

NetBackup™ Release Notes

Release 10.4

Document Version 2

NetBackup™ Release Notes

Last updated: 2024-03-28

Legal Notice

Copyright © 2024 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

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

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1	About NetBackup 10.4	8
	About the NetBackup 10.4 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 10.4 new features, changes, and enhancements	11
	Changes in Veritas terminology	12
	RESTful APIs included in NetBackup 10.4	13
	Client-side deduplication control from policies in NetBackup web UI	18
	Changes to the dashboard in the NetBackup web UI	18
	Malware scan improvements	18
	Enhancement in multifactor authentication	19
	Enhancements in anomaly detection	19
	Enhancements in multi-person authorization	19
	NetBackup support for OCSF-formatted audit events	20
	End-of-support-life (EOSL) for NetBackup Replication Director, replaced with NetBackup Snapshot Manager (NBSM)	20
	NetBackup 10.4 support additions and changes	21
	Deprecating support for Red Hat Enterprise Linux 7	21
	Support for CIS Level 2 v2 benchmark for Red Hat Enterprise Linux 8 machines	21
	Several shutdown commands to be deprecated in a future release	21
	Windows compiler and security requirements for NetBackup 10.4 and later installation and upgrade	22
	Script for setting up image sharing with cloud recovery servers to be deprecated	22
	AMI is used to create virtual machine in the AWS cloud environment	22
	Upgraded containerized services	23
	Oracle Cloud Infrastructure support for cloud workloads	23

Support for VMware vSAN Express Storage Architecture (ESA)	23
Browse ability for vApps with VMware policy in NetBackup web UI	23
New features for NetBackup for VMware in the NetBackup web UI	24
Support for XFS-formatted volumes and LVM2 Thin Pool Volumes	24
New features and changes for NetBackup for Microsoft SQL Server	24
New features and changes for NetBackup for Oracle	25
Support for Kubernetes workload type for malware scanning	26
Patching mechanism for primary and media servers	26
New features for Dynamic NAS (D-NAS)	26

Chapter 3	Operational notes	27
	About NetBackup 10.4 operational notes	27
	NetBackup installation and upgrade operational notes	28
	If NetBackup 10.4 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
	Updates 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	30
	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
	NetBackup services may not start automatically after BMR restore on a Linux client	33

NetBackup Cloud Object Store Workload operational notes	34
Auto Image Replication (AIR) from NetBackup version 10.4 requires NetBackup 10.2 or later	34
For Azure, backups fail when an older policy is updated with a new backup host	34
Replicated backups cannot be restored to older NetBackup versions	35
Changing the authentication method of existing Cloud object store accounts on Ceph may fail	35
Red Hat Ceph does not support the Assume role credential type	35
NetBackup Snapshot Manager (formerly NetBackup CloudPoint)	36
Indexing not supported on instances created from AWS Marketplaces AMIs	36
Verifying the storage array certificate	36
NetBackup database and application agent operational notes	36
NetBackup for Microsoft SQL Server operational notes	36
NetBackup NAS operational notes	37
Parent directories in the path of a file may not be present in an NDMP incremental image	37
RD storage units are not listed as Replication targets	38
NetBackup for OpenStack operational notes	38
NetBackup for OpenStack appliance re-initialization feature is removed from NetBackup for OpenStack 10.4	38
Excluding volumes from the backup is not supported in NetBackup for OpenStack 10.4	38
NetBackup for OpenStack 10.4 imports only policies from the older versions	38
NetBackup for OpenStack Datamover API (NBOSDMAPI) service times out in the haproxy connection	39
Instance volumes in the incremental backups cannot be mounted	39
Success message appears along with the error message when you delete the protection that has recovery points	39
Restored VMs have blank metadata config_drive attached	39
No operation is permitted in insecure way for SSL-enabled Keystone URL	39
If the OpenStack project is deleted, importing policy does not work in NetBackup for OpenStack 10.4	40
NetBackup internationalization and localization operational notes	40
Support for localized environments in database and application agents	40

	Certain NetBackup user-defined strings must not contain non-US ASCII characters	41
Appendix A	About SORT for NetBackup Users	42
	About Veritas Services and Operations Readiness Tools	42
Appendix B	NetBackup installation requirements	44
	About NetBackup installation requirements	44
	Required operating system patches and updates for NetBackup	45
	NetBackup 10.4 binary sizes	46
Appendix C	NetBackup compatibility requirements	49
	About compatibility between NetBackup versions	49
	About NetBackup compatibility lists and information	50
	About NetBackup end-of-life notifications	50
Appendix D	Other NetBackup documentation and related documents	52
	About related NetBackup documents	52

About NetBackup 10.4

This chapter includes the following topics:

- [About the NetBackup 10.4 release](#)
- [About NetBackup Late Breaking News](#)
- [About NetBackup third-party legal notices](#)

About the NetBackup 10.4 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 10.4 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 10.4 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 42.

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 10.4 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 10.4 release”](#) on page 8.

See [“About NetBackup compatibility lists and information”](#) on page 50.

NetBackup 10.4 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 10.4 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 10.4](#)
- [Client-side deduplication control from policies in NetBackup web UI](#)
- [Changes to the dashboard in the NetBackup web UI](#)
- [Malware scan improvements](#)
- [Enhancement in multifactor authentication](#)
- [Enhancements in anomaly detection](#)
- [Enhancements in multi-person authorization](#)
- [NetBackup support for OCSF-formatted audit events](#)

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 10.4 from a release earlier than 8.1, make sure that you read and understand the *NetBackup Read This First for Secure Communications* document. NetBackup 8.1 includes many enhancements that improve the secure communications of NetBackup components. The *NetBackup Read This First for Secure Communications* document describes the features and benefits of these enhancements:

[NetBackup Read This First for Secure Communications](#)

Support changes and enhancements

- [End-of-support-life \(EOSL\) for NetBackup Replication Director, replaced with NetBackup Snapshot Manager \(NBSM\)](#)
- [NetBackup 10.4 support additions and changes](#)
- [Deprecating support for Red Hat Enterprise Linux 7](#)
- [Support for CIS Level 2 v2 benchmark for Red Hat Enterprise Linux 8 machines](#)
- [Several shutdown commands to be deprecated in a future release](#)

Installation, upgrade, and configuration changes and enhancements

- Windows compiler and security requirements for NetBackup 10.4 and later installation and upgrade

Cloud-related changes and enhancements

- Script for setting up image sharing with cloud recovery servers to be deprecated
- AMI is used to create virtual machine in the AWS cloud environment
- Upgraded containerized services
- Oracle Cloud Infrastructure support for cloud workloads

Virtualization changes and enhancements

- Support for VMware vSAN Express Storage Architecture (ESA)
- Browse ability for vApps with VMware policy in NetBackup web UI
- New features for NetBackup for VMware in the NetBackup web UI
- Support for XFS-formatted volumes and LVM2 Thin Pool Volumes

Workload and database agent changes and enhancements

- New features and changes for NetBackup for Microsoft SQL Server
- New features and changes for NetBackup for Oracle
- Support for Kubernetes workload type for malware scanning
- Patching mechanism for primary and media servers

NAS data protection changes and enhancements

- New features for Dynamic NAS (D-NAS)

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

Deprecated term	New term
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 10.4

NetBackup 10.4 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 > 10.4](#)
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 10.4 includes these new and enhanced APIs:

- Robots:
 - Delete robots.
 - Update a robot.
 - Get robot details by robot name.
 - Retrieve list of unique device hosts for configured robots.
- Robot Inventory:
 - Get robot contents.
 - Fetch the list of bar code rules.
 - Create a new bar code rule on the media manager server.
 - Update the specified bar code rule.
 - Delete the specified bar code rule.
 - Fetch the list of media server's media ID generation rules.
 - Set the list of media server's media ID generation rules.
 - Fetch the list of media server's media ID prefixes.
 - Set the list of the media server's media ID prefixes.
 - Manage robot volume configuration.
 - Get media type mappings for a specified robot type.
- Tape media volumes:
 - Retrieve list of tape media volumes.
 - Create tape media volumes.
 - Retrieve details for a tape media volume.
 - Perform quick erase or long erase on a volume.
 - Perform label operation on a volume.
 - Retrieve list of external media types.
 - Rescan and update bar codes for one or more tape volumes.
 - Move volumes between robots.
 - Update one or more tape volumes.
 - Delete one or more tape volumes.

- Eject one or more tape media volumes from a robot.
- Tape media volume groups:
 - Retrieve list of tape volume groups.
 - Retrieve details of a tape volume group.
 - Update a tape volume group.
 - Delete a tape volume group.
- Volume pools:
 - Create a new tape volume pool.
 - Retrieve details of a volume pool by ID.
 - Update a volume pool.
 - Delete one or more volume pools.
- Tape Media Owners:
 - Retrieve a list of media owner names.
- Media Settings:
 - Retrieve associated EMM server settings.
 - Update associated EMM server setting.
- Storage devices:
 - Retrieve tape robots and standalone drives used for storage unit configuration.
- Malware:
 - Delete failed/canceled scan result with specified ID.
 - Validate configuration for malware scan.
- Anomaly:
 - Update the feedback parameters of a policy and client.
- File Hash Search:
 - Search files by file hash.
- Multifactor Authentication:
 - The existing multifactor authentication infrastructure is enhanced to be adaptive.

Versioned APIs

These APIs that have been versioned in NetBackup 10.4 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.

- Get tape-volume-pools API:
GET /storage/tape-volume-pools` no longer supports filtering on `policyType`.
- Establish trust with a primary server API:
`POST /config/servers/trusted-master-servers`
Request Payload for credential based trust will require one additional
`remotePrimaryAuthMode` field from version 11.0 onwards.
API v10.0 example:

```
"trustedMasterServerName": "String",
"authenticationType": "CREDENTIAL",
"userName": "String",
"password": "String",
"fingerprint": "String"
```

API v11.0 example:

```
"trustedMasterServerName": "String",
"authenticationType": "CREDENTIAL",
"userName": "String",
"password": "String",
"fingerprint": "String",
"remotePrimaryAuthMode": "String"
```

- Add scan host API:
`POST /malware/scan-hosts` new mandatory parameter. `mediaServerName`
has been added to the payload, which is used for validating the scan host before
adding it.
API v10.0 example:

```
{
  "data": {
    "type": "createScanHost",
    "attributes": {
      "hostName": "scanhost.example.com",
      "maxNoOfParallelScans": 0,
      "state": "ACTIVE",
      "scanHostCredentialName": "sample_creds"
    },
    "relationships": {
```

```

    "malwareTool": {
      "data": {
        "type": "malwareTool",
        "id": "1"
      }
    },
    "scanHostPool": {
      "data": {
        "type": "scanHostPool",
        "id": "2"
      }
    }
  }
}

```

API v11.0 example:

```

{
  "data": {
    "type": "createScanHost",
    "attributes": {
      "hostName": "scanhost.example.com",
      "maxNoOfParallelScans": 0,
      "state": "ACTIVE",
      "scanHostCredentialName": "sample_creds",
      "mediaServerName": "mediaserver.example.com"
    },
    "relationships": {
      "malwareTool": {
        "data": {
          "type": "malwareTool",
          "id": "1"
        }
      },
      "scanHostPool": {
        "data": {
          "type": "scanHostPool",
          "id": "2"
        }
      }
    }
  }
}

```

Client-side deduplication control from policies in NetBackup web UI

The client-side deduplication options for policies are updated in the NetBackup web UI. Users now select from the following options: **Use individual client settings configured in host properties**, **Disable for all clients**, or **Enable for all clients**.

Changes to the dashboard in the NetBackup web UI

The NetBackup web UI includes changes to the appearance and functionality of the **Dashboard** in the NetBackup web UI.

- The dashboard displays NetBackup environment details in doughnut charts so you can visually assess the status of jobs, certificates, and tokens in the environment.
- Specific information for jobs, certificates, and tokens is now clickable. Click on a link and you see a filtered view with only the items that meet that criteria. For example, you can click on a link to view Active jobs for the timeframe that you selected or to view Expired certificates. The dashboard now includes links in the certificates and the tokens widgets that send you to those respective pages and use the existing filtering capabilities on those pages.
- For job information, when you click on a link on the **Dashboard** NetBackup opens the Jobs list and creates a temporary filter for those jobs on the **Jobs** tab. See the [NetBackup Web UI Administrator's Guide](#) for details.
- The timeframe that you select in a widget is persisted across sessions. For example, if you select **48 hours** for the Jobs widget, that timeframe is selected the next time that you open NetBackup.

Malware scan improvements

- Ansible script for scan host configuration is available on GitHub: <https://github.com/VeritasOS/netbackup-scanhost-config>
- New functionality: **Validate configuration**
 This functionality provides support to check for any configuration issues after adding or updating the scan host.
- For validation of scan host, scan host entries must be saved again after upgrading to NetBackup version 10.4 from versions 10.2 and below.
- The latest version of NetBackup Malware Scanner 2.4 is available on the Download Center. It is recommended to upgrade to the latest version.

Enhancement in multifactor authentication

If multifactor authentication is configured, you need to reauthenticate yourself by entering the one-time password that you see in the authenticator application on your smart device before you perform the following operations:

- Managing the global security settings for the primary server
- Adding an API key

This provides enhanced security of your NetBackup domain.

For more details about these operations, see the respective topics in the *NetBackup Web UI Administrator's Guide*.

Enhancements in anomaly detection

Anomaly detection is enabled by default

- Starting with NetBackup 10.4, for fresh installation, anomaly detection is by default enabled for the following policy types: Standard, MS-Windows, NAS-Data-Protection, and Universal share.

NetBackup risk engine

- The new NetBackup risk engine detects certain system anomalies in a proactive manner and sends respective alerts. It helps you take corrective action before you face any security threat in your environment.

You can configure the following options that the risk engine uses to detect anomalies for the given critical operations:

- Detect suspicious image expiration
- Secure critical operations
- Detect possible session hijack

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

Enhancements in multi-person authorization

Starting with NetBackup 10.4, multi-person authorization is supported for operations that are performed using command-line (CLI) options, and NetBackup Administration Console along with NetBackup web UI, and REST APIs. You can now enable multi-person authorization for new operations such as changing security properties, removing image hold, removing WORM retention lock, changing WORM configuration and so on.

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

NetBackup support for OCSF-formatted audit events

You can now export audit events with the Open Cybersecurity Schema Framework (OCSF) format to SIAM platforms.

For more information, see this article:

https://www.veritas.com/support/en_US/article.100063252

End-of-support-life (EOSL) for NetBackup Replication Director, replaced with NetBackup Snapshot Manager (NBSM)

Veritas plans to end-of-support-life (EOSL) NetBackup Replication Director in an upcoming release. Replication Director provided the ability to create and backup NAS and SAN Storage snapshots from replicated primary storage volumes on secondary controllers. This included Index and Backup from Replica Snapshot. This feature was available in policy types including Standard, VMware, Oracle, and NDMP policies.

Replication Director has been replaced with NetBackup Snapshot Manager (NBSM). NBSM is an integral part of NetBackup and provides snapshot and snapshot replica (replicated snapshot) orchestration by integrating API interfaces to Arrays and Cloud Storage Tiers through a “plug-in” service that communicate to the Storage RestAPI Endpoints.

NBSM differs from Replication Director’s OST integration and allows NetBackup to make requests to NBSM using a common set of commands for discovery, creation, and retention of storage snapshots and Snapshot replicas. By abstracting these interfaces, NetBackup can leverage new and updated storage interfaces across workloads when new or updated NBSM plug-ins get introduced without changing NetBackup software. NBSM supports a wide range of Array Controller Architectures and Cloud Storage Platforms that support Storage and Storage replica protection.

Unlike Replication Director that defined Replication Policies for Storage, NBSM ‘Discovers’ existing Replication Policies on storage controllers and maps the volumes between the controllers. This passive approach insures that you can leverage existing storage replication policies for backup operations without modification of the existing storage replication strategies.

Replication Director Customers should transition policies that use Storage Lifecycle Policies (SLP) specified with Replication Director arguments to new SLPs that used NBSM Snapshot and Replica arguments.

For more information about NBSM, see the *NetBackup Snapshot Manager for Data Center Administrator’s Guide*.

Support for Replication Director on older versions of NetBackup follow the published [Veritas Product End of Life](#) policy guidelines.

NetBackup 10.4 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 10.4:

- Database agents
 - Cassandra 4.1.3 for Red Hat Enterprise Linux 8.x
 - PostgreSQL 14.x for SUSE Enterprise Linux 15 SP5 (x86_64)
 - PostgreSQL 15.x for SUSE Enterprise Linux 12 SP5
 - PostgreSQL 15.x for SUSE Enterprise Linux 15 SP5 (x86_64)
 - PostgreSQL 16.x - SUSE Enterprise Linux 15 SP5 (x86_64)

Deprecating support for Red Hat Enterprise Linux 7

Red Hat Enterprise Linux 7 platform support is now deprecated. In the next major release, support for Red Hat Enterprise Linux 7 will no longer be available. For more information, see the [NetBackup Compatibility List for all Versions](#).

Support for CIS Level 2 v2 benchmark for Red Hat Enterprise Linux 8 machines

NetBackup Snapshot Manager deployment is now supported on CIS Level 2 v2 benchmark for Red Hat Enterprise Linux 8 machines.

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`
- `bpdwn`
- `bpclusterkill`

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

Windows compiler and security requirements for NetBackup 10.4 and later installation and upgrade

NetBackup 10.4 and later for Windows uses the Visual Studio 2022 compiler and the Windows 11 Software Development Kit (SDK). The installation and the upgrade process use Microsoft redistributable utilities to install Visual Studio 2022 C++ run-time libraries on Windows hosts where they are not already installed. The redistributable utilities can alter Windows hosts such that a restart is required. Veritas recommends that you install Visual Studio 2022 C++ run-time libraries on Windows hosts independently of NetBackup installation or upgrade, within a maintenance window where you can safely perform restarts.

See the *NetBackup Installation Guide* or the *NetBackup Upgrade Guide* for more information.

Script for setting up image sharing with cloud recovery servers to be deprecated

The `ims_system_config.py` script is being deprecated. This script is used to set up the NetBackup image sharing server. (This server is also called the cloud recovery server (CRS).)

Starting with NetBackup 10.4, you must use MSDP cloud APIs to integrate with new cloud features.

The `ims_system_config.py` script is still available in NetBackup 10.4 but without the new cloud features. The script will be removed in a future release.

AMI is used to create virtual machine in the AWS cloud environment

An Amazon Machine Image (AMI) is used to create virtual machine (Amazon Elastic Compute Cloud or EC2 instances) in the Amazon Web Services (AWS) cloud environment during restore operation.

- For NetBackup Snapshot Manager version 10.4 onwards, following change is applicable for AWS virtual machine protection and recovery: AMI ID used to create AWS virtual machine that is protected is stored with the along with the other info during backup. During VM restore, the AMI recorded during backup would be re-used as default input, the user can replace the default value with valid and compatible AMI ID.
- For snapshots/backups taken with NetBackup Snapshot Manager versions prior to 10.4, the user must provide a valid AMI ID which is compatible with the VM being restored since this AMI information was not recorded.

Note: An AMI parameter input is not required for other cloud providers. Hence it is an optional attribute for pre-recovery and recover cloud NetBackup APIs.

Upgraded containerized services

NetBackup 10.4 introduces support for deploying PostgreSQL as a container by default for Cloud Scale deployment.

Oracle Cloud Infrastructure support for cloud workloads

NetBackup now provides the capability to back up and restore virtual machines and Oracle applications running on Linux, within Oracle Cloud Infrastructure (OCI). Here are the supported features in this release:

- VM-based deployment of NetBackup Snapshot Manager in OCI on Oracle Enterprise Linux (OEL).
- A dedicated NetBackup Snapshot Manager plug-in for discovering assets and automating protection tasks in OCI. The plug-in is compatible with API-keys and IAM-based source accounts.
- You can capture snapshots of VMs and Oracle applications running on Linux, and subsequently restore them from the captured snapshots.
- NetBackup provides backup from snapshot and restore from backup copies for the VMs.
- Cloud Intelligent Policies and RBAC support for OCI VMs.
- Use the Linux flexsnap agent to take application-consistent snapshots.

For more information, see the *NetBackup Web UI Cloud Administrator's Guide* and the *NetBackup Snapshot Manager for Cloud Install and Upgrade Guide*.

Support for VMware vSAN Express Storage Architecture (ESA)

Support for VMware vSAN Express Storage Architecture (ESA) starts with NetBackup 10.4. For earlier NetBackup versions 10.3, 10.3.0.1, and 10.2.0.1, an EEB can be obtained from Veritas Support.

For more information about vSAN ESA, see this article from VMware:

<https://core.vmware.com/resource/vsan-frequently-asked-questions-faq>

Browse ability for vApps with VMware policy in NetBackup web UI

For a VMware policy, the NetBackup web UI adds the ability to browse for vApps when you add clients to the policy.

New features for NetBackup for VMware in the NetBackup web UI

The following features are available in this release:

- The user can apply the RBAC role permissions from a selected VM to other VMs in the environment. To perform this action, the user must have the **View** and **Manage access** permissions on the VMs.
- Apply limits to restore jobs check box

Support for XFS-formatted volumes and LVM2 Thin Pool Volumes

NetBackup supports the indexing of files on XFS-formatted volumes and partitions for VMware Replication Director and Integrated Snapshot Manager for VMware.

Also, support is added for LVM2 Thin Pool Volumes for VMware.

Note: The Windows backup host is not supported for the indexing of files on LVM2 thin volumes for VMware policy and VMware Replication Director and Integrated Snapshot Manager for VMware.

For more information, see the *NetBackup for VMware Administrator's Guide*.

New features and changes for NetBackup for Microsoft SQL Server

The following features are available and updates are made in this release:

- Added support for backups of non-readable secondary replicas. To provide the port number of the primary to NetBackup, additional configuration is needed. See the [NetBackup Web UI Microsoft SQL Server Administrator's Guide](#) for information on how to use the `hostProperties` API endpoint to configure this setting. Or, see the `MSSQL_CONFIG_LIST` option in the *NetBackup Administrator's Guide, Volume I*.
- Added support for RBAC on NetBackup for SQL Server job operations. Users can be granted permission on SQL Server assets so they can then view individual SQL Server jobs. The ability to restart and cancel jobs is available for parent jobs. For example, for availability groups and database instances.
- Support for use of encrypted connections with the Microsoft ODBC driver, release 18, for SQL Server clients that are updated to NetBackup 10.4. (Encryption is not supported for back-level clients.) The following default settings are applied:
 - NetBackup encrypts ODBC connections.
 - The certificate for the target SQL Server instance is trusted.
 - The ODBC driver is configured to use the oldest available driver.

- Added the **Enable T-SQL snapshots** option to support a full backup of SQL Server (not a copy-only backup) with a VMware policy or protection plan. This backup can be the basis for SQL Server incremental and transaction log backups, which removes the need for a separate full backup with a SQL Server policy.
- The resume option **Save work and restart at the point of failure** is removed from the **NetBackup MS SQL Client**. The `MAXRESTARTSETS` keyword for batch files is no longer valid.

New features and changes for NetBackup for Oracle

The following changes and features are available in this release:

- Role-based access control (RBAC) can be applied to all types of Oracle assets. For example, in the web UI click on a database. Then on the **Permissions** tab, select the RBAC roles that you want to have access to the database.
- The NetBackup web UI includes the following changes and additions:
 - Both non-RAC and RAC databases are managed on the **Databases** tab. The **Instances** tab is removed from the **Workloads > Oracle** page. Instances are now managed by clicking on a database name and then clicking the **Instances** tab.
 - RMAN catalogs are managed on the **RMAN catalogs** tab. You can register an RMAN catalog with a credential you have saved in Credential management. On the **Databases** tab, you can select an RMAN catalog that you want to associate with an Oracle database.
 - Data Guards are managed on the **RMAN catalogs** tab.
- A new command `nboracmd` provides the ability to manage Oracle assets, credentials, and Oracle jobs from the command line. Note that any delegation privileges that were configured with the command `nboradm -add_dba` are not converted to RBAC. Administrators must separately apply the needed RBAC role or roles to Oracle administrators.

The following items are deprecated in the NetBackup 10.4 release:

- The **Applications > Oracle** node in the NetBackup Administration Console is removed. Oracle assets can be managed from the NetBackup web UI.
- Oracle Intelligent Policies (OIP) are removed from the NetBackup Administration Console. OIP policies can be managed in the NetBackup web UI.
- Instance groups are removed from the NetBackup Administration Console, the NetBackup web UI, and the command line options. The Credential Management System (CMS) supersedes instance groups. OIP policies that contained instance groups are updated during an upgrade. A new policy is created with the

databases contained in the previous policy. Then a new credential is created and is applied to the databases in the new policy.

- The command `nboradm` is deprecated.
 The command-line options to configure instance groups and credentials are no longer applicable and are not available with the new command `nboracmd`. The CMS supersedes instance groups and credentials are now managed in the CMS.

Support for Kubernetes workload type for malware scanning

NetBackup 10.4 now provides support for malware scanning on Kubernetes workload type.

Patching mechanism for primary and media servers

NetBackup 10.4 provides the ability to patch container deployments of primary, media and PostgreSQL containers.

Patching introduces the ability for customers to patch images in a Kubernetes native way by specifying the image tags for respective containers using the `serviceImageTag` field of the environment.

New features for Dynamic NAS (D-NAS)

NetBackup 10.4 includes the following new features for Dynamic NAS (D-NAS):

- Volume multi-host backups
- Support for Cloud Volume ONTAP AWS
- Support for Cloud Volume ONTAP Azure
- Support for AWS FSx for NetApp ONTAP

See the *NetBackup NAS Administrator's Guide* and the *NetBackup Snapshot Manager for Data Center Administrator's Guide* for more details.

Operational notes

This chapter includes the following topics:

- [About NetBackup 10.4 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 database and application agent operational notes](#)
- [NetBackup NAS operational notes](#)
- [NetBackup for OpenStack operational notes](#)
- [NetBackup internationalization and localization operational notes](#)

About NetBackup 10.4 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 10.4.

If NetBackup 10.4 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 10.4 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 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 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 10.4.

Updates to database commands

nbddb_admin -update_user_list

The command `nbddb_admin` includes a new option: `update_user_list`. Use this option if the account and password information in the pgbouncer's `userlist.txt` file are out of sync with the NetBackup database. If you continue to see connection issues, restart the NetBackup services.

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

Following an upgrade from NetBackup 9.0 or earlier to NetBackup 9.1 or later, 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 10.4.

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 50.

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 10.4.

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

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

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

Workaround:

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

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

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

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

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

Workaround:

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

```
/usr/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 10.4.

Auto Image Replication (AIR) from NetBackup version 10.4 requires NetBackup 10.2 or later

You cannot run Auto Image Replication (AIR) from a computer with NetBackup version 10.4 to a target computer with a NetBackup version that is earlier than version 10.2.

Workaround:

None. Upgrade the target computer to NetBackup version 10.2 or later.

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 or later 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.

Changing the authentication method of existing Cloud object store accounts on Ceph may fail

Changing the authentication method of existing Cloud object store accounts on Ceph may fail with the message:

```
Credential validation failed. Provide the correct Cloud account name and credentials.
```

For a Cloud object store account on Ceph that uses Access key authentication, this error appears if you change the authentication method to Security token service-based authentication. After this update, credential validation, discovery, and backups may fail.

Workaround:

Do one of the following actions:

- Create a new account with a new name. Configure it to use the Security token service-based Assume role access on Ceph.
- To update an old account, note the details of the existing account, and then delete the old account. Next, create a new account with the same name and use the Security token service-based access method.

Note: This issue affects only the Ceph cloud provider. You can still update other providers, like Amazon and AWS GovCloud, to use the Security token service-based access method.

Red Hat Ceph does not support the Assume role credential type

The Red Hat Ceph cloud provider does not support the Assume role credential type, though this credential type is available as an option for Ceph in the NetBackup web UI.

NetBackup Snapshot Manager (formerly NetBackup CloudPoint)

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.
```

Verifying the storage array certificate

NetBackup 10.3.0.1 and later provide an option to verify the storage array certificate for any communication that happens between NetBackup Snapshot Manager (NBSM) and the storage array. For the verification to succeed, the root certificate of the storage array must be maintained in the trust store of NetBackup Snapshot Manager.

You must manually download the storage array certificate and add it to the NBSM trust store. After the certificate is added in the trust store, during the plug-in configuration or plug-in update operations, select the **Verify Certificate** option to enable the certificate verification.

For more information, see the following technical article:

<http://www.veritas.com/docs/100062212>

NetBackup database and application agent operational notes

NetBackup offers several methods of protecting various database and application technologies. This topic contains some of the operational notes and known issues that are associated with the protection of database technologies in NetBackup 10.4.

NetBackup for Microsoft SQL Server operational notes

NetBackup for SQL Server extends the capabilities of NetBackup for Windows to include backups and restores of SQL Server databases. These capabilities are provided for a Windows client using either a Linux or Windows NetBackup primary

server. This topic contains some of the operational notes and known issues that are associated with NetBackup for Microsoft SQL Server in NetBackup 10.4.

VMware backups that use T-SQL snapshots fail with error code 114

VMware backups that use T-SQL snapshots fail if they are performed concurrently with MS-SQL backups.

Workaround:

To ensure that the backups are successful, configure the policy schedules so that they do not overlap.

SQL Server filegroup backups not supported on non-readable secondary

For SQL Server 2022, an issue exists with filegroup backups on a non-readable secondary. They are not supported at this time due to a Microsoft limitation.

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 10.4.

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 10.4.

NetBackup for OpenStack appliance re-initialization feature is removed from NetBackup for OpenStack 10.4

The re-initialization feature re-initializes the NetBackup for OpenStack appliance to delete all policy-related information from the NetBackup for OpenStack database. This feature is removed from NetBackup for OpenStack 10.4.

Excluding volumes from the backup is not supported in NetBackup for OpenStack 10.4

You cannot exclude the volumes from the backup in NetBackup for OpenStack 10.4.

NetBackup for OpenStack 10.4 imports only policies from the older versions

The NetBackup for OpenStack 10.4 migrates or imports only the policies from the older versions. It does not import the snapshots.

After importing the policies, you cannot recover the instance from the snapshot. However, if you create snapshots or backups after importing the policies, you can recover the instance from the snapshot or backup copy.

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

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

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

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

Instance volumes in the incremental backups cannot be mounted

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

Success message appears along with the error message when you delete the protection that has recovery points

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

- This protection contains the recovery points that may have unexpired copies.
- Success: Deleted: <protection name>

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.

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`

If the OpenStack project is deleted, importing policy does not work in NetBackup for OpenStack 10.4

While importing the policies in NetBackup for OpenStack, if the OpenStack project with the existing policies is deleted, you are asked to use the `policy-reassign` command. Because the `policy-reassign` command is not supported in NetBackup for OpenStack, such policies cannot be imported.

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 10.4.

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 10.4 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 10.4, 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 10.4 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 50.

See [“About Veritas Services and Operations Readiness Tools”](#) on page 42.

NetBackup 10.4 binary sizes

[Table B-1](#) contains the approximate binary sizes of the NetBackup 10.4 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	1789 MB	No longer supported	
Alma Linux		2029 MB		
Amazon Linux		2029 MB		

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

OS	CPU Architecture	64-bit client	64-bit server	Notes
BC-Linux		2029 MB		
Canonical Ubuntu	x86-64	2029 MB		
CentOS	x86-64	2029 MB	8992 MB	
Debian GNU/Linux	x86-64	2029 MB		
Kylin Linux Advanced Server 10.0		2029 MB		
NeoKylin Linux Advanced Server		2029 MB		
Oracle Linux	x86-64	2029 MB	8992 MB	
Red Hat Enterprise Linux Server	POWER	1437 MB		
Red Hat Enterprise Linux Server	x86-64	1989 MB	8730 MB	
Red Hat Enterprise Linux Server	z/Architecture	1086 MB	No longer supported	Media server or client compatibility only.
Rocky Linux client		2029 MB		
Solaris	SPARC	946 MB	No longer supported	
Solaris	x86-64	905 MB	No longer supported	
SUSE Linux Enterprise Server	POWER	443 MB		
SUSE Linux Enterprise Server	x86-64	1642 MB	7083 MB	
SUSE Linux Enterprise Server	z/Architecture	1102 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64	713 MB	5087 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: NetBackup Snapshot Manager computer, primary server, media server, and then clients. For example, the scenario that is shown is supported: 10.2 NetBackup Snapshot Manager > 10.0 primary server > 9.0 media server > 8.3.0.1 client.

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

The NetBackup catalog resides on the primary server. Therefore, the primary server is considered to be the client for a catalog backup. If your NetBackup configuration

includes a media server, it must use the same NetBackup version as the primary server to perform a catalog backup.

For complete information about compatibility between NetBackup versions, refer to the [Veritas SORT website](#).

Veritas recommends that you review the [End of Support Life](#) information available online.

About NetBackup 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 42.

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 42.

About changes in platform compatibility

The NetBackup 10.4 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 10.4. 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.
