

NetBackup™ Release Notes

Release 10.3

Document Version 3

NetBackup™ Release Notes

Last updated: 2023-11-20

Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

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

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	About NetBackup 10.3	8
	About the NetBackup 10.3 release	8
	About NetBackup Late Breaking News	9
	About NetBackup third-party legal notices	9
Chapter 2	New features, enhancements, and changes	10
	About new enhancements and changes in NetBackup	10
	NetBackup 10.3 new features, changes, and enhancements	11
	Changes in Veritas terminology	12
	RESTful APIs included in NetBackup 10.3	13
	Introducing universal share accelerator	16
	Restore logs in the NetBackup web UI and location of restore logs	16
	Restore types added to NetBackup web UI for MS-Windows, Standard, and VMware policy types	17
	Recovery for additional policy types added to the NetBackup web UI	17
	NetBackup web UI new policy features	17
	Enhancements in system anomaly detection	17
	Entropy computation in NetBackup	18
	About multi-person authorization	18
	About multi-factor authentication	18
	Certificate-based transport layer security (TLS) authentication	19
	NetBackup 10.3 support additions and changes	20
	Support for AWS Snowball Edge	20
	End of life (EOL) for the Enhanced Auditing feature in NetBackup	21
	End of life (EOL) for the NetBackup Access Control (NBAC) authorization model in NetBackup	21
	Protecting assets with Snapshot Manager's agentless restore feature will require Microsoft Windows Server 2019 or later	21
	NetBackup for OpenStack support for CentOS has ended	21

Several shutdown commands to be deprecated in a future release	21
License file required for upgrade	22
Upgrades to NetBackup 10.3 may take a long time	22
Before upgrade, default credentials category is NONE	23
Data-in-transit encryption (DTE) mode is set to 'Preferred On' by default	23
Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.3	23
Additional permissions added for new features	24
Integrate MSDP Cloud credentials into NetBackup generic Credential Management System	24
MSDP Cloud is now supported on SUSE Linux Enterprise Server	24
Cloud Catalyst to MSDP Cloud migration is not supported on 10.3 MSDP servers	25
New features for NetBackup for Microsoft SQL Server	25
New features for NetBackup for Oracle	26
Upgrading to Snapshot Manager for Data Center 10.3 for Qumulo plug-in users	26
New D-NAS features	26

Chapter 3	Operational notes	27
	About NetBackup 10.3 operational notes	27
	NetBackup installation and upgrade operational notes	28
	If NetBackup 10.3 upgrade fails on Windows, revert to previous log folder structure	28
	Native installation requirements	28
	NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952	29
	About support for HP-UX Itanium vPars SRP containers	29
	NetBackup administration and general operational notes	30
	Changes to database commands	30
	For some workload environments, reduce the size of the job database before upgrade	30
	Policies using Replication Director fail with error code 4224	31
	Failed to get response from NetBackup malware utility	31
	NetBackup administration interface operational notes	32
	Delay in NetBackup web UI when adding or removing columns in Catalog area	32
	Intermittent issues with X forwarding of NetBackup Administration Console	32

NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later	33
NetBackup Bare Metal Restore operational notes	33
After PIT restore, "The host ID does not exist" error appears	33
AIX BMR Shared Resource Tree (SRT) creation fails in NetBackup 10.3	33
NetBackup services may not start automatically after BMR restore on a Linux client	34
NetBackup Cloud Object Store Workload operational notes	35
Auto Image Replication (AIR) from NetBackup version 10.3 to 10.1 does not work.	35
For Azure, backups fail when an older policy is updated with a new backup host	35
Replicated backups cannot be restored to older NetBackup versions	35
NetBackup Snapshot Manager (formerly NetBackup CloudPoint)	35
Indexing not supported on instances created from AWS Marketplaces AMIs	36
NetBackup NAS operational notes	36
Parent directories in the path of a file may not be present in an NDMP incremental image	36
RD storage units are not listed as Replication targets	36
NetBackup for OpenStack operational notes	37
CentOS repository mirror URL is updated	37
NetBackup for OpenStack Datamover API (NBOSDMAPI) service times out in the haproxy connection	37
Instance volumes in the incremental backups cannot be mounted	37
NetBackup primary server does not re-issue the token if NetBackup VM is a 3-node cluster	37
Success message appears along with the error message when you delete the policy that has snapshots	38
Unable to connect to NetBackup primary server using NBICA	38
Excluded Ceph Volume after restore is not mountable or formattable	38
Restored VMs have blank metadata config_drive attached	38
NBOSVM reconfig fails when you add new NetBackup VM to the cluster	39
Database does not sync after NetBackup cluster gets new nodes	39
Data on boot disk gets backed up despite exclusion	39

	After reinitialization and import, OpenStack certificates are missing	39
	CLI import changes scheduler trust value to disabled	39
	Unable to get node details after you reinitialize the NetBackup Appliance	40
	Snapshots fails with "object is not subscribable" for many policy jobs at the exact same time	40
	No operation is permitted in insecure way for SSL-enabled Keystone URL	40
	NetBackup internationalization and localization operational notes	40
	Support for localized environments in database and application agents	41
	Certain NetBackup user-defined strings must not contain non-US ASCII characters	41
Appendix A	About SORT for NetBackup Users	43
	About Veritas Services and Operations Readiness Tools	43
Appendix B	NetBackup installation requirements	45
	About NetBackup installation requirements	45
	Required operating system patches and updates for NetBackup	46
	NetBackup 10.3 binary sizes	47
Appendix C	NetBackup compatibility requirements	50
	About compatibility between NetBackup versions	50
	About NetBackup compatibility lists and information	51
	About NetBackup end-of-life notifications	51
Appendix D	Other NetBackup documentation and related documents	53
	About related NetBackup documents	53

About NetBackup 10.3

This chapter includes the following topics:

- [About the NetBackup 10.3 release](#)
- [About NetBackup Late Breaking News](#)
- [About NetBackup third-party legal notices](#)

About the NetBackup 10.3 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 10.3 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 10.3 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 43.

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 10.3 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 List for all Versions](#) for the most up-to-date platform support listings.

See [“About the NetBackup 10.3 release”](#) on page 8.

See [“About NetBackup compatibility lists and information”](#) on page 51.

NetBackup 10.3 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 10.3 are grouped below by category. Select a link to read more information about the topic.

New features

- [Changes in Veritas terminology](#)
- [RESTful APIs included in NetBackup 10.3](#)
- [Introducing universal share accelerator](#)
- [Restore logs in the NetBackup web UI and location of restore logs](#)
- [Restore types added to NetBackup web UI for MS-Windows, Standard, and VMware policy types](#)
- [Recovery for additional policy types added to the NetBackup web UI](#)
- [NetBackup web UI new policy features](#)
- [Enhancements in system anomaly detection](#)
- [Entropy computation in NetBackup](#)

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 10.3 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](#)

- [About multi-person authorization](#)
- [About multi-factor authentication](#)
- [Certificate-based transport layer security \(TLS\) authentication](#)

Support changes and enhancements

- [NetBackup 10.3 support additions and changes](#)
- [Support for AWS Snowball Edge](#)

- End of life (EOL) for the Enhanced Auditing feature in NetBackup
- End of life (EOL) for the NetBackup Access Control (NBAC) authorization model in NetBackup
- Protecting assets with Snapshot Manager's agentless restore feature will require Microsoft Windows Server 2019 or later
- NetBackup for OpenStack support for CentOS has ended
- Several shutdown commands to be deprecated in a future release

Installation, upgrade, and configuration changes and enhancements

- License file required for upgrade
- Upgrades to NetBackup 10.3 may take a long time
- Before upgrade, default credentials category is NONE
- Data-in-transit encryption (DTE) mode is set to 'Preferred On' by default

Cloud-related changes and enhancements

- Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.3
- Additional permissions added for new features
- Integrate MSDP Cloud credentials into NetBackup generic Credential Management System
- MSDP Cloud is now supported on SUSE Linux Enterprise Server
- Cloud Catalyst to MSDP Cloud migration is not supported on 10.3 MSDP servers

Workload and database agent changes and enhancements

- New features for NetBackup for Microsoft SQL Server
- New features for NetBackup for Oracle

NAS data protection changes and enhancements

- Upgrading to Snapshot Manager for Data Center 10.3 for Qumulo plug-in users
- New D-NAS features

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

RESTful APIs included in NetBackup 10.3

NetBackup 10.3 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 > 10.3](#)
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 10.3 includes these new and enhanced APIs:

- Licensing:
 - Add entitlements.
 - Get entitlements.
 - Delete entitlements.
- Multi-person Authorization:
 - Update MPA tickets by ID.
 - Obtain list of MPA tickets.
 - Obtain MPA ticket by ID.
 - Obtain list of MPA configurations.
 - Update MPA configure by ID.
- Pre-Check:
 - Perform pre-check on workload asset.
- Rate Limiter:
 - Create rate-limit configuration.
 - Update rate-limit configuration.
 - Delete rate-limit configuration.
 - Obtain list of rate-limit configurations.
 - Obtain rate-limit configuration by ID.
- OpenStack Workload:
 - Create instant access mount for OpenStack recovery point.
 - Obtain instant access mount by ID.
 - Obtain list of instant access mounts.
 - Delete instant access mount by ID.
- NetBackup OpenStack VM Servers:

- Register NetBackup OpenStack VM.
- Delete NetBackup OpenStack VM.
- Media Servers:
 - Remove media servers.
 - Obtain media server directory information.
 - Update media server state.
 - Update media service daemon state.
- Restore Logs:
 - Obtain details of restore log by ID.
 - Download restore log file by ID.
 - Delete restore log file by ID.
- Snapshot Managers:
 - Register Snapshot Manager with NetBackup.
- Anomaly Extension:
 - Obtain list of anomalies for extension.
 - Obtain anomaly for extension by ID.
 - Delete anomaly record for extension by ID.
 - Update anomaly status by ID.
 - Obtain template configuration by ID.
 - Create configuration by ID.
 - Update configuration by ID.
 - Obtain configuration by ID.

Versioned APIs

These APIs that have been versioned in NetBackup 10.3 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 more details.

Post snapshot-mgmt-servers:

- ``POST /config/servers/snapshot-mgmt-servers`` has the following attribute changes:
``username``, ``password``, ``fingerprint`` and ``securityToken`` removed from the request body payload of the object ``snapshotMgmtServer``.

These attributes are not supported as TLS certificate based authentication mechanism is used for Snapshot Manager communication.

Introducing universal share accelerator

The universal share accelerator leverages the universal share with object store feature. The major difference is that universal share with object store is on the storage server side and universal share accelerator is on the client side. The universal share accelerator is delivered with NetBackup client packages. It requires you to install the NetBackup client with universal share accelerator feature enabled before user can create a universal share accelerator from the NetBackup web console.

For more information, see the *NetBackup Deduplication Guide*.

Restore logs in the NetBackup web UI and location of restore logs

NetBackup 10.3 adds restore logs to the NetBackup web UI. Click on a job ID and the restore logs are displayed. The restore logs are created for the following policy types:

BigData	Hyper-V	NDMP
Cloud-object-store	Hypervisor – Nutanix	Standard
FlashBackup	MS-Windows	Universal-Share
FlashBackup-Windows	NAS-Data-Protection	VMware, agent-based recovery

Logs for the web UI and NetBackup APIs are written to the following directories on the primary server. (Logs for the NetBackup Administration Console are written to a different location and are not visible in the web UI. Similarly, web UI logs are not visible in the Administration Console.)

Windows:

```
install_path\NetBackup\var\global\wmc\user_ops\username\logs
install_path\NetBackup\var\global\wmc\user_ops\username\jobs
```

UNIX:

```
/usr/opensv/var/global/wmc/user_ops/username/logs
/usr/opensv/var/global/wmc/user_ops/username/jobs
```


Restore types added to NetBackup web UI for MS-Windows, Standard, and VMware policy types

NetBackup 10.3 adds the following restore types for the MS-Windows, Standard, and VMware policy types:

- Archived backups
- Optimized backups (MS-Windows only)
- Raw partition backups
- True image backups
- Point-in-time rollback (Standard only)
- Virtual disk restore (VMware)
- Virtual machine backups (Hypervisor-Nutanix)

Recovery for additional policy types added to the NetBackup web UI

NetBackup 10.3 adds recovery support for the following policy types:

- BigData (Hadoop, HBase, and MongoDB)
- FlashBackup
- FlashBackup-Windows
- Hyper-V
- Hypervisor - Nutanix
- NAS-Data-Protection

NetBackup web UI new policy features

This release offers the following new capabilities for policy types:

- NetBackup web UI ability to edit policy type.
 The user can change the **Policy type** for a policy. Changing the policy type may cause the schedule types and other settings in the policy to become invalid.
- Support for additional policy types: Hyper-V

Enhancements in system anomaly detection

NetBackup can now detect system anomalies during critical operations as follows:

- NetBackup clients that are offline under suspicious circumstances.

The 'Client offline' anomaly adds the ability to detect offline clients because of a compromised file system on a NetBackup host. Once the anomaly is detected, NetBackup generates a critical alert for the affected client.

- Any unusual manual NetBackup image expirations or expiry date modifications. The 'Image expiration' anomaly detects unusual attempts that are made by privileged users to expire backup images. Once the anomaly is detected, NetBackup generates a critical alert and identifies the user.

You can also use predefined rules or criteria to generate system anomalies.

For more information, refer to the *NetBackup Web UI Administrator's Guide*.

Entropy computation in NetBackup

NetBackup 10.3 and later clients compute an additional risk signal in-line, called entropy. It improves the quality of detected anomalies. Entropy is a measure of randomness of file contents. Threat vectors that encrypt files tend to abruptly change the entropy. The entropy metric will be used with the anomaly detection in Veritas Alta View to help you detect such potential malicious activity. When this indicates anomaly activities, it is recommended to check the system for potential malicious actors and not to use those images as a recovery point if suspicious activities are found.

About multi-person authorization

Starting with version 10.3, NetBackup supports multi-person authorization. NetBackup Security Administrator can configure multi-person authorization. It proactively protects NetBackup primary servers from an undesirable or a malicious act by ensuring that a second authorized user approves that action before it is allowed to take place. If you configure multi-person authorization for a certain operation, you can perform the associated operation only using the NetBackup web UI or REST APIs. You cannot perform the operation using the NetBackup Administration Console.

To bypass multi-person authorization, you can add the associated users as exempted users who do not require approval for performing the required operations.

See the *NetBackup Web UI Administrator's Guide* for more information.

About multi-factor authentication

Multi-factor authentication is a multi-step account login process that requires users to enter more information than just a password. The second level of authentication can help prevent unauthorized account access if a system password is compromised. This method protects against stolen credentials by requiring additional authentication

steps (or factors) before granting access. Common factors are username and password, numeric codes from an authentication application, or physical security keys. NetBackup supports time-based one-time password. The one-time password works with commonly available authentication applications, such as Microsoft Authenticator or Google Authenticator. NetBackup users can configure multi-factor authentication for their user accounts. If the NetBackup Security Administrator has enforced it in the domain, all users must configure it for a successful web UI sign-in.

See the *NetBackup Web UI Administrator's Guide* for more information.

Certificate-based transport layer security (TLS) authentication

Starting with NetBackup 10.3, the credential-based authentication has been replaced with certificate-based transport layer security (TLS) authentication between NetBackup primary server and Snapshot Manager. Snapshot Manager will continue to provide support for NetBackup CA/external CA configurations.

The `flexsnap_configure` CLI resides on Snapshot Manager and has been enhanced to provide a simplified deployment experience. It is a wrapper over multiple supportability options, such as:

- Checking health status of containers
- Install-uninstall and start-stop containers
- Serverinfo option fetches certificate information from Primary server and Snapshot Manager hosts
- Verify option validates health of the ECA certificates
- Truststore option lists or updates Snapshot Manager truststore
- Renew option used for Snapshot Manager and extension certificate renewal

The Snapshot Manager upgrade will seamlessly handle on-premises Storage and Cloud workload scenarios.

The back-level media servers and clients will use dynamically generated temporary credentials in place of older Snapshot Manager credentials and will continue to work seamlessly with the NetBackup 10.3 primary server and Snapshot Manager.

Other deployments methods such as Marketplace and Cloud Scale have also been updated.

NetBackup 10.3 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 10.3:

- Platforms
 - AlmaLinux 8 and 9
- Virtualization
 - Veritas NetBackup plug-in for VMWare vRealize Version 2.3 VMWare vRealize Orchestrator Versions 8.11, 8.13
- Database agents
 - MariaDB 10 on Ubuntu 22.04
 - MariaDB 10 on Ubuntu 20.04
 - PostgreSQL 15 on Windows Server 2022
 - PostgreSQL 15 on Red Hat Enterprise Server 8
 - PostgreSQL 15 on Red Hat Enterprise Server 7
 - PostgreSQL 15 on Oracle Linux 8
 - MongoDB 6.0 on Red Hat Enterprise Linux 9
 - MongoDB 7.0 on Red Hat Enterprise Linux 9
 - MySQL 8.0 on Ubuntu 20.04
 - MySQL 8.0 on Ubuntu 22.04
 - PostgreSQL 15 on Rocky Linux 8
 - PostgreSQL 15 on Rocky Linux 9

Support for AWS Snowball Edge

NetBackup supports an Amazon Web Services (AWS) Snowball Edge device which uses on-board storage for data import to or export from AWS S3. When the device arrives on-premises, NetBackup can store data onto the device which is then imported into AWS. NetBackup can also recover NetBackup data which has been loaded onto the device by image sharing.

See the *NetBackup Deduplication Guide* for more information.

End of life (EOL) for the Enhanced Auditing feature in NetBackup

NetBackup 10.2.0.1 was the last NetBackup version to support the Enhanced Auditing feature.

Starting with NetBackup 10.3, Enhanced Auditing is not supported.

The Enhanced Auditing functionality is available with the role-based access control (RBAC) feature. For more information, see the following article:

[Migrating the Enhanced Auditing functionality](#)

End of life (EOL) for the NetBackup Access Control (NBAC) authorization model in NetBackup

NetBackup Access Control (NBAC) authorization model will attain end-of-life (EOL) and will no longer be supported in an upcoming release. 10.3 recommends that you map existing NBAC user groups to NetBackup role-based access control (RBAC) default roles or custom roles. For more details refer to https://www.veritas.com/support/en_US/article.100060497.

Protecting assets with Snapshot Manager's agentless restore feature will require Microsoft Windows Server 2019 or later

With an upcoming version of NetBackup, protecting assets with NetBackup Snapshot Manager's agentless feature will require Microsoft Windows Server 2019 or later. More information about this feature is available in the following topic:

[Protecting assets with NetBackup Snapshot Manager's agentless feature](#)

NetBackup for OpenStack support for CentOS has ended

Veritas plans to end support for NetBackup for OpenStack running on CentOS. The operating system will no longer be a supported platform, and the last release supporting it will be the NetBackup 10.3 release.

Support will continue on older versions of Veritas for OpenStack and follow the published [Veritas Product End of Life](#) policy guidelines.

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*.

License file required for upgrade

Starting with NetBackup 10.3, NetBackup uses license files instead of license keys. As part of the primary server upgrade process, you must either download a license file or use a temporary production license. You don't need to download the temporary production license as it's included with NetBackup.

Upgrades from versions earlier than NetBackup 8.1.2 only support the production licenses that are downloaded from Veritas Entitlement Management System (VEMS) or the evaluation license. You don't need to download the evaluation license as it's included with NetBackup. You cannot use the temporary production license when you upgrade from a NetBackup version earlier than 8.1.2.

Veritas recommends the use of your production license that is downloaded from VEMS, for all upgrades. If you do not have access to your production license, you can use one of the built-in non-downloaded licenses. Which license you use depends on your version of NetBackup.

The evaluation license is only used during upgrades if the upgrade is from NetBackup versions earlier than NetBackup 8.1.2. The evaluation license is valid for 60 days. Alerts appear in the web UI immediately after upgrade, indicating the number of days remaining in the evaluation.

The temporary license is used in upgrades of NetBackup 8.1.2 or later to NetBackup 10.3 or later. The temporary license is valid for 60 days. Alerts appear in the web UI immediately after upgrade, indicating the number of days remaining before the temporary license expires.

More information about license files is available.

https://www.veritas.com/support/en_US/article.100058779

Upgrades to NetBackup 10.3 may take a long time

When upgrading from NetBackup 9.1 or later releases, the NetBackup primary server upgrade on Windows takes a long time depending upon the number of files in the NetBackup installation directory. See the *NetBackup Upgrade Guide* for more information.

Before upgrade, default credentials category is NONE

When you upgrade to NetBackup 10.3 from a version that is earlier than version 10.2, the default category of the credentials created before upgrade is **NONE**.

Also, the default category is **NONE** for any credential which is created apart from the **Credential Management** tab in the web UI and for which category is not specified.

Data-in-transit encryption (DTE) mode is set to 'Preferred On' by default

In the case of a fresh NetBackup primary server installation, the global data-in-transit encryption (DTE) mode is set to **Preferred On** by default.

With a primary server upgrade, the existing global DTE mode value will not be changed.

Note that, with the DTE mode set to **Preferred On** by default, the job throughput performance may be affected.

Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.3

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 10.3. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 10.3, 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 2.11.0.

The following cloud support has been added to version 2.11.1 and later but was not included in the NetBackup 10.3 final build:

- Cloud Object Store Protection (COSP) - Quantum ActiveScale Systems (S3)

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>

Additional permissions added for new features

The following table list the features for the respective cloud providers for which additional permissions are documented in the *NetBackup Snapshot Manager Install and Upgrade Guide*:

Cloud provider	Feature
Microsoft Azure	■ List the customer managed keys. ■ Obtain and install Azure disk encrypted (ADE) extension details if installed. ■ Assign permissions to key vault used for encryption.
Amazon Web Services	Application-consistent snapshots using AWS Systems Service Manager.
Google Cloud Platform	Restore of CMK-encrypted disks.

Integrate MSDP Cloud credentials into NetBackup generic Credential Management System

CMS and MSDP Cloud are now integrated to store cloud LSU credentials. NetBackup is changed from using Cloud Connector to using OCSD to manage LSUs. Credentials are now stored in and accessed from NetBackup CMS and this feature replaces the current credential management implementation (username and password).

For more information, review the *NetBackup Web UI Administrator's Guide*

MSDP Cloud is now supported on SUSE Linux Enterprise Server

Basic functionality for MSDP Cloud is now enabled on SUSE Linux Enterprise Server (SLES).

Advanced features such as image sharing, malware scanning, universal share, and instant access are not yet supported for SLES.

See the *NetBackup Deduplication Guide* for details.

Cloud Catalyst to MSDP Cloud migration is not supported on 10.3 MSDP servers

To migrate Cloud Catalyst to MSDP Cloud using the `nbdecommission -migrate_cloudcatalyst` command, you must use an MSDP server running NetBackup versions 10.0.0.1 to 10.2.0.1.

The primary server can be running NetBackup 10.3, but the MSDP server on which `nbdecommission` is executed must be running one of the NetBackup versions in the range above.

See the *NetBackup Deduplication Guide Appendix B* for more details.

New features for NetBackup for Microsoft SQL Server

The following features are available in this release:

- Log truncation is turned off for log shipping environments.
 NetBackup detects log shipping environments and turns off log truncation in the backups that are performed with SQL Server Intelligent Policies, batch file-based policies, or protection plans. This feature prevents out-of-sequence events for the target of log shipping.
- Added capabilities for grouped snapshots.
 Grouped snapshots quiesce a group of databases together and create a snapshot to back them up as a group.
 - Added support for dynamic grouped snapshots with SQL Server Intelligent Policies. NetBackup automatically discovers and groups any databases up to the specified **Group size for snapshots** value. This attribute is new for SQL Server Intelligent Policies in NetBackup 10.3.
 - When the group size limit (64) is reached, an additional snapshot is created.
 - A separate snapshot is created if the master database is included in the policy.
 - If both availability databases and standard databases are included in the same policy, separate snapshots are created for each availability group and for the standard databases.
- Increased group size limit for grouped snapshots with batch-file based policies.
 For batch-file based policies, support for grouped snapshots is still available with the keyword `GROUPSIZE`. The group size limit has increased from 32 to 64.

New features for NetBackup for Oracle

In NetBackup 10.3 the following new Oracle features are added to the NetBackup web UI.

- Clone from databases and pluggable databases.
For a description of the requirements and limitations of Oracle cloning with NetBackup, see the *Oracle cloning* chapter in the *NetBackup for Oracle Administrator's Guide*.
- Oracle credential type that you can use to store Oracle credential for use with cloning operations.
- Ability to create a custom RBAC role with limited permissions for any Oracle administrators that perform cloning operations.

Upgrading to Snapshot Manager for Data Center 10.3 for Qumulo plug-in users

Qumulo plug-in users who are upgrading to Snapshot Manager for Data Center 10.3 should follow these steps:

- Expire the all the earlier snapshots before starting the upgrade for Snapshot Manager for Data Center 10.3.
- To retain the older snapshots, first configure a new Snapshot Manager for Data Center 10.3 for the new snapshots and backup image management. Use the earlier Snapshot Manager for Data Center for the earlier images. Once the older snapshots become obsolete, remove the older Snapshot Manager for Data Center.

New D-NAS features

NetBackup 10.3 includes the following new features for dynamic NAS (D-NAS):

- Major improvements in D-NAS backup performance. Now your backups are three to five times faster, depending on your environment.
- NetApp SnapDiff V3 integration for D-NAS backups and support for indexing.
- Support for NetApp Cloud Volumes ONTAP (CVO).
- Support for snapshot replication using Dell EMC PowerScale (Isilon)

See the *NetBackup NAS Administrator's Guide* for more details.

Operational notes

This chapter includes the following topics:

- [About NetBackup 10.3 operational notes](#)
- [NetBackup installation and upgrade operational notes](#)
- [NetBackup administration and general operational notes](#)
- [NetBackup administration interface operational notes](#)
- [NetBackup Bare Metal Restore operational notes](#)
- [NetBackup Cloud Object Store Workload operational notes](#)
- [NetBackup Snapshot Manager \(formerly NetBackup CloudPoint\)](#)
- [NetBackup NAS operational notes](#)
- [NetBackup for OpenStack operational notes](#)
- [NetBackup internationalization and localization operational notes](#)

About NetBackup 10.3 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 10.3.

If NetBackup 10.3 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 [NetBackup Logging Reference Guide](#).

For Windows, if the upgrade to NetBackup 10.3 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 [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 `VRTSnbpc` 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 VRTSnbpc.k.rpm  
rpm -U VRTSnbpc.k.rpm VRTSnbclt.k.rpm VRTSpddea.k.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 compliant 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 10.3.

Changes to database commands

`nbd_b_admin -start` and `-stop` command changes

The commands `nbd_b_admin -start` and `nbd_b_admin -stop` no longer start and stop the NetBackup database server. Now they start or stop a specific database in the NetBackup database server.

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

`nbd_b_admin -vxd_bms_nb_server` command changes

The command `nbd_b_admin -vxd_bms_nb_server` was removed in the NetBackup 10.2 release. This command is added again in NetBackup 10.3.

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>

Policies using Replication Director fail with error code 4224

When you try to modify any existing policy with the **Use Replication Director** and **Perform snapshot backups** options selected in the NetBackup web UI, this error appears:

```
Error code 4224: Host. STS Internal Error
```

You can see the following message in the BPFIS logs:

```
15:16:13.416 [35337] <2> onlfi_vfms_logf: INF - snapshot services:
ostfi:2023-09-26 15:16:13.416029 <Thread id - 1> Failed to wait for
operation result, Error code [2060017] and message [system call failed]
15:16:13.417 [35337] <2> onlfi_vfms_logf: INF - snapshot services:
ostfi:2023-09-26 15:16:13.417125 <Thread id - 1> OST Library call
failed with message (STS API waitForAsyncCall failed with error
code : 2060017)
```

Workaround:

Do any of the following actions:

- In the **Policy validation** dialog displaying the error, click **Ignore errors** and save. Open the NetBackup Administration Console (Java UI), edit the policy, and then save it.
- In the **Policy validation** dialog displaying the error, click **Edit policy**. To save the policy, click **Save**. In the **Policy validation** dialog displaying topology validation options, select the topology validation option as **None** or **Basic**, instead of **Complete**, and save.

Failed to get response from NetBackup malware utility

This issue is applicable for scan hosts with RHEL 8.x and NFS version 4.x.

When scanning large backups of 200 million or more files, the following error is displayed on the NetBackup web UI for a failed job:

```
Failed to get response from NetBackup malware utility.
```

While a scan is in progress on the scan host, NFS mount points are not accessible from the scan host. The scan job remains in progress and times out after two days. NFS exports on storage server are accessible.

Workaround:

Ensure that you use NFS version 3 for mounting IA mounts on scan host over NFS by setting the following configuration in the `/etc/nfsmount.conf` file on the scan host:

```
# grep Defaultvers /etc/nfsmount.conf Defaultvers=3
```

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 10.3.

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 for the interface to refresh if you add or remove columns. This issue will be fixed in an upcoming release.

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 10.3.

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.

AIX BMR Shared Resource Tree (SRT) creation fails in NetBackup 10.3

The following error message appears on the command-line console while creating the Shared Resource Tree (SRT):

```
ls1pp: Fileset libcpp.rte not installed.
```

```
ERROR: Could not resolve major version level from [].
```

```
ERROR: Detected an attempt to install incorrect platform and/or  
operating system and version client binaries on  
falcnal2c3.abcus.abc.com.
```

```
Required AIX OS libcpp runtime is not present.
```

```
File /tmp/install_trace.xxxxxxxx contains a trace of this  
install. That file can be deleted after you are sure the  
install was successful.
```

```
Do you want to retry install of Veritas NetBackup Client? (y/n) [y] :
```

During AIX BMR SRT creation, when you install NetBackup 10.3 client, you must have libcpp runtime version 16.1.0.7 or later inside the SRT. If a libcpp runtime version is not present in the AIX BMR SRT when you create it, then the NetBackup 10.3 client installation fails, which leads to the SRT creation failure.

Workaround:

See this technical article for workaround details:

https://www.veritas.com/support/en_US/article.100060647

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/opensv/netbackup/bin/bp.start_all
```

NetBackup Cloud Object Store Workload operational notes

This topic contains some of the operational notes and known issues that are associated with the NetBackup Cloud Object Store Workload in version 10.3.

Auto Image Replication (AIR) from NetBackup version 10.3 to 10.1 does not work.

Auto Image Replication (AIR) from NetBackup version 10.3 to 10.1 does not work.

Workaround:

None. Upgrade the target computer to at least NetBackup version 10.2.

For Azure, backups fail when an older policy is updated with a new backup host

For Azure, if you update a policy that was created on a NetBackup version prior to 10.3, with a new backup host, backups fail.

The modified form of the queries in version 10.3 causes this issue.

Workaround:

Update all existing queries in the buckets to the new format.

Replicated backups cannot be restored to older NetBackup versions

If you replicate a backup image created on NetBackup 10.3 to an older NetBackup version, you cannot restore the buckets or containers having default retention enabled using the older version of NetBackup.

Workaround:

1. Restore with NetBackup version 10.3 or later.
2. Replicate the image to NetBackup version 10.3 or later.

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 10.3.

Indexing not supported on instances created from AWS Marketplaces AMIs

The indexing process for the instances created from AWS Marketplaces AMIs fails with the following error:

```
Failed to attach new volume: Cannot attach volume <vol-xxx>  
with Marketplace codes as the instance <i-xxx>  
is not in the 'stopped' state.
```

NetBackup NAS operational notes

NetBackup Snapshot Manager and NDMP V4 snapshot extension can make snapshots of client data on a NAS host. A NAS snapshot is a point-in-time disk image. You can retain the Snapshots on the disk for any duration. Using the Instant Recovery feature in NetBackup, you can efficiently restore the data from the disk. Broadly, in NetBackup, snapshot-based data protection for NAS can be performed using NAS-Data-Protection policy and NDMP policy. This topic contains some of the operational notes and known issues that are associated with NetBackup NAS in NetBackup 10.3.

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>

RD storage units are not listed as Replication targets

While configuring a storage lifecycle policy (SLP) from the NetBackup web UI, the Replication Director (RD) storage units are not listed in the **Replication target** drop-down, under **Destination storage attributes**. This situation occurs when you have configured both ISM and RD replication targets on the same primary server.

Workaround:

Configure the SLP using the NetBackup Administration Console (Java UI) or the command line interface (CLI).

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 10.3.

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 (NBOSDMPAPI) service times out in the haproxy connection

The NBOSDMPAPI 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 NBOSDMPAPI 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 10.3.

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

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](#)
- [Required operating system patches and updates for NetBackup](#)
- [NetBackup 10.3 binary sizes](#)

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 28.

- 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 10.3, 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/opensv/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 10.3 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 43.

NetBackup 10.3 binary sizes

[Table B-1](#) contains the approximate binary sizes of the NetBackup 10.3 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: The table 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	1735 MB	No longer supported	
Canonical Ubuntu	x86-64	2148 MB		
CentOS	x86-64	2148 MB	9652 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	2148 MB		
Kylin Linux Advanced Server 10.0		2148 MB		
NeoKylin Linux Advanced Server		2148 MB		
Oracle Linux	x86-64	2148 MB	9652 MB	
Red Hat Enterprise Linux Server	POWER	427 MB		
Red Hat Enterprise Linux Server	x86-64	2105 MB	9370 MB	
Red Hat Enterprise Linux Server	z/Architecture	1082 MB	No longer supported	Media server or client compatibility only.
Rocky Linux client		2148 MB		
Solaris	SPARC	1521 MB	No longer supported	
Solaris	x86-64	1506 MB	No longer supported	
SUSE Linux Enterprise Server	POWER	432 MB		
SUSE Linux Enterprise Server	x86-64	1474 MB	6903 MB	
SUSE Linux Enterprise Server	z/Architecture	1082 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64	716 MB	5061 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 the table.

- 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 the table. The additional required space is equivalent to 15 to 20 percent of the total binary size.

NetBackup compatibility requirements

This appendix includes the following topics:

- [About compatibility between NetBackup versions](#)
- [About NetBackup compatibility lists and information](#)
- [About NetBackup end-of-life notifications](#)

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 43.

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 43.

About changes in platform compatibility

The NetBackup 10.3 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 10.3. 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.
