NetBackup™ Release Notes

Release 10.2

Document Version 2

VERITAS™

NetBackup™ Release Notes

Last updated: 2023-04-07

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://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

About NetBackup 10.2

This chapter includes the following topics:

About the NetBackup 10.2 release

The *NetBackup Release Notes* document is meant to act as a snapshot of information about a version of NetBackup at the time of its release. Old information and any information that no longer applies to a release is either removed from the release notes or migrated elsewhere in the NetBackup documentation set.

See "About new enhancements and changes in NetBackup" on page 10.

About EEBs and release content

NetBackup 10.2 incorporates fixes to many of the known issues that affected customers in previous versions of NetBackup. Some of these fixes are associated with the customer-specific issues. Several of the customer-related fixes that were incorporated into this release were also made available as emergency engineering binaries (EEBs).

Listings of the EEBs and Etracks that document the known issues that have been fixed in NetBackup 10.2 can be found on the Veritas Operations Readiness Tools (SORT) website and in the *NetBackup Emergency Engineering Binary Guide*.

See "About Veritas Services and Operations Readiness Tools" on page 38.

About NetBackup appliance releases

The NetBackup appliances run a software package that includes a preconfigured version of NetBackup. When a new appliance software release is developed, the

latest version of NetBackup is used as a basis on which the appliance code is built. For example, NetBackup Appliance 3.1 is based on NetBackup 8.1 This development model ensures that all applicable features, enhancements, and fixes that were released within NetBackup are included in the latest release of the appliance.

The NetBackup appliance software is released at the same time as the NetBackup release upon which it is based, or soon thereafter. If you are a NetBackup appliance customer, make sure to review the *NetBackup Release Notes* that correspond to the NetBackup appliance version that you plan to run.

Appliance-specific documentation is available at the following location:

http://www.veritas.com/docs/000002217

About NetBackup Late Breaking News

For the most recent NetBackup news and announcements, visit the NetBackup Late Breaking News website at the following location:

http://www.veritas.com/docs/000040237

Other NetBackup-specific information can be found at the following location:

https://www.veritas.com/support/en_US/15143.html

About NetBackup third-party legal notices

NetBackup products may contain third-party software for which Veritas is required to provide attribution. Some of the third-party programs are available under open source or free software licenses. The license agreement accompanying NetBackup does not alter any rights or obligations that you may have under those open source or free software licenses.

The proprietary notices and the licenses for these third-party programs are documented in the *NetBackup Third-party Legal Notices* document, which is available at the following website:

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

Chapter 2

New features, enhancements, and changes

This chapter includes the following topics:

About new enhancements and changes in NetBackup

In addition to new features and product fixes, NetBackup releases often contain new customer-facing enhancements and changes. Examples of common enhancements include new platform support, upgraded internal software components, interface changes, and expanded feature support. Most new enhancements and changes are documented in the *NetBackup Release Notes* and the NetBackup compatibility lists.

Note: The *NetBackup Release Notes* only lists the new platform support that begins at a particular NetBackup version level at the time of its release. However, Veritas routinely backdates platform support to previous versions of NetBackup. Refer to the NetBackup compatibility lists for the most up-to-date platform support listings.

See "About the NetBackup 10.2 release" on page 8.

See "About NetBackup compatibility lists and information" on page 46.

NetBackup 10.2 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 10.2 are grouped below by category. Select a link to read more information about the topic.

New features

- Changes in Veritas terminology
- Improvements to the NetBackup web UI
- New EEB management view
- Configuring Veritas Alta Recovery Vault Azure and Azure Government
- RESTful APIs included in NetBackup 10.2

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 10.2 from a release earlier than 8.1, make sure that you read and understand the *NetBackup Read This First for Secure Communications* document. NetBackup 8.1 includes many enhancements that improve the secure communications of NetBackup components. The *NetBackup Read This First for Secure Communications* document describes the features and benefits of these enhancements:

  NetBackup Read This First for Secure Communications

Support changes and enhancements

- NetBackup 10.2 support additions and changes
- Bare Metal Restore (BMR) operating system support additions
- End of support for older authorization models
- Accurate licensing support
- Several shutdown commands to be deprecated in a future release

Installation, upgrade, and configuration changes and enhancements

- New NetBackup Scale-Out Relational Database in NetBackup 10.2
- Prerequisites for upgrading to NetBackup 10.2

- Linux environments require a new non-root database user when the root user starts NetBackup daemons
- New connection pooler on port 13787

Cloud-related changes and enhancements

- Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.2

Virtualization changes and enhancements

- Web UI support for single-file recovery from a VMware guest VM backup using a stored credential (access to username or password is not required)
- Default VMware Administrator role has new credential permissions

Workload and database agent changes and enhancements

- Support for Oracle Copilot with multiple universal shares

Other announcements

- Using Azure recovery points with Snapshot Manager
- Single file restore from a backup of snapshot
- Elastic media server provides autoscaling of replicas
- Documentation changes

Changes in Veritas terminology

To modernize our terminology, Veritas has begun to replace certain outdated terms with more current terms.

Note: As Veritas continues to update its terminology, the deprecated terms and the new terms may be used interchangeably.

Deprecated term	New term
Master	Primary
Slave	Secondary or media server
Whitelist or white list	Allowed list
Blacklist or black list	Blocked list
White hat	Ethical

Deprecated term	New term
Black hat	Unethical

Improvements to the NetBackup web UI

This release contains the following improvements to the NetBackup web UI:

- Ability to select multiple policies for a manual backup.
- Ability to browse for the storage location when you create a Media Server Deduplication Pool (MSDP) storage server.
- Ability to start and stop NetBackup daemons from the Activity Monitor.

New EEB management view

New to NetBackup 10.2 is the **EEB management** tab under **Deployment management**. This tab provides a window into your environment's use of NetBackup emergency engineering binaries (EEBs).

The **EEB management** tab displays all the EEBs deployed in your NetBackup environment. Each EEB lists a description of the issue as well as the formal NetBackup releases in which the issue was resolved. You can export all this information into a CSV file for review and analysis.

For the description and fixed version information to display, the computer running the NetBackup web UI must have access to the internet. This information is collected from the latest data on the NetBackup SORT website.

You can review each individual EEB and determine which hosts use a given EEB. Like the description information, you can export these details to a CSV file.

Currently, this view only allows for reporting. You can, however, use the information that is provided to develop an upgrade strategy for your environment. Be aware pre-8.0 and earlier clients and media servers cannot use this feature.

Configuring Veritas Alta Recovery Vault Azure and Azure Government

Veritas Alta Recovery Vault Azure and Azure Government can be configured in the web UI or using the CLI. Also, `csconfig cldinstance`, `nbcldutil`, and `msdpcldutil` are updated for Veritas Alta Recovery Vault Azure and Azure Government.

Refer to the following sections in the *NetBackup Deduplication Guide*:

- *Configuring NetBackup Alta Recovery Vault Azure and Azure Government*

- *Configuring NetBackup Alta Recovery Vault Azure and Azure Government using the CLI*

RESTful APIs included in NetBackup 10.2

NetBackup 10.2 includes both updated and new RESTful application programming interfaces (APIs). These APIs are built on the Representational State Transfer (REST) architecture. They provide a web-service-based interface that lets you configure and administer NetBackup in your environments.

API documentation

You can find documentation for the NetBackup APIs in on SORT and on your primary server. Make sure to review the *Versioning* topic and the *What's New* topic in the *Getting Started* section.

- On SORT:
  NetBackup API documentation is available on SORT:
  HOME > KNOWLEDGE BASE > Documents > Product Version > 10.2
  Look under **API Reference**. A *Getting Started* document provides background information about using NetBackup APIs. The API YAML files are also available for reference, however, they are not functional. You cannot test the APIs from the documents on SORT.
- On your primary server:
  APIs are stored in YAML files on the primary server:
  `https://<primary_server>/api-docs/index.html`
  The APIs are documented in Swagger format. This format lets you review the code and test the functionality by making actual calls with the APIs. You must have the appropriate security permissions to access the primary server and APIs to use the Swagger APIs.

Caution: Veritas recommends that you test APIs only in a development environment. Because you can make actual API calls from the Swagger files, you should not test the APIs in a production environment.

New APIs

NetBackup 10.2 includes these new and enhanced APIs:

- Drives:
  Retrieve list of drives.
- Images:
  Retrieve the contents for raw partition eligible images.

- Jobs: Retrieve job ID for new job after restarting specified original job.
- NAS Workloads:
  Recover individual files and folders from a NAS system.
- FlashBackup Windows Workloads:
  - Recover individual files and folders from a FlashBackup backup.
  - Recover individual files and folders from a FlashBackup Windows backup.
- Log Records:
  - Retrieve the logging level values of hosts and its components for specified record ID.
  - Update the logging level settings to the host and its components for specified record ID.
- External Credential Management System Provider:
  - Obtain list of External Credential Management System (ECMS) providers.
  - Add External Credential Management System provider.
  - Retrieve details of the ECMS provider for specified configuration name.
  - Update the ECMS provider for specified configuration name.
  - Delete the ECMS provider for specified configuration name.
- External Credential Management System Agent:
  - Obtain list of External Credential Management System (ECMS) agents.
  - Add an External Credential Management System agent.
  - Retrieve details of the ECMS agent for specified agent ID.
  - Update the ECMS agent for specified agent ID.
  - Delete the ECMS agent for specified agent ID.

Versioned APIs

There are no versioned APIs in NetBackup 10.2.

NetBackup 10.2 support additions and changes

Note: This information is subject to change. See the NetBackup Compatibility List for all Versions for the most recent product and services support additions and changes.

The following products and services are supported starting with NetBackup 10.2:

- Red Hat Enterprise Linux Server 9.0 as a primary and a media server
- Oracle Linux 9.0 as a primary and a media server
- Azure Stack Hub 2206
- MariaDB 10 on Red Hat Enterprise Linux 9.0
- **Note:** Support for PaaS database protection for AWS RDS SQL began with NetBackup 10.1.1. For more information, see the *NetBackup Web UI Cloud Administrator's Guide*.

Bare Metal Restore (BMR) operating system support additions

NetBackup Bare Metal Restore (BMR) has added support for the following operating system versions:

- BMR Client/Boot support for Red Hat Enterprise Linux (RHEL) 9

End of support for older authorization models

- Enhanced Auditing (EA)
  Veritas would like to make you aware that future versions of NetBackup will no longer support the Enhanced Auditing (EA) authorization model.
- NetBackup Access Control (NBAC)
  Veritas would also like to make you aware that NetBackup Access Control (NBAC) authorization model will attain end-of-life (EOL) and will no longer be supported in an upcoming release.

Support will continue on older versions of NetBackup and follow the published Veritas Product End of Life policy guidelines.

Accurate licensing support

The following workloads support accurate licensing with NetBackup 10.2:

- NetBackup for Hyper-V
- NetBackup for FlashBackup
- NetBackup for Lotus Notes
- NetBackup for Microsoft SharePoint
- NetBackup for Enterprise Vault

- NetBackup for Sybase
- NetBackup for Informix
- NetBackup for DB2
- NetBackup for SAP HANA
- NetBackup for SAP MaxDB
- NetBackup for SAP Oracle

Several shutdown commands to be deprecated in a future release

A new, fully documented command for shutting down NetBackup processes and daemons will be provided in an upcoming release. At that point, the following commands will no longer be available:

- `bp.kill_all`
- `bpdown`
- `bpclusterkill`

Please plan accordingly. The new command will be announced in future release notes and in the *NetBackup Commands Reference Guide*.

New NetBackup Scale-Out Relational Database in NetBackup 10.2

In NetBackup 10.2 the database technology is changing to a new database solution.

During an upgrade, the existing NetBackup relational database is automatically migrated to the new database solution. See Prerequisites for upgrading to NetBackup 10.2 for prerequisites. Refer to the *NetBackup Upgrade Guide* for full details.

Prerequisites for upgrading to NetBackup 10.2

Internal testing shows that the upgrade process may be faster than for previous releases. However, be prepared to allow for extra time for the database conversion during the upgrade process. Refer to the NetBackup Upgrade Guide for full details and time estimates for the database conversion.

As part of the upgrade to NetBackup 10.2, the following prerequisites exist:

- Veritas strongly recommends that before you upgrade, you run the `nbdb_admin -validate` command and resolve any issues that are reported.
- Veritas recommends that you run the database precheck tool to identify any potential data issues before you upgrade NetBackup. See

https://sort.veritas.com/utility/nbdb-utf8-check for instructions about how to use the precheck tool.

For the best performance of the database precheck tool, install the EEB Hotfix for the `nbdb_unload` utility. See the following article:

https://www.veritas.com/content/support/en_US/downloads/update.UPD714038

- Veritas recommends that you search for the `pgsql_utf8_error.txt` file after the successful upgrade of the active node of a clustered primary server. Notification of invalid UTF-8 characters is not displayed on clustered servers. Details on the location of this file are found in the **Solution** section of this technical article: https://www.veritas.com/support/en_US/article.100055347
- Veritas recommends that you defragment the NetBackup database before upgrade to improve the overall conversion experience. See the *NetBackup Administrator's Guide, Volume I* for additional information on the **Reorganize** option to defragment the database.
- You must run a catalog backup within 24 hours of the upgrade.
- Ensure that you have the free disk space that is twice the size of the NetBackup database.
  Also refer to the Appendix *NetBackup installation requirements* in this guide.

Linux environments require a new non-root database user when the root user starts NetBackup daemons

For Linux environments, the new NetBackup database must have a non-root user for operations. You are prompted for the non-root user if the root user starts the NetBackup daemons. See “Database user, port, and disk space requirements” in the section “How to plan for an upgrade to NetBackup 10.2” in the *NetBackup Upgrade Guide*. Also refer to the following article: https://www.veritas.com/docs/100053091.

New connection pooler on port 13787

In NetBackup 10.2, the new NetBackup Scale-Out Relational Database introduces a new connection pooler. By default it uses port 13787. For details see the section “Database user, port, and disk space requirements” in the *NetBackup Upgrade Guide*.

Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.2

If you use cloud storage in your NetBackup environment, you may need to update your cloud configuration file on the NetBackup primary server immediately after you install or upgrade to NetBackup 10.2. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 10.2, related operations fail.

Veritas continuously adds new cloud support to the cloud configuration files between releases. Updating your cloud configuration files is necessary only if your cloud storage provider was added to the cloud configuration package after version 2.10.0.

The following cloud support has been added to version 2.10.6 and later but was not included in the NetBackup 10.2 final build:

- Amazon Glacier Instant Retrieval (IR)
- Backblaze B2 Cloud Storage (S3)
- DataCore Swarm (S3)
- iTernity iCAS FS (S3)
- Quantum ActiveScale Glacier Storage Class
- Spectra Vail (S3)
- STACKIT Object Storage (S3)
- NEC Cloud IaaS Object Storage N2 (S3)
- Amazon (S3) - Asia Pacific (Jakarta) region
- Amazon (S3) – ME (UAE) region
- Google (S3) - Asia South2 (Delhi) region
- Google (S3) - Australia-Southeast2 (Melbourne) region
- Google (S3) - EU West8 (Milan) region
- Google (S3) - EU West9 (Paris) region
- Google (S3) - EU Southwest1 (Madrid) region
- Google (S3) - North America Northeast2 (Toronto) region
- Google (S3) - US East5 (Columbus) region
- Google (S3) - US South1 (Dallas) region
- Wasabi (S3) - AP Southeast 1 (Singapore) region
- Wasabi (S3) - AP Southeast 2 (Sydney) region

- Wasabi (S3) - EU Central 2 (Frankfurt) region
- Wasabi (S3) - CA Central 1 (Toronto) region
- Wasabi (S3) - EU West 2 (Paris) region

For the latest cloud configuration package, see the following article:

https://www.veritas.com/content/support/en_US/downloads/update.UPD971796

For additional information on adding cloud storage configuration files, refer to the following tech note:

http://www.veritas.com/docs/100039095

Web UI support for single-file recovery from a VMware guest VM backup using a stored credential (access to username or password is not required)

This release adds support for using a **VMware guest VM** credential to perform an agentless single-file recovery to a target guest VM. A user can then perform the recovery without needing to know the actual username and password for the VM.

An **Administrator** (or user with a similar RBAC role) creates the credential in the NetBackup credential management. The Default VMware Administrator RBAC role has permissions to view and use this credential (and any credential). Alternatively, a NetBackup administrator can create a custom RBAC role that gives a VMware administrator access to only a specific credential.

Default VMware Administrator role has new credential permissions

In this release, the RBAC Default VMware Administrator role has new permissions for credentials. Users with this role can now “View” and “Assign credentials”. These changes mean that users can view all credentials in credential management and use any credential for recovery.

If you do not want a user to have access to all credentials, create a custom role and select only the wanted credentials for that role.

Support for Oracle Copilot with multiple universal shares

NetBackup 10.2 supports Oracle Copilot with multiple universal shares from BYO servers.

Using Azure recovery points with Snapshot Manager

NetBackup 10.2 includes the following changes for using Azure recovery points with NetBackup Snapshot Manager:

- Application consistency using Azure recovery points
  By default, the create snapshot operation in Snapshot Manager creates recovery points instead of snapshots.
- Post-upgrade tasks for application consistency using Azure recovery points
  After you upgrade to use Azure recovery points, for the snapshots to be application consistent, ensure that the additional permissions are configured to enable Azure restore points.
  For more information, see the “Post-upgrade tasks” section of the *NetBackup Snapshot Manager Install and Upgrade Guide*.

Single file restore from a backup of snapshot

With this release, you can create a backup of a snapshot and at the same time locate and restore individual files and folders. This feature also supports cross platform restores of NetBackup and Snapshot Manager. For more information, see the *NetBackup Web UI Cloud Administrator's Guide*.

Elastic media server provides autoscaling of replicas

All the replicas for the media server are always up and running which incurs unnecessary cost. The basic media server pod power management (elastic media server) feature provides autoscaling of media server replicas based on the CPU and memory usage to reduce the cost. By default, this feature is disabled. For more information, see the *NetBackup Deployment Guide for Kubernetes Clusters*.

Documentation changes

With this release, the *NetBackup Deployment Guide for Azure Kubernetes Services (AKS) Cluster* and the *NetBackup Deployment Guide for Amazon Elastic Kubernetes Services (EKS) Cluster* will no longer be published. These guides are now combined into one guide:*NetBackup Deployment Guide for Kubernetes Clusters*. NetBackup

Chapter 3

Operational notes

This chapter includes the following topics:

About NetBackup 10.2 operational notes

NetBackup operational notes describe and explain important aspects of various NetBackup operations that may not be documented elsewhere in the NetBackup documentation set or on the Veritas Support website. The operational notes can be found in the *NetBackup Release Notes* for each version of NetBackup. Typical operational notes include known issues, compatibility notes, and additional information about installation and upgrade.

Operational notes are often added or updated after a version of NetBackup has been released. As a result, the online versions of the *NetBackup Release Notes* or other NetBackup documents may have been updated post-release. You can access the most up-to-date version of the documentation set for a given release of NetBackup at the following location on the Veritas Support website:

NetBackup Release Notes, Administration, Installation, Troubleshooting, Getting Started, and Solutions Guides

NetBackup installation and upgrade operational notes

NetBackup can be installed and upgraded in heterogeneous environments using a variety of methods. NetBackup is also compatible with a mixture of servers and clients that are at various release levels in the same environment. This topic contains some of the operational notes and known issues that are associated with the installation, upgrade, and software packaging of NetBackup 10.2.

If NetBackup 10.2 upgrade fails on Windows, revert to previous log folder structure

The legacy log folder structure for non-root or non-admin invoked process logs has changed. The new folder structure is created under the process log directory name. For more information, refer to the *File name format for legacy logging* section from the Veritas NetBackup Logging Reference Guide.

For Windows, if the upgrade to NetBackup 10.2 fails and rollback occurs, run the following command to continue working on an earlier NetBackup version:

```
mklogdir.bat -fixFolderPerm
```

For more information, refer to the `mklogdir` command from the Veritas NetBackup Commands Reference Guide.

Information for NetBackup native installs and upgrades is incorrect in the installation and upgrade guides

The 10.2 versions of the *NetBackup Installation Guide* and the *NetBackup Upgrade Guide* do not include the following change: starting in NetBackup 10.2, the Red Hat Linux primary and media servers require the rpm `VRTSpddeu.rpm`. Also, the guides do not reflect the correct order for the installation sequence for the rpm packages `VRTSpddea.rpm` and `VRTSpddes.rpm`.

Corrections to the documentation are available in the following technical article:

https://www.veritas.com/support/en_US/article.100055465

Native installation requirements

In NetBackup 8.2, a change was made to initial installs such that the answer file is now required. This change may have some negative effect on users who want to use the native packages to create VM templates or otherwise install the NetBackup packages without configuring the product. On Linux, one possible way of obtaining the previous behavior is with the `-noscripts` option of the RPM Package Manager. Providing this option when installing the `VRTSnbpck` package avoids the configuration steps. This option does not need to be provided when you install other packages. The answer file must still exist, but the only value that must be provided is the role of the machine, either a client or a media server. For example:

```
echo "MACHINE_ROLE=CLIENT" > /tmp/NBInstallAnswer.conf
rpm -U --noscripts VRTSnbpck.rpm
rpm -U VRTSpbx.rpm VRTSnbclt.rpm VRTSpddea.rpm
```

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

Starting with NetBackup 8.0, 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 952

RFC 1123

http://www.veritas.com/docs/000125019

These standards should be applied to all computing hosts, including all NetBackup hosts. To accommodate legacy environments and functionality, features of NetBackup that were implemented before 2010 continue to allow some non-compliant characters. But newer features, as well as more recently integrated 3rd-party components, are not tested with nor expected to be compatible with host names that do not adhere to the industry standards.

In some situations, it may be possible to configure name services with a network hostname alias that is standards-compliant, and then use the alias when you configure NetBackup. But using host names that are standards-compliant is the only way to ensure compatibility with all features.

About support for HP-UX Itanium vPars SRP containers

Hewlett-Packard Enterprise (HPE) introduced a new type of container for HP-UX Virtual Partitions (vPars)-enabled servers called Secure Resource Partitions (SRPs). As part of the security changes introduced by SRPs, native HP-UX install tools such as `swinstall` and `swremove` are disabled from being run within the SRP environment. The `swinstall` and `swremove` tools can only be called from the global host running vPars, which then pushes the native packages to the SRP containers.

NetBackup only supports installing into the global view. NetBackup installation fails if you try to install into an HPE Itanium SRP container (private file system, shared file system, or workload).

NetBackup administration and general operational notes

NetBackup provides a complete, flexible data protection solution for a variety of platforms. The platforms include Windows, UNIX, and Linux systems. In addition to a standard set of data protection features, NetBackup can also utilize several other licensed and non-licensed components to better protect a variety of different systems and environments. This topic contains some of the general operational notes and known issues that are associated with the administration of NetBackup 10.2.

Changes to database commands

As a result of the change to the NetBackup Scale-Out Relational Database in NetBackup 10.2, some options for database commands have been changed or removed.

nbdb_* commands changes

The commands `nbdb_admin -start` and `nbdb_admin -stop` no longer start and stop a specific database in the NetBackup database server. Now they start or stop the NetBackup database server. On Windows, any dependent services are also stopped. You must manually restart these services when you start the NetBackup database server again.

Note: Before you take the NetBackup database server offline with the `-stop` option, stop all services that are running except the NetBackup Scale-Out Relational Database.

-staging option removed

The `-staging` option is removed from the following commands: `cat_export`, `cat_import`, and `nbdb_unload`.

After PIT restore, "The host ID does not exist" error appears

After a point in time (PIT) restore operation (which may include either a **Full File System** restore or a **BMR restore**), the error message **The host ID does not exist** appears.

In this scenario, a full backup is taken when a SERVICE_USER as root/administrator account is configured. This account takes the backup of the NetBackup installed binaries with root/administrator ownership. Before a restore, SERVICE_USER is configured with an account other than root/administrator, and then an incremental backup is taken where the service user is backed up as part of `bp.conf`. In a PIT restore operation with the incremental backup, the SERVICE_USER entry gets restored. However, the binaries are restored in the root account ownership.

Workaround:

After changing the service user, you must take a full backup, whether it is a **MS-Windows\Standard Policy** for File System or **BMR** policy configuration.

After DR, jobs using Veritas Alta Recovery Vault volumes may fail

After a disaster recovery is performed for NetBackup 10.2, the refresh token of a Veritas Alta Recovery Vault credential may become invalid. This situation can lead to failure for jobs that use Veritas Alta Recovery Vault volumes. For more information, see the following technical article:

https://veritas.com/en_US/article.100055366

Multiple postgres processes on Linux NetBackup servers

Some users may notice that with the new NetBackup database in 10.2, a number of instances of `postgres` run on the NetBackup server. One instance is the primary server process that runs the database cluster. It is the first process started and performs recovery operations, initializes shared memory, and runs background processes.

PostgreSQL also spawns additional processes when there is a connection request from a client process. (For more information, see the PostgreSQL documentation: https://www.postgresql.org/docs/current/app-postgres.html.) Each background instance is dedicated to specific purpose. For example: automatic database maintenance, logging error messages, updating and collecting statistics, and

handling the client connection from the various programs that want to perform database activities.

For some workload environments, reduce the size of the job database before upgrade

Following an upgrade to NetBackup 9.1, existing jobs for certain workloads are assigned an asset namespace to enable access control at an asset level. This process may take some time. You should reduce the size of the jobs database before upgrade. This action minimizes the amount of processing required to perform the association and minimizes the effect on web services performance. Very large job databases may see an alert regarding high heap space usage.

The affected workloads include: Cloud, Nutanix AHV, RHV, and VMware

For further details see the following article:

http://www.veritas.com/docs/100049808

NetBackup administration interface operational notes

The NetBackup administrator has a choice of several interfaces to use to administer NetBackup. All of the interfaces have similar capabilities. This topic contains some of the operational notes and known issues that are associated with these interfaces in NetBackup 10.2.

For more information about the specific NetBackup administration interfaces, refer to the *NetBackup Web UI Administrator's Guide* or the *NetBackup Administrator's Guide, Volume I*.

For information about how to install the interfaces, refer to the *NetBackup Installation Guide*. For information about platform compatibility with the administration consoles, refer to the various NetBackup compatibility lists available on the Veritas Support website.

See “About NetBackup compatibility lists and information” on page 46.

Delay in NetBackup web UI when adding or removing columns in Catalog area

In the **Catalog** area of the web UI, you can add or remove columns from the table of images. The more images that are displayed, the longer it takes for the interface to refresh if you add or remove columns. This issue will be fixed in an upcoming release.

Job actions not available for workload administrators with limited RBAC permissions on assets

Note following issues for view and managing jobs with the NetBackup web UI:

- A job does not receive an asset ID until it runs, which means a queued job does not have an asset ID. Users that have roles with more granular asset permissions for a workload are not able to view or cancel queued jobs.

  This behavior does not affect users with an RBAC role that has full job permissions or a role that can manage all assets for a particular workload.
- A job does not receive an asset ID if the asset is not yet discovered. Users that have roles with more granular asset permissions for a workload are not able to cancel or restart a job for the asset.

  This behavior does not affect users with an RBAC role that has full job permissions or a role that can manage all assets for a particular workload.

Example 1 - VMware administrator with limited asset permissions cannot cancel any queued jobs

Consider a user that has RBAC permissions only for a VMware vCenter or one or more VMs.

- The user cannot see queued jobs for the vCenter or for the VMs.
- Similarly, the user is not able to cancel any queued jobs for the vCenter or for the VMs.

Example 2 - VMware or RHV administrator with limited asset permissions cannot cancel or restart jobs for undiscovered assets

Consider a user that has RBAC permissions only for a VMware vCenter or an RHV server. This user also has one or more job permissions for these assets, but does not have job permissions for all workload assets.

- A new asset is added to the environment, but the discovery process hasn't run yet.
- An existing intelligent group is configured so it includes the new asset.
- When the backup runs, it includes the new asset in the backup.
- The user is not able to cancel or restart a job for the new asset.

Intermittent issues with X forwarding of NetBackup Administration Console

Intermittent issues may occur with X forwarding of the NetBackup Administration Console. This behavior only occurs when you use X forwarding. This issue does not occur at the local console. The issue is most commonly seen on Linux servers, but not exclusively. The issue generally occurs when older versions of X viewers are used, such as Xming and XBrowser.

The use of MobaXterm seems to minimize or eliminate the issue. If you experience issues with X forwarding, consider upgrading your X viewer and retrying the operation or access the server from the local console.

NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later

The NetBackup Administration Console may encounter a core dump issue when the Simplified Chinese UTF-8 locale is used on a Solaris SPARC 64-bit system with Solaris 10 Update 2 and later installed. For more information, refer to Bug ID 6901233 at the following URL on the Oracle Technology Network website:

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6901233

If you encounter this issue, apply the appropriate Solaris patches or upgrades that Oracle provides for this issue.

NetBackup Bare Metal Restore operational notes

NetBackup Bare Metal Restore (BMR) automates and streamlines the server recovery process, making it unnecessary to reinstall operating systems or configure hardware manually. This topic contains some of the operational notes and known issues that are associated with BMR in NetBackup 10.2.

After PIT restore, "The host ID does not exist" error appears

After a point in time (PIT) restore operation (which may include either a **Full File System** restore or a **BMR restore**), the error message **The host ID does not exist** appears.

In this scenario, a full backup is taken when a SERVICE_USER as root/administrator account is configured. This account takes the backup of the NetBackup installed binaries with root/administrator ownership. Before a restore, SERVICE_USER is configured with an account other than root/administrator, and then an incremental

backup is taken where the service user is backed up as part of `bp.conf`. In a PIT restore operation with the incremental backup, the SERVICE_USER entry gets restored. However, the binaries are restored in the root account ownership.

Workaround:

After changing the service user, you must take a full backup, whether it is a **MS-Windows\Standard Policy** for File System or **BMR** policy configuration.

NetBackup services may not start automatically after BMR restore on a Linux client

NetBackup services may not start automatically after a Bare Metal Restore (BMR) restore operation is performed on the Linux client.

The NetBackup services may run for a while after a BMR restore operation, and the BMR post-restore scripts may complete successfully. Later, however, NetBackup services may stop.

This issue happens only if a service user is different than the root user that is defined on the NetBackup Linux client.

Workaround:

Start the NetBackup services manually on the Linux client. To start the services, run the following command:

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

BMR direct P2V VM conversion task fails with status code 7

The Bare Metal Restore (BMR) direct physical-to-virtual (P2V) virtual machine (VM) conversion task fails with status code 7. After VM creation, the issue occurs when BMR tries to mount the disks on the Virtual Instance Converter (VIC) VDDK mount call.

The following example shows how the error appears in the `bmrb2vrst` logs:

```
0,51216,434,434,1225074,1669017201225,3136,3144,0:,211:MountManagerApi::AddMountPoint() -
 Error: Failed to create mountpoint:
\\?\Volume{7427BE07-4C03-4849-8B50-4BB2186EAFE0} for device:
 \Device\vstor2-mntapi20-shared-90B9CB4700001000000000001000000.
 Error code:
87,42:CVmwareOffHostVmRestoreWorker.cpp:ubslog(),5
0,51216,434,434,1225075,1669017201225,3136,3144,0:,188:SetupVirtVolumeAccess
 The device \Device\vstor2-mntapi20-shared-90B9CB4700001000000000001000000 has no
drive letter. Using the volume guid \\?\Volume{9d318822-6695-11ed-80b4-806e6f6e6963},
```

```
42:CVmwareOffHostVmRestoreWorker.cpp:ubslog(),5
0,51216,434,434,1225076,1669017201242,3136,3144,0:,91:FormatEx was unable to complete
 successfully 126-The specified module could not be
found.!!,
42:CVmwareOffHostVmRestoreWorker.cpp:ubslog(),5
```

Workaround:

Because this issue is specific to NetBackup 10.2 Virtual Instance Converter (VIC), you can use NetBackup 10.1 Virtual Instance Converter (VIC) to do BMR direct VM conversion of NetBackup 10.2 backups.

NetBackup Snapshot Manager (formerly NetBackup CloudPoint)

This topic contains some of the operational notes and known issues that are associated with NetBackup Snapshot Manager (formerly NetBackup with Veritas CloudPoint) and NetBackup 10.2.

Backups from snapshot jobs for NAS data protection policy fail with error 927

Backups from snapshot jobs for NAS data protection policy fail with error 927. This issue occurs if the backup host pool does not contain a host that is of the same or lower version of NetBackup than the media server.

Workaround:

Ensure that all media servers associated with the storage unit, specified in the Storage Lifecycle Policy (SLP), have a higher version NetBackup than the lowest version of backup host in the backup host pool.

To exclude a media server, go to the storage unit properties for the STU specified in the SLP. Select the **Only use the following media servers** option. Then select the media servers with a NetBackup version higher or equal to the lowest NetBackup version of the hosts in the backup host pool.

NetBackup for NDMP operational notes

NetBackup for NDMP is an optional NetBackup application. It enables NetBackup to use the Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems. This topic contains some of the operational notes and known issues that are associated with NetBackup for NDMP in NetBackup 10.2.

Parent directories in the path of a file may not be present in an NDMP incremental image

An issue can occur if a NetBackup Network Data Management Protocol (NDMP) backup policy is configured with the directive `set type=tar` in the backup selection. Parent directories in the path of a file that an incremental NDMP backup saves may not be present in the backup image. For more information on this issue, refer to the following tech note on the Veritas Support website:

http://www.veritas.com/docs/000095049

NetBackup for OpenStack operational notes

NetBackup for OpenStack is an optional NetBackup application. This topic contains some of the operational notes and known issues that are associated with NetBackup for OpenStack in NetBackup 10.2.

CentOS repository mirror URL is updated

The CentOS repository mirror URL is updated to `vault.centos.org` from `mirror.centos.org`. You must update it in all Yum repository files located at `/etc/yum.repos.d/CentOS-*`.

NetBackup for OpenStack Datamover API (NBOSDMAPI) service times out in the haproxy connection

The NBOSDMAPI service in the haproxy connection may time out due to slow response time in highly-used environments.

The default haproxy configuration works fine with most of the environments. When the time-out issue with the NBOSDMAPI is observed, customize the haproxy configuration. For more information, see the following tech note:

https://www.veritas.com/support/en_US/article.100052551

Instance volumes in the incremental backups cannot be mounted

Newly added disks of an instance for incremental backup get backed up successfully but these disks cannot be mounted.

NetBackup primary server does not re-issue the token if NetBackup VM is a 3-node cluster

Re-issue of the tokens for NetBackup certificate in the NetBackup configurator does not work if NetBackup VM is a 3-node cluster.

Workaround:

To resolve this issue, enable allow auto re-issue token on the primary server. You must enter **""** in the **Token** field on the NetBackup configurator. This configuration lets you proceed if the NetBackup OpenStack VM already has the certificates that primary server provides.

Success message appears along with the error message when you delete the policy that has snapshots

When you delete the policy that has snapshots, the following success and error messages appear. However, the policy is not deleted and only error message should appear.

- `Error: Invalid state: This policy contains snapshots. Please delete all snapshots and try again.`
- `Success: Deleted: <policy name>`

Unable to connect to NetBackup primary server using NBCA

While configuring NetBackup VM, if you enter NetBackup Primary Server name, the following error message appears:

```
Failed to establish connection with the NetBackup master server.
Error: HTTPSConnectionPool(host='NBU.master.server', port=443): Max
retries exceeded with url: /netbackup/security/ping (Caused by
NewConnectionError('<urllib3.connection.HTTPSConnection object at
0x7f9e466b0ef0>: Failed to establish a new connection: [Errno -2]
Name or service not known',))
```

Workaround:

Add IP host name mapping in `/etc/hosts` to resolve this issue.

For more information, see the following Support article:

https://www.veritas.com/support/en_US/article.100045941

Excluded Ceph Volume after restore is not mountable or formattable

VM Volumes stored on Ceph are successfully excluded from backup if desired.

Restore creates empty Ceph Volume, which is not attachable or formattable.

Restored VMs have blank metadata config_drive attached

For every restore, the metadata `config_drive` is set as blank value.

Workaround:

Delete metadata `config_drive` or set the desired value.

NBOSVM reconfig fails when you add new NetBackup VM to the cluster

NetBackup re-configuration fails when you add the nodes to the existing NetBackup VM.

Reason is that the previous MySQL password was not working and MySQL root access has been reset.

Workaround:

Remove `/root/.my.cnf` file on already configured NetBackup VM and reconfigure it.

Database does not sync after NetBackup cluster gets new nodes

After NetBackup re-configuration post addition of two more nodes to existing NetBackup VM cluster ("import policies" was not selected), the databases do not sync against already existing NetBackup VM.

It is expected that while adding the two new nodes, the databases on node1 should get synced up with the two new nodes, and the existing policies must be available post the reconfig on the new 3-node NetBackup VM cluster.

Workaround:

Run the policy import from CLI.

Data on boot disk gets backed up despite exclusion

VM was set with metadata exclude_boot_disk_from_backup set to true. Restored instance shows that data was backed up and restored.

After reinitialization and import, OpenStack certificates are missing

Reinitialization does not keep the already uploaded OpenStack certificates used to communicate with OpenStack.

Workaround:

Upload the certificates again.

CLI import changes scheduler trust value to disabled

When the import functionality is used by CLI, the scheduler trust changes from enabled to disabled.

Workaround:

Configure NetBackup with import option from UI after reinitialization.

Unable to get node details after you reinitialize the NetBackup Appliance

After you reinitialize the NetBackup Appliance, the UI and CLI do not display the node information.

Workaround:

Restart `nbosjm-policies` and `nbosjm-cron` services on NetBackup nodes.

```
systemctl restart nbosjm-policies
```

```
systemctl restart nbosjm-cron
```

Snapshots fails with "object is not subscriptable" for many policy jobs at the exact same time

Running more than 25 policies at the same time leads to an error. The `nbosdmapi` service does not respond.

Snapshots fail with `Object is not subscriptable.` error.

Workaround:

Contact Veritas Support to implement a known workaround.

No operation is permitted in insecure way for SSL-enabled Keystone URL

For SSL enabled OpenStack, Backup and Restore jobs fail with missing TLS CA certificate bundle error.

Workaround:

Configure the NetBackup appliance with OpenStack CA provided.

Or provide OpenStack CA to `/etc/nbosjm/ca-chain.pem`

NetBackup internationalization and localization operational notes

This topic contains some of the operational notes and known issues that are associated with internationalization, localization, and non-English locales in NetBackup 10.2.

Support for localized environments in database and application agents

Non-ASCII characters are supported in the following fields for NetBackup database and application agents.

- Oracle:
  Datafile path, Tablespace name, TNS path
- DB2:
  Datafile path, Tablespace name
- SAP:
  English SAP runs on localized OS. (No specific SAP fields are localized.)
- Exchange:
  Mailboxes, Mails, Attachment names and contents, Public folders, Contacts, Calendar, Folders and Database paths
- SharePoint:
  Site Collection Names, Libraries and lists within the site collection
- Lotus Notes:
  Emails data /.nsf files
- Enterprise Vault (EV) agent:
  Vault store, Partitions, Data
- VMWare:
  Username, Password, VM display name, DataCenter, Folder, Datastore, Resource pool, VApp, Network name, VM disk path

Certain NetBackup user-defined strings must not contain non-US ASCII characters

The following NetBackup user-defined strings must not contain non-US ASCII characters:

- Host name (primary server, media server, Enterprise Media Manager (EMM) server, volume database host, media host, client, instance group)
- Policy name
- Policy KEYWORD (Windows only)
- Backup, Archive, and Restore KEYWORD (Windows only)
- Storage unit name
- Storage unit disk pathname (Windows only)
- Robot name
- Device name
- Schedule name
- Media ID
- Volume group name
- Volume pool name
- Media description
- Vault policy names
- Vault report names
- BMR Shared Resource Tree (SRT) name
- Token name
- Storage lifecycle policy (SLP) names

Appendix A

About SORT for NetBackup Users

This appendix includes the following topics:

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

Appendix B

NetBackup installation requirements

This appendix includes the following topics:

About NetBackup installation requirements

This release of NetBackup may contain changes to the minimum system requirements and procedures that are required for installation. These changes affect the minimum system requirements for both Windows and UNIX platforms. Much of the installation instructional information in the *NetBackup Release Notes* is provided for convenience. Detailed installation instructions are found in the *NetBackup Installation Guide* and the *NetBackup Upgrade Guide*.

See "NetBackup installation and upgrade operational notes" on page 23.

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- Before upgrading to NetBackup 10.2, you must ensure that you have the free disk space that is twice the size of the NetBackup relational database. That means for default installations of the primary server, you are required to have that amount of free space on the file system containing the `/usr/openv/db/data` (UNIX) or `<install_path>\Veritas\NetBackupDB\data` (Windows) directories. If you have changed the location of some of the files in either of these directories, free space is required in those locations equal to or greater than the size of the

files in those locations. Refer to the *NetBackup Administrator's Guide, Volume I* for more information about storing NBDB database files in alternate locations.

Note: This free disk space requirement assumes that you have already performed the best practice of completing a successful catalog backup before you begin the upgrade.

- Primary and media servers must have a minimum soft limit of 8000 file descriptors per process for NetBackup to run correctly.
  For more information about the effects of an insufficient number of file descriptors, refer to the following articles on the Veritas Support website:
  http://www.veritas.com/docs/000013512
- NetBackup primary and media servers exchange server version information at startup, and every 24 hours. This exchange occurs automatically. During startup after an upgrade, the upgraded media server uses the `vmd` service to push its version information to all of the servers that are listed in its server list.
- Veritas recommends that you have the primary server services up and available during a media server upgrade.
- All compressed files are compressed using gzip. The installation of these files requires gunzip and gzip, so make sure that they are installed on the computer before you attempt to install NetBackup. For all UNIX platforms except HP-UX, the binaries are expected to be in `/bin` or `/usr/bin` and that directory is a part of the root user's `PATH` variable. On HP-UX systems, the `gzip` and `gunzip` commands are expected to be in `/usr/contrib/bin`. Installation scripts add that directory to the `PATH` variable. These commands must be present to have successful UNIX installations.

Required operating system patches and updates for NetBackup

NetBackup server and client installations are only supported on a defined set of operating systems (OSs) that are listed in the NetBackup Compatibility Lists for All Versions. Most OS vendors provide patches, updates, and service packs (SPs) for their products. The best practice of NetBackup Quality Engineering is to test with the latest SP or update level of the OS when a platform is tested. Therefore, NetBackup is supported on all vendor GA updates (n.1, n.2, and so on) or SPs (SP1, SP2, and so on). However, if a known compatibility issue exists on a specific SP or updated OS level, this information is identified in the compatibility lists. If no

such compatibility issues are noted, Veritas recommends that you install the latest OS updates on your servers and clients before you install or upgrade NetBackup.

The most up-to-date required OS patch information for NetBackup 10.2 and other NetBackup releases can be found on the Veritas Services and Operational Readiness Tools (SORT) website and in the NetBackup Compatibility Lists for All Versions. The compatibility lists include information about the minimum OS level that is required to support a minimum NetBackup version in the latest major release line. In some cases, new releases of NetBackup may require specific vendor OS updates or patches.

See "About NetBackup compatibility lists and information" on page 46.

See "About Veritas Services and Operations Readiness Tools" on page 38.

NetBackup 10.2 binary sizes

Table B-1 contains the approximate binary sizes of the NetBackup 10.2 primary server, media server, and client software for the various supported operating systems. These binary sizes indicate the amount of disk space occupied by the product after an initial installation. Note that for the sizes listed in the table, 1 MB equals 1024 KB.

Note: As of NetBackup 8.3, the Java GUI and JRE packages are optional with most clients and media servers. The package sizes were calculated with the Java GUI and JRE included.

Note: Table B-1 lists only the supported operating systems. For up-to-date information about the specific operating system versions that NetBackup currently supports, check the Installation and Upgrade Checklist on the Services and Operations Readiness Tools (SORT) website, or the NetBackup Compatibility List for all Versions.

Table B-1 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	64-bit client	64-bit server	Notes
AIX	POWER	1659 MB	No longer supported	
Canonical Ubuntu	x86-64	1602 MB		
CentOS	x86-64	1602 MB	10780 MB	

Table B-1 NetBackup binary sizes for compatible platforms *(continued)*

OS	CPU Architecture	64-bit client	64-bit server	Notes
Debian GNU/Linux	x86-64	1602 MB		
Kylin Linux Advanced Server 10.0		1570		
NeoKylin Linux Advanced Server		1671		
Oracle Linux	x86-64	1602 MB	10780 MB	
Red Hat Enterprise Linux Server	POWER	328 MB		
Red Hat Enterprise Linux Server	x86-64	1570 MB	10466 MB	
Red Hat Enterprise Linux Server	z/Architecture	889 MB	No longer supported	Media server or client compatibility only.
Rocky Linux client		1602 MB		
Solaris	SPARC	1333 MB	No longer supported	
Solaris	x86-64	1327 MB	No longer supported	
SUSE Linux Enterprise Server	POWER	329 MB		
SUSE Linux Enterprise Server	x86-64	1202 MB	6645 MB	
SUSE Linux Enterprise Server	z/Architecture	904 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64	557 MB	4720 MB	Covers all compatible Windows x64 platforms.

The following space requirements also apply to some NetBackup installations on Windows:

- If you install NetBackup in a custom location on a Windows system, some portions of the software are installed on the system drive regardless of the primary application folder location. The space that is required on the system drive generally accounts for 40 to 50 percent of the total binary size that is listed in Table B-1.

- If you install NetBackup server on a Windows cluster, some portions of the software are installed on the cluster shared disk. Note, the space that is required on the cluster shared disk is in addition to the binary size that is listed in Table B-1. The additional required space is equivalent to 15 to 20 percent of the total binary size.

Appendix C

NetBackup compatibility requirements

This appendix includes the following topics:

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: primary server, media server, and then clients. For example, the scenario that is shown is supported: 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 compatibility lists and information

The *NetBackup Release Notes* document contains a great deal of the compatibility changes that are made between NetBackup versions. However, the most up-to-date compatibility information on platforms, peripherals, drives, and libraries can be found on the Veritas Operations Readiness Tools (SORT) for NetBackup website.

See "About Veritas Services and Operations Readiness Tools" on page 38.

For NetBackup, SORT provides an Installation and Upgrade Checklist report as well as the ability to collect, analyze, and report on host configurations across your environments. In addition, you can determine which release contains the hot fixes or EEBs that you may have installed in your environment. You can use this data to assess whether your systems are ready to install or upgrade to a given release.

NetBackup compatibility lists

In addition to SORT, Veritas has made available a variety of compatibility lists to help customers quickly reference up-to-date compatibility information for NetBackup:

NetBackup Compatibility Lists for All Versions

Note: For information about which versions of NetBackup are compatible with each other, select a **Software Compatibility List (SCL)**, and then select **Compatibility Between NetBackup Versions** from within the SCL.

About NetBackup end-of-life notifications

Veritas is committed to providing the best possible data protection experience for the widest variety of systems: platforms, operating systems, CPU architecture, databases, applications, and hardware. Veritas continuously reviews NetBackup system support. This review ensures that the proper balance is made between maintaining support for existing versions of products, while also introducing new support for the following:

- General availability releases
- Latest versions of new software and hardware

- New NetBackup features and functionality

While Veritas continually adds support for new features and systems, it may be necessary to improve, replace, or remove certain support in NetBackup. These support actions may affect older and lesser-used features and functionality. The affected features and functionality may include support for software, OS, databases, applications, hardware, and 3rd-party product integration. Other affected items may include the products that are no longer supported or nearing their end-of-support life with their manufacturer.

Veritas provides advance notification to better help its customers to plan for upcoming changes to the support status of the various features in NetBackup. Veritas intends to list older product functionality, features, systems, and the 3rd-party software products that are no longer supported in the next release of NetBackup. Veritas makes these support listings available as soon as possible with a minimum of 6 months where feasible before major releases.

Using SORT

Advance notification of future platform and feature support including end-of-life (EOL) information is available through a widget on the Veritas Services and Operations Readiness Tools (SORT) for NetBackup home page. The NetBackup Future Platform and Feature Plans widget on the SORT for NetBackup home page can be found directly at the following location:

https://sort.veritas.com/nbufutureplans

NetBackup end-of-support-life (EOSL) information is also available at the following location:

https://sort.veritas.com/eosl/show_matrix

See “About Veritas Services and Operations Readiness Tools” on page 38.

About changes in platform compatibility

The NetBackup 10.2 release may contain changes in support for various systems. In addition to using SORT, you should make sure to review the *NetBackup Release Notes* document and the NetBackup compatibility lists before installing or upgrading NetBackup software.

See “About new enhancements and changes in NetBackup” on page 10.

http://www.netbackup.com/compatibility

Appendix D

Other NetBackup documentation and related documents

This appendix includes the following topics:

About related NetBackup documents

Veritas releases various guides that relate to NetBackup software. Unless otherwise specified, the NetBackup documents can be downloaded in PDF format or viewed in HTML format from the NetBackup Documentation Landing Page.

Not all documents are published with each new release of NetBackup. In the guides, you may see references to other documents that were not published for NetBackup 10.2. In these cases, refer to the latest available version of the guide.

Note: Veritas assumes no responsibility for the correct installation or use of PDF reader software.

All references to UNIX also apply to Linux platforms unless otherwise specified.
