rpm
- VRTSpddes.rpm
- VRTSpostgresql.rpm

7 Extract the client binaries and copy them to the primary server.

Extract the client binaries:

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

Change directory to your desired operating system:

- RedHat: `openv/netbackup/client/Linux/RedHat3.10.0`
- SuSE: `openv/netbackup/client/Linux/SuSE3.0.76`

Copy the files that are shown to the primary server.

- VRTSnbpck.rpm
- VRTSpbx.rpm
- VRTSnbclt.rpm
- VRTSnbclibs.rpm
- VRTSnbjre.rpm
- VRTSnbjava.rpm
- VRTSpddea.rpm
- VRTSnbcfg.rpm
- VRTSpddeu.rpm

8 (Conditional) To install NetBackup IT Analytics Data Collector:

- Create the `/usr/openv/tmp` directory with the `mkdir -p /usr/openv/tmp` command.
- Copy the `ita_dc.tar.gz` tarball from the media's `/catalog/anb/` directory to `/usr/openv/tmp`.
- Verify the `INSTALL_ITA_DATA_COLLECTOR` value is set to `YES` in the `NBInstallAnswer.conf` file.
  If you do not want to install NetBackup IT Analytics Data Collector, make sure the `INSTALL_ITA_DATA_COLLECTOR` value is set to `NO` in the `NBInstallAnswer.conf` file.

9 Install the files in the order that is shown with the commands that are shown:

RedHat Linux

```
rpm -U VRTSnbpck.rpm
rpm -U VRTSpbx.rpm
rpm -U VRTSnbclt.rpm
rpm -U VRTSnbclibs.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjava.rpm
rpm -U VRTSpddes.rpm
rpm -U VRTSpddeu.rpm
rpm -U VRTSpddea.rpm
rpm -U VRTSnbcfg.rpm
rpm -U VRTSpostgresql.rpm
rpm -U VRTSnetbp.rpm
rpm -U VRTSnbprimary.rpm
rpm -U VRTSnbmqbrkr.rpm
rpm -U VRTSnbweb.rpm
rpm -U VRTSnbslibs.rpm
```

SuSE Linux

```
rpm -U VRTSnbpck.rpm
rpm -U VRTSpbx.rpm
rpm -U VRTSnbclt.rpm
rpm -U VRTSnbclibs.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjava.rpm
rpm -U VRTSpddeu.rpm
rpm -U VRTSpddea.rpm
rpm -U VRTSpddes.rpm
rpm -U VRTSnbcfg.rpm
rpm -U VRTSpostgresql.rpm
rpm -U VRTSnetbp.rpm
rpm -U VRTSnbprimary.rpm
rpm -U VRTSnbmqbrkr.rpm
rpm -U VRTSnbweb.rpm
rpm -U VRTSnbslibs.rpm
```

10 If you decide to install the Java GUI or the JRE after the installation completes, additional information is available.

See "Add or Remove Java GUI and JRE after install" on page 218.

Continuing with NetBackup software installation

After you have installed the primary server software, you are ready to install media server software or client software depending on your environment.

- If you have media servers in your system, you are ready to install media server software.
  See "Installing NetBackup media server software on Linux" on page 52.
- If there are no media servers in your environment, you are ready to install client software on client computers.
  - See "Installing UNIX clients locally" on page 120.
  - To install client software on clients from the primary server location (recommended), you must first install the client type software on the primary server.
    See "Installing client type software on a primary server" on page 65.

Installing NetBackup media server software on Linux

This section describes how to install a new NetBackup media server. After you have installed the primary server, you are ready to install media server software on media server computers. Use this information to install the server software on a computer with no existing version of NetBackup.

Veritas supports two media server installation methods: either the NetBackup installation script or the native Linux installers. The NetBackup installation script is the standard installation method and is recommended for new users. The native Linux installers are potentially more difficult and require additional steps.

Customers who use the NetBackup installation script for their Linux media servers 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.

Media server software manages the robotic and the storage devices within your NetBackup environment.

You can use the `nbserviceusercmd` command to change the service user on media servers after the installation completes. Refer to the *NetBackup Commands Reference Guide* for more information about the `nbserviceusercmd` command. For more details about the service user account, refer to https://www.veritas.com/support/en_US/article.100053035.

Use the following guidelines when you install new media servers:

Designate media servers	Designate the computers that you want to be media servers and install the media server software on them.

CA Certificate fingerprint	If you use a NetBackup Certificate Authority, you must know the CA Certificate fingerprint of the primary 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	In some cases, if you use a NetBackup Certificate Authority, the installer requires an authorization token to successfully deploy security certificates. This requirement only applies if you use a NetBackup Certificate Authority. 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
External certificate authority	If you use an external certificate authority (ECA), you need to know the location of your certificate. You also need know how you want to configure the Certificate Revocation Lists (CRLs).
Install method	■ NetBackup installation script See "To install NetBackup media server software with the NetBackup installation script" on page 53. ■ Native Linux installers See "Silently installing NetBackup media server software on Linux" on page 60.
Java GUI and JRE	Installation of the Java GUI and the JRE is optional. Decide if you want to install the Java GUI and JRE on this computer. If you change your mind after the installation completes, you can add or remove the Java GUI and the JRE after the installation. More information about the Java GUI and the JRE is available. See "Add or Remove Java GUI and JRE after install" on page 218.

To install NetBackup media server software with the NetBackup installation script

1. Log in to the server 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 1993 - 2016 Veritas Corporation, All Rights Reserved.


        Installing NetBackup Server 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 out the Veritas Services and
Operations Readiness Tools (SORT) Installation and Upgrade Checklist
and Hot fix and EEB Release Auditor, respectively, at
https://sort.veritas.com/netbackup.

ATTENTION!  To help ensure a successful upgrade to NetBackup 10.4,
please visit the NetBackup 8.x Upgrade Portal:
http://www.veritas.com/docs/000115678.

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

4 Indicate if the current computer is the primary server by answering the following question when it appears:

```
Is this host the primary server? [y,n]
```

5 Verify or enter the correct computer name when prompted by the following message:

```
Installing NetBackup Enterprise Server version: 10.4
If this machine will be using a different network interface than
the default (name), the name of the preferred interface
should be used as the configured server name. If this machine
will be part of a cluster, the virtual name should be used as the
configured server name.
The domainname of your server appears to be "domain". You
may choose to use this domainname in your configured NetBackup
server name, or simply use "name" as the configured
NetBackup server name.
```

```
Would you like to use "name" as the configured NetBackup server
name of this machine? [y, n] (y)
```

Note: Incorrect information for the domain name results in failures during the configuration of Authentication Broker and NetBackup Access Controls. To correct this problem, use the `bpnbaz -configureauth` command to configure Authentication Broker. More information about the `bpnbaz -configureauth` command is available.

NetBackup Commands Reference Guide

- If the displayed (default) media server name is correct, press **Enter**.
- If the displayed (default) media server name is not correct, type **n** and enter the correct name.

6 Identify the name of the primary server when prompted with this question:

```
What is the fully qualified name of the primary server?
```

If the primary server is clustered, enter the virtual name of the primary server.

7 For the NetBackup installation location, enter the appropriate platform information as follows:

- When the following question appears, press **Enter** to accept the default (**y**).

```
The NetBackup and Media Manager software is built
for use on <platform> hardware. Do you want to install
NetBackup and Media Manager files? [y,n] (y)
```

- When the following question appears, select where to install NetBackup and Media Manager software:

```
NetBackup and Media Manager are normally
installed in /usr/openv.
Is it OK to install in /usr/openv? [y,n] (y)
```

  To accept the default (**y**), press **Enter**.

  To change the installation location, type **n** and press **Enter**. Then enter the appropriate destination.

Additional information about installation folder restrictions is available.

See "Restrictions on the NetBackup installation directory" on page 17.

8 After you confirm the installation location for the binaries, the installer fetches the certificate authority certificate details.

```
Getting CA certificate mode from the primary server.
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.

9 The installer then looks to see what certificate authority the local system is configured to use. The options for certificate authority on the local system are: NetBackup Certificate Authority, external certificate authority, or indeterminate.

The installer then uses a combination of the primary server certificate authority mode and the local system certificate authority configuration to determine the next steps.

10 If the installer prompts you for a certificate file path, your environment uses an external certificate authority. Proceed to step 11.

If the installer prompts you for fingerprint information, your environment uses a NetBackup Certificate Authority. Proceed to step 17.

If the installer cannot determine the configuration of the certificate authority on the primary server, you are presented with two options:

- Skip the security configuration and configure your certificate authority after installation. More information about post-installation certificate authority 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.
  Proceed to step 21.
- Exit the installation and restart the installation once you configure your certificate authority.

11 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.

12 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):
```

13 (Conditional) If you specify 2, you must enter the path to the CRL location:

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

14 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.
```

15 (Conditional) 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) Update external certificate values.
3) Abort the installation.
Default option (1):
```

Proceed to step 21.

16 (Conditional) 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):
```

Proceed to step 21.

17 When prompted, review the fingerprint information and confirm that it is accurate.

```
Primary server [primary_name] reports the following CA Certificate
fingerprints:
SHA-256 Fingerprint: [sha-256_fingerprint],
SHA-1 Fingerprint: [sha-1_fingerprint].
Is this correct?
```

After you confirm the fingerprint information, the installer stores the certificate authority certificate details.

```
Storing CA certificate.
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.

18 After the Certificate Authority certificate is stored, the installer fetches the host certificate.

```
Getting host certificate.
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.

19 (Conditional) If prompted for the Authorization Token, please enter it.

```
An authorization token is required in order to get the host
certificate for this host. At the prompt, enter the authorization
token or q to skip the question. NOTE: The answer entered will
not be displayed to the terminal.

Enter the authorization token for primary_server_FQDN or q to
skip:
```

20 When prompted, specify if you want Java GUI and the JRE packages installed.

```
The Java GUI and JRE packages are currently not installed 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) Include the Java GUI and JRE.

2) Exclude the Java GUI and JRE.
```

If you specify `1`, you see: `Including the installation of Java GUI and JRE packages`. If you specify 2, you see: `Excluding the installation of Java GUI and JRE packages`.

21 When the following message appears, press **Enter** and accept the default name of the EMM server. You must configure EMM on the primary server. All primary servers must have their own EMM configuration. Remote EMM or shared EMM is no longer supported.

```
Enter the name of the Enterprise Media Manager (default: <name>)
```

The primary server name is displayed by default.

22 Repeat steps 1 through 21 to install media server software on any remaining media servers.

Silently installing NetBackup media server software on Linux

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

For Linux: `rpm`, `yum`, etc.

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

To install 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 178.

2. Populate `NBInstallAnswer.conf` with the following required information:

   ```
   SERVER=primary_server_name
   CLIENT_NAME=media_server_name
   MACHINE_ROLE=MEDIA
   ```

   Be aware you can use `CLIENT_NAME=XLOCALHOSTX` instead of stating the media server name explicitly.

3. (Conditional) If your environment uses a NetBackup Certificate Authority, 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 178.

4. (Conditional) If your environment uses an external certificate authority, 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.

- 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.

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

- INSTALL_PATH
- Additional SERVER entries

More information about each option is available.

See "About the NetBackup answer file" on page 178.

6 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_10.4_LinuxR_x86_64.tar.gz
  ```

- For Linux SuSE:

  ```
  tar -xzvf NetBackup_10.4_LinuxS_x86_64.tar.gz
  ```

7 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_10.4_LinuxR_x86_64/linuxR_x86/anb
  ```

- For Linux SuSE:

  ```
  NetBackup_10.4_LinuxS_x86_64/linuxS_x86/anb
  ```

Copy server files to the computer to be installed

- Linux: `VRTSnetbp.rpm`, `VRTSnbslibs.rpm`, and `VRTSpddes.rpm`
- Linux Red Hat: `VRTSpddei.rpm`

8 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/RedHat3.10.0`
- SuSE: `openv/netbackup/client/Linux/SuSE3.0.76`

Copy the files that are shown to the media server.

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

- `VRTSnbpck.rpm`
- `VRTSpbx.rpm`
- `VRTSnbclt.rpm`
- `VRTSnbclibs.rpm`
- `VRTSnbjre.rpm`
- `VRTSnbjava.rpm`
- `VRTSpddea.rpm`
- `VRTSnbcfg.rpm`
- `VRTSpddeu.rpm`

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

RedHat Linux

```
rpm -U VRTSpbx.rpm
rpm -U VRTSnbclt.rpm
rpm -U VRTSnbclibs.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjava.rpm
rpm -U VRTSpddes.rpm
rpm -U VRTSpddeu.rpm
rpm -U VRTSpddea.rpm
rpm -U VRTSpddei.rpm (optional)
rpm -U VRTSnbcfg.rpm
rpm -U VRTSnetbp.rpm
rpm -U VRTSnbslibs.rpm
```

SuSE Linux

```
rpm -U VRTSnbpck.rpm
rpm -U VRTSpbx.rpm
rpm -U VRTSnbclt.rpm
rpm -U VRTSnbclibs.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjava.rpm
rpm -U VRTSpddeu.rpm
rpm -U VRTSpddea.rpm
rpm -U VRTSpddes.rpm
rpm -U VRTSnbcfg.rpm
rpm -U VRTSnetbp.rpm
rpm -U VRTSnbslibs.rpm
```

10 If you decide to install the Java GUI or the JRE after the installation completes, additional information is available.

See "Add or Remove Java GUI and JRE after install" on page 218.

About pushing client software from a primary server to clients

You can increase the speed of client installation by pushing the software from the primary server to the clients. This method eliminates the need for a local installation at each client.

The following describes how to prepare your NetBackup environment for client software installation from the primary server.

- Install the client type software on the primary server. Be sure to install all of the client types that pertain to your NetBackup configuration.
  See "Installing client type software on a primary server" on page 65.
- Before you can push client software from the primary server, each client name must be assigned to a NetBackup policy. Policies are created on the primary server.
  When you create a policy, you must identify the policy type, which indicates the operating system on the clients that are assigned to that policy. Without a policy, the remote installation (or push) fails because the primary server does not know the operating system of the client.
  For information on how to create NetBackup policies, refer to the NetBackup Administrator's Guide, Volume I.
- After the required policies are created, you can push client software from the primary server to the clients.
  See "About remote installation methods for UNIX and Linux clients" on page 138.

Installing client type software on a primary server

Client type software must be installed on the primary server to perform the following operations:

- Assign clients to NetBackup policies so that those clients can be backed up.
- Install (or push) client software from the primary server to clients.
  For each UNIX client type, the client installation script lets you install the client software onto the primary server. You can then install (or push) the client software from the primary server to the clients.

To install client type software on a primary server

1. Log in to the server 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 1993 - 2016 Veritas Corporation, 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 out the Veritas Services and
Operations Readiness Tools (SORT) Installation and Upgrade Checklist
and Hot fix and EEB Release Auditor, respectively, at
https://sort.veritas.com/netbackup.

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

4 Select all of the client types that you want to install and follow the installation prompts.

Chapter 4

Installing server software on Windows systems

This chapter includes the following topics:

- Installation requirements for Windows and Windows clusters
- Requirements for Windows cluster installations
- Performing local, remote, or clustered server installation on Windows systems
- Post-installation tasks for NetBackup cluster environments
- Verifying Windows cluster installations or upgrades
- Installing NetBackup servers silently on Windows systems

Installation requirements for Windows and Windows clusters

Table 4-1 describes the requirements to prepare your Windows systems for 10.4 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 10.4 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 10.4 catalog back to the default location for the upgrade to succeed. Do not attempt a 10.4 upgrade if the catalog is not in the default location. You primary 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.

10.4 Commands Reference Guide

Table 4-1 10.4 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	Use the information that is shown to correctly size your server: ■ The SORT website. See "About Veritas Services and Operations Readiness Tools" on page 22. ■ General details on how to size your NetBackup environment. See "Size guidance for the NetBackup primary server and domain" on page 223. ■ Detailed information about planning and tuning your NetBackup environment are available. These details are found in the *NetBackup Backup Planning and Performance Tuning Guide*.

Table 4-1 10.4 requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	Disk space	■ An NTFS partition. ■ The exact amount of space that is required to accommodate the server software and the 10.4 catalogs depends on the hardware platform. More information about this topic is available. 10.4 Release Notes for 10.4 ■ 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. ■ 10.4 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 10.4 catalog requires considerably more space once the primary server is placed in a production environment.
	General requirements	Make sure that you have all of the following items: ■ 10.4 installation ESD images ■ Appropriate license files More information is available: https://www.veritas.com/support/en_US/article.100058779 ■ Administrator account and password for all servers ■ Screen resolution configured for at least 1024x768, 256 colors. **Note:** To install 10.4 on Windows 2012 R2, Windows 2012 UAC-enabled, Windows Server 2016, Windows 2019, and Windows 2022 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 10.4 in UAC-enabled environments. To allow users in the Administrators Group to install 10.4, disable UAC.

Table 4-1 10.4 requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	Remote and cluster installations	

Table 4-1 10.4 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 10.4 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 10.4 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.` ■ 10.4 virtual name and IP address Have the virtual name and IP address for 10.4 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 10.4 Group uses must already be configured in the cluster and online on the active node. ■ Install 10.4 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 10.4 disk resources must be configured in Veritas Enterprise Administrator (VEA) before you install 10.4. ■ 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 10.4 virtual name is employed for other uses, such as the robot control host.

Table 4-1 10.4 requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
		More information about cluster requirements is available.
	Remote Administration Console host names	You must provide the names of the Remote Administration Console hosts during primary server installation.
	10.4 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 10.4. ■ 10.4 services and port numbers must be the same across the network. ■ Veritas suggests that you use the default port settings for 10.4 services and Internet service ports. If you modify the port numbers, they must be the same for all primary 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 10.4 or manually edit the `services` file.
	CIFS-mounted file systems	Veritas does not support installation of 10.4 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 10.4 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 10.
	Installations on Windows 2012/2012 R2 Server Core/Windows 2016	You can only install 10.4 on these computers with the silent installation method. See "Installing NetBackup servers silently on Windows systems" on page 94.
	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 10.4 installs and functions.

Table 4-1 10.4 requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	Web Services	Beginning with 10.4 8.0, the 10.4 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 primary server web server user and group creation" on page 214. **Note:** Veritas recommends that you save the details of the user account that you use for the 10.4 Web Services. A primary server recovery requires the same 10.4 Web Services user account and credentials that were used when the 10.4 catalog was backed up. **Note:** If the 10.4 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 primary 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 4-1 10.4 requirements for Windows and Windows clusters *(continued)*

Check	Requirement	Details
	External certificate authority	For primary 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 10.4 Security and Encryption Guide and refer to the chapter on external CA and external certificates.

See "Installation requirements for UNIX and Linux" on page 34.

Requirements for Windows cluster installations

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

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

Table 4-2 Windows cluster requirements for installation and upgrade

Item	Requirement
Server 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 operating systems, refer to the Software Compatibility List (SCL) at the following website: ■ http://www.netbackup.com/compatibility ■ https://sort.veritas.com/netbackup
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.

Table 4-2 Windows cluster requirements for installation and upgrade *(continued)*

Item	Requirement
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)	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 operating systems, refer to the Software Compatibility List (SCL) at the following website: ■ http://www.netbackup.com/compatibility ■ https://sort.veritas.com/netbackup
Cluster Server (VCS) clusters	■ All NetBackup disk resources must be configured in Veritas Enterprise Administrator (VEA) before you install NetBackup. ■ You must take the VCS NetBackup resource offline before you begin the install or the upgrade. **Note:** Make sure that shared disk and IP resources are online during the install or the upgrade on active node.
Cluster node device configuration and upgrades	

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

Use the following procedure to perform a local, a remote, or a clustered install of NetBackup on a Windows computer.

NetBackup uses the Local Service account for starting most of the primary server services during an install. You can change this account to use the Local System

account or an administrator account during a custom installation. Follow the steps for a custom installation to make this change.

You can use the `nbserviceusercmd` command to change the service user on media servers after the installation completes. Refer to the *NetBackup Commands Reference Guide* for more information about the `nbserviceusercmd` command. For more details about the service user account, refer to https://www.veritas.com/support/en_US/article.100053035.

To install NetBackup 10.4 server software on a local, remote, or clustered Windows server

1. Log on to the system. Be sure to log on with administrator privileges.
   - For local installations, log on to the system where you want to install NetBackup.
   - For remote installations, log on to a system with network access to all of the hosts where you want to install NetBackup.
   - For cluster installations, log on to the active node (the node with the shared disk).
2. Navigate to the directory where the images 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 **NetBackup Server Software Installation**.
5. If you are prompted about the absence of required Visual C++ run-time libraries, review the information and respond accordingly. More information is available.

   See "Windows compiler and security requirements for NetBackup 10.4 and later installation" on page 18.
6. On the **Welcome** screen, review the content and click **Next**.
7. (Conditional) If you previously installed NetBackup 10.4 on this host, you see the **Program Maintenance** dialog.
   - Select **Modify** to change installation settings for the local host, or to use the local host as a platform to perform push installation to remote hosts.
   - Select **Repair** to restore NetBackup 10.4 to its original state on the local host.
   - Select **Remove** to remove NetBackup 10.4 from the local host.
8. On the **License Agreement** screen, do the following and click **Next**:

   I agree to and accept the terms of the license agreement.

   You must select this item to install the software.

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

Where to install	■ For a local installation, select **Install to this computer only**. ■ For a remote installation, select **Install to multiple computers on your network**. ■ For a cluster installation, select **Install a clustered Primary Server**. This option is available only if the installation process determines that your system is configured for a Windows Server Failover Cluster (WSFC) or VCS clustered environment.
Typical	Select this option to install NetBackup with the default settings. **Note:** The **Typical** installation does not install the Java GUI or the JRE on Windows media servers. You must select **Custom** if you want the Java GUI and the JRE installed on Windows media servers.
Custom	Select this option to install NetBackup with the settings that you want.

Click **Next**.

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

Licenses	You can download your license from Veritas Entitlement management system or use an evaluation license. More information is available: https://www.veritas.com/support/en_US/article.100058779. License files are not required for media server installations. For remote and cluster installations: **Note:** The license that you enter here gets pushed to the other nodes. For clustered primary server, the licenses are stored in the shared drive that is accessible only to the active node. As such, license doesn't gets pushed to the inactive 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). During this installation process, the following occurs to verify that you have proper credentials to perform remote installations: ■ When you select a clustered system for installation, 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.
NetBackup Primary Server	Select the radio button and then **Next** to install primary server software. If you have downloaded license files, browse and add those license files. If you select **Next** without adding any license files, NetBackup uses an evaluation license.
NetBackup Media Server	Select the radio button and then **Next** to install media server software.
Disaster Recovery Primary Server	Select this radio button and then **Next** to perform a disaster recovery of your primary server. The disaster recovery process requires additional steps and information that is not covered in this manual. More information is available. NetBackup Troubleshooting Guide

11 Enable or disable FIPS mode in NetBackup on the **FIPS Compliance in NetBackup** screen. By default FIPS mode is disabled.

By enabling FIPS, the NetBackup installer and any further operations run in FIPS mode. Please check requisite before you enable FIPS mode in your NetBackup Domain.

The NetBackup installation and all further options on remote hosts run in FIPS-compliant mode if you enable FIPS mode during remote installation.

Enabling FIPS mode during clustered server installation enables FIPS mode on the nodes which are added on the **NetBackup Remote Hosts** screen. When you add new nodes to an existing cluster group using the Windows Installer, make sure that the FIPS mode configuration value matches the other nodes in the cluster group.

For more information about FIPS, see the *NetBackup Encryption and Security Guide*.

Click **Next**.

12 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.

Note: After installation, you cannot change the user account for the NetBackup web server. Do not delete this account, as you cannot reconfigure the account for the web server after installation.

More information is available.

See "Installation requirements for Windows and Windows clusters" on page 67.

13 (Conditional) This step applies only to the local installations that are **Custom**. For **Typical** installations, skip to the next step.

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

- **NetBackup Installation Folder**
  On this screen, you can select where the NetBackup files are installed.

  Destination Folder

  By default, NetBackup files are installed to the following location:

  `C:\Program Files\VERITAS`

  To change the folder destination where NetBackup is installed:

  - Click **Change**.
  - Browse to the preferred location and designate a new or an existing folder.
  - Click **Next**.

  Additional information about installation folder restrictions is available.

  See "Restrictions on the NetBackup installation directory" on page 17.

Click **Next**.

- **Java GUI and JRE Options**
  The options that are provided are:
  - **Include Java GUI and JRE**: Install the Java GUI and the JRE to the specified computer.
  - **Exclude Java GUI and JRE**: Exclude the Java GUI and the JRE from the specified computer.
  - **Match Existing Configuration** (remote installs only): Preserve the current state of the Java GUI and JRE components. If the Java GUI and JRE are present, they are upgraded. If they are not present, they are not upgraded. If you specify this option on an initial installation, the packages are not installed.
- **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 account: ■ Select **Custom account**. ■ Enter the account information in the following fields: **Domain** **Username** **Password**

Non-Privileged Account Details	(Conditional) For primary servers only. Specify either **Same as the Privileged Account specified above** or **Local Service** account. For more information for the non-privileged service user account, refer to: https://www.veritas.com/docs/100048220
Service Options	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 installation 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 installation proceeds if a restart is required as part of the installation. If you select this option and the installation process determines that a restart is required, the installation stops. The system is then rolled back to its original state. If you do not select this option, the installation proceeds even if the installation process determines that a restart is required.

Click **Next**.

- When prompted about installation of the NetBackup IT Analytics Data Collector, determine if you want it installed and proceed accordingly. If you opt to not install it and determine you need it later, you can install the NetBackup IT Analytics Data Collector after the NetBackup installation finishes. More information about the NetBackup IT Analytics Data Collector and how to manually install it after completing the NetBackup installation is available:
  See “About the NetBackup IT Analytics Data Collector” on page 206.
  See “Manually install or uninstall NetBackup IT Analytics Data Collector binaries” on page 207.

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

Primary Server Name	(Conditional) For local primary server installations, enter the name of the local computer. For a cluster installation, enter the cluster virtual server name. For media server installations, you must change the name to the primary server name to which the media server is configured.
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 local NetBackup Enterprise media server installations. When you install media server software, this field defaults to the local server name.

Click **Next**.

15 After you provide the required computer names, the installer determines your security configuration.

- If the installer finds your environment uses an external certificate authority, you are presented with the **External Certificate** screen. Proceed to step 16.
- If the installer finds your environment uses NetBackup Certificate Authority, you are presented with the **NetBackup Certificate** screen. Proceed to step17 .

16 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. Go to step 21 in this procedure.

17 After you confirm you want to continue, the installer fetches the certificate authority certificate details. You have the option to click **Cancel** to halt this action. Be aware if you click **Cancel**, 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.

18 Enter the Certificate Authority Fingerprint as prompted.

After you confirm the fingerprint information, the installer stores the certificate authority certificate details. You have the option to click **Cancel** to halt this action. Be aware if you click **Cancel**, 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.

19 After the Certificate Authority certificate is stored, the installer fetches the host certificate. You have the option to click **Cancel** to halt this action. Be aware if you click **Cancel**, 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.

20 (Conditional) If prompted by the **Security Token** screen, enter the security token.

If you were issued a security token, enter it below.

The token format is 16 upper case letters. Alternatively, you can also select the **Proceed without providing a security token** option. When the option is selected, this warning is shown:

In some environments, failure to provide a security token can result in failed backups. Contact your backup administrator if you have questions.

After you enter a security token, you have the option to click **Cancel** to halt the deployment of the host certificate. Be aware if you click **Cancel**, 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.

21 After you enter all the security information, you are prompted with the certificate status screen. If the screen indicates there are no issues, click **Next** to continue. If the screen **Security Certificate Status** indicates there are issues, click **Back** to reenter the required security information.

If this install is a push install or if you selected **Proceed without security**, this dialog is skipped.

22 (Conditional) For remote installations 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 install 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** and the **Password** of the account to be used to perform the installation on the remote computers. ■ If you plan to install to 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**. ■ On the **Remote Destination Folder** dialog box, verify or change the **Destination Folder** where NetBackup is installed. The default location is `C:\Program Files\Veritas`. If you plan to install to multiple remote computers and you want to use the same location, click the box next to **Use this folder for subsequent systems**. Selecting this option prevents the need to enter the location for each remote computer.
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 installation on the remote computers. If you plan to add and install to 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**. ■ On the **Remote Destination Folder** dialog box, verify or change the **Destination Folder** where NetBackup is installed. The default location is `C:\Program Files\Veritas\`. If you plan to install to multiple remote computers and you want to use the same location, click the box next to **Use this folder for subsequent systems**. Selecting this option prevents the need to enter the location 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**.

23 (Conditional) For cluster installations only:

On the **NetBackup Remote Hosts** screen, specify the remote system information for installation on those computers.

- On the initial screen, right-click **Browse**.
- On the **Available Systems** dialog box, select the computer that you want to add. Control-click to select multiple computers.
  Click **Next**.

- On the **Remote Computer Login Credentials** dialog box, enter the user name, password, and domain that NetBackup is to use on the remote system(s).

  If you intend to add more remote computers, click the check box next to **Remember user name and password**.

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

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

■ NetBackup not installed	Considers the remote to be verified.
■ NetBackup already installed	Compares the installation type on that system to the installation 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 installation 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 install 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 installed with the push method. Add-on products must be installed on each individual node in the cluster group. For instructions on how to install these products, refer to the NetBackup documentation that supports each product.

- NetBackup pushes to the other nodes only the licenses you enter at the beginning of the installation. Your licenses 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 **Next**.

24 (Conditional) For cluster installations only:

On the **Cluster Settings** screen, you provide the virtual and the physical network information.

Note: You can add only one virtual IP address during installation. If your virtual name can resolve into more than one IP address, you can add multiple IP addresses after the installation using the `bpclusterutil -addIP` option. More information about the `bpclusterutil` command is available.

NetBackup Commands Reference Guide

For new installations, the following configuration settings that you enter apply to all nodes:

Create a new Cluster Group	For new cluster installations, select this option.
IPv4 Clusters	The default cluster setting is IPv4. Enter the following addresses: ■ **Virtual IPv4 Address** The IP address to which the virtual server name should resolve. For new cluster installations, you must enter the address manually. ■ **IPv4 Subnet Mask** Identifies a subnetwork so that IP addresses can be shared on a local area network. This number correlates directly to the virtual IP address of the cluster.
IPv6 Clusters	To enable IPv6 clusters, select this option. Enter the following IP address: ■ **Virtual IPv6 Address** The IPv6 address must be entered in CIDR format.
NB Cluster Group Name	The name that is used to identify a NetBackup service group or resource group. The resources in any resource group are related and interdependent.

Virtual Host Name	The name by which NetBackup is known in the cluster. When you install the client software, this host name must be added to the **Additional Servers** field on the **NetBackup System Names** screen. The server uses this name when it communicates with the client nodes.
Path to Shared Data	A directory on one of the shared disks in the cluster where NetBackup stores configuration information. If the letter for the disk (or drive) does not appear in the pull-down list, enter only the letter.
Public Network	For NetBackup clustered environments, select a public network that is assigned to the node of the cluster. **Warning:** You must not select a private network that is assigned to this cluster.
Cluster Configuration	After you set all of the parameters, click this icon to configure the cluster for use with NetBackup. The **Next** icon is not available until after successful cluster configuration. The text box provides the following information about the configuration: ■ Identifies any existing clusters or NetBackup cluster groups. ■ Indicates a successful configuration. ■ Identifies any problems or errors that occurred during the configuration (configuration failure). **Note:** If you click **Cancel** after a successful cluster configuration for new installations, a pop-up message appears. The message asks if you are sure that you want to proceed with the cancelation. To cancel the installation and remove the new cluster group, click **Yes**. To continue with the installation and retain the new cluster group, click **No** and then click **Next**. If the cluster configuration fails, see the NetBackup Clustered Primary Server Administrator's Guide for information about how to resolve the problem.

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

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

Note: Veritas recommends that you review the summary screen for any warning messages. You can prevent installation and upgrade issues if you resolve any problems before you continue the installation.

Then 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 installation.

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

For remote and cluster installations, up to five installations occur simultaneously. When an installation is completed, another one begins so that a maximum of five installations are in progress.

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

View installation log file

The installation 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 installation log at the following location:

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

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

Search the installation 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 installation: ■ If you are done installing 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 install, click **Finish**. You can move on to the next computer and install the necessary server software.

27 (Conditional) On a clustered NetBackup primary server, you must copy the Certificate Authority certificate and the host certificate to the inactive node. More information is available:

See "Generate a certificate on the inactive nodes of a clustered primary server" on page 176.

If you performed a disaster recovery of the primary server, you must first generate the token and then copy it to each of the inactive nodes. More information about how to handle disaster recoveries is available.

NetBackup Troubleshooting Guide

28 (Conditional) If you plan to configure customized settings for your Tomcat web server, determine if those settings can persist across upgrades. More information is available:

See "Persistent Java Virtual Machine options" on page 211.

29 Repeat the steps in this procedure for any other servers.

30 After all server software is installed, you are ready to install client software.

See "About NetBackup client installation" on page 103.

See "Post-installation tasks for NetBackup cluster environments" on page 92.

See "Verifying Windows cluster installations or upgrades" on page 93.

Post-installation tasks for NetBackup cluster environments

You may need to take one or more of the following actions after the NetBackup server software is installed in a cluster:

Obtain certificates	You must obtain the Certificate Authority certificate and the host certificate for each inactive node. More information is available: See "Generate a certificate on the inactive nodes of a clustered primary server" on page 176.
External certificate authority	Configure your external certificate authority. If you opted to skip the security configuration or if you have a primary server, you may need to configure an ECA. More information about configuring ECAs is available: https://www.veritas.com/support/en_US/article.100044300
Restart	You may need to restart each of the cluster nodes after the installation is complete.
WSFC and VCS clusters	Under normal circumstances, cluster configuration is one of the final steps when you install NetBackup in a cluster. If this step is not done or does not complete successfully, you can use the `bpclusterutil` command from the active node to perform this step. For information on how to run `bpclusterutil`, see the NetBackup Commands Reference Guide.
WSFC clusters	Any NetBackup resources that you took offline come back online automatically.

See "Verifying Windows cluster installations or upgrades" on page 93.

Verifying Windows cluster installations or upgrades

The Cluster Administration console lets you verify the installation or upgrade and view your current system structure.

To verify a successful WSFC cluster installation or upgrade through the Cluster Administration console

1. During a cluster installation, you can open the Cluster Administration console to see your current structure.
2. After you have completed the installation and the configuration process, the console shows the new cluster group configuration.

To verify a successful VCS cluster installation or upgrade through the Cluster Manager console

1. During a cluster installation, you can open the Cluster Administration console to see your current structure.
2. After you have completed the installation and the configuration process, the console shows the new cluster group configuration.

See "About NetBackup server configuration" on page 145.

Installing NetBackup servers silently on Windows systems

A silent installation avoids the need for interactive input in the same manner as performing a remote installation.

To perform a silent installation, you must first modify the appropriate NetBackup script. After script modification, you can run the script to initiate the silent installation. More information is available.

See "About the NetBackup answer file" on page 178.

To install NetBackup server software silently

1. Log on to the system where you want to install NetBackup. Be sure to log on as a user with administrator privileges.
2. Navigate to the location where the ESD images (downloaded files) reside.
3. Open Windows Explorer and copy the contents of the X86 or 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 install a primary server, edit `silentprimary.cmd`
   - To install a media server, edit `silentmedia.cmd`
6. Edit the following lines as needed for your installation:
   - `LICENSE=`*`license_file_path`*`|EVALUATION`

     Enter the appropriate information for the required license. More information about this option is available. See "About the NetBackup answer file" on page 178.

- `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=`*`num`*

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

  0 (zero, default) — By default, a silent installation 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 installation 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 installation 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 installation or roll back the system to its original state.

  1 (one) — Select this setting to abort the installation if it is determined that a restart is required.

  If a restart is needed, this setting cancels the installation and the system is rolled back to its original state.

- `SET CA_CERTIFICATE_FINGERPRINT=`*`fingerprint`*

  If you use a NetBackup Certificate Authority, you must know the CA Certificate fingerprint of the primary server at time of installation. 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

- `SET AUTHORIZATION_TOKEN=`*`token`*

  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

Caution: Because providing the authorization token in plain text presents a security risk, restrict access to the `silentmedia.cmd` file to read access. Grant read access to NetBackup administrators and system administrators only. Delete the `silentmedia.cmd` file after successful installation.

- `SET ECA_CERT_STORE=`*`cert_store_string`*
  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`*
  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_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.
- `SET ECA_CRL_PATH=`*`path`*
  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`*

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 NetBackup.
  - EXCLUDE: Exclude the Java GUI and JRE when installing NetBackup.
  - MATCH: Match the existing configuration on the host. If you specify this option on an initial installation, the packages are not installed.

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 (Conditional) If you plan to configure customized settings for your Tomcat web server, determine if those settings can persist across upgrades. More information is available:

See "Persistent Java Virtual Machine options" on page 211.

After all server software is installed, you are ready to install client software.

See "About NetBackup client installation" on page 103.

Chapter 5

About the administrative interfaces

This chapter includes the following topics:

- About the NetBackup web user interface
- About the NetBackup Administration Console
- Installing the NetBackup Administration Console
- Installing multiple versions of the NetBackup Administration Console on Windows
- Removing earlier versions of the NetBackup Administration Console on Windows
- About the NetBackup Remote Administration Console
- Installing the NetBackup Remote Administration Console

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 primary 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 Administration Console

The NetBackup Administration Console can be used to administer one or more UNIX or Windows NetBackup servers. It provides all of the standard NetBackup server interfaces. The console can be used to create backup policies, manage volumes, view status, monitor tape drives, and other operations.

The NetBackup Administration Console is always installed when you install or upgrade NetBackup primary server packages. The NetBackup Administration Console may be installed when you install or upgrade NetBackup media server packages.

Installing the NetBackup Administration Console

You do not need to install the NetBackup Administration Console separately. 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: Veritas recommends that after you install or upgrade NetBackup server software, you should 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.

A NetBackup environment may contain multiple servers with multiple NetBackup versions. You can install and remove multiple versions of the NetBackup Administration Console. More information is available.

See "Installing multiple versions of the NetBackup Administration Console on Windows" on page 100.

See "Removing earlier versions of the NetBackup Administration Console on Windows" on page 101.

Installing multiple versions of the NetBackup Administration Console on Windows

To install multiple versions of the NetBackup Administration Console in a mixed version environment, note the following restrictions and guidelines:

Updates	Only the most recent version of the NetBackup Administration Console can be updated (or patched).
`auth.conf` file	The NetBackup-Java Capabilities Authorization configuration file (`auth.conf`), must always be located in *`install_path`*`\java`. For example, `C:\Program Files\Veritas\java`. The file must exist there regardless of how many versions of the console are installed, or in which directories they are installed. The file is only used for administering NetBackup on this Windows host, and default settings exist if the file is not present. For more information about these defaults, see the section "Authorizing NetBackup users" in the NetBackup Administrator's Guide, Volume I.
Console version location	You must install each console version to a different folder.

To install earlier versions of the NetBackup-Java Administration Console

1. Insert the appropriate version NetBackup Windows installation media with the NetBackup-Java Administration Console that you want to install.
2. For NetBackup 7.0 and 7.1 versions, select **Installation** and click **Java Windows Administration Console Installation**.
3. If a different version of the Java console has already been installed, specify a new folder location to prevent overwriting the earlier installation.

   For example, specify `C:\Program Files\Veritas\nbjava65` for version 6.5 Java consoles.
4. To complete the installation, click **Finish**.

See "Removing earlier versions of the NetBackup Administration Console on Windows" on page 101.

See "Installing the NetBackup Administration Console" on page 99.

Removing earlier versions of the NetBackup Administration Console on Windows

In some cases, you can remove earlier versions of the NetBackup Administration Console by using the **Add/Remove Programs** feature. You can use this method if the version that you want to remove appears in the list of programs.

If the version that you want to remove does not appear in the list of programs, you must manually remove it. Use the following procedure.

To manually remove earlier versions of the NetBackup Administration Console

1. Remove the folder where the earlier version NetBackup Administration Console is installed.
2. Remove the appropriate menu item from the **Start > Programs > NetBackup** menu.
3. Remove any relevant desktop shortcuts.

About the NetBackup Remote Administration Console

The NetBackup Remote Administration Console is an interface-only version of NetBackup that you can use to administer NetBackup servers from another computer. The computer that runs the NetBackup Remote Administration Console does not require NetBackup software.

The following is a brief description of the NetBackup Remote Administration Console operation:

- The console lets you perform all NetBackup operations exactly like the NetBackup Administration Console on a local NetBackup server. You can create backup policies, manage volumes, view status, monitor tape drives, and perform other operations.
- The console displays the name of the server it administers, rather than a local host name.
- The console can only administer other NetBackup servers. It cannot act as a primary or a media server.

Installing the NetBackup Remote Administration Console

The procedure shown details how to install the NetBackup Remote Administration Console on a non-NetBackup computer.

To install the NetBackup Remote Administration Console

1. Navigate to the location where the downloaded files reside and run `Browser.exe`.

   Note: You cannot install NetBackup Remote Administration Console on a computer where NetBackup server software is already installed.

2. On the initial screen, select **Installation**.
3. On the **Installation** screen, click **NetBackup Java Remote Administration Console Installation**.
4. On the **Welcome** screen, review the content and click **Next**.
5. On the **License Agreement** screen, accept the agreement and click **Next**.
6. On the **NetBackup Installation Type** screen, select **Install to this computer only** and **Typical Installation** and then click **Next**.

   If an earlier version of the console already exists, you have the following options:

   - Cancel the installation and remove the earlier version of the console. Then run the new console installation again.
   - Specify an alternate installation location for the new version of the console.
7. On the **Ready to Install the Program** screen, review the Installation Summary and click **Install**.
8. On the **Installation Complete** screen, click **Finish**.
9. To open the console, click **Start > Programs > Veritas NetBackup > NetBackup *Version* Administration Console**.

Note: 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

See “About the NetBackup Remote Administration Console” on page 101.

Chapter 6

Installing NetBackup client software

This chapter includes the following topics:

- About NetBackup client installation
- About NetBackup client installation on Windows
- About NetBackup client installation on UNIX and Linux

About NetBackup client installation

By definition, NetBackup servers are also clients. When you install NetBackup server software, client software is also installed.

When you install client software, you perform a true client installation since no server software is installed.

Client software can be installed locally at each individual computer or remotely. The operating system determines which clients can be installed remotely.

Windows	A Windows host can only push client software to Windows clients. NetBackup does not need to be installed on the host that is used to perform the remote client installation.
UNIX or Linux	A NetBackup Linux server can only push client software to UNIX or Linux clients. NetBackup software and client type software must be installed on the server that is used to perform the remote client installation.

You can use the `nbserviceusercmd` command to change the service user on clients after the installation completes. Refer to the *NetBackup Commands Reference Guide* for more information about the `nbserviceusercmd` command. For more details about the service user account, refer to https://www.veritas.com/support/en_US/article.100053035.

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.

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

About NetBackup client installation on Windows

The NetBackup client installation wizard for Microsoft Windows lets you select the appropriate setup and installation options from a series of wizard screens. After you select options, a window appears that lets you verify your selections before the installation begins.

While the installation is in progress, a dialog box provides details of the installation and the setup progress. When the installation is completed, a final window shows the results.

Note the following when you install NetBackup client software on Windows systems:

Client installation restrictions	You cannot install NetBackup client software on the computers that currently have NetBackup server software. In these cases, you must first remove the NetBackup server software. See "Removing NetBackup server and client software from Windows servers, clusters, and clients" on page 171.
User permissions	■ By default on Windows 2012, 2012 R2, and 2016 Server systems, only administrators have write permission to the `Program Files` directory. ■ NetBackup writes log files and progress files to the following location: `Program Files\Veritas\NetBackup\Logs` To perform backups and restores with the Backup, Archive, and Restore interface, users must have write permission to the `Logs` directory. Users without write permission to this directory receive an error message, and the backup or restore is canceled. The administrator account has write permission by default, but you must ensure that other users also have write permission.

About Windows client installation methods and requirements

You can install NetBackup clients on Windows systems with the following methods:

Table 6-1 Installation methods and requirements

Method	Requirements	Details
Local installation	To install NetBackup client software locally, the system must meet the following configuration requirements: ■ Any TCP/IP transport that is Windows Sockets compliant. (Use of the TCP/IP transport that comes with the server or the operating system is recommended.) ■ A network adapter that your TCP/IP transport supports	The installation wizard installs the client software only on the computer where you run the installation. See "Installing NetBackup Windows clients locally or remotely" on page 107.

Table 6-1 Installation methods and requirements *(continued)*

Method	Requirements	Details
Remote installation	To install NetBackup client software remotely, the system must meet the following configuration requirements: ■ All the requirements for local installations must be met. ■ Administrator privileges are required for the user that performs remote installations. ■ Remote Registry service must be started on the remote system. If the Remote Registry service is not started, the installation receives this 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.`	The installation wizard scans the network for available clients where you can install the client software. Also, a remote installation requires system administrator privileges. **Note:** You cannot install clients remotely from NetBackup Windows servers to UNIX computers. See "Installing NetBackup Windows clients locally or remotely" on page 107.
Silent installation	The requirements for silent installation are the same as the requirements for a local installation.	A silent installation is a process that does not require interactive input. However, you must edit the `silentclient.cmd` file before you run it. See "Installing NetBackup Windows clients silently" on page 116.

An NTFS disk partition is required for all installation types.

The NetBackup client version that you install must be the same or earlier than the installed version of NetBackup server software. Later client versions cannot be used with earlier server versions.

See "About compatibility between NetBackup versions" on page 10.

See "About NetBackup client installation" on page 103.

Installing NetBackup Windows clients locally or remotely

Use this procedure to install NetBackup on your local computer or on multiple computers on your network. You can stop the installation process at any time by clicking **Cancel** or by clicking **Back** to return to the previous window.

When you install Windows clients remotely, note the following:

Requirements	Review the requirements for Windows client installation. See "About Windows client installation methods and requirements" on page 105.
Privileges	You must have administrator privileges on the remote clients for the NetBackup installation to complete successfully.
Client name entries	During installation, the client name is written to the registry in lowercase. For backups to work, the policies on the NetBackup server must specify the client names in lowercase.

Note: After client installation, you may need to restart the system for the changes to take effect. A message appears to alert you if a restart is necessary.

To install NetBackup client software locally or remotely on Windows systems

1. Log on as administrator on the host where you want to install the client software.
2. Navigate to the directory where the images reside and run `Browser.exe` to start the NetBackup Installation Wizard.
3. On the initial screen, select **Installation**.
4. On the **Installation** screen, select **NetBackup Client Software Installation**.
5. If you are prompted about the absence of required Visual C++ run-time libraries, review the information and respond accordingly. More information is available.

   See "Windows compiler and security requirements for NetBackup 10.4 and later installation" on page 18.
6. On the **Welcome** screen, review the content and click **Next**.

7 (Conditional) If you previously installed NetBackup 10.4 on this host, you see the **Program Maintenance** dialog.

- Select **Modify** to change installation settings for the local host, or to use the local host as a platform to perform push installation to remote hosts.
- Select **Repair** to restore NetBackup 10.4 to its original state on the local host.
- Select **Remove** to remove NetBackup 10.4 from the local host.

8 On the **License Agreement** screen, accept the terms of the agreement and click **Next**.

9 On the **Veritas NetBackup Client Installation Type** screen, provide the following information:

Where to install	For a local installation, select **Install to this computer only**. For remote installation, select **Install to multiple computers on your network**. The procedure does not install the client on the local host unless you add it to the list of systems that you want to install.
Typical	Select this option to install NetBackup with the default settings.
Custom	Select this option to install NetBackup with the settings that you want.

Click **Next**.

10 Enable or disable FIPS mode in NetBackup on the **FIPS Compliance in NetBackup** screen. By default FIPS mode is disabled.

By enabling FIPS, the NetBackup installer and any further operations run in FIPS mode. Please check requisite before you enable FIPS mode in your NetBackup Domain.

The NetBackup installation and all further options on remote hosts run in FIPS-compliant mode if you enable FIPS mode during remote installation.

For more information about FIPS, see the *NetBackup Encryption and Security Guide*.

Click **Next**.

11 (Conditional) This step applies only to local **Custom** installations.

On the **Veritas NetBackup Client Destination Folder** screen, you can select where the NetBackup files are installed.

Destination Folder

By default, NetBackup files are installed to the following location:

```
C:\Program Files\VERITAS
```

To change the folder destination where NetBackup is installed:

- Click **Change**.
- Browse to the preferred location and designate a new or an existing folder.
- Click **Next**.

Additional information about installation folder restrictions is available.

See "Restrictions on the NetBackup installation directory" on page 17.

Note: For upgrades, you cannot change the destination.

12 (Conditional) This step applies only to **Custom** installations.

On the **NetBackup Options** screen, select from the following options:

At System Startup

Enable or disable the following options:

- **Start NetBackup Client Service Automatically**
  By default, this option is enabled so that NetBackup services are available immediately after system startup.
- **Start NetBackup Client Job Tracker Automatically**
  By default, this option is disabled. To start this option manually after installation, click **Start > All Programs > Veritas NetBackup > NetBackup Client Job Tracker**.

Ports

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**.

13 (Conditional) This step applies only to **Custom** installations.

On the **NetBackup Services** screen, provide the following startup account and startup type information for NetBackup client services:

Log On

Specify either **Local System account** or **This 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 this option.
- Enter the account information in the following fields:
  Domain
  Username
  Password

Safe Abort Option

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

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

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

14 On the **NetBackup System Names** screen, the following fields are populated automatically. Changes are not normally required.

Primary Server Name	If necessary, change this name to the appropriate primary server where the client backup images are to be stored.
Additional Servers	Enter all of the primary server and media server names that you want this client to access.

15 After you provide the required computer names, the installer determines your security configuration.

- If the installer finds your environment uses an external certificate authority, you are presented with the **External Certificate** screen. Proceed to step 16.
- If the installer finds your environment uses NetBackup Certificate Authority, you are presented with the **NetBackup Certificate** screen. Proceed to step 17.

16 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. Go to step 21 in this procedure.

17 After you confirm you want to continue, the installer fetches the certificate authority certificate details. You have the option to click **Cancel** to halt this action. Be aware if you click **Cancel**, 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.

18 On the **Confirm the CA fingerprint** screen, select **I recognize the fingerprint for this host. Proceed with the certificate deployment.** if the fingerprint displayed is one you recognize and trust. Click **Next** to continue.

If you do not recognize or trust the displayed fingerprint, select **Proceed without the certificate deployment**.

After you confirm the fingerprint information, the installer stores the certificate authority certificate details. You have the option to click **Cancel** to halt this action. Be aware if you click **Cancel**, 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.

19 After the Certificate Authority certificate is stored, the installer deploys the host certificate. You have the option to click **Cancel** to halt this action. Be aware if you click **Cancel**, 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.

20 (Conditional) If prompted by the **Authorization Token** screen, enter the security token.

Please enter an authorization token

The token format is 16 upper case letters. Alternatively, you can also select the **Proceed without providing a security token** option. When the option is selected, this warning is shown:

In some environments, failure to provide a security token can result in failed backups. Contact your backup administrator if you have questions.

After you enter a security token, you have the option to click **Cancel** to halt the deployment of the host certificate. Be aware if you click **Cancel**, 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 this installation is a remote installation, the specification of an authorization token is optional. Contact your backup administrator to determine if authorization tokens are required for your environment.

21 After you enter all the security information, you are prompted with the certificate status screen. If the screen indicates there are no issues, click **Next** to continue. If the screen **Security Certificate Status** indicates there are issues, click **Back** to reenter the required security information.

If this install is a push install or if you selected **Proceed without security**, this dialog is skipped.

22 On the **Veritas NetBackup Remote Hosts** screen, specify the hosts where you want NetBackup installed.

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

Browse	Click here to search the network for the hosts where you want to install 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** and the **Password** of the account to be used to perform the installation on the remote computers. ■ If you plan to install to 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**. ■ On the **Remote Destination Folder** dialog box, verify or change the **Destination Folder** where NetBackup is installed. The default location is `C:\Program Files\Veritas`. If you plan to install to multiple remote computers and you want to use the same location, click the box next to **Use this folder for subsequent systems**. Selecting this option prevents the need to enter the location for each remote computer.
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 installation on the remote computers. If you plan to add and install to 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**. ■ On the **Remote Destination Folder** dialog box, verify or change the **Destination Folder** where NetBackup is installed. The default location is `C:\Program Files\Veritas`. If you plan to install to multiple remote computers and you want to use the same location, click the box next to **Use this folder for subsequent systems**. Selecting this option prevents the need to enter the location 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**.

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

Note: Veritas recommends that you review the summary screen for any warning messages. You can prevent installation and upgrade issues if you resolve any problems before you continue the installation.

Then 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 installation.

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

Up to five remote installations occur simultaneously. When a remote installation is completed, another one begins so that a maximum of five installations are in progress.

If you click **Cancel** after you click **Install**, the installation does not stop immediately. Installation continues on all remote hosts where the installation has already started. Any specified hosts after that point do not get client software installed.

NetBackup considers any remote installations that were completed when you clicked **Cancel** to be successful.

24 On the **Installation Complete** screen, click **Finish**.

Examine the installation log on the following location:

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

An installation log file provides detailed installation information and shows whether any errors occurred.

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

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.

Installing NetBackup Windows clients silently

A silent installation process does not require interactive input. It does, however, require that you edit the `silentclient.cmd` file before you run it.

See "About the NetBackup answer file" on page 178.

Silent installations of NetBackup clients are not supported if you want to run the NetBackup services as a user instead of a local administrator.

To install NetBackup with a custom services account, refer to the following topics:

See "Installing NetBackup Windows clients locally or remotely" on page 107.

Use the following procedure to perform a silent installation of a local NetBackup client.

To perform a silent installation of NetBackup client software on Windows

1. Navigate to the location where the ESD images (downloaded files) reside.
2. Copy the contents of the directory shown to a temporary folder on your hard drive. For example, C:\temp.

   `x64`
3. Since the original source files are read-only, change the permissions for the copied files on the hard drive to allow the update.
4. In the temporary directory, use a text editor to edit the `silentclient.cmd` file so the script installs the client software as needed.
5. Run the `silentclient.cmd` script.
6. To verify that the installation was successful, check the installation log file in the following directory:

   `%ALLUSERSPROFILE%\Veritas\NetBackup\InstallLogs`

How to configure NetBackup clients

You can configure NetBackup clients by performing one of the following actions:

To add servers or media servers:	■ Start the Backup, Archive, and Restore interface. ■ Click **File > Specify NetBackup Machines**.
To display and change the client properties:	■ Start the Backup, Archive, and Restore interface. ■ Click **File > NetBackup Client Properties**.
To display and change the server properties:	■ Open the NetBackup Administration Console. ■ Expand **Host Properties** and click **Clients**. ■ In the right pane, right-click on the client and choose **Properties**. In the dialog box that appears, on the **Servers** tab, all NetBackup servers that require access to your Windows client must be listed.

For complete information on client configuration, see the NetBackup Administrator's Guide, Volume I.

About NetBackup client installation on UNIX and Linux

You can install UNIX/Linux clients either locally at the client computer or remotely from your UNIX/Linux NetBackup server. To install client software remotely from a UNIX/Linux NetBackup server, the client type software must first be installed on the UNIX/Linux server.

Note the following when you install NetBackup client software on UNIX/Linux systems:

UNIX/Linux package consolidation	Many of the add-on products and database agents are now installed with the NetBackup client package. Separate installation for these products is no longer needed. The following products are now included in the NetBackup 10.4 client package (if the platform supports the product): ■ BMR Boot server ■ DB2 ■ Encryption ■ Informix ■ Lotus Notes ■ Oracle ■ SAP ■ Snapshot Client ■ Sybase The binaries for the listed products are laid down with the client package. A valid license is still required to enable the product. If product configuration was required previously (such as `db2_config`), configuration is still required. The French, Japanese, and Chinese language packages remain as separate add-ons. The process to install and upgrade these products remains the same.
`gzip` and `gunzip` commands	The `gzip` and the `gunzip` commands must be installed on each system. The directories where the commands are installed must be part of the root user's `PATH` environment variable setting.

NetBackup-Java compatibility

To initiate a backup or a restore from a UNIX/Linux client, the following graphical interfaces are available:

- Clients that are compatible with NetBackup-Java may use the NetBackup-Java interface (jbpSA). Several versions of the interface exist. Use the `-h` option and review the `-r` options to find out which versions are supported.
- Clients that are not compatible with NetBackup-Java can use the `bp` interface.

More information about compatibility with graphical interfaces is available. Refer to the NetBackup Software Compatibility List (SCL).

http://www.netbackup.com/compatibility

Note: If a client is listed in the *Client Selections for Backup Policies* section of the SCL but not in the *NetBackup Administration Consoles* section, the client is supported for backup and restore, but it does not support any of the available graphical interfaces.

About UNIX and Linux client installation methods

You can install NetBackup clients on UNIX/Linux systems with the following methods:

Local installations

- This method installs the client software on the computer where you run the installation script.
- To install clients to a location other than the default, you must create and link a directory before you install the client software. First create the directory where you want the software to reside, then create `/usr/openv` as a link to that directory.
- On IBM zSeries and IBM pSeries Linux clients, you must transfer the NetBackup ESD image contents to a location that is readable by the virtual Linux environment. You can transfer the image with NFS mounting commands.

See “Installing UNIX clients locally” on page 120.

Remote (push) installations	■ You can "push" the client software from your Linux NetBackup server to your UNIX or Linux client computers. The UNIX or Linux client must be a true client and not a media server or a primary server. The preferred installation method is to push the client software. ■ Before you can push to a UNIX or Linux client, you must first install the NetBackup client type software on the server. Then, you must create a policy that includes the client name. NetBackup Administrator's Guide, Volume I See "Installing client type software on a primary server" on page 65. ■ You cannot install Windows client software remotely from a NetBackup Linux server. ■ Firewalls can prevent remote client installation. ■ Clients such as the IBM zSeries and the IBM pSeries Linux may not have access to the ESD images. In these cases, you must push the client software from a Linux primary server or a media server. ■ The following remote installation methods are available: See "Installing client software with the ssh method" on page 139. See "Installing client software with the sftp method" on page 140.
Native UNIX and Linux installer	You can install and 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 installed or upgraded with the NetBackup install script. More information is available: See "Install of the UNIX and Linux client binaries with native installers" on page 126.

See "About NetBackup client installation" on page 103.

Installing UNIX clients locally

The following procedure installs the NetBackup client software on a local computer.

To install client software locally on a UNIX client

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 "Install of the UNIX and Linux client binaries with native installers" on page 126.

2 When the following message appears, press **Enter** to continue:

```
Veritas Installation Script
Copyright 1993 - 2016 Veritas Corporation, 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 out the Veritas Services and
Operations Readiness Tools (SORT) Installation and Upgrade Checklist
and Hot fix and EEB Release Auditor, respectively, at
https://sort.veritas.com/netbackup.

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. The installation procedure attempts to load the appropriate binaries for your system. If the script does not recognize the local operating system, it presents choices.

3 Type **y** and press **Enter** to continue with the software installation.

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

4 Type the name of your NetBackup primary server and press **Enter** to continue.

```
Enter the name of the NetBackup primary server:
```

5 Confirm the NetBackup client name and press **Enter** to continue.

```
Would you like to use "client_name" as the configured name of the
NetBackup client? [y,n] (y)
```

6 (Conditional) Enter one or more media servers if prompted:

```
This host cannot connect directly to the primary server; therefore,
one or more media servers are required in order to contact the
primary server for security information.  Enter the media servers
(one per line) or X to skip the question.  Enter Q to indicate all
media servers have been entered.

Enter a media server for host primary.domain, Q to quit, or X to
skip this question:
media.domain
q
```

7 After you confirm you want to continue, the installer fetches 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.

8 The installer then looks to see what certificate authority the local system is configured to use. The options for certificate authority on the local system are: NetBackup Certificate Authority, external certificate authority, or indeterminate.

The installer then uses a combination of the primary server certificate authority mode and the local system certificate authority configuration to determine the next steps.

9 If the installer prompts you for a certificate file path, your environment uses an external certificate authority. Proceed to step 10.

If the installer prompts you for fingerprint information, your environment uses a NetBackup Certificate Authority. Proceed to step 16.

If the installer cannot determine the configuration of the certificate authority on the primary server, you are presented with two options:

- Skip the security configuration and configure your certificate authority after installation. More information about post-installation certificate authority 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.
  Proceed to step 20.
- Exit the installation and restart the installation once you configure your certificate authority.

10 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.

11 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):
```

12 (Conditional) If you specify 2, you must enter the path to the CRL location:

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

13 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.
```

14 (Conditional) 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) Update external certificate values.
3) Abort the installation.
Default option (1):
```

Proceed to step 20.

15 (Conditional) 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):
```

Proceed to step 20.

16 When prompted, review the fingerprint information and confirm that it is accurate.

```
Primary server [primary_name] reports CA Certificate fingerprint
[fingerprint]. Is this correct? [y/n] (y)
```

After you confirm the fingerprint information, the installer stores the certificate authority certificate details.

```
Storing CA certificate.
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.

17 After the Certificate Authority certificate is stored, the installer fetches the host certificate.

```
Getting host certificate.
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.

18 (Conditional) If prompted for the Authorization Token, please enter it.

```
An authorization token is required in order to get the host
certificate for this host. At the prompt, enter the authorization
token or q to skip the question. NOTE: The answer entered will
not be displayed to the terminal.

Enter the authorization token for primary_server_FQDN or q to
skip:
```

The token format is 16 upper case letters. 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.

19 If prompted, specify if you want Java and the JRE packages installed.

```
The Java GUI and JRE packages are currently not installed 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) Include the Java GUI and JRE.

2) Exclude the Java GUI and JRE.
```

If you specify `1`, you see: `Including the installation of Java GUI and JRE packages`. If you specify 2, you see: `Excluding the installation of Java GUI and JRE packages.`

20 Follow the prompts to complete the installation.

Additional information about installation folder restrictions is available.

See "Restrictions on the NetBackup installation directory" on page 17.

21 After the installation is complete, select **Exit from this Script**.

Install of the UNIX and Linux client binaries with native installers

You can install 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 installed with the NetBackup install script.

- For AIX: `lslpp`, `installp`

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

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

To install 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 178.

2. (Conditional) If your environment uses a NetBackup Certificate Authority, 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 178.

3. (Conditional) If your environment uses an external certificate authority, 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.
- `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 178.

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

- `SERVICES=no`
- `INSTALL_PATH=path`
- `MERGE_SERVER_LIST=value`

More information about each option is available.

See "About the NetBackup answer file" on page 178.

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_10.4_CLIENTS1.tar.gz; tar -xvf NetBackup_10.4_CLIENTS1.tar`
Linux	`tar -xzvf NetBackup_10.4_CLIENTS2.tar.gz`
Solaris	`tar -xzvf NetBackup_10.4_CLIENTS1.tar.gz`

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

AIX	`CLIENTS1/NBClients/anb/Clients/usr/openv/netbackup/client/RS6000/AIX7/`

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 installation of the Java GUI and the JRE is optional. If you do not want them installed, omit the copy and the install of the `VRTSnbjava` and `VRTSnbjre` packages.

AIX

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

Linux

```
VRTSnbpck.rpm
VRTSpbx.rpm
VRTSnbclt.rpm
VRTSnbclibs.rpm
VRTSnbjre.rpm
VRTSnbjava.rpm
VRTSpddeu.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.

Note: The `VRTSpddeu.rpm` package is optional, and is not supported on IBM pSeries and zSeries clients.

Solaris

```
.pkg_defaults
VRTSnbpck.pkg.gz
VRTSpbx.pkg.gz
VRTSnbclt.pkg.gz
VRTSnbclibs.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 the `VRTSnbjre.pkg.gz` and `VRTSnbjava.pkg.gz` files are not supported on Solaris clients.

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

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

7 (Conditional) For Solaris 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
VRTSnbclibs.pkg
VRTSnbjre.pkg
VRTSnbjava.pkg
VRTSpddea.pkg
VRTSnbcfg.pkg
```

Note: The `VRTSnbjre.pkg` and `VRTSnbjava.pkg` files are not supported on Solaris clients so they are not included.

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

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

AIX

```
installp -ad VRTSnbpck.image all
installp -ad VRTSpbx.image all
installp -ad VRTSnbclt.image all
installp -ad VRTSnbclibs.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
```

Linux

```
rpm -U VRTSnbpck.rpm
rpm -U VRTSpbx.rpm
rpm -U VRTSnbclt.rpm
rpm -U VRTSnbclibs.rpm
rpm -U VRTSnbjre.rpm
rpm -U VRTSnbjava.rpm
rpm -U VRTSpddeu.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.

Note: The `VRTSpddeu.rpm` package is optional, and is not supported on IBM pSeries and zSeries clients.

Solaris

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

```
pkgadd -a .pkg_defaults -d VRTSnbpck.pkg VRTSnbpck
pkgadd -a .pkg_defaults -d VRTSpbx.pkg VRTSpbx
pkgadd -a .pkg_defaults -d VRTSnbclt.pkg VRTSnbclt
pkgadd -a .pkg_defaults -d VRTSnbclibs.pkg VRTSnbclibs
pkgadd -a .pkg_defaults -d VRTSpddea.pkg VRTSpddea
pkgadd -a .pkg_defaults -d VRTSnbcfg.pkg VRTSnbcfg
```

- Be aware the `VRTSnbjre.pkg.gz` and `VRTSnbjava.pkg.gz` files are not supported on Solaris clients.
- 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.

9 (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

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 6-2 shows some of the actions and the message that is generated.

Table 6-2 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 install the UNIX or Linux client binaries using native installers:" on page 127.

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 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 install the UNIX or Linux client binaries using native installers:" on page 127.

Table 6-2 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 6-2 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 6-2 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 6-2 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 install the UNIX or Linux client binaries using native installers:" on page 127.

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.

About remote installation methods for UNIX and Linux clients

You can push the client software from a Linux primary server to a client host by using the following methods:

- `ssh`
  See "Installing client software with the ssh method" on page 139.
- `sftp`
  See "Installing client software with the sftp method" on page 140.

Note: For installation in clustered environments, enter the virtual name for the NetBackup server and not the actual local host name. You can only push client software from the active node.

Installing client software with the ssh method

This client installation method is based on the usage of the SunSSH and the OpenSSH products, which must be at specific version and patch levels. For more information about these patches, please refer to the NetBackup 10.4 Release Notes.

Before you perform this procedure, read the following guidelines:

SSH daemon (`sshd`)	To use the ssh method, the UNIX client must have `sshd` enabled and configured to allow root user logins.
Client software location	If you want to install client software to a location other than the default, you must first create and link the desired directory. Create the directory where you want the client software to reside, and then create `/usr/openv` as a link to that directory. Additional information about installation folder restrictions is available. See "Restrictions on the NetBackup installation directory" on page 17.
Backup policies	Make sure that the clients are assigned to a backup policy.
Security configuration	The `install_client_files` scripts may prompt you for security information based on your environment. The information that is required is based on the primary server security mode and the target host security configuration. For details on how to respond to these prompts, refer to the NetBackup Security and Encryption Guide.

To install client software from a Linux primary server to UNIX clients with the ssh method

- On the NetBackup server, run the `install_client_files` script.
  Use one of the following commands:

- To move software to only one client at a time:
  `/usr/openv/netbackup/bin/install_client_files ssh client`
  The *client* is the host name of the client.
- To move software to all clients at once:
  `/usr/openv/netbackup/bin/install_client_files ssh ALL`
  The *ALL* option specifies that you want to install all clients that are configured in any backup policy on the server.

Installing client software with the sftp method

This client installation method is based on the usage of the SunSSH and the OpenSSH products, which must be at specific version and patch levels. For more information about these patches, please refer to the NetBackup 10.4 Release Notes.

Before you perform this procedure, read the following guidelines:

SSH daemon (`sshd`)	To use this method, the UNIX client must have `sshd` enabled and configured to allow root or non-root user logins.
Client file location	If you want to install client software to a location other than the default, you must first create and link the desired directory. Create the directory where you want the software to reside, and then create `/usr/openv` as a link to that directory. Additional information about installation folder restrictions is available. See "Restrictions on the NetBackup installation directory" on page 17.
Backup policies	Make sure that the clients are assigned to a backup policy.
Security configuration	The `install_client_files` scripts may prompt you for security information based on your environment. The information that is required is based on the primary server security mode and the target host security configuration. For details on how to respond to these prompts, refer to the NetBackup Security and Encryption Guide.

To install client software from a Linux primary server to UNIX clients with the sftp method

1. To move the client software from the server to the `/tmp` directory on the client, run the `install_client_files` script on the NetBackup server.

   Use one of the following commands:

   - To move software to one client at a time:

```
/usr/openv/netbackup/bin/install_client_files sftp client user
```

The *client* is the host name of the client.

The *user* is the login ID that SSH requires on the client.

- To move software to all clients at once:

  ```
  /usr/openv/netbackup/bin/install_client_files sftp ALL user
  ```

  The *ALL* option specifies that you want to install all clients that are configured in any backup policy on the server.

  The *user* is the login ID required by the client.

2 After the script runs, the root user on each client computer must run the following script:

```
sh /tmp/bp.<pid>/client_config
```

The *pid* is the process ID. The `client_config` script installs the binaries.

Adding a UNIX/Linux client after initial server installation

You may want to add UNIX/Linux clients after the server installation if you forgot to select one during the installation. You may also add a new UNIX/Linux client type to your backup environment.

To install client software later, you must first install the NetBackup client software onto the NetBackup server.

To add UNIX/Linux client types to servers after initial installation

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 "Install of the UNIX and Linux client binaries with native installers" on page 126.

2 When the following message appears, press **Enter** to continue:

```
Veritas Installation Script
Copyright 1993 - 2013 Veritas Corporation, 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 out the Veritas Services and
Operations Readiness Tools (SORT) Installation and Upgrade Checklist
and Hot fix and EEB Release Auditor, respectively, at
https://sort.veritas.com/netbackup.

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. The installation procedure attempts to load the appropriate binaries for your system. If the script does not recognize the local operating system, it presents choices.

3 Select the client type that you want to load and follow the prompts to install that client type. Repeat as necessary until all of the client types you want are loaded.

Make sure that you load the software for all of the UNIX/Linux client types that you intend to install remotely from the server.

4 Install the NetBackup client software on the clients you specified.

See "About remote installation methods for UNIX and Linux clients" on page 138.

Chapter 7

Configuring NetBackup

This chapter includes the following topics:

- About NetBackup startup and shutdown scripts
- About NetBackup server configuration

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 7-1 lists the links for the startup and the shutdown scripts for the various platforms that are installed during NetBackup installation.

Table 7-1 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`

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`

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`

Table 7-1 NetBackup startup and shutdown script links by platform *(continued)*

Platform	Links

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`

About NetBackup server configuration

After all server software is installed, you are ready to configure NetBackup to work with the robotic and the storage devices in your environment. Remember the operating system must recognize these devices as configured before you can configure them in NetBackup.

See "About storage device configuration" on page 15.

Use the following guidelines when you configure NetBackup:

NetBackup Enterprise servers

The procedures for configuring primary and media servers are very similar. Veritas recommends, however, that you configure all server information such as storage devices and volumes from the primary server. Following this order helps ensure that the primary servers properly administer the media servers.

Warning: Communication problems between the primary server and the media server do not prevent you from running the configuration wizards. Therefore, do not run the wizards on the media server until the problems are corrected. If you run any of the wizards when a communication problem exists, the primary server cannot recognize the information that you enter. You must first correct the problem. After you correct the problem, run the configuration wizards from the primary server.

Clustered environments	■ Configure devices on every node in the cluster. ■ Start by configuring all storage devices from the active node so that they work with NetBackup. ■ For a NetBackup failover server, attach all of the devices to each node in the cluster on which NetBackup is installed. Refer to the clustering vendor's documentation for information on how to migrate to another node. ■ Unless otherwise noted, configure NetBackup to use the virtual host names of primary servers and media servers in the cluster. For complete information on to how to configure an add-on product to fail over, see the NetBackup Clustered Primary Server Administrator's Guide.

For initial NetBackup server configuration, Veritas recommends that you launch the NetBackup Administration Console and click the **Getting Started** icon. A series of wizards guide you through the following configuration procedures:

- **Configure Storage Devices**
  See "About the Device Configuration Wizard" on page 148.
- **Configure Volumes**
  See "About the Volume Configuration Wizard" on page 150.
- **Configure the Catalog Backup**
  See "About the Catalog Backup Wizard" on page 151.
- **Create a Backup Policy**
  See "About the Backup Policy Configuration Wizard" on page 152.

If NetBackup is already configured and you want to change a specific area, click the appropriate wizard on the NetBackup Administration Console.

For complete information on all of the NetBackup wizards and how to configure NetBackup, see the NetBackup Administrator's Guide, Volume I.

See "About storage device configuration" on page 15.

Starting the NetBackup Administration Console

Use the following procedures to open the NetBackup Administration Console to configure NetBackup. The **Getting Started** wizard guides you through the primary configuration steps to make NetBackup function.

Note: Other wizards are available from the initial NetBackup Administration Console window that are not part of the **Getting Started** wizard. For example, you can configure disk pools or create a snapshot backup policy. See the NetBackup Administrator's Guide, Volume I for complete information about all NetBackup wizards.

On Windows systems, if you clicked the check box **Launch Administration Console** that appears at the end of NetBackup installation, you can skip this procedure.

To start the NetBackup Administration Console on Windows

1. Log on to the NetBackup server as the Administrator.
2. Click **Start > Programs > Veritas NetBackup > NetBackup Administration Console**.
3. To begin configuration, on the Administration Console, click **Getting Started**.

   The **Getting Started** screen appears and prompts you to begin device configuration.

   Note: If you still need to configure devices to work with the operating system, close the wizard. You must first configure those devices as specified by the device and the operating system vendors.

To start the NetBackup Administration Console on UNIX

1. Log in to the NetBackup server as root.

   For clustered environments, log in to the active node as root.

   If you need to run the user interface on a computer other than the NetBackup server, log on to that computer. For UNIX systems, log in as root.
2. Enter the following command:

   ```
   /usr/openv/netbackup/bin/jnbSA &
   ```
3. Enter the password for root.

   For clustered environments, when you log in to the NetBackup Administration Console, specify the virtual host name in the **Host** field.
4. Click **Login**.

5 To begin configuration, on the Administration Console, click **Getting Started**.

6 On the initial **Getting Started** screen, review the content and click **Next**.

The following screen prompts you to **Configure Storage Devices**.

Note: If you still need to configure devices to work with the operating system, close the wizard. You must first configure those devices as specified by the device and the operating system vendors.

About the Device Configuration Wizard

Before you can run backups, you must define your storage devices for NetBackup. This wizard guides you through this process. You must, however, be certain that you have configured your storage devices correctly for your operating system. NetBackup cannot function reliably unless devices are installed and configured correctly.

See "About storage device configuration" on page 15.

For clustered environments, begin configuring all storage devices from the active node. For a NetBackup failover server, Veritas recommends that you attach all of the devices to every node on which NetBackup is installed.

For complete instructions, refer to the NetBackup Clustered Primary Server Administrator's Guide.

This wizard takes you through the following processes:

- Scans the hosts for backup devices
- Verifies the devices that were automatically detected
- Verifies and corrects the drive configuration
- Updates the device configuration

The wizard presents the following information when you configure devices:

Device configuration	■ When the wizard displays the **Device Hosts** screen, you must specify the hosts on which to auto-discover and configure devices (NetBackup Enterprise servers only). ■ When the wizard displays the **Backup Devices** screen, confirm that the list of devices is complete and accurate. If a known backup device does not appear in this list, take the following action: ■ Verify that the backup device is physically attached to the host. ■ Verify that all that specified device and operating system vendor installation procedures are performed successfully. ■ Verify that all drives correspond to the proper device. If you need to move a drive, select the drive and drag it to the correct location. ■ For clusters, ensure that you perform storage device configuration on each node. Begin on the active node, then move the NetBackup active node to another node and perform the storage device configuration on that node. Repeat for each node of the cluster on which NetBackup runs. **Note:** By default, robotic daemons and NetBackup add-on products do not cause NetBackup to failover if they fail. You can configure robotic devices and NetBackup add-on products to fail over NetBackup if the robot or the add-on product fails. The operating system must recognize the robots as configured before you can configure NetBackup to failover. For complete details about fail over configuration, refer to the NetBackup Clustered Primary Server Administrator's Guide.
Defining storage units	■ You define storage units from the **Configure Storage Units** screen. If your system does not have a tape device, you can store data on a disk by defining disk storage units. ■ When you enter a path for a storage unit, the following rules apply: ■ Use the correct path separators (forward slash (/) for UNIX and backward slash (\) for Windows). ■ Use a colon (:) to specify a drive separation on Windows platforms. ■ Use the following characters only: Alphabetic characters (ASCII A-Z, a-z) Numeric characters (0-9) Miscellaneous characters: plus (+), minus (-), underscore (_), or period (.)

See “About the Volume Configuration Wizard” on page 150.

About the Volume Configuration Wizard

After you have configured your storage devices, the Getting Started Wizard starts the Volume Configuration Wizard. However, if you only have disk storage capability, NetBackup skips this wizard.

This wizard lets you initiate an inventory of each configured robot. NetBackup automatically updates the volume database if it finds new robotic media during the inventory. In addition, you can define new volumes for use in standalone drives.

For complete information about volumes or volume configuration for standalone drives, refer to the NetBackup Administrator's Guide, Volume I.

Note: For clustered environments, configure volumes from the active node.

This wizard lets you do the following tasks:

- Select a device for volume configuration
- Perform an inventory of the robot
- Create new volumes
- Create new volume groups

The wizard presents the following information when you configure volumes and perform inventory:

Robot or device inventory	■ NetBackup conducts an inventory of the robot or the device that you selected. To view the results after the inventory has completed, see the **Results:** field. ■ After the device inventory has completed, the wizard prompts you to identify which device slots contain cleaning media. If you upgraded NetBackup and have pre-existing barcode rules, the barcode reader automatically detects the designated slots for the cleaning media. If you do not designate cleaning slots, NetBackup considers all media (including cleaning media) as typical media and tries to overwrite it. ■ After the inventory has completed, you are prompted to identify which device slots contain cleaning media. If you identify one or more slots as cleaning media in the **Identify Cleaning Media** screen, you see the **Robot Inventory (Cleaning Media)** screen. This screen displays the results after the software updates the EMM database. If you do not designate cleaning media, NetBackup considers all media to be typical media (including cleaning media) and tries to overwrite it.
Standalone drives	■ Specify the number of volumes for the device. ■ The wizard does not let you configure cleaning tapes for standalone drives.
Multiple drive types	When you specify multiple drive types, the following are true: ■ Media that is written by one robot drive may not work in any other drive. If this situation occurs, NetBackup considers the robot to have more than one type of drive. ■ If the robot has more than one type of drive, the wizard cannot inventory the robot.

See “About the Catalog Backup Wizard” on page 151.

About the Catalog Backup Wizard

The NetBackup catalog contains information about your configuration and the locations of backed up files and directories. If a disk fails and your catalog is lost, a catalog backup makes it easy to restore your data and resume your backup schedule.

Therefore, you must configure a catalog backup policy before any data gets backed up.

This wizard lets you create a policy for an online, hot catalog backup. Online, hot catalog backups can back up the catalog while normal client backups are in progress.

A catalog backup policy lets you specify the following information:

- The destinations for the catalog backup
  A backup destination can be any configured storage device. For additional disaster recovery protection, you can specify a second location for your catalog backup.

  Note: Although NetBackup supports catalog backup to disk, Veritas recommends that you back up the catalog to a removable media that gets stored off-site.

- The disaster recovery passphrase. More information about the passphrase is available. See the NetBackup Troubleshooting Guide.
- When the catalog backup occurs
- The location of the disaster recovery file that is needed to recover from the catalog backup

Use the following guidelines to configure a catalog backup:

- Configure a catalog backup policy before any other files or data are backed up.
- For clustered systems, configure the catalog backup policy from the active node.

For complete details about catalog backups, see the chapter “Protecting the NetBackup catalog” in the NetBackup Administrator's Guide, Volume I.

For instructions on how to configure a catalog backup in clustered environments, see the NetBackup Clustered Primary Server Administrator's Guide.

About the Backup Policy Configuration Wizard

This wizard lets you define a backup policy for a group of one or more clients. For clustered environments, configure the policy from the active node.

The wizard lets you specify the following:

- Policy names and types
- Clients
- Files and directories to back up
- Backup types
- Backup rotations
- Starting times of backups

The wizard prompts you to choose the type of backup that you want a policy to perform.

Table 7-2 describes the available backup types.

Table 7-2 Backup type descriptions

Backup type	Description
Full backup	Backs up all files that are specified in the file list.
Incremental backup	Backs up all the changed files that are specified in the file list.
Differential backup	Also referred to as a Differential incremental backup. Backs up the files that have changed since the last successful incremental or full backup. All files are backed up if no previous backup has been done.
Cumulative backup	Also referred to as a Cumulative incremental backup . Only the files that changed since the last full backup that was successful are backed up. All files are backed up if no previous backup has been done.
User backup	Initiated manually by a user to back up specific files.

Use the following guidelines when you create backup policies:

- The list that appears on the **Client List** screen of the Backup Policy Wizard is a list of clients that are backed up. You can add, change, or delete clients from the list.
- You can select how often you want a backup policy to run for full or incremental backups. In addition, you can select the retention period for the backups.

After you have completed the Backup Policy Wizard , you are asked if you want to perform an installation verification test. To do this test, click the **Activity Monitor** in the left pane of the NetBackup Administration Console. You can now monitor the progress of the backup job.

Chapter 8

Removing NetBackup server and client software

This chapter includes the following topics:

- About NetBackup server software removal on Linux systems
- About NetBackup client software removal on UNIX and Linux systems
- Removing NetBackup from UNIX and Linux servers and clients
- About NetBackup server software removal on Windows systems
- Removing NetBackup server and client software from Windows servers, clusters, and clients
- About removal of the Java Console state data from Windows servers and Windows clients
- Removing a clustered media server by migrating all data to a new media server

About NetBackup server software removal on Linux systems

NetBackup removal procedures remove NetBackup completely, along with any installed add-on products. Each procedure gives you the opportunity to save any data that you want and to remove add-on products before you remove NetBackup.

Veritas recommends that you use the following order when you remove NetBackup server software:

- Save any data that you require.
  This task is very important if you plan to reinstall NetBackup at a later date.

- Remove any add-on products before you remove NetBackup server software.
- Remove the NetBackup server software.

Note: As part of the removal of the NetBackup server software, the security certificates are automatically deleted. If you want to retain the certificates, please save them before removing NetBackup.

More information about this topic is available. Please refer to the information on retaining host ID-based certificates when reinstalling NetBackup in the NetBackup Security and Encryption Guide.

See "Removing NetBackup from UNIX and Linux servers and clients" on page 156.

See "About NetBackup client software removal on UNIX and Linux systems" on page 155.

About NetBackup client software removal on UNIX and Linux systems

Use the following guidelines when you remove NetBackup from UNIX/Linux clients:

When you remove NetBackup client software, PBX is not removed. You must remove PBX manually. The client software removal procedure in this document includes a step that describes how to perform this task.

As part of the removal of the NetBackup client software, the security certificates are automatically deleted. If you want to retain the certificates, please save them before removing NetBackup.

More information about this topic is available. Please refer to the information on retaining host ID-based certificates when reinstalling NetBackup in the NetBackup Security and Encryption Guide.

Warning: Do not remove PBX if your client uses other Veritas software products that require PBX to run.

Removing NetBackup from UNIX and Linux servers and clients

Use this procedure to remove NetBackup from UNIX and Linux servers and clients. You may also need to reference other documents for procedures of specific tasks to remove NetBackup successfully.

Use the following guidelines when you remove NetBackup from UNIX and Linux servers and clients:

NetBackup relational database (NBDB) location	If you moved the NBDB files in `/usr/openv/db/data` from their default installation location, this procedure includes a step that describes how to remove these files.
Clustered environments	Before you begin to remove NetBackup, you must remove NetBackup from the cluster application. Follow the instructions in your cluster documentation on how to remove a group, then you can remove NetBackup. The virtual host name security certificates are automatically removed from the shared drive of the cluster as a part of NetBackup server software removal. You must remove NetBackup from each node in the cluster.
PBX	When you remove NetBackup, PBX is not removed. You must remove PBX manually. This procedure includes a step that describes how to perform this task. **Warning:** Do not remove PBX if your server uses other Veritas software products that require PBX to run.
NetBackup Administration Console	The NetBackup Administration Console must be closed when you remove NetBackup. Otherwise, NetBackup may cause a failure that forces you to restart the procedure.
NetBackup IT Analytics Data Collector install location	NetBackup IT Analytics Data Collector is installed at `/usr/openv/analyticscollector` by default. If IT analytics DC is installed at any other location, a symbolic link is created at `/usr/openv/analyticscollector`.

Note: Since the `VRTSpddeu.rpm` package is optional, you may not need to remove it.

To remove NetBackup from Linux servers

1. Log on as the root user on the server or the client.
2. (Conditional: servers only) Perform a catalog backup.
3. If the NetBackup Administration Console is open, you must close it now.
4. (Conditional: servers only) Save all important data from any add-on products that you have installed.
5. Stop the NetBackup/Media Manager daemons with the following command:

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

6. Identify any installed add-on products by using the following command:

AIX	`lslpp -L`
Linux	`rpm -qa`
Solaris	`pkginfo`

   Look for any of the seven add-on products listed:

   ```
   VRTSfrnb (Applies only to servers)
   VRTSfrnbclt
   VRTSjanb (Applies only to servers)
   VRTSjanbclt
   VRTSzhnb (Applies only to servers)
   VRTSzhnbclt
   VRTSnbsds (Applies only to servers)
   ```

   Remove any add-on products found.

7. To unregister NetBackup from the VxUL primary configuration that is stored in the `/etc/vx/vrtslog.conf` file, run the following command:

   ```
   /usr/openv/netbackup/bin/vxlogcfg -r -p 51216
   ```

   The `-p` option specifies the product ID, which is 51216 for NetBackup.

8. (Conditional: servers only) If BMR is supported and enabled on the server, remove the associated files with the following command:

   ```
   /usr/openv/netbackup/bin/bmrsetupmaster -undo -f
   ```

9. (Conditional: servers only) If you moved the NBDB files from their default installation location, you must delete these files manually as follows:

   - Navigate to the following directory where the NBDB files reside:

```
/usr/openv/db/data
```

- Open the `vxdbms.conf` file.

  This file contains a list of the database-related files and the path for each file.
- Delete each of the database-related files.

10 (Conditional: servers only) If NetBackup Fibre Transport is supported and enabled on the server, remove the associated files.

- If NetBackup Fibre Transport is enabled with BSI driver on Red Hat 7.x, run the command shown:

  ```
  /usr/openv/netbackup/bin/admincmd/nbftsrv_config -d
  ```
- If NetBackup Fibre Transport is enabled with SCST driver, run the command shown:

  ```
  /usr/openv/netbackup/bin/admincmd/nbftsrv_config -scst
  -uninstall
  ```

11 (Conditional: servers only) To remove the NetBackup server libraries, run the command shown.

Note: The virtual host name security certificates are automatically removed from the shared drive of the cluster as a part of NetBackup server software removal.

More information about this topic is available. Please refer to the information on retaining host ID-based certificates when reinstalling NetBackup in the NetBackup Security and Encryption Guide.

Linux: `rpm -e VRTSnbslibs`

12 (Conditional: primary servers only) Remove the packages shown, in the order shown, with the listed command:

- `rpm -e VRTSnbweb`
- `rpm -e VRTSnbmqbrkr`

13 (Conditional: servers only) To remove the NetBackup server package, run the commands shown.

Note: The virtual host name security certificates are automatically removed from the shared drive of the cluster as a part of NetBackup server software removal.

More information about this topic is available. Please refer to the information on retaining host ID-based certificates when reinstalling NetBackup in the NetBackup Security and Encryption Guide.

- Linux primary server:

  ```
  rpm -e VRTSnbprimary
  rpm -e VRTSnetbp
  ```

- Linux media server:

  ```
  rpm -e VRTSnetbp
  ```

14 (Conditional: primary servers only) Remove the package shown with the command shown:

```
rpm -e VRTSpostgresql
```

15 Remove the NetBackup configuration package with the appropriate command as follows:

AIX	`installp -u VRTSnbcfg`
Linux	`rpm -e VRTSnbcfg`
Solaris	`pkgrm VRTSnbcfg`

16 For the clients that support PureDisk, remove all PureDisk files with the following command:

```
/opt/pdde/pddeuninstall.sh -forceclean
```

17 (Conditional: servers only) For the clients that support MSDP, remove all MSDP files with the following command:

```
/opt/pdde/pddeuninstall.sh -basedir /usr/openv/pdde/ -ostdir
/usr/openv/lib/ost-plugins/ -forceclean
```

Note: Be aware the preceding command is a single command which takes three parameters (`basedir`, `, ostdir`, and `forceclean`), and two directory parameters take paths as input.

18 Remove the NetBackup-Java Display Console by using the appropriate native command as follows:

AIX	`installp -u VRTSnbjava`
Linux	`rpm -e VRTSnbjava`
Solaris	`pkgrm VRTSnbjava`

19 Remove the NetBackup Java Runtime Environment by using the appropriate native command as follows:

AIX	`installp -u VRTSnbjre`
Linux	`rpm -e VRTSnbjre`
Solaris	`pkgrm VRTSnbjre`

20 Remove the NetBackup client libraries by using the appropriate native command as shown.

Note: As part of the removal of the NetBackup server software, the security certificates are automatically deleted. If you want to retain the certificates, please save them before removing NetBackup.

More information about this topic is available. Please refer to the information on retaining host ID-based certificates when reinstalling NetBackup in the NetBackupSecurity and Encryption Guide.

AIX	`installp -u VRTSnbclibs`
Linux	`rpm -e VRTSnbclibs`
Solaris	`pkgrm VRTSnbclibs`

21 Remove the NetBackup client by using the appropriate native command as shown.

Note: As part of the removal of the NetBackup server software, the security certificates are automatically deleted. If you want to retain the certificates, please save them before removing NetBackup.

More information about this topic is available. Please refer to the information on retaining host ID-based certificates when reinstalling NetBackup in the NetBackupSecurity and Encryption Guide.

AIX	`installp -u VRTSnbclt`
Linux	`rpm -e VRTSnbclt`
Solaris	`pkgrm VRTSnbclt`

Note: If there are running NetBackup processes and daemons, terminate them manually for a successful NetBackup removal.

22 Remove PBX with the appropriate native command as follows:

Note: Remember, you should not remove PBX if your server uses other Veritas software products that require PBX to run.

AIX	`installp -u VRTSpbx`
Linux	`rpm -e VRTSpbx`
Solaris	`pkgrm VRTSpbx`

23 Remove NetBackup Pre-Check package with the appropriate command as follows:

AIX	`installp -u VRTSnbpck`
Linux	`rpm -e VRTSnbpck`
Solaris	`pkgrm VRTSnbpck`

24 (Conditional: Linux only): Remove the Veritas PDDE package with the command shown:

```
rpm -e VRTSpddei
```

25 Remove PostgreSQL package

```
rpm -e VRTSpostgresql.rpm
```

26 Run the script that is shown to remove NetBackup IT Analytics Data Collector on Linux.

```
/usr/openv/analyticscollector/UninstallerData/uninstall_dc.sh -r
```

Remove the symbolic link from `/usr/openv/analyticscollector` if it exists.

If the `uninstall_dc.sh` script is unavailable for any reason, complete the steps shown:

1. Stop the NetBackup IT Analytics Data Collector services:

```
/usr/openv/analyticscollector/mbs/bin/aptare_agent stop
systemctl stop aptare_kafka.service
systemctl stop aptare_zookeeper.service
systemctl disable aptare_zookeeper.service
systemctl disable aptare_kafka.service
```

2. Delete the files. If `/usr/openv/analyticscollector/` is a symbolic link, follow the link and identify the actual install path:

```
rm -rf /usr/openv/analyticscollector/
```

If `/usr/openv/analyticscollector/` is symbolic link, be sure to delete the actual DC install path.

```
rm -f /etc/systemd/system/aptare_kafka.service
rm -f /etc/systemd/system/aptare_zookeeper.service
systemctl daemon-reload
rm -f /etc/init.d/aptare_agent
```

3. Remove the RC scripts if they exist:

```
rm -f /etc/rc3.d/K*aptare_agent
rm -f /etc/rc3.d/S*aptare_agent
rm -f /etc/rc5.d/K*aptare_agent
rm -f /etc/rc5.d/S*aptare_agent
```

4. If any stale processes are active on the system, stop them with the `kill -9 pid` command.

```
ps -ef | grep aptare
kill -9 pid
```

27 Remove the `/usr/openv` directory.

Warning: The `rm` commands used remove any add-on products that are installed on the computer where you perform this command.

- Determine if `/usr/openv` is a symbolic link with the command shown. If `/usr/openv` is a symbolic link, make note of the actual path. The path is required for a later command.

  ```
  file -h /usr/openv
  /usr/openv: symbolic link to /opt/openv
  ```

- If `/usr/openv` is a symbolic link, run the commands shown:

`cd /usr/openv`	This command changes you into the directory that symbolic link points to, such as `/opt/openv`.
`ls`	List the contents of the directory. Review this information to confirm what you are about to delete.

  Warning: Before you continue, make sure that you are at the correct location and verify that the subdirectories are what you expect them to be. To help prevent removing the wrong directories, the previous commands verify your current location and list the files in that directory. After you verify the directory location and its contents, remove the directory with the next commands.

`cd /`	Change to the root directory.
`rm -rf` *`directory`*	For the *`directory`* value, enter the information from the `file` command. This command deletes the directory that contains the NetBackup binaries. Example: `rm -rf /opt/openv`
`rm -f /usr/openv`	Delete the symbolic link.

- If `/usr/openv` is the actual directory, run the command shown:

  ```
  rm -rf /usr/openv
  ```

  Note: Depending on your operating system, you may need to use the `rmdir` command to remove the `/usr/openv` directory.

  ```
  rmdir /usr/openv
  ```

28 For Linux systems only:

If you modified the startup and the shutdown scripts, run the following command:

```
/sbin/chkconfig --del netbackup
```

Depending on the distribution of Linux, the startup and the shutdown scripts may already be deleted.

See “About NetBackup startup and shutdown scripts” on page 143.

29 Remove the scripts shown. Depending on the operating system, the startup and the shutdown scripts may already be deleted.

On AIX systems:

```
/etc/rc.netbackup.aix
```

On Linux Debian systems:

```
/etc.init.d/netbackup
/etc/rc0.d/K01netbackup
/etc/rc1.d/K01netbackup
/etc/rc2.d/S95netbackup
```

On Linux Red Hat systems:

```
/etc/rc.d/init.d/netbackup
/etc/rc.d/rc0.d/K01netbackup
/etc/rc.d/rc1.d/K01netbackup
/etc/rc.d/rc2.d/S77netbackup
/etc/rc.d/rc3.d/S77netbackup
/etc/rc.d/rc5.d/S77netbackup
/etc/rc.d/rc6.d/K01netbackup
```

The following startup scripts are only on servers and appear only if NetBackup Fiber Transport was enabled on the server:

```
/etc/rc.d/init.d/nbftserver
/etc/rc.d/rc0.d/K03nbftserver
/etc/rc.d/rc1.d/K03nbftserver
/etc/rc.d/rc2.d/S21nbftserver
/etc/rc.d/rc3.d/S21nbftserver
/etc/rc.d/rc5.d/S21nbftserver
/etc/rc.d/rc6.d/K03nbftserver
```

On Linux SUSE systems:

```
/etc/init.d/netbackup
/etc/init.d/rc0.d/K01netbackup
/etc/init.d/rc2.d/S77netbackup
/etc/init.d/rc3.d/S77netbackup
/etc/init.d/rc5.d/S77netbackup
/etc/init.d/rc6.d/K01netbackup
```

The following startup scripts are only on servers and appear only if NetBackup Fiber Transport was enabled on the server:

```
/etc/init.d/nbftserver
/etc/init.d/rc2.d/K01nbftserver
/etc/init.d/rc2.d/S05nbftserver
/etc/init.d/rc3.d/K01nbftserver
/etc/init.d/rc3.d/S05nbftserver
/etc/init.d/rc5.d/K01nbftserver
/etc/init.d/rc5.d/S05nbftserver
```

On other servers and clients:

```
/etc/init.d/netbackup
/etc/rc0.d/K01netbackup
/etc/rc1.d/K01netbackup
/etc/rc2.d/S77netbackup
```

The following startup scripts are only on servers and appear only if NetBackup Fiber Transport was enabled on the server:

```
/etc/init.d/nbftserver
/etc/rc0.d/K03nbftserver
/etc/rc1.d/K03nbftserver
/etc/rc2.d/S21nbftserver
```

30 For AIX systems only:

- In the `/etc/inittab` file, remove the following NetBackup entry:

  ```
  /etc/rc.netbackup.aix
  ```

- In the `/etc/rc.shutdown` file, remove the following line:

  ```
  /etc/rc.netbackup.aix stop
  ```

31 Remove the LiveUpdate components as follows:

- First, examine the following file to see if NetBackup is the only product that uses LiveUpdate:

  `/etc/Product.Catalog.JavaLiveUpdate`

- If NetBackup is the only product that currently uses LiveUpdate, run the following command:

  `/opt/Symantec/LiveUpdate/uninstall.sh -a`

- If LiveUpdate is the only product installed in the `/opt/Symantec` directory, remove the following files:

  `rm -f /etc/Symantec.conf`

  Note: Before you remove the following product catalog file, make sure that it is empty. The empty file size is equal to 0 bytes. If the product catalog file is not empty, do not remove it because other products still require it.

  `rm -f /etc/Product.Catalog.JavaLiveUpdate`

32 To remove the NetBackup-Java application state data for the root account, run the appropriate command as follows:

Warning: Do not insert a space between the slash character (/) and the period or the dot character (.) of `/.veritas`. A space between these characters removes all of your files from the root level and beyond.

- To remove the NetBackup-Java application state data for the root account for all releases, run the following command:

  `/bin/rm -rf /.veritas`

- To remove the NetBackup-Java application state data for the root account for a specific release, run the following command:

  `/bin/rm -rf /.veritas/java/`*`version`*

  Where *version* is the six-digit NetBackup version number. For example, NetBackup version 8.0 with no upgrades applied would be entered as **800000**.

33 Inform NetBackup-Java users that they can remove their `$HOME/.veritas` directory.

The `$HOME/.veritas` and the `$HOME/.veritas/java` directories contain application state information, that is saved when the user exits NetBackup-Java applications. The saved information includes table column order and size. The process removes this directory for the root user only.

The `common` subdirectory in `$HOME/.veritas/java/.userPrefs/vrts` can be removed.

34 If you enabled NetBackup Access Control, NetBackup placed several files on clients and servers. These files can be divided into the following categories:

- NetBackup application temporary files
  These files are removed with NetBackup.
- Individual user (cache) files
  These cache files reside in the `$HOME/.vxss` directory. Inform all users that they can remove this directory.
  Files are generated in the `/.vxss` directory by a Single Sign-On operation of the NetBackup Administration Console on the host where the console runs. The NetBackup Administration Console cleans these files when an exit function is performed, so the directory does not always contain temporary files. However, if a system crash were to occur, any files in the directory may be left behind. With the console shutdown , you can delete these files safely with no data loss.
  NetBackup also creates cached certificates for client and server NetBackup applications. These files reside within the `/.vxss` directory. These files typically have a name that is consistent with a DNS entry for a network interface, as in `machine.company.com`. Example directory entries are as follows:

  ```
  /usr/openv/var/vxss/credentials/machine.company.com
  /usr/openv/var/vxss/credentials/dhcp
  ```

  These files are created with the command `bpnbat -LoginMachine`. If you plan to reinstall NetBackup on the same computer at a later date, do one of the following:

  - Preserve the certificates in the `vxss/credentials` directory.
  - If you do not preserve the certificates, you must provide the computer identity password as originally set on the Root+AB broker. As an alternative, you can reset the password on the Root+AB broker when you reinstall.

  For more information on Root+AB brokers, see the .NetBackup Security and Encryption Guide

For more information on NetBackup Access Control and how to remove it, see the NetBackup Security and Encryption Guide.

About NetBackup server software removal on Windows systems

When you remove NetBackup server software, the process deletes the `VERITAS/NetBackup` directories from the server.

You can remove NetBackup server software in the following ways:

- Remove server software, configuration, and catalog information.
- Remove server software and save NetBackup configuration and catalog information.
  If you intend to reinstall NetBackup, use this procedure to save the configuration, catalog, and log file information before you remove NetBackup.
  If the `postgresql.msi` does not uninstall PostgreSQL, you must set a registry key to allow a manual uninstall. The key name is `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup Scale Out Relational Database Service`. The value name is `BlockUninstall`. It is set to 1 by default. Set the value to 0, save, and retry the uninstall.

  Note: As part of the removal of the NetBackup server software, the security certificates are automatically deleted. If you want to retain the certificates, please save them before removing NetBackup.

  More information about this topic is available. Please refer to the information on retaining host ID-based certificates when reinstalling NetBackup in the NetBackup Security and Encryption Guide.

  Note: After an uninstall, some registry and some directory information remain on a Windows computer. This behavior is by design, as these files may be in use by either the NetBackup Authentication Service or the NetBackup Authorization Service.

  See "Removing NetBackup server and client software from Windows servers, clusters, and clients" on page 171.
- For clusters, perform all steps on all nodes of the cluster.

Removing NetBackup server and client software from Windows servers, clusters, and clients

Use the following procedures to remove NetBackup software and NetBackup configuration and catalog information.

To remove NetBackup server and client software

1. (Conditional: cluster only) Follow the instructions in your cluster documentation for removing a group.

   No method exists to remove NetBackup from multiple nodes at the same time.

2. (Conditional: server and cluster only) If the NetBackup Administration Console is open, close it.

   (Conditional: client only) If the NetBackup Backup, Archive, and Restore interface is open, close it.

   If either of these interfaces is open when you try to remove NetBackup, a failure may occur that forces you to restart this procedure.

3. Select **Start > Settings > Control Panel**.

4. On the **Control Panel** window, select the appropriate utility for installed programs and applications.

5. On the **Currently Installed Programs** list, click **Veritas NetBackup** for servers and clusters. Select **Veritas NetBackup Client** for clients.

Note: Be aware that the removal of the **Veritas NetBackup** item for servers and clusters removes the Veritas NetBackup Java GUI and the Veritas NetBackup JRE packages.

---

6 Click **Remove**.

For Windows, after you click **Yes** to continue, another dialog box appears to inform you that PBX is still running.

Veritas recommends that you click **Do not close applications. (A reboot will be required.)** to continue with NetBackup removal. PBX is stopped and restarted automatically as needed for removal.

7 (Conditional: server and cluster only) Remove the NetBackup deduplication user directory as follows:

In the **Documents and Settings** directory, delete the **purediskdbuser** directory.

The virtual host name security certificates are automatically removed from the shared drive of the cluster as a part of NetBackup server software removal.

Use the following procedure to remove NetBackup server software and save NetBackup configuration and catalog information.

To remove and save NetBackup configuration and catalog information

1 If the NetBackup Administration Console is open, close it.

If a console session is open when you try to remove NetBackup, a failure may occur that forces you to restart this procedure.

2 Select **Start > Settings > Control Panel**.

3 On the **Control Panel** window, select the appropriate utility for installed programs and applications. .

4 In the **Currently Installed Programs** list, click **Veritas NetBackup** .

5 Click **Change**. This action lets you modify, repair, or remove NetBackup.

6 On the **Program Maintenance** dialog box, select **Remove**.

7 Clear the check mark next to **Remove all NetBackup Configuration, Catalog, and Log files** to disable this function. (The box is checked by default.)

8 Click **Next**.

9 If you enabled NetBackup Access Control, NetBackup placed several files on clients and servers. These files can be divided into the following categories:

NetBackup application temporary files	These files are removed with NetBackup.

Individual user (cache) files	User cache files exist in their home directories, as follows:
	`user\Local Settings\Application Data\VERITAS\NetBackup`
	Files are generated in the `\NetBackup` directory by a Single Sign-On operation of the NetBackup Administration Console on the host where the console runs. The NetBackup Administration Console cleans these files when an exit function is performed, so the directory does not always contain temporary files. If a system crash were to occur, however, any files in the directory may be left behind. With the console shutdown, you can delete these files safely with no data loss.
	NetBackup also creates cached certificates for client and server NetBackup applications. These files reside within the `\NetBackup` directory. These files typically have a name that is consistent with a DNS entry for a network interface, such as `machine.company.com`. Example directory entries are as follows:
	`user\Local Settings\Application Data\VERITAS\NetBackup\pc.comp.com`
	`user\Local Settings\Application Data\VERITAS\NetBackup\dhcp`
	These files are created with the command `bpnbat -LoginMachine`. If you plan to reinstall NetBackup on the same computer at a later date, do one of the following:
	■ Preserve the certificates in the `\NetBackup` directory.
	■ If you do not preserve the certificates, you must provide the computer identity password as originally set on the Root+AB broker. As an alternative, you can reset the password on the Root+AB broker when you reinstall. See the NetBackup Security and Encryption Guide.

10 Remove the NetBackup deduplication user directory as follows:

Note: This step is necessary only if you upgraded to version 10.4 from a previous or earlier version of NetBackup.

In the **Documents and Settings** directory, delete the `puredisk\dbuser` directory.

About removal of the Java Console state data from Windows servers and Windows clients

The NetBackup Java Console stores state data on a per-user basis. This information includes user preferences, toolbar locations, and related settings. After you uninstall the NetBackup Java Console, remove the state data by deleting the following folder:

USERPROFILE_DIR\Veritas\Java*JAVA_VERSION*

- For roaming user profiles, *USERPROFILE_DIR* is `%APPDATA%`.
- For local user profiles on Windows, *USERPROFILE_DIR* is `%LOCALAPPDATA%`.
- *JAVA_VERSION* is a six-digit NetBackup version number. For example, NetBackup version 8.0 with no upgrades applied would be `800000`.

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.

Chapter 9

Reference

This chapter includes the following topics:

- Generate a certificate on the inactive nodes of a clustered primary server
- NetBackup database user
- About the NetBackup answer file
- About the NetBackup IT Analytics Data Collector
- Manually install or uninstall NetBackup IT Analytics Data Collector binaries
- Manually configure the NetBackup IT Analytics Data Collector
- Persistent Java Virtual Machine options
- About RBAC bootstrapping
- NetBackup primary server web server user and group creation
- About the NetBackup Java Runtime Environment
- Add or Remove Java GUI and JRE after install
- Using NetApp disk arrays with Replication Director
- Security updates to the NetBackup database
- Size guidance for the NetBackup primary server and domain

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

After finishing a clustered primary 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 primary 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.

   Linux: `/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 primary server nodes in the *NetBackup Security and Encryption Guide*.

NetBackup database user

As part of the NetBackup 10.2 upgrade, the NetBackup database is converted to a new database. That database operates under a user account with limited privileges. For Linux, this account must be a non-root user. The account must be on each primary server (or each node of a clustered primary server).

Note: For security purposes, do not create an account with administrator or superuser privileges. Do not add the user to the `sudoer` list.

You can use numerous procedures to create this user. Some specific approaches are shown, but other methods may accomplish the same goal. The user must have sufficient permissions to run daemons. More information about this topic is available.

See "Installation requirements for UNIX and Linux" on page 34.

Be aware of the operating system-specific account requirements:

- A separate database user account is required for Linux only if the service account is root. If the service account is non-root, you do not need to create an additional user.
- In 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 primary servers, you must use a domain account. You can use a domain account for non-clustered environments, but it is not required.

The NetBackup primary server installation fails if 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 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 NetBackup catalog remains active, NetBackup continues to operate normally.

When you attempt to restart NetBackup, the restart fails due to the expired password. Navigate to the appropriate area in the operating system, supply the correct password, and restart the service.

To create the database user account

1. Create a local user.
   - **Linux:** `useradd -c 'NetBackup database user account' username`
   - **Windows:** `C:\>net user username strong_password /add`
2. (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.
   - Save your changes and close the **Properties** dialog for **Log on as a service**.

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 primary, 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 primary, 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 `silentprimary.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 9-1 All template options and required computers

Option	NetBackup role	Platform	Required for install?
ABORT_REBOOT_INSTALL	Primary, media, and client	Windows	No
ACCEPT_EULA	Primary, media, and client	UNIX and Linux	No
ACCEPT_REVERSE_CONNECTION	Client	All	No
ADDITIONALSERVERS	Primary, media, and client	Windows	No
ALLOW_PRE_90_UPGRADE	Primary	All	No
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	Yes
DATABASE_USER	Primary	Linux	Review DATABASE_USER for details.
DISASTER_RECOVERY_INSTALL	Primary	Linux	No
ECA_CERT_PATH	Media and client	All	Review About security configuration considerations for details.

Table 9-1 All template options and required computers *(continued)*

Option	NetBackup role	Platform	Required for install?
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.
INCLUDE_JAVA_GUI_AND_JRE	Media and clients	All	UNIX and Linux media servers and clients: No Windows media servers: Yes
INCLUDE_VRTSPDDEU_CLIENT	Client	Linux	No See the option details for more information related to role and platform.
INSTALL_ITA_DATA_COLLECTOR	Primary	All	No
INSTALL_PATH	Media and client	All	No
INSTALLDIR	Primary, media, and client	Windows	Yes
LICENSE	Primary	All	Yes
MACHINE_ROLE	Media and client	UNIX and Linux	Yes
MEDIA_SERVER	Primary, media, and client	UNIX and Linux	No

Table 9-1 All template options and required computers *(continued)*

Option	NetBackup role	Platform	Required for install?
MEDIASERVER	Media	Windows	No
MERGE_SERVERS_LIST	Client	UNIX and Linux	No
NB_FIPS_MODE	Primary, media, and client	All	No
PRIMARYSERVER	Primary, media, and client	Windows	Yes
PROCEED_WITH_INSTALL	Primary, media, and client	UNIX and Linux	No
RBAC_DOMAIN_NAME	Primary	Linux	No
RBAC_DOMAIN_TYPE	Primary	Linux	No
RBAC_PRINCIPAL_NAME	Primary	Linux	No
RBAC_PRINCIPAL_TYPE	Primary	Linux	No
SECURITY_CONFIGURATION	Media and client	All	No
SERVER	Media and client	UNIX and Linux	Yes
SERVICES	Client	UNIX and Linux	No
SERVICESTARTTYPE	Primary, media, and client	Windows	No
SERVICE_USER	Primary	Linux	Yes
START_JOB_DAEMONS	Primary	Linux	No
STOP_NB_BEFORE_VCREDIST	Primary, media, and client	Windows	No
STOP_NBU_PROCESSES	Primary, media, and client	Windows	No
USE_URANDOM	Primary, media, and client	UNIX and Linux	No
VCREDIST_ATTEMPT_PREFERENCE	Primary, media, and client	Windows	No
VCREDIST_RESTART_PREFERENCE	Primary, media, and client	Windows	No

Table 9-1 All template options and required computers *(continued)*

Option	NetBackup role	Platform	Required for install?
VNETD_PORT	Primary, media, and client	Windows	No
VXDBMS_POSTGRESQL_POOLER_ODBC_PORT	Primary	All	No
WEBSVC_DOMAIN	Primary	Windows	Yes
WEBSVC_GROUP	Primary	All	UNIX and Linux: No Windows: Yes
WEBSVC_PASSWORD_PLAIN	Primary	Windows	Yes
WEBSVC_USER	Primary	All	UNIX and Linux: No Windows: Yes

Answer file options by platform and role

These tables show the possible answer file options based on platform and role. Not all listed options are required. Refer to Table 9-1 or the option details for further information.

Table 9-2 Platform and role

Role	Windows computers	UNIX and Linux computers
Primary	ABORT_REBOOT_INSTALL ADDITIONALSERVERS ALLOW_PRE_90_UPGRADE INSTALL_ITA_DATA_COLLECTOR INSTALLDIR LICENSE NB_FIPS_MODE PRIMARYSERVER SERVICESTARTTYPE STOP_NB_BEFORE_VCREDIST STOP_NBU_PROCESSES VCREDIST_ATTEMPT_PREFERENCE VCREDIST_RESTART_PREFERENCE VNETD_PORT VXDBMS_POSTGRESQL_POOLER_ODBC_PORT WEBSVC_DOMAIN WEBSVC_GROUP WEBSVC_PASSWORD_PLAIN WEBSVC_USER	ACCEPT_EULA ALLOW_PRE_90_UPGRADE CLIENT_NAME DATABASE_USER DISASTER_RECOVERY_INSTALL INSTALL_ITA_DATA_COLLECTOR INSTALL_PATH LICENSE MACHINE_ROLE MEDIA_SERVER NB_FIPS_MODE PROCEED_WITH_INSTALL RBAC_DOMAIN_NAME RBAC_DOMAIN_TYPE RBAC_PRINCIPAL_NAME RBAC_PRINCIPAL_TYPE SERVER SERVICE_USER START_JOB_DAEMONS USE_URANDOM VXDBMS_POSTGRESQL_POOLER_ODBC_PORT WEBSVC_GROUP WEBSVC_USER

Table 9-2 Platform and role *(continued)*

Role	Windows computers	UNIX and Linux computers
Media	ABORT_REBOOT_INSTALL ADDITIONALSERVERS AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT ECA_CERT_PATH ECA_CERT_STORE ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INSTALL_PATH INSTALLDIR MEDIASERVER NB_FIPS_MODE PRIMARYSERVER SERVICESTARTTYPE STOP_NB_BEFORE_VCREDIST STOP_NBU_PROCESSES VCREDIST_ATTEMPT_PREFERENCE VCREDIST_RESTART_PREFERENCE VNETD_PORT	ACCEPT_EULA AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT CLIENT_NAME ECA_CERT_PATH ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INSTALL_PATH MACHINE_ROLE NB_FIPS_MODE PROCEED_WITH_INSTALL SERVER USE_URANDOM

Table 9-2 Platform and role *(continued)*

Role	Windows computers	UNIX and Linux computers
Client	ABORT_REBOOT_INSTALL ACCEPT_REVERSE_CONNECTION ADDITIONALSERVERS AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT CLIENT ECA_CERT_PATH ECA_CERT_STORE ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INSTALL_PATH INSTALLDIR NB_FIPS_MODE PRIMARYSERVER SERVICESTARTTYPE STOP_NB_BEFORE_VCREDIST STOP_NBU_PROCESSES VCREDIST_ATTEMPT_PREFERENCE VCREDIST_RESTART_PREFERENCE VNETD_PORT	ACCEPT_EULA ACCEPT_REVERSE_CONNECTION AUTHORIZATION_TOKEN CA_CERTIFICATE_FINGERPRINT CLIENT_NAME ECA_CERT_PATH ECA_CRL_CHECK_LEVEL ECA_CRL_PATH ECA_KEY_PASSPHRASEFILE ECA_PRIVATE_KEY_PATH ECA_TRUST_STORE_PATH INCLUDE_JAVA_GUI_AND_JRE INCLUDE_VRTSPDDEU_CLIENT INSTALL_PATH MACHINE_ROLE MEDIA_SERVER MERGE_SERVERS_LIST NB_FIPS_MODE PROCEED_WITH_INSTALL SERVER SERVICES USE_URANDOM

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. You can skip the security configuration but that requires manual steps on each target host after installation or upgrade.

To use the NetBackup primary server as your Certificate Authority, the `CA_CERTIFICATE_FINGERPRINT` of the primary server must be provided. The `AUTHORIZATION_TOKEN` option may be required depending on either the security level of the primary server or if this computer is already configured on the primary

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, include the SECURITY_CONFIGURATION key and set it to SKIP. Remove the CA_CERTIFICATE_FINGERPRINT, AUTHORIZATION_TOKEN, and all ECA_ values from the answer file. If you continue the installation or the upgrade without the required certificate authority components, backups and restores fail.

ABORT_REBOOT_INSTALL

- Description: This option specifies whether to proceed with remaining steps if one or more files being held in use have been overwritten such that a restart is required. If set to 1, the installation halts, the system is restored to its original state, and the restart is not required.

- Applicable platforms: Windows only.
- Default value: `0`
- Required: No.
- `ABORT_REBOOT_INSTALL 0 | 1`
- Return to Table 9-1.

ACCEPT_EULA

- Description: This option specifies if you accept the terms of the EULA and want to proceed with the installation or the upgrade.
- Applicable platforms: UNIX and Linux
- Default value: None
- Required: No
- `ACCEPT_EULA = yes | no`
- Return to Table 9-1.

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 9-1.

ADDITIONALSERVERS

- Description: Use this option to Include NetBackup media servers that are used to proxy security requests to the primary 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 9-1.

`ALLOW_PRE_90_UPGRADE`

- Description: This field is for primary 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 primary server platform.
  - **Windows**
    This value is required for silent upgrades of Windows primary servers. Specify `1` to allow the upgrade to continue, specify `0` to prevent the upgrade. This value is ignored during an interactive Windows primary 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.
  - **Linux**
    For Linux primary 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 9-1.

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 primary server.
  - The primary 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 9-1.

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.
  Be aware that CA_CERTIFICATE_FINGERPRINT is ignored under either of these conditions:
  - ECA is in use on the primary server.
  - The primary 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*

- Return to Table 9-1.

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 primary 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 9-1.

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 primary 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: Yes
- CLIENT_NAME=*name* | XLOCALHOSTX
- Return to Table 9-1.

DATABASE_USER

- Description: This option specifies the user name of the account that owns the NetBackup scale-out database instance.
  This user must already exist on the system. The DATABASE_USER cannot be root. The DATABASE_USER cannot be an account with access to the sudo utility. If the specification resolves to root, the installation fails. If the SERVICE_USER defined previously is not root, you can specify SAME_AS_SERVICE_USER. Otherwise, specify a non-root user account name.

- Applicable platforms: Linux
- Default value: `SAME_AS_SERVICE_USER`
- Required: Conditional.
  This value is required if the service user is root. Additionally, this value is required if `DATABASE_USER` does not exist in the `bp.conf` file and the configured `SERVICE_USER` entry is root. If the value is provided and the `DATABASE_USER` exists in `bp.conf`, this value must match the configured database user on the machine.
- `DATABASE_USER = username | SAME_AS_SERVICE_USER`
- Return to Table 9-1.

`DISASTER_RECOVERY_INSTALL`

- Description: This option specifies if the installation is a disaster recovery installation. This operation applies only to installations that use the disaster recovery file through an interactive installation.
- Applicable platforms: Linux only
- Default value: None
- Required: No
- `DISASTER_RECOVERY_INSTALL = no`
- Return to Table 9-1.

`ECA_CERT_PATH`

- Description: This option specifies the path and the file name of the external certificate file.
  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 primary 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 9-1.

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 9-1.

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.
  - 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 primary server.
- Applicable platforms: All.
- Default value: None.
- Required: Review About security configuration considerations for details.
- `ECA_CRL_CHECK_LEVEL=`*`value`*
- Return to Table 9-1.

ECA_CRL_PATH

- Description: This option specifies the path and the file name of the CRL associated with the external CA certificate.
  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 primary 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 9-1.

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 primary server.
- Applicable platforms: All.
- Default value: None.
- Required: No
- `ECA_KEY_PASSPHRASEFILE=`*`path/filename`*
- Return to Table 9-1.

ECA_PRIVATE_KEY_PATH

- Description: This option specifies the path and the file name of the file representing the private key.
  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 primary server.
- Applicable platforms: All.
- Default value: None.
- Required: Review About security configuration considerations for details.
- `ECA_PRIVATE_KEY_PATH=`*`path/filename`*
- Return to Table 9-1.

ECA_TRUST_STORE_PATH

- Description: This option specifies the path and the file name of the file representing the trust store location.
  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 primary server.
- Applicable platforms: All.
- Default value: None.
- Required: Review About security configuration considerations for details.
- `ECA_TRUST_STORE_PATH=`*`path/filename`*
- Return to Table 9-1.

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.
  - 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.
- INCLUDE_JAVA_GUI_AND_JRE = INCLUDE | EXCLUDE
- Return to Table 9-1.

INCLUDE_VRTSPDDEU_CLIENT

- Description: This option specifies whether the VRTSpddeu package is installed in the client. This option only affects the Red Hat client installations that are neither pSeries nor zSeries. Installation of VRTSpddeu package is optional. The supported values for the option are:
  - MATCH: Match the current configuration on the client. If you specify this value for an initial install, the VRTSpddeu package is not installed.
  - INCLUDE: Include the VRTSpddeu package for the installation or upgrade of a client.
  - EXCLUDE: Exclude the VRTSpddeu package for the installation or upgrade of a client.
- Applicable platforms: Linux. Specifically, Red Hat Linux clients that are neither pSeries nor zSeries.
- Default value: MATCH
- Required: No
- INCLUDE_VRTSPDDEU_CLIENT = INCLUDE | EXCLUDE | MATCH
- Return to Table 9-1.

INSTALL_ITA_DATA_COLLECTOR

- Description: This option determines if the NetBackup IT Analytics Data Collector option is installed. Acceptable values are 1, install, or 0, do not install.

- Applicable platforms: All
- Default value: Windows: `1`, UNIX and Linux: `Yes`
- Required: Yes
- `INSTALL_ITA_DATA_COLLECTOR=1|0`
- Return to Table 9-1.

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 9-1.

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 9-1.

LICENSE

- Description: This option specifies the path of the license file to apply to the primary server. For Linux, additional `LICENSE` lines may be added if more licenses are to be applied. For Windows, use a single `LICENSE` line with multiple license file paths separated with semicolons. This option only adds additional keys. Any conflicting licenses are removed.
  Veritas recommends the use of your production license that is downloaded from VEMS, for all upgrades. If you do not have access to your production license,

you can use one of the built-in non-downloaded licenses. Which license you use depends on your version of NetBackup.
The evaluation license (EVALUATION) is only used during upgrades if the upgrade is from NetBackup versions earlier than NetBackup 8.1.2. The evaluation license is valid for 60 days. Alerts appear in the web UI immediately after upgrade, indicating the number of days remaining in the evaluation.
The temporary license (TEMP_PRODUCTION) is used in upgrades of NetBackup 8.1.2 or later to NetBackup 10.3 or later. The temporary license is valid for 60 days. Alerts appear in the web UI immediately after upgrade, indicating the number of days remaining before the temporary license expires.

Note: After an upgrade to NetBackup 10.3 or later, existing NetBackup licenses become obsolete. They remain in the `license.txt` file. This file is located in either `/usr/openv/var/` on Linux or *install_path*`\NetBackup\var\` on Windows.

- Applicable platforms: All
- Default value: None.
- Required: Yes, for primary servers. Not required for media servers and clients.
- `LICENSE = EVALUATION | slf_filepath`
  You can only use `TEMP_PRODUCTION` for an upgrade.
  More information is available:
  https://www.veritas.com/support/en_US/article.100058779
- Return to Table 9-1.

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 `PRIMARY`, `MEDIA`, and `CLIENT`.
- Applicable platforms: UNIX and Linux only.
- Required: Yes.
- `MACHINE_ROLE = PRIMARY | MEDIA | CLIENT`
- Return to Table 9-1.

MEDIA_SERVER

- Description: For clients, 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 primary server is blocked. This communication is required to obtain a host certificate during the NetBackup installation or upgrade.
  For primary servers and media servers, the `MEDIA_SERVER` entry effects what the specified host can do on the primary server. Hosts that are listed in a `MEDIA_SERVER` entry have limited privileges on the primary server. For example, hosts that are listed in a `MEDIA_SERVER` entry do not have access to add new devices on the primary server. For primary and media servers, all `MEDIA_SERVER` lines in the answer file are added to the `bp.conf` file as part of the install or upgrade.
  Regardless of role, you can have multiple `MEDIA_SERVER` entries in the answer file.
- Applicable platforms: UNIX and Linux only.
- Default value: None.
- Required: No.
- `MEDIA_SERVER=`*`media_server_name`*
- Return to Table 9-1.

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 9-1.

MERGE_SERVERS_LIST

- Description: Merge the servers present in `bp.conf` on the primary 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 9-1.

NB_FIPS_MODE

- Description: This option specifies whether to install NetBackup in FIPS mode. NetBackup does not support modifying FIPS mode during upgrades. If the existing NetBackup version supports FIPS, change the FIPS mode before the upgrade. Otherwise, change it after the upgrade finishes. Refer to the *NetBackup Security and Encryption Guide* for details on FIPS configuration in NetBackup.
- Applicable platforms: All.
- Default value: Disable
- Required: No.
- NB_FIPS_MODE = Enable | Disable
- Return to Table 9-1.

PRIMARYSERVER

- Description: This option specifies the server name this computer recognizes as the current NetBackup primary server. If this host is the primary server, %COMPUTERNAME% can be used for the value. The use of IP addresses is not supported. Additional primary servers can be specified with the ADDITIONALSERVERS option.
- Applicable platforms: Windows only.
- Default value: None.
- Required: Yes.
- PRIMARYSERVER=*primary_server_name*
- Return to Table 9-1.

PROCEED_WITH_INSTALL

- Description: This option specifies the answer to two possible prompts during the install or the upgrade of NetBackup. The first prompt determines if the install or the upgrade proceeds after NetBackup passes critical preinstallation checks. The user may receive a second prompt if there are potential disk space concerns. In both cases, if YES, the install or upgrade proceeds to install the NetBackup and media manager files on the file system. If NO, the install or the upgrade halts and allows the user to make changes.

- Applicable platforms: UNIX and Linux
- Default value: None
- Required: No
- `PROCEED_WITH_INSTALL = yes | no`
- Return to Table 9-1.

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 9-1.

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 9-1.

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 9-1.

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 9-1.

SECURITY_CONFIGURATION

- Description: Applicable only if neither NetBackup certificate authority nor external certificate authority are configured on the host. Set this option to `SKIP` to continue the installation or upgrade without configuring the host to use NBCA or ECA. If you skip security, you must take additional manual steps on all target hosts when the installation or the upgrade finishes. When this option is set to `SKIP`, values cannot be specified for `CA_CERTIFICATE_FINGERPRINT`, `AUTHORIZATION_TOKEN`, and the `ECA_` options.
- Applicable platforms: All.
- Default value: None.
- Required: No.
- `SECURITY_CONFIGURATION = SKIP`
- Return to Table 9-1

SERVER

- Description: This option specifies the server name this computer recognizes as the current NetBackup primary 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 primary server. These entries are added to the `bp.conf` file.
- Applicable platforms: UNIX and Linux only.
- Default value: None.
- Required: Yes.

- SERVER=*primary_server_name*
- Return to Table 9-1.

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 9-1.

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 9-1.

SERVICE_USER

- Description: This option specifies the service user account is used to start most of the NetBackup services or daemons on the primary 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: Linux only.
- Default value: None.
- Required: Yes.
- `SERVICE_USER=`*`name`*
- Return to Table 9-1.

START_JOB_DAEMONS

- Description: This option specifies whether the NetBackup daemons that control the execution of jobs should be started.
- Applicable platforms: Linux only.
- Default value: yes
- Required: No.
- `START_JOB_DAEMONS=yes|no`
- Return to Table 9-1.

STOP_NB_BEFORE_VCREDIST

- Description: This option specifies if NetBackup processes should be stopped automatically before NetBackup attempts to update Visual C++ run-time libraries using Microsoft's redistributable installers. In some cases, stopping NetBackup processes reduces the chances of a restart being required.
- Applicable platforms: Windows only.
- Default value: YES
- Required: No
- `STOP_NB_BEFORE_VCREDIST=YES|NO`
- Return to Table 9-1

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 9-1.

VCREDIST_ATTEMPT_PREFERENCE

- Description: This option specifies the NetBackup behavior on Windows computers where the compatible Visual C++ run-time libraries are not already present. If set to YES, the setup attempts to update Visual C++ run-time libraries using Microsoft's redistributable installers. The setup halts with an error if a computer does not have the required run-time libraries and this option is set to NO.
- Applicable platforms: Windows only.
- Default value: YES
- Required: No
- `VCREDIST_ATTEMPT_PREFERENCE=YES|NO`
- Return to Table 9-1

VCREDIST_RESTART_PREFERENCE

- Description: This option determines how the NetBackup setup proceeds if the Visual C++ run-time libraries were updated and a restart is required to complete the operation. If the option is set to STOP, the setup halts. If the option is set to PROCEED, NetBackup continues the setup but does not restart the computer. Veritas recommends performing a required restart as soon as possible.
- Applicable platforms: Windows only.
- Default value: STOP
- Required: No
- `VCREDIST_RESTART_PREFERENCE=PROCEED|STOP`
- Return to Table 9-1

USE_URANDOM

- Description: This option lets you to specify `/dev/urandom` as the entropy source for random number generation.
- Applicable platforms: All.
  Applicable platforms: UNIX and Linux

- Default value: DISABLE
- Required: No.
- `USE_URANDOM = ENABLE | DISABLE`
- Return to Table 9-1.

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 9-1.

VXDBMS_POSTGRESQL_POOLER_ODBC_PORT

- Description: This option specifies the port that the NetBackup scale-out database connection pool service uses.
- Applicable platforms: All.
- Default value: `13787`
- Required: No.
  If the value is provided for upgrade, it must match the current value that is stored in the `VXDBMS_POSTGRESQL_POOLER_ODBC_PORT` field in `vxdbms.conf`.
- `VXDBMS_POSTGRESQL_POOLER_ODBC_PORT =` *`port_number`*
- Return to Table 9-1

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 9-1.

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: Linux primary servers, no. Windows primary servers, yes.
- `WEBSVC_GROUP=`*`custom_group_account_name`*
- Return to Table 9-1.

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 9-1.

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: Linux primary servers, no. Windows primary servers, yes.
- `WEBSVC_USER=`*`custom_user_account_name`*
- Return to Table 9-1.

About the NetBackup IT Analytics Data Collector

NetBackup IT Analytics is the solution for NetBackup reporting and analytics. NetBackup IT Analytics 11.0 introduces a NetBackup-only feature set that is specifically created to help customers transition from OpsCenter to NetBackup IT Analytics.

You can install the NetBackup IT Analytics Data Collector during either the installation or the upgrade of NetBackup primary server. Only the binaries are deployed with NetBackup. You must configure the NetBackup IT Analytics Data Collector to communicate with the NetBackup IT Analytics Portal once the installation completes successfully.

Once the NetBackup primary server is configured with Veritas Alta Analytics or NetBackup IT Analytics, the process configures the Data Collector for data collection. You are required to configure the Data Collector manually if your NetBackup primary server is designed with an on-premises NetBackup IT Analytics Portal.

Once the Data Collector is installed and configured, the Data Collector reports NetBackup information to NetBackup IT Analytics Portal or Veritas Alta Analytics.

How NetBackup handles the Data Collector values in the answer file depends on the NetBackup version and the current state of the NetBackup IT Analytics Data Collector.

New installations

- For new installations, NetBackup always honors the user-provided information. The answers you provide during an interactive installation or the values in the answer file determine if the NetBackup IT Analytics Data Collector is installed. If you do not provide a value in the answer file, Veritas installs the NetBackup IT Analytics Data Collector by default.

References

For additional information:

- See *Installing the Data Collector software* in the *NetBackup IT Analytics Data Collector Installation Guide*.
- See *Clustering Data Collectors with VCS and Veritas NetBackup* in *NetBackup IT Analytics Data Collector Notes and Troubleshooting* guide.

Manually install or uninstall NetBackup IT Analytics Data Collector binaries

The NetBackup IT Analytics Data Collector reports NetBackup information to NetBackup IT Analytics or Veritas Alta Analytics. The Data Collector is installed along with NetBackup installation or upgrade. The following steps help you manually install or uninstall the Data Collector.

You may need to manually install the Data Collector if it fails to install during the NetBackup install or upgrade. A failure to install the Data Collector does not cause the entire NetBackup primary server installation or upgrade to fail. If you don't plan to use the Data Collector, you may want to uninstall it.

The steps that are shown do not configure the Data Collector to connect with any portal. These steps only install the Data Collector. The Data Collector is configured after the NetBackup primary server connects with Veritas Alta Analytics or NetBackup IT Analytics Portal.

More information about how to configure the Data Collector is available.

See "Manually configure the NetBackup IT Analytics Data Collector" on page 208.

To manually install the Data Collector on a Linux primary server:

1. Copy `/catalog/anb/ita_dc.tar.gz` to a temporary location.
2. Extract the `ita_dc.tar.gz` tarball in that temporary location.
3. Run *`temporary_location`*`/dc_installer -i /usr/openv -n`

To manually install the Data Collector on a Windows primary server:

1. Locate the installation media kit and navigate to the `x64/ITA_DC` folder.
2. Run `silentinstall.cmd /INSTALL_PATH:NetBackup_install_path /INSTALL_TYPE:INSTALL /REMOVE_NON_OEM_DIR:Y`

To manually uninstall the Data Collector from a Linux primary server

- Run `/usr/openv/analyticscollector/UninstallerData/uninstall_dc.sh -r`

To manually uninstall the Data Collector from a Windows primary server

1. In **Windows Programs and Features**, locate NetBackup IT Analytics Data Collector. Right-click this item and select **Uninstall**.
2. An uninstall script is also available. The script is located in:

   `C:\ProgramData\Veritas\NetBackup IT Analytics\DC\silentuninstall.cmd`

Manually configure the NetBackup IT Analytics Data Collector

The primary server installation deploys the NetBackup IT Analytics Data Collector binaries automatically as part of a successful NetBackup installation. The binaries are installed to *install_path*\Veritas\AnalyticsCollector (Windows) or /usr/openv/analyticscollector (Linux). This section details the steps that are required to manually configure the Data Collector.

Keep the following details handy when you configure the Data Collector:

- Name of the Data Collector (as configured on the Veritas Alta or NetBackup IT Analytics Portal).
- Passcode of the Data Collector (as configured on the Veritas Alta or NetBackup IT Analytics Portal).
- Data receiver URL (generated when you create the Data Collector on the Veritas Alta or NetBackup IT Analytics Portal). Ensure the NetBackup primary server can resolve the host name of the Data Receiver URL.
- Key file path (generated when you create the Data Collector on the Veritas Alta or NetBackup IT Analytics Portal and copied to the NetBackup primary server).

See the *Add/Edit Data Collectors* section in the *NetBackup IT Analytics User Guide* for more information.

To configure the Data Collector manually on Windows:

1. Create a response file as a batch script `responsefile.cmd` with the contents shown. These are the responses to the user input required to configure the Data Collector.

```
SET DATACOLLECTOR_NAME=name_of_the_data_collector
SET DATACOLLECTOR_PASSCODE=passcode_for_the_data_collector
SET DATARECEIVER_URL=data_receiver_URL
SET DATACOLLECTOR_KEY_FILE_PATH=path_to_the_key_file
SET HTTP_PROXY_CONF=N
SET PROXY_HTTP_URL=
SET PROXY_HTTP_PORT=
SET PROXY_HTTPS_URL=
SET PROXY_HTTPS_PORT=
SET PROXY_USERID=
SET PROXY_PASSWORD=
SET PROXY_NOT_FOR=
```

2. Update the value for each field with appropriate data. A sample response file is also available in the installer media in `x64\ITA_DC\responsefile.cmd`.

3. Run the command shown:

```
"C:\ProgramData\Veritas\NetBackup IT Analytics\DC\configure.cmd"
\RESPFILE:response_file_path \INSTALL_TYPE:CONFIG
```

4. Validate the Data Collector integration with NetBackup IT Analytics by going to `C:\Program Files\Veritas\analyticscollector\mbs\bin\` and running this command:

```
checkinstall.bat
```

   If the Data Collector is configured with the Portal, the response is displayed as **SUCCESSFUL**.

Note: If there is a version mismatch of `aptare.jar` between the Data Collector and the portal, execution of the `checkinstall.bat` command starts an auto-update of the Data Collector.

To configure the Data Collector manually on Linux:

1. Create a response file with the contents shown. These are the responses to the user input required to configure the Data Collector:

```
COLLECTOR_NAME=name_of_the_data_collector
COLLECTOR_PASSCODE=passcode_for_the_data_collector
DR_URL=data_receiver_URL
COLLECTOR_KEY_PATH=path_to_the_key_file
HTTP_PROXY_CONF=N
HTTP_PROXY_ADDRESS=
HTTP_PROXY_PORT=
HTTPS_PROXY_ADDRESS=
HTTPS_PROXY_PORT=
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

2. Update the value for each field with appropriate data.

   A sample response file is available on the install media and from `/usr/openv/analyticscollector/installer/responsefile.sample` on the primary server.

3. Run the command:

```
/usr/openv/analyticscollector/installer/dc_installer.sh -c
responsefile_path
```

4. Validate the Data Collector integration with NetBackup IT Analytics by navigating to `/usr/openv/analyticscollector/mbs/bin/` and running `./checkinstall.sh`

   If the Data Collector is able to communicate with the NetBackup IT Analytics Portal, the response is displayed as **SUCCESSFUL**.

Note: If there is a version mismatch of `aptare.jar` between the Data Collector and the portal, execution of the `checkinstall.sh` command starts an auto-update of the Data Collector.

Start, stop, and get the status of the Data Collector

On Linux:

- To start the Data Collector processes, run:

  ```
  /usr/openv/analyticscollector/mbs/bin/aptare_agent start
  ```

- To stop the Data Collector processes, run:

  ```
  /usr/openv/analyticscollector/mbs/bin/aptare_agent stop
  ```

- To get the status of the Data Collector processes, run:

  ```
  /usr/openv/analyticscollector/mbs/bin/aptare_agent status
  ```

On Windows: Review the status of Aptare Agent, Aptare Kafka, and Aptare Zookeeper services on the Windows service panel.

Note: If the Data Collector is configured with an on-premises NetBackup IT Analytics Portal, then to edit any of the Data Collector properties on the Portal, refer to *Edit NetBackup IT Analytics Data Collector credentials* section in the *NetBackup IT Analytics User Guide*.

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 Linux platforms. The Linux 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 Linux platforms to assign RBAC permissions. The command is available only on the primary server. For more information about this command, see the NetBackup Commands Reference Guide.

RBAC Bootstrapping during installation and upgrades on Linux platforms:

Use the answer file template `NBInstallAnswer-primary.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 178.

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.

NetBackup primary server web server user and group creation

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).

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 "Installation requirements for UNIX and Linux" on page 34.

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

- In 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 primary 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 primary servers, you must use a domain group.

The NetBackup primary 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 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:** `# groupadd nbwebgrp`
   - **Windows:** `C:\>net localgroup nbwebgrp /add`
2. Create a local user.
   - **Linux:** `# 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**.

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 primary server, media server, or UNIX and Linux client software
- NetBackup Java Remote Administration Console

Starting with NetBackup 8.3, the Java GUI and the JRE packages are optional for 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 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 install" on page 218.

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

- NetBackup primary server, media server, or UNIX and Linux client software
- NetBackup Java Remote Administration Console

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 9-3 to determine the location of the `nbcomponentupdate` utility.

Table 9-3 Location of JRE update utility

Product	Operating system	Path
NetBackup	Windows	*install_path*\netbackup\java\nbcomponentupdate.exe
	UNIX or Linux	/usr/openv/java/nbcomponentupdate
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 install

You can add or remove the Java GUI and the JRE packages after the install 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 installation media and run the commands shown:

Linux	`rpm -U VRTSnbjre.rpm` `rpm -U VRTSnbjava.rpm`
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`
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**.

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 9-1).
- 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 primary server, or any media servers (Figure 9-2).

Both modes support the same topologies.

Table 9-4 describes the association between NetBackup versions and the NetApp plug-ins.

Table 9-4 Version compatibility

NetBackup version	NetApp plug-in version	Description	Ratio of primary server to OCUM server	Supported policy types
7.7 and later	1.1	Provides 7-mode support for all NetBackup Replication Director features.	One primary 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 primary server supports many OCUM servers.	MS-Windows, Standard, NDMP, VMware, Oracle
	2.0	Provides cDOT support.	One primary 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 primary 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 primary servers, media servers, clients, and any hosts which communicate with the plug-in.

Figure 9-1 Communication between NetBackup and the NBUPlugin for 7-mode

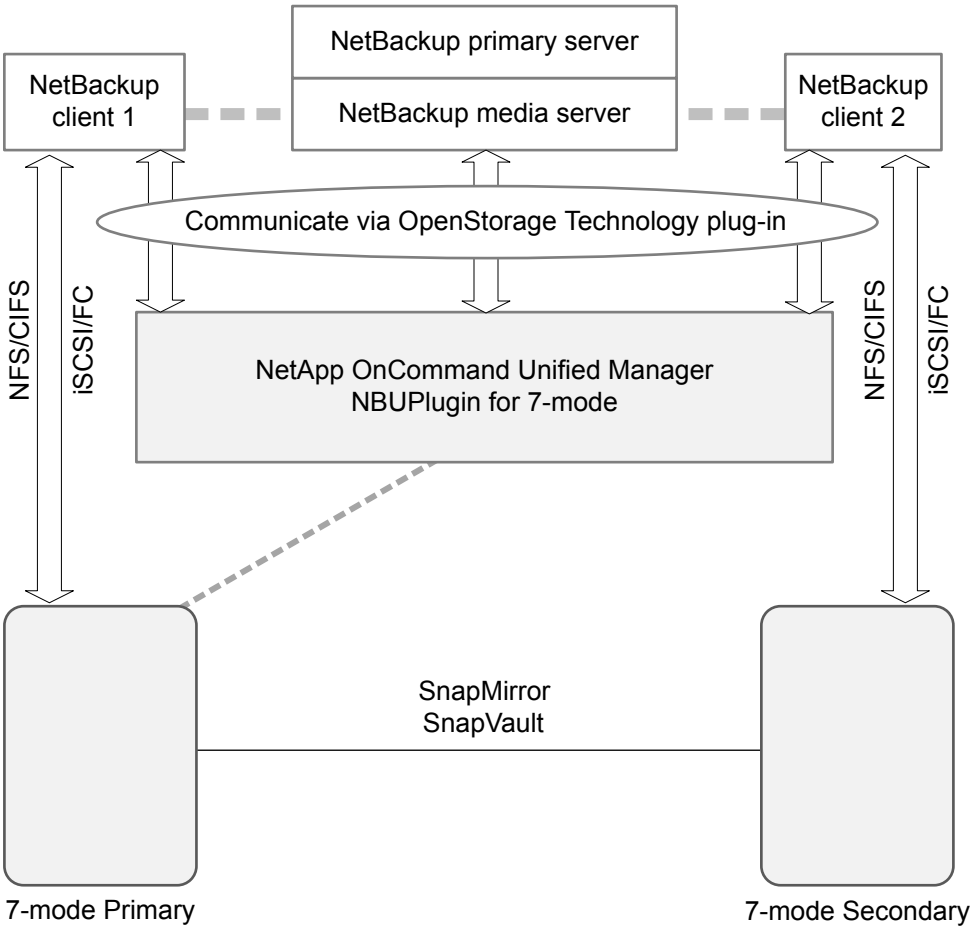
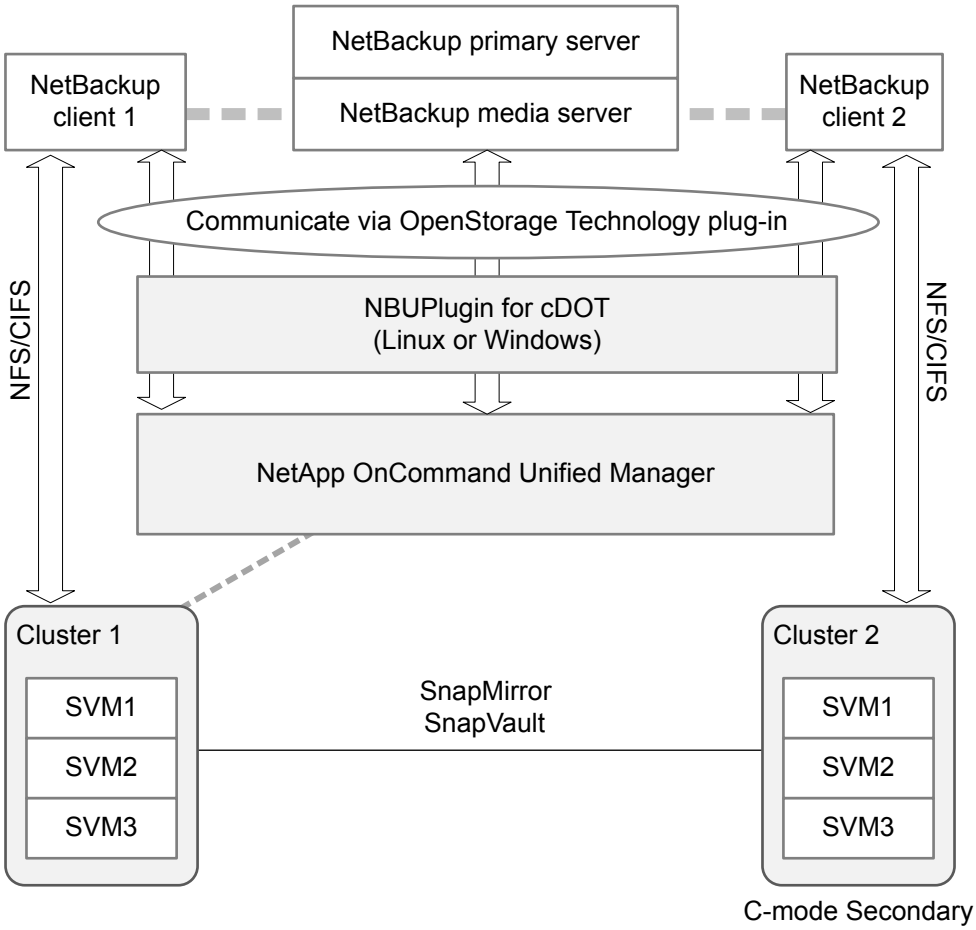


Figure 9-2 Communication between NetBackup and the NBUPlugin for Clustered Data ONTAP



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

Security updates to the NetBackup database

As a part of security changes in NetBackup, Veritas may make changes to your NetBackup (NBDB) database password. If you changed the password on the NetBackup database from the default value, no changes to the password are made. Any existing NetBackup databases which still have the default password are updated with a new, randomly generated password. All new installations of NetBackup have a randomly generated password assigned to the NetBackup database for improved security. This password is not provided to the user during installation or upgrade. You can use the nbdb_admin command to change this randomly generated password. See the NetBackup Commands Reference Guide for more information about the nbdb_admin command.

Size guidance for the NetBackup primary server and domain

NetBackup primary server sizing is an important activity as part of an overall NetBackup solution design. Veritas always recommends a comprehensive data protection assessment to determine the optimal configuration for a NetBackup primary and NetBackup domain.

The following information is meant as guidelines:

- NetBackup has no hard limit on catalog size. However, Veritas recommends as a best practice that you keep the catalog size under 4 TB to ensure good catalog backup and recovery performance.
  The size of the NetBackup catalog and the performance that is related to reading data from the NetBackup catalog is driven by the I/O performance and more specifically the disk speed. Veritas recommends the use of solid-state drives (SSDs) where possible for the catalog. The disks require good read and write performance, which is even more critical in large environments.

Managing the size of the catalog through compression and catalog archiving is recommended for images with a long-term retention (LTR).

For additional information about managing the catalog size through compression and catalog archiving, see the *NetBackup Backup Planning and Performance Tuning Guide*.

- The number of devices in the EMM database should not exceed 1500.
  Examples of devices are a tape drive, a tape library, a disk pool, and so on.
- The number of media servers should not exceed 50.
  It is important to maintain a manageable number of media servers and storage targets within each NetBackup domain. Every media server and storage target that is deployed must be managed, maintained, and eventually patched and upgraded. Each of those media servers has a configuration that has to also be maintained. Therefore, it is important to consider the manageability, usability, and the administrative implications. Veritas recommends deploying media servers and storage targets that are properly sized with the necessary CPU, memory, network bandwidth, and disk I/O to support the backup workloads. It is also important to consider whether the same workloads require duplication or replication to a DR location. Sizing the media servers and storage targets to accommodate those secondary options is crucial. In summary, Veritas recommends that you deploy properly sized media servers and storage targets, while keeping the number less than 50 per domain.
- The number of jobs must not exceed one job per second per client, but it is possible to submit multiple jobs per second, each sent from a different client. Each backup client has the "one job per second per client" limit, so multiple clients may run in parallel.
- Computing resources such as CPU and memory affect how well the primary server scales.

To accommodate the processing of the metadata streams from media servers, it is critical that the primary server has the requisite amount of system resources. A media server sends metadata about the files it has backed up to the primary server. This metadata is batched and sent periodically. The batch size, which is determined by the tuning parameter `MAX_ENTRIES_PER_ADD`, has significant effect on primary server performance, especially for backup images that contain many small files.

For additional information about batch size for sending metadata to the NetBackup catalog, see the *NetBackup Backup Planning and Performance Tuning Guide*.

The primary server must then process each of these metadata message payloads. Each payload requires an operating system process, each of which consumes system resources. The consumed system resources are disk capacity, CPU cycles, memory capacity, network bandwidth, and disk I/O.

Table 9-5 provides additional information.

Table 9-5 Sizing guidelines

Number of processors	Recommended memory requirement	Maximum number of media servers per primary server *
8	128 GB	20
16	256 GB	100

*Veritas recommends that you limit the number of media servers to less than 50 media servers per domain.

Additional recommendations about processor and memory requirements are available.

See “Installation requirements for UNIX and Linux” on page 34.

See “Installation requirements for Windows and Windows clusters” on page 67.