NetBackup™ Release Notes

Release 10.1

Document Version 1

VERITAS™

NetBackup™ Release Notes

Last updated: 2022-09-07

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

About NetBackup 10.1

This chapter includes the following topics:

- About the NetBackup 10.1 release
- About NetBackup Late Breaking News
- About NetBackup third-party legal notices

About the NetBackup 10.1 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 10.1 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 10.1 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 44.

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

New features, enhancements, and changes

This chapter includes the following topics:

- About new enhancements and changes in NetBackup
- NetBackup 10.1 new features, changes, and enhancements

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 10.1 release” on page 8.

See “About NetBackup compatibility lists and information” on page 51.

NetBackup 10.1 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 10.1 are grouped below by category. Select a link to read more information about the topic.

New features

- Changes in Veritas terminology
- Malware detection enhancements
- RESTful APIs included in NetBackup 10.1
- Additional policy types supported in the NetBackup web UI
- Activity monitor improvements in the NetBackup web UI

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 10.1 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

- Enhancements in FIPS support
- About the TLS session resumption feature in Global security

Support changes and enhancements

- NetBackup 10.1 support additions and changes
- Support updates for universal share
- Support updates for instant access for cloud backups
- Several shutdown commands to be deprecated in a future release

Installation, upgrade, and configuration changes and enhancements

- NetBackup Snapshot Manager must run the same version as NetBackup primary and media servers

Cloud-related changes and enhancements

- Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.1
- Migrating Google Cloud Platform (GCP) configurations from zones to regions
- Support for new PaaS databases
- Support for cloud immutable (WORM) storage in a cluster environment
- Support for S3 interface for MSDP
- Malware scanner available in the Microsoft Azure Marketplace and the AWS Marketplace
- Setting the cloud cache size in the MSDP disk pool cloud LSU
- Cloud object store workload support

Virtualization changes and enhancements

- VMware NAS storage snapshots and replication using NetBackup Snapshot Manager

Workload and database agent changes and enhancements

- Reinstall Kubernetes-based extension for Azure
- MySQL enhancements
- PostgreSQL enhancements
- Workloads that require a custom RBAC role for specific job permissions in the NetBackup web UI
- Web UI support for Microsoft SQL Server recovery using existing credentials and gMSA credentials
- Accurate licensing support
- XBSA workloads available with the NetBackup client

Other announcements

- No release of NetBackup OpsCenter and OpsCenter Analytics
- Transition from Replication Director to NetBackup Snapshot Manager Replication
- NetBackup Bare Metal Restore (BMR) operations in the NetBackup web UI
- IRE limitations
- Limitations for running NetBackup services with non-privileged user (service user) account in NetBackup 10.1

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
Black hat	Unethical

Malware detection enhancements

Malware detection and recovery web UI enhancements:

- Recover a clean copy of an infected file if available from another backup image in selected data and time range for Standard and MS-Windows policy type.
- A new RBAC permission (“Allow recovery from infected images”) lets you restore files from the infected images. Without this permission, you can restore files only from clean or not scanned images.
- Search and scan backup images based on Policy Name, Policy Type, Schedule Type (type of backup), Client Name, Backup copy number, MSDP Disk Pool Name, Malware Scan Status, and date and time range.
- Viewing of infected files now supports searching on the file path. The list of infected files can be exported as CSV file.
- Scan jobs which are in a pending state or an in-progress state can be canceled from the web UI.

Malware detection support is extended to VMware VM backup images:

- On-demand scan support for the Administrator user from Malware Detection by selecting the VMware asset (VM) and triggering a malware scan.

- On-demand scan support for the VMware administrator from **Workloads > VMware** in the web UI.
- Recovery from a malware-infected recovery point is disabled by default. You must enable “Allow the selection of recovery points that are malware-affected” to recover.
- Single or Bulk Instant VM rollback from a clean recovery point.

In addition following features and enhancements are available with this release:

- Support for non-root users on Linux scan hosts.
- Automated cleanup of scan jobs that are older than 30 days are in clean, failed, or canceled state. This feature is configurable.
- NetBackup Malware Scanner version 2.0 contains improvements that are related to scanning performance and includes multi-threaded scanning support.

  Note: If you currently use NetBackup Malware Scanner version 1.0, which is available with NetBackup 10.0, Veritas recommends that you update to NetBackup Malware Scanner version 2.0.

RESTful APIs included in NetBackup 10.1

NetBackup 10.1 includes both updated and new RESTful application programming interfaces (APIs). These APIs 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 > 10.1
  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 10.1 includes these new and enhanced APIs:

- Cloud Object Store:
  List cloud providers which support cloud object protection.
- Proxy Servers:
  Create and update internet proxy server details.
- Paused Clients:
  Pause and unpause protection for a client.
- Disk Array Hosts:
  Create, update, and delete disk array host credentials.
- DBPaaS:
  Associate a named credential to a DBPaaS asset.
- DMP:
  Recover individual NDMP files and folders.
- Cloud Workloads:
  Create and delete instant access mounts.
- VMware:
  - Query VMware Cloud vApp information.
  - Create and delete malware scan mounts.
- Catalog Images:
  - View the contents of rollback images.
  - List images associated with SLPs.
- Snapshot Providers:
  - List security groups in a region.

    - Retrieve supported replication destinations for on-premise storage array snapshot replication.

- Bare Metal Restore (BMR):
    - List Windows driver packages that are attached to the BMR configuration.
    - Map a configuration ID from the configuration.
    - Update `zfs` file system and volume attributes.
    - Create and delete physical volumes in the configuration.
    - List available disks.
    - List and update licenses.
    - Update volume group properties.

Versioned APIs

These APIs that have been versioned in NetBackup 10.1 due to breaking changes. The previous version of these APIs is still supported by specifying the correct version. See the *Versioning* section in the **API Reference** on SORT for examples and more details.

- Get Token List:
  `GET /security/securitytokens` has changed the properties of the object `getTokenResponse` to return the list of objects from `getTokenDataList` with pagination attributes.
- Get Valid Token List:
  `GET /security/securitytokens/state/valid` has changed the properties of the object `getTokenResponse` to return the list of objects from `getTokenDataList` with pagination attributes.
- Initiate CA migration:
  `POST /security/certificate-authorities/initiate-migration` has removed the support for generating CA of keysize 16384. If you already have an active CA with keysize 16384, use the existing CA migration mechanism to downgrade to supported values.

Additional policy types supported in the NetBackup web UI

The NetBackup web UI now supports the configuration of the following policy types:

- BigData
- DB2
- MS-Exchange-Server

- NDMP
- Informix
- SAP

Activity monitor improvements in the NetBackup web UI

The following improvements were made to the Activity monitor in this release.

- Ability to maximize the view of the Activity monitor so you can use the entire browser window and view more jobs.
- Ability to view the job details in a new window. This action lets you more easily compare the details of different jobs.
- In the details for a job, the **Attempts** field displays the latest attempt first. Previously the job details displayed attempt 1 as the first. For example, consider that a job is attempted three times: Attempt 1 (6:00 A.M.), attempt 2 (8:00 A.M.), attempt 3 (10:00 A.M.). Attempt 3 (10:00 A.M.) is the latest attempt and is displayed first in the job details.

Enhancements in FIPS support

Enabling FIPS mode during NetBackup installation

Starting with NetBackup 10.1, you can enable FIPS mode during installation. For more information, refer to the *NetBackup Installation Guide*.

Workloads supported in the FIPS-compliant mode

Starting with NetBackup 10.1, the following workloads are supported in the FIPS-compliant mode in addition to the existing workloads:

- Cassandra
- Sybase
- Informix
- MS-Exchange
- Enterprise Vault
- BMR
- Universal Shares
- OpenStack (cloud-based solution)

For more details on the FIPS configurations, refer to the *NetBackup Security and Encryption Guide*.

NetBackup 10.1 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 10.1:

- Azure stack hub version 2108
- PostgreSQL 14 on Ubuntu 20.4 ELS
- PostgreSQL 13 on Ubuntu 20.4 ELS
- MongoDB 5.0 on RedHat Linux Enterprise Server 8 (x86-64)
- SAP Oracle 7 on SUSE Linux Enterprise Server 15 SP3 (x86-64)
- VMWare on Windows 2022 as a Backup Host (VDDK 7.0.3.2)
- VMWare on RedHat 8.6 as a Backup Host (VDDK 7.0.3.2)
- Red Hat Open Shift 4.10
- Wasabi S3 Object Lock
- iTernity - Cloud (S3)
- Cloudian S3 - Object Lock
- EMC-ECS S3 - Object Lock
- Scality Ring S3 - Object Lock (Compliance mode)

About the TLS session resumption feature in Global security

NetBackup uses TLS (Transport Layer Security) to secure communications between NetBackup hosts. Each new TCP connection between NetBackup hosts must perform a TLS handshake and verify the peer identity before NetBackup sends traffic across that connection.

The session resumption feature optimizes the TLS handshake so that a full handshake is not required for every TCP connection. The security level determines how long NetBackup allows a TLS session to be reused before a full handshake is required.

You can set the security level interval as follows:

- Default to current security level (10, 30, or 60 minutes)
- Custom – 1 minute to 720 minutes

This feature currently only applies to NBCA. ECA to be supported in a future release.

For more information, review the *About TLS session resumption* section in the *NetBackup Web UI Administrator's Guide*.

Support updates for universal share

NetBackup now supports universal share with the following platforms:

- NetBackup Appliance
- Flex Appliance
- Flex Scale
- Flex WORM
- MSDP AKS (Azure Kubernetes Services)/EKS (Amazon Elastic Kubernetes Service) deployment
- Build-your-own (BYO)

Support updates for instant access for cloud backups

NetBackup now supports instant access for cloud backups with the following policies:

- Windows
- Standard
- Universal share
- VMware
- MS-SQL
- Oracle

NetBackup now supports instant access for cloud backups with the following platforms:

- MSDP AKS (Azure Kubernetes Services)/EKS (Amazon Elastic Kubernetes Service) deployment
- Build-your-own (BYO) in cloud (manually enabled)

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*.

NetBackup Snapshot Manager must run the same version as NetBackup primary and media servers

For NetBackup version 10.1, NetBackup primary servers, media servers, and Snapshot Manager should all run the same version.

When you upgrade, first upgrade Snapshot Manager, and then upgrade NetBackup servers to version 10.1.

Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.1

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 10.1. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 10.1, 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 2.9.2.

The following cloud support has been added to version 2.9.5 and later but was not included in the NetBackup 10.1 final build:

- Amazon Glacier Instant Retrieval (IR)
- iTernity iCAS FS (S3)
- Amazon (S3) - Asia Pacific (Jakarta) region
- Google (S3) - Asia South2 (Delhi) region
- Google (S3) - Australia-Southeast2 (Melbourne) region
- Google (S3) - EU West9 (Paris) region
- Google (S3) - EU Southwest1 (Madrid) region
- Google (S3) - US East5 (Columbus) region
- Google (S3) - US South1 (Dallas) region
- Google (S3) - North America Northeast2 (Toronto) region

- Wasabi (S3) - EU-West-2 (Paris) 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

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

Migrating Google Cloud Platform (GCP) configurations from zones to regions

With NetBackup Snapshot Manager 10.1, Google Cloud Platform (GCP) configurations are being migrated from zones to regions. This migration allows improved setup and maintenance of GCP configurations.

Before you upgrade to NetBackup Snapshot Manager 10.1, make sure that you review details about the migration to regional GCP configurations in the *NetBackup Snapshot Manager Install and Upgrade Guide*.

See “NetBackup Snapshot Manager must run the same version as NetBackup primary and media servers” on page 20.

Support for new PaaS databases

NetBackup 10.1 now supports the following new platform-as-a-service (PaaS) databases, under the **Cloud** workload. The **Applications** tab displays the RDS assets, whereas the **PaaS** tab displays the non-RDS assets. You can view, protect, and recover PaaS assets from these two tabs.

- Azure SQL
- Azure SQL Managed Instance
- Azure PostgreSQL
- Azure MySQL
- Azure MariaDB
- AWS RDS PostgreSQL and MySQL

- AWS Aurora DB PostgreSQL and MYSQL
- AWS MariaDB
- AWS DynamoDB
- GCP SQL (PostgreSQL and MySQL)

For more information, see *NetBackup Web UI Cloud Administrator's Guide*.

Support for cloud immutable (WORM) storage in a cluster environment

NetBackup now supports deployment of cloud-immutable storage in the cluster environments such as Azure Kubernetes Service (AKS), Amazon Elastic Kubernetes Service (EKS), and NetBackup Flex Scale. For more information, see *NetBackup Deduplication Guide*.

Support for S3 interface for MSDP

The S3 interface for MSDP provides S3 APIs. You can use the S3 interface for MSDP to store the data on the MSDP server. For more information, see *NetBackup Deduplication Guide*.

Malware scanner available in the Microsoft Azure Marketplace and the AWS Marketplace

You can download a malware scanner from the Microsoft Azure Marketplace and the AWS Marketplace. Follow the instructions on how to install, configure, and use the malware scanner for AWS and Azure.

Refer to the following for more information about AWS:

AWS Marketplace

Cloud NetBackup Marketplace Deployment on AWS

Refer to the following for more information about Microsoft Azure:

Microsoft Azure Marketplace

NetBackup Marketplace Deployment on Azure Cloud

Setting the cloud cache size in the MSDP disk pool cloud LSU

When you add an MSDP disk pool, you can set the **Cloud cache size** for the disk pool cloud LSU. Use the Request cloud cache disk space feature to set the cloud cache disk space size.

The following attribute values are derived from the **Request cloud cache disk space** value:

- `UploadCacheGB`
- `DownloadDataCacheGB`
- `DownloadMetaCacheGB`
- `MapCacheGB`

Those values are written into the appropriate cloud LSU section within the `<MSDP storage path>/etc/puredisk/cloud.json` configuration file on the media server.

Cloud object store workload support

NetBackup now supports backup and restore of Cloud object store. NetBackup can protect Azure Blob Storage, and a wide variety of S3 API-compatible object store types like AWS S3, Google Cloud Storage (GCS), Hitachi Cloud Platform object store, and so on.

You can deploy the NetBackup environment in the same cloud network as the object store or a different one. For more information, see *NetBackup Web UI Cloud Object Store Administrator's Guide*.

VMware NAS storage snapshots and replication using NetBackup Snapshot Manager

NetBackup introduces hardware snapshot-based solution for VMware storage array snapshots for protecting VMware VMs. Hardware snapshots significantly reduce stun time for VMs. NetBackup retains the VM snapshot only for the duration of hardware snapshot

This solution uses the NetBackup snapshot manager for performing hardware snapshots. For details, see *NetBackup Web UI VMware Administrator’s Guide*.

Reinstall Kubernetes-based extension for Azure

When you upgrade the Kubernetes-based extension on Azure Kubernetes Service (AKS) from version 9.1 to 10.0 or later, you must reinstall the Kubernetes extension. For more information, see “Snapshot Manager upgrade on Kubernetes based extension for Azure” in the *NetBackup Snapshot Manager Install and Upgrade Guide*.

MySQL enhancements

NetBackup 10.1 includes state-of-art features for the protection of MySQL. NetBackup 10.1 provides following enterprise-level capabilities to protect MySQL using the NetBackup web UI:

- Integration with NetBackup web UI:
  MySQL features are integrated with NetBackup web UI to provide ability to configure, protect, recover, and monitor MySQL resources from a web browser.
- Role Base Access Control (RBAC):
  Let's the administrator configure user access and delegate NetBackup tasks such as MySQL Asset management, Credentials access, workload protection.
- Credential Management:
  MySQL credentials are added in the NetBackup Credential Management database as named credentials. The owner can share named credentials with other users or administrators for reuse without revealing actual credentials.
- Automatic Asset Discovery:
  MySQL Instances are auto discovered and added in NetBackup asset. NetBackup runs automatic resource-discovery process and adds all databases in the NetBackup asset. The resource discovery process runs at a scheduled interval which is configurable. This option ensures that any newly added databases are included in the NetBackup asset.
- Backup Now:
  Lets you perform ad hoc backup outside the backup schedule.
- Supported backup methods:
  Snapshot (LVM/VSS) and `mysqldump` are supported for Instance backup. Databases are protected using the `mysqldump` method.
- Incremental backup
  Incremental backup (bin log) is supported only for instance-level protection.
- Restore options using the NetBackup web UI recovery wizard:
  - Instance restores.
    Lets you restore the entire MySQL Instance to the same or a different MySQL.
  - Database restore.
    Lets you restore the entire MySQL Database to the same or a different MySQL Instance.
- NetBackup APIs.
  You can also use NetBackup APIs for all these new features.

For details, refer to the *NetBackup Web UI MySQL Administrator's Guide*.

PostgreSQL enhancements

NetBackup 10.1 includes state-of-art features for the protection of PostgreSQL. NetBackup 10.1 provides following enterprise-level capabilities to protect PostgreSQL using the NetBackup web UI:

- Integration with NetBackup web UI.

  PostgreSQL features are integrated with NetBackup web UI to provide ability to configure, protect, recover, and monitor PostgreSQL resources from a web browser.
- Role-based access control (RBAC).

  Lets the administrator configure user access and delegate NetBackup tasks such as PostgreSQL asset management, credentials access, and workload protection.
- Credential Management.

  PostgreSQL credentials are added in the NetBackup Credential Management database as named credentials. The owner can share named credentials with other users or administrators for reuse without revealing actual credentials.
- Automatic Asset Discovery.

  PostgreSQL Instances are auto discovered and added in NetBackup asset. NetBackup runs automatic resource-discovery process and adds all databases in the NetBackup asset. The resource discovery process runs at a scheduled interval which is configurable. This option ensures that any newly added databases are included in the NetBackup asset.
- Backup Now.

  Lets you perform ad hoc backups outside the backup schedule.
- Supported backup methods.

  Snapshot (LVM/VSS) and `pg_basebackup` are supported for Instance backup. Databases are protected using `pg_dump` method.
- Incremental backup.

  Incremental backup (WAL) is supported only for instance-level protection.
- Restore options using the NetBackup web UI recovery wizard:
  - Instance restores.

    Lets you restore the entire PostgreSQL Instance to the same or a different PostgreSQL.
  - Database restore.

    Lets you restore the entire PostgreSQL Database to the same or a different PostgreSQL Instance.
- NetBackup APIs.

You can also use NetBackup APIs for all these new features.

For details, refer to the *NetBackup Web UI PostgreSQL Administrator's Guide*.

Workloads that require a custom RBAC role for specific job permissions in the NetBackup web UI

The 10.1 release now offers granular job access for certain workloads in the NetBackup web UI. This functionality lets you create a custom RBAC role with job permissions for a particular workload.

Note that these workloads do not have a corresponding default RBAC role. When you configure the custom role, the permissions in the **Workloads** card do not apply for these workloads. You can configure job permissions for the following workload types:

BackTrack

DataStore

DB2

Enterprise Vault

Exchange

FlashBackup

FlashBackup Windows

Hyper-V

Informix

Lotus Notes

SharePoint

MS-Windows

NAS Data Protection

NBU Catalog

NDMP

PureDisk Export

SAP

Standard

Sybase

Vault

RBAC job permissions for BigData workloads

In this release, you cannot configure job permissions specifically for Hadoop, HBase or MongoDB. To view and manage jobs for these workloads, create a role that includes all NetBackup job permissions. (In **Global > NetBackup management > Jobs**.)

Web UI support for Microsoft SQL Server recovery using existing credentials and gMSA credentials

The NetBackup web UI now supports SQL Server recovery using existing credentials, including gMSA credentials. In previous releases, there was only an option to manually enter credentials.

- Ensure that the gMSA credential has sufficient recovery permissions. Then configure the gMSA credential with the option **Use credentials that are defined**

locally on the client. (This option is available when you create a credential in Credential management.)

- Configure the NetBackup Client Service and the NetBackup Legacy Network Service to log on with the gMSA account.
- During recovery in the NetBackup web UI, select the NetBackup credential that you created for the gMSA account.

Accurate licensing support

The following workloads support accurate licensing with NetBackup 10.1:

- NetBackup for SQLite
- NetBackup for MariaDB
- NetBackup for MySQL
- NetBackup for PostgreSQL

XBSA workloads available with the NetBackup client

The following XBSA workloads are available with the NetBackup client in NetBackup 10.1:

- NetBackup for SQLite
- NetBackup for MariaDB
- NetBackup for MySQL
- NetBackup for PostgreSQL

No release of NetBackup OpsCenter and OpsCenter Analytics

Starting with NetBackup 10.1, NetBackup OpsCenter and OpsCenter Analytics is not part of NetBackup software. NetBackup IT Analytics (formerly APTARE) is the solution for NetBackup reporting and analytics.

Transition from Replication Director to NetBackup Snapshot Manager Replication

Starting with NetBackup 10.1, administrators can use the NetBackup Snapshot Manager for Data Center to replicate the NAS storage array snapshots that NetBackup captures. Currently, NAS-Data-Protection and VMware policies are supported with NetBackup Snapshot Manager Replication. See the *NetBackup*

Snapshot Manager for Data Center Administrator’s Guide for more details on storage array replication.

For the transition of existing Replication Director policies for NAS storage, refer to the following technical article:

https://www.veritas.com/content/support/en_US/article.100053716.html

NetBackup Bare Metal Restore (BMR) operations in the NetBackup web UI

NetBackup 10.1 includes the following capabilities for Bare Metal Restore in the NetBackup web UI:

- View and manage the BMR clients and configurations.
- Perform pre-restore operations like prepare-to-restore, prepare-to-discover, dissimilar disk restores operations on the client configuration, and VM conversion client’s configurations.
- View and manage boot servers.
- View and manage resources like shared resource trees, discovered configurations, and Windows device driver packages.
- View and manage BMR restore or discover tasks.

For complete information on BMR, refer to the *NetBackup Bare Metal Restore Administrator's Guide*.

IRE limitations

Limitations to use the isolated recovery environment (IRE) feature in NetBackup:

- The IRE air gap does not support adding IPv6 subnets or addresses in the allowed list.
- The replication source MSDP server needs to be NetBackup 10.1 or Flex WORM 17.0.
- Windows MSDP server is not supported.

The support matrix for NetBackup secure communication based on production server environment and IRE is as follows:

Table 2-1 NetBackup secure communication based on production server environment and IRE

Production server environment	IRE		
	NBCA	**ECA**	**NBCA+ECA mixed mode**
NBCA	Supported	Not supported	Supported
ECA	Not supported	Supported	Supported
NBCA+ECA mixed mode	Supported	Not supported	Supported (use only NBCA)

Limitations for running NetBackup services with non-privileged user (service user) account in NetBackup 10.1

If the `bpcd` and `vnetd` processes run under an application account such as Oracle Admin, you must not change that account to the service user account.

Chapter 3

Operational notes

This chapter includes the following topics:

About NetBackup 10.1 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 10.1.

If NetBackup 10.1 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 10.1 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.

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 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 10.1.

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 51.

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 to 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.

Child job details for a NetBackup catalog backup display the policy type “Sybase”

If you view the child job details for a NetBackup catalog backup, the details show the policy type as "Sybase" instead of "NBU-Catalog".

Cloud snapshot replication jobs are not visible to the Default Cloud Administrator in the NetBackup web UI

NetBackup web UI users with the Default Cloud Administrator role are not able to view Cloud snapshot replication jobs.

Workaround:

Create an additional custom role for the cloud administrator. In that role, add the permission to view all NetBackup jobs.

To create a custom role with the View jobs

1. Create a custom RBAC role.
2. On the **Permissions** card, click **Assign**.
3. On the **Global** tab, expand **NetBackup management**.
4. Locate **Jobs** and select the **View** permission. You can also add any other job permissions you want for the role.
5. Add the wanted users to the role.

Policy name link does not work for some failed jobs in the web UI Activity Monitor

For some failed jobs that are displayed in the Activity Monitor in the NetBackup web UI, the **Policy name** link is not functional. For these jobs, you cannot click the policy name to view further details.

Workaround:

To view details about these jobs, navigate to the **Policies** page and find the policy.

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 10.1.

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
```

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 10.1.

Warning during NetBackup Snapshot Manager upgrade from 10.0 to 10.1

While upgrading NetBackup Snapshot Manager from 10.0 to 10.1 on computers running RHEL 8, you can see the following warning in the upgrade logs:

```
/opt/VRTScloudpoint/scripts/cp_start.sh: line 139: [:
localhost/veritas/flexsnap-mongodb:10.1.0.0.1027: binary operator
expected
```

Workaround:

You can ignore this warning.

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 10.1.

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 10.1.

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

Policy schedule start time on the Horizon UI is different than configured in the policy

The policy schedule start time that is displayed on the **Policy Details** page of the Horizon UI may be different by 23 minutes than what is configured in the policy.

The difference in time is caused by the wrong offset value that is obtained during the time conversions from one time zone to another time zone. This issue exists in the **pytz** library component that is used in NetBackup for OpenStack.

However, this issue is limited to the UI only. The backend and API have the correct UTC timings. This issue has no effect on the snapshot job scheduler, which runs on time as configured.

Instance volumes in the incremental backups cannot be mounted

Newly added disks of an instance for incremental backup get backed up successfully but these discs 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 10.1.

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

Appendix A

About SORT for NetBackup Users

This appendix includes the following topics:

- About Veritas Services and Operations Readiness Tools

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

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 31.

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- Database rebuilds are likely to occur in each major, minor (single-dot), and release update (double-dot) version of NetBackup. Therefore, before upgrading to NetBackup 10.1, you must ensure that you have an amount of free disk space available that is equal to or greater than the size of the NetBackup database. That means for default installations, 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 10.1 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 51.

See "About Veritas Services and Operations Readiness Tools" on page 44.

NetBackup 10.1 binary sizes

Table B-1 contains the approximate binary sizes of the NetBackup 10.1 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	1471 MB	No longer supported	
Canonical Ubuntu	x86-64	1394 MB		
CentOS	x86-64	1394 MB	6756 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	1394 MB		
Oracle Linux	x86-64	1394 MB	6756 MB	
Red Hat Enterprise Linux Server	POWER	309 MB		
Red Hat Enterprise Linux Server	x86-64	1366 MB	6559 MB	
Red Hat Enterprise Linux Server	z/Architecture	1085 MB	No longer supported	Media server or client compatibility only.
Rocky Linux client		1394 MB		
Solaris	SPARC	1168 MB	No longer supported	
Solaris	x86-64	1163 MB	No longer supported	
SUSE Linux Enterprise Server	POWER	311 MB		
SUSE Linux Enterprise Server	x86-64	1039 MB	5327 MB	
SUSE Linux Enterprise Server	z/Architecture	1039 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64	521 MB	3737 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 44.

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 44.

About changes in platform compatibility

The NetBackup 10.1 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

Other NetBackup documentation and related documents

This appendix includes the following topics:

- About related NetBackup documents

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 10.1. 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.