

Veritas NetBackup™ Release Notes

Release 9.0

Document Version 1

VERITAS™

Veritas NetBackup™ Release Notes

Last updated: 2020-12-17

Legal Notice

Copyright © 2020 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, 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 9.0	9
	About the NetBackup 9.0 release	9
	About NetBackup Late Breaking News	10
	About NetBackup third-party legal notices	10
Chapter 2	New features, enhancements, and changes	11
	About new enhancements and changes in NetBackup	11
	NetBackup 9.0 new features, changes, and enhancements	12
	Preventing a rogue media server after the decommissioning of a media server	13
	HSTS is enabled for the web UI	14
	NDMP policy management in the NetBackup web UI	14
	Configure Samba users for SQL Server instant access and universal shares	14
	RESTful APIs included in NetBackup 9.0	14
	API keys support for SAML users	16
	Instance groups for Oracle and <code>nboradm</code> command to be deprecated in a future release	16
	RBAC enhancements	16
	Retention Periods with end dates beyond 2038	17
	New infinity value for NetBackup images affects OpsCenter custom SQL query building	17
	Deprecation of BigData policy to protect Nutanix AHV VMs	18
	About restore from a backup in Microsoft Azure Archive	18
	Take checkpoints every __ minutes attribute support for NAS-Data-Protection policy	19
	Accelerator disabled for NAS-Data-Protection policy	19
	NetBackup 9.0 support additions and changes	19
	Support for MongoDB 4.2	20
	Support for Azure Stack with managed disks	20
	Several shutdown commands to be deprecated in a future release	20
	Infinite expiration conversion	20
	Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 9.0	20

Cloud Catalyst now removed from NetBackup 21

Support for Qumolo storage arrays 21

Support for Dell EMC PowerScale (Isilon) storage arrays 21

Restricted restore mode for VMware agentless restore 22

VMware agentless support for Windows User Account Control
(UAC) 22

Veritas Smart Meter is now Veritas Usage Insights 22

OpsCenter Agent and deduplication functionality removed from
OpsCenter after the NetBackup 9.0 22

Chapter 3 **Operational notes** 24

About NetBackup 9.0 operational notes 24

NetBackup installation and upgrade operational notes 25

 After initiating CA migration, connection errors may occur 25

 If NetBackup 9.0 upgrade fails on Windows, revert to previous log
 folder structure 25

 Native installation requirements 26

 NetBackup servers must use a host name that is compliant with
 RFC 1123 and RFC 952 26

 Do not install from the menu that appears when the installation
 DVD is inserted 26

 About support for HP-UX Itanium vPars SRP containers 27

NetBackup administration and general operational notes 27

 Starting NetBackup services may generate a warning on Solaris
 platforms 27

 NetBackup Messaging Broker (mqbroker) not listed in services
 lists even if it is running 28

 Backup fails with the Status Code 2074 "Disk volume is down"
 28

 Restore of the Root ("/") folder for NAS-Data-Protection policy
 fails 29

 Backups for workloads that use the BigData policy may fail 29

 Child backup jobs may enter a queued state for workloads that
 use BigData policy 29

 Errors are shown in the jobs detail when NetBackup attempts to
 expire images from non-WORM capable storage 30

 NetBackup web server certificate renewal failure during initiation
 of NetBackup CA migration or upgrade 30

 Microsoft Azure backup fails if the resource group name contains
 a period (.) 31

 SLP does not retry multistreaming backup if child job fails or is
 canceled 31

Stale devices shown on the device tree	31
Temporary devices listed as file system assets	32
NetBackup administration interface operational notes	32
Global NDMP credentials option is unavailable from the NetBackup web UI	33
Differences exist between browsers in functionality of the NetBackup web UI	33
Search limitations for security events lists in the NetBackup web UI	33
Access control methods supported in NetBackup 9.0	33
Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms	34
Intermittent issues with X forwarding of NetBackup Administration Console	34
NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later	34
NetBackup Bare Metal Restore operational notes	34
BMR boot server not supported on a NetBackup appliance or a Flex appliance	35
BMR restore may take significant amount of time for formatting and volume creation step	35
NetBackup Cloud operational notes	35
Configuring a cloud recovery host on RHEL 8	35
NetBackup with Veritas CloudPoint operational notes	36
CloudPoint CFT upgrade	36
Defunct processes continue on the CloudPoint host	36
Snapshot jobs fail due to exceptions	36
Deleted snapshots still visible in the NetBackup web UI	37
Granular restore fails if target path is deleted and recreated	37
Public cloud not supported with gov cloud or China region	37
Indexing not supported on instances created from AWS Marketplaces AMIs	37
Consistent host snapshot might fail	37
Configuring AWS plug-in with IAM role showed that the Authentication Method field is blank	38
MongoDB create snapshot job may freeze	38
Updating a cloud plug-in while a job runs causes job failure	39
Permission denied error occurs if both user and password are updated	39
Different source and target zones for Google Cloud Platform are not supported	39
Broken files system detected	40

NetBackup database and application agent operational notes	40
NetBackup for Microsoft SQL Server operational notes	40
NetBackup deduplication operational notes	40
Backup jobs fail with "Storage server is down ..." for WORM storage servers in multi-domain environments	41
Backup job fails after media server with MSDP on Solaris 10 is upgraded to NetBackup 9.0	41
Configuring MSDP storage server on Solaris 10 fails	42
The ampersand character (&) not allowed in NetBackup deduplication engine credentials	42
NetBackup internationalization and localization operational notes	43
Support for localized environments in database and application agents	43
Certain NetBackup user-defined strings must not contain non-US ASCII characters	43
NetBackup for NDMP operational notes	44
Parent directories in the path of a file may not be present in an NDMP incremental image	44
NetBackup Snapshot Client operational notes	45
HPE 3PAR array snapshot import fails with status code 4213	45
Snapshots are deleted after point-in-time rollbacks	45
Index from Snapshot operation does not populate contents of the snapshot accurately in the catalog	45
NetBackup virtualization operational notes	46
NetBackup for VMware operational notes	46
Appendix A About SORT for NetBackup Users	48
About Veritas Services and Operations Readiness Tools	48
Recommended SORT procedures for new installations	49
Recommended SORT procedures for upgrades	53
Appendix B NetBackup installation requirements	55
About NetBackup installation requirements	55
Required operating system patches and updates for NetBackup	56
NetBackup 9.0 binary sizes	59
Appendix C NetBackup compatibility requirements	63
About NetBackup compatibility lists and information	63
About NetBackup end-of-life notifications	64

Appendix D	Other NetBackup documentation and related documents	66
	About related NetBackup documents	66

About NetBackup 9.0

This chapter includes the following topics:

- [About the NetBackup 9.0 release](#)
- [About NetBackup Late Breaking News](#)
- [About NetBackup third-party legal notices](#)

About the NetBackup 9.0 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 11.

About EEBs and release content

NetBackup 9.0 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 9.0 can be found on the Veritas Operations Readiness Tools (SORT) website and in the .

See [“About Veritas Services and Operations Readiness Tools”](#) on page 48.

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 9.0 new features, changes, and enhancements](#)

About new enhancements and changes in NetBackup

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

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

See [“About the NetBackup 9.0 release”](#) on page 9.

See [“About NetBackup compatibility lists and information”](#) on page 63.

NetBackup 9.0 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 9.0 are grouped below by category. Select a link to read more information about the topic.

New features

- [Preventing a rogue media server after the decommissioning of a media server](#)
- [HSTS is enabled for the web UI](#)
- [NDMP policy management in the NetBackup web UI](#)
- [Configure Samba users for SQL Server instant access and universal shares](#)
- [RESTful APIs included in NetBackup 9.0](#)
- [API keys support for SAML users](#)
- [Instance groups for Oracle and `nboradm` command to be deprecated in a future release](#)
- [RBAC enhancements](#)
- [Retention Periods with end dates beyond 2038](#)
- [New infinity value for NetBackup images affects OpsCenter custom SQL query building](#)
- [Deprecation of BigData policy to protect Nutanix AHV VMs](#)
- [About restore from a backup in Microsoft Azure Archive](#)
- [Take checkpoints every __ minutes attribute support for NAS-Data-Protection policy](#)
- [Accelerator disabled for NAS-Data-Protection policy](#)

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 9.0 from a release earlier than 8.1, make sure that you read and understand the *NetBackup Read This First for Secure Communications* document. NetBackup 8.1 includes many enhancements that improve the secure communications of NetBackup components. The *NetBackup Read This First for Secure Communications* document describes the features and benefits of these enhancements:

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

Support changes and enhancements

- [NetBackup 9.0 support additions and changes](#)
- [Support for MongoDB 4.2](#)
- [Support for Azure Stack with managed disks](#)
- [Several shutdown commands to be deprecated in a future release](#)

Installation, upgrade, and configuration changes and enhancements

- [Infinite expiration conversion](#)

Cloud-related changes and enhancements

- [Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 9.0](#)
- [Cloud Catalyst now removed from NetBackup](#)
- [Support for Qumolo storage arrays](#)
- [Support for Dell EMC PowerScale \(Isilon\) storage arrays](#)

Virtualization changes and enhancements

- [Restricted restore mode for VMware agentless restore](#)
- [VMware agentless support for Windows User Account Control \(UAC\)](#)

Other announcements

- [Veritas Smart Meter is now Veritas Usage Insights](#)
- [OpsCenter Agent and deduplication functionality removed from OpsCenter after the NetBackup 9.0](#)

Preventing a rogue media server after the decommissioning of a media server

Veritas recommends that you perform multiple tasks after you run the `nbdecommission` command. Veritas has added another recommendation to this list:

- Uninstall NetBackup from the media server or remove that media server from the environment. After this configuration change, the media server daemons do not have permissions to communicate with the master server and should no longer be started.

For more information about the decommission recommendations, review the *Post decommission recommendations* section in the [NetBackup Administrator's Guide, Volume I](#)

HSTS is enabled for the web UI

Starting with NetBackup 9.0, HTTP Strict Transport Security (HSTS) is enabled by default for the NetBackup web UI.

NDMP policy management in the NetBackup web UI

You can now manage NDMP policies in the NetBackup web UI. Options for the NDMP policy are the same as in the NetBackup Administration Console. For more information about NDMP policies, continue to refer to [NetBackup for NDMP Administrator's Guide](#).

Configure Samba users for SQL Server instant access and universal shares

Starting with NetBackup 9.0 and later, you must first configure Samba users for SQL Server instant access and universal shares. For more information, refer to the [NetBackup Web UI Microsoft SQL Server Administrator's Guide](#) and the section *MSDP build-your-own (BYO) server prerequisites and hardware requirements to configure Universal shares* in the [NetBackup Deduplication Guide](#).

RESTful APIs included in NetBackup 9.0

NetBackup 9.0 includes both updated and new RESTful application programming interfaces (APIs). These APIs provide a web-service-based interface that lets you configure and administer NetBackup in your environments.

You can find documentation for the NetBackup APIs in these locations:

- On your master server
APIs are stored in YAML files on the master server:
`https://<master_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 master 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.

- On SORT
NetBackup API documentation is also available on SORT:
[HOME > KNOWLEDGE BASE > Documents > Product Version > 9.0](#)
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.

New APIs

NetBackup 9.0 includes these new and enhanced APIs:

- Access Control: List roles for a principal, list effect ACLs for a managed object.
- Diagnostics: Provides diagnostic information about the NetBackup Web Management Console.
- External CA Certificates: Manage external CA certificates for smart card authentication.
- Passphrase Constraints: Provides ability to configure passphrase constraints per workflow.
- Recovery: Pre-recovery check for full VM restores with VMware.

See the *New APIs* topic in the *What's New in NetBackup 9.0* section of the [NetBackup 9.0 API Reference on SORT](#) for more information.

Versioned APIs

The following APIs have been versioned in NetBackup 9.0. The previous version of these APIs is still supported if you specify the correct version.

- Images:
GET Images `/catalog/images` and GET Image By Backup ID `/catalog/images/{backupId}` have renamed and changed data types for several fields.
- RecoveryPoints:
GET RecoveryPoints `/recovery-point-service/workloads/{workload}/recovery-points` and GET RecoveryPoint By RecoveryPoint ID `/recovery-point-service/workloads/{workload}/recovery-points/{recoveryPointId}` have renamed and changed data types for several fields.

- Configuration:
GET Configuration /security/properties is modified. The existing response fields in version 4.0 do not change, but the values may differ depending on whether authentication token is passed with the request or not.

See the *Versioned APIs* topic in the *What's New in NetBackup 9.0* section of the [NetBackup 9.0 API Reference on SORT](#) for more information.

Note: See the [NetBackup 9.0 API Reference on SORT](#) for more information. Make sure to review the *Versioning* topic and the *What's New* topic in the *Getting Started* section.

API keys support for SAML users

This release of NetBackup allows a Security Assertion Markup Language (SAML) user to create and delete their own API key. Note in this release that the administrator cannot add a key for a SAML user or change the validity period (expiration) of the key.

Instance groups for Oracle and `nboradm` command to be deprecated in a future release

NetBackup will remove instance groups for Oracle and the `nboradm` command in a future release. In future releases, NetBackup replaces the functions of the instance groups and the `nboradm` command with options in the web UI and APIs.

RBAC enhancements

NetBackup 9.0 includes the following preconfigured roles in RBAC:

- VMware Administrator
- RHV Administrator
- Cloud Administrator
- Microsoft SQL Server Administrator
- Resiliency Administrator
- Storage Administrator
- Security Administrator

You can add users to these roles and use the preconfigured permissions. The name, description, and permissions for these roles cannot be changed. Or, you

can create a new role based on one of the default roles and then customize the role permissions to fit your security needs.

Note: Veritas reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded.

See the [NetBackup 9.0 Web UI Administrator's Guide](#) for more information:

Retention Periods with end dates beyond 2038

Starting with NetBackup version 9.0, retention periods that extend beyond the year 2038 are supported. This retention period support is applicable not only to images but tape media as well.

Some backup images that are created with earlier versions may have expiration dates of January 19, 2038 after upgrade. You can correct the date issue with any of the images during upgrade or the records with end dates of January 19, 2038.

To correct the retention periods of infinity during upgrade, refer to the following article:

https://www.veritas.com/content/support/en_US/article.100048600

To correct the records with end dates of January 19, 2038, refer to the following article:

https://www.veritas.com/content/support/en_US/article.100048744

New infinity value for NetBackup images affects OpsCenter custom SQL query building

Starting with NetBackup 9.0, the infinity value that is used to indicate that NetBackup images never expire is changed from 2147483647 to 32535212400.

The OpsCenter equivalent of these values is a value of 143667764470000000 for old infinity in NetBackup (2147483647) and a value of 447545052000000000 for new infinity in NetBackup (32535212400).

Infinity Value	NetBackup	OpsCenter	ISO-8601
Old	2147483647	143667764470000000	2038-01-19T03:14:07.000Z
New	32535212400	447545052000000000	3000-12-31T23:00:00.000Z

This change in the infinity value impacts the OpsCenter data collection of NetBackup images. If OpsCenter monitors or reports on NetBackup master servers 9.0 or later, the value that indicates the infinity is now 44754505200000000 – the new infinity value – for the following OpsCenter database columns:

- `expirationTime`, `resumeExpiration`, `tirExpiration` from the `domain_Image` table
- `expirationTime` from the `domain_ImageCopy` table
- `expirationTime` from the `domain_ImageFragment` table
- `requiredExpirationDate` from the `domain_SLPImage` table

If you use any of these database columns in your custom SQL queries with old infinity values (14366776447000000), you need to consider "OR"ing your query with new infinity value (44754505200000000) for NetBackup master servers 9.0 or later.

Note that the old infinity values will remain unchanged for the master servers earlier than 9.0. Therefore, if OpsCenter monitors or reports on master servers earlier than 9.0 only, the infinity value changes do not impact OpsCenter 9.0 or later.

For more information, see the [NetBackup OpsCenter Administrator's Guide](#).

Deprecation of BigData policy to protect Nutanix AHV VMs

Starting with NetBackup 9.0, the BigData policy cannot be used to protect Nutanix AHV VMs.

If a backup host that is configured in a BigData policy has a NetBackup version earlier than 8.3, that policy can protect the Nutanix AHV VMs. After that backup host is upgraded to NetBackup 8.3 or later, the policy stops protecting the Nutanix AHV VMs.

Migrate the existing BigData policy to the Hypervisor policy to protect Nutanix AHV on the supported NetBackup versions.

For more information, refer to the [NetBackup for Nutanix AHV Administrator's Guide](#).

About restore from a backup in Microsoft Azure Archive

The rehydrate process completes when the data is transitioned to the Hot tier. The number of days specified while the configuring LSU measures the time the data will stay on the Hot tier. Afterward the data is transitioned to the Archive tier.

For more information, see the [NetBackup Deduplication Guide](#).

Take checkpoints every __ minutes attribute support for NAS-Data-Protection policy

The NAS-Data-Protection policy lets you enable the **Take checkpoint every __minutes** attribute. By taking checkpoints periodically during the backup, NetBackup can retry a failed backup from the beginning of the last checkpoint.

For more information, see the [NetBackup Snapshot Client Administrator's Guide](#).

Accelerator disabled for NAS-Data-Protection policy

With NetBackup 9.0, the Accelerator support for NAS-Data-Protection policy that was introduced with NetBackup 8.3 is disabled. If you upgrade from NetBackup version 8.3 or 8.3.0.1 to version 9.0, the Accelerator option for the NAS-Data-Protection policy in the policy configuration will be disabled.

For existing NAS-Data-Protection policies, if you have enabled the Accelerator and the Accelerator forced rescan options, you must delete the schedule manually and create a new schedule for the policies.

NetBackup 9.0 support additions and changes

Note: This information is subject to change. See the [NetBackup Master Compatibility Lists](#) for the most recent product and services support additions and changes.

The following products and services are supported starting with NetBackup 9.0:

- MongoDB 4.2
- MongoDB 4.4
- NetBackup FlexScale 1.3
- Red Hat Enterprise Linux 6.x.
NetBackup master and media servers and clients are no longer supported on this operating system version.
- Oracle 19c on Oracle Linux 8
- VMware Vsphere 7 U1

The following products and services are no longer supported starting with NetBackup 9.0:

- Red Hat Enterprise Linux 6.x.
NetBackup master and media servers and clients are no longer supported on this operating system version.

Support for MongoDB 4.2

NetBackup now supports protection of MongoDB version 4.2.

The following features are supported:

- Support for incremental backup based on Feature Compatibility Version (FCV)
- Support for backup, restore and recovery using TLS 1.2
- Additional backup validation based on MongoDB or FCV versions

For more information, refer to the [NetBackup for MongoDB Administrator's Guide](#).

Support for Azure Stack with managed disks

NetBackup now protects Azure Stack VMs with managed disks.

For more information, refer to the [NetBackup for Azure Stack Administrator's Guide](#).

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*.

Infinite expiration conversion

Upgrades from pre-NetBackup 9.0 to NetBackup 9.0 and later include the infinite expiration conversion. This conversion supports expiration dates beyond 2038. This conversion may extend the time that is required to complete the upgrade. Review the following article for more information:

https://www.veritas.com/content/support/en_US/article.100048600

Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 9.0

If you use cloud storage in your NetBackup environment, you may need to update your cloud configuration file on the NetBackup master server immediately after you

install or upgrade to NetBackup 9.0. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 9.0, 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 2.7.2. The following cloud support has been added to version 2.8.1 and later but was not included in the NetBackup 9.0 final build:

- Tencent Cloud - Cloud Object Storage (COS)

For the latest cloud configuration package, see the following tech note:

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>

Cloud Catalyst now removed from NetBackup

Cloud Catalyst was deprecated in favor of MSDP Direct Cloud Tiering (MSDP Cloud) in NetBackup 8.3, and is now removed in NetBackup 9.0 (except for back-level support).

For MSDP cloud setup information, refer to the [NetBackup Web UI Administrator's Guide](#).

Support for Qumolo storage arrays

NetBackup CloudPoint now adds support for Qumolo storage arrays. You can configure the new CloudPoint plug-in for Qumolo to discover and protect assets on Qumolo storage array.

For more details, refer to the [NetBackup CloudPoint Install and Upgrade Guide](#).

Support for Dell EMC PowerScale (Isilon) storage arrays

NetBackup CloudPoint now adds support for Dell EMC PowerScale (Isilon) storage arrays. You can configure the new CloudPoint plug-in for Dell EMC PowerScale (Isilon) to discover and protect assets on Dell EMC PowerScale (Isilon) storage array.

For more details, refer to the [NetBackup CloudPoint Install and Upgrade Guide](#).

Restricted restore mode for VMware agentless restore

The restricted restore mode option is a form of VMware agentless restore for restricted environments such as Windows User Account Control (UAC). Since the files are restored into a restricted environment, there are specific limitations on the restore. Review the details in the *NetBackup Web UI VMware Administrator's Guide*. Additionally, the file transport through the required infrastructure for this restore method is significantly slower than VMware agentless restores. As a result of performance concerns, Veritas recommends limiting the restore to fewer than 100 files and less than 1 GB of data. More information is available: NetBackup

[NetBackup Web UI VMware Administrator's Guide](#)

VMware agentless support for Windows User Account Control (UAC)

VMware agentless restore now supports restores to a guest VM that uses Windows UAC. This feature uses a restricted restore mode to restore to the UAC environment.

Veritas Smart Meter is now Veritas Usage Insights

Starting with NetBackup 9.0, Veritas Smart Meter has a new name - Veritas Usage Insights.

Veritas Usage Insights is a one-stop solution to help you effectively track your capacity usage in real time and compare it against your entitlements. You can access it from Veritas NetInsights Console, a SaaS-based unified platform with Veritas products and features. The platform leverages product telemetry and support data to offer software and appliance insights within a single interface. It delivers a cohesive experience and eliminates the need to switch between multiple products.

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

<https://netinsights.veritas.com>

OpsCenter Agent and deduplication functionality removed from OpsCenter after the NetBackup 9.0

The OpsCenter Agent can collect data from certain backup products such as Backup Exec, PureDisk, and EMC Legato.

However, OpsCenter no longer supports these backup products. Therefore, the OpsCenter Agent functionality will be removed from OpsCenter after the NetBackup 9.0 release. As OpsCenter no longer supports collecting data from PureDisk, the deduplication functionality will also be removed from OpsCenter after the NetBackup 9.0 release.

As a result of this end of support, the following options, tabs, and reports will not be visible in OpsCenter after 9.0.

- The **Settings > Configuration > Agent** tab in the OpsCenter user interface
- The **Monitor > Appliance Hardware > Deduplication** tab in the OpsCenter user interface
- **Deduplication** reports in the OpsCenter user interface

Ensure that you have saved the required data before you upgrade OpsCenter after 9.0.

Operational notes

This chapter includes the following topics:

- [About NetBackup 9.0 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 operational notes](#)
- [NetBackup with Veritas CloudPoint operational notes](#)
- [NetBackup database and application agent operational notes](#)
- [NetBackup deduplication operational notes](#)
- [NetBackup internationalization and localization operational notes](#)
- [NetBackup for NDMP operational notes](#)
- [NetBackup Snapshot Client operational notes](#)
- [NetBackup virtualization operational notes](#)

About NetBackup 9.0 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 9.0.

After initiating CA migration, connection errors may occur

NetBackup now supports certificate authorities with the following key strengths: 2048 bits, 4096 bits, 8192 bits, and 16384 bits. After NetBackup 9.0 installation or upgrade, by default a new root CA with 2048-bits key strength is deployed.

If you are connected to the NetBackup web UI during NetBackup CA migration, you should again sign in to the web UI for successful communication.

If NetBackup 9.0 upgrade fails on Windows, revert to previous log folder structure

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

For Windows, if the upgrade to NetBackup 9.0 fails and rollback occurs, run the following command to continue working on an earlier NetBackup version:

```
mklogdir.bat -fixFolderPerm
```

For more information, refer to the `mklogdir` command from the [Veritas NetBackup Commands Reference Guide](#).

Native installation requirements

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

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

Do not install from the menu that appears when the installation DVD is inserted

The operating system may open a user interface window (such as File Manager on Solaris) when the installation DVD is inserted into the disc drive. Veritas recommends that you do not use this window to install NetBackup products because unpredictable results may occur. Make sure to follow the installation instructions that are found in the [NetBackup Installation Guide](#).

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 executed 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 installation aborts if you try to install into an HPE Itanium SRP container (private file system, shared file system, or workload). If you install into the global container, a parameter is added to all `swremove` and `swinstall` commands to install only to the global view.

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 9.0.

Starting NetBackup services may generate a warning on Solaris platforms

In NetBackup 9.0 on Solaris systems, when you start NetBackup services with the `bp.start_all` command, a warning is displayed if the NetBackup Messaging Broker service is already in running state NetBackup:

```
Starting nbmqbroker...
Starting NetBackup Messaging Queue Broker could take a couple of minutes
./usr/opensv/mqbroker/bin/nbmqbroker: test: unknown operator ==
```

Workaround:

This warning can be ignored.

NetBackup Messaging Broker (mqbroker) not listed in services lists even if it is running

In NetBackup 9.0 on Solaris systems, the NetBackup Administration Console services list and the output of the `bpps` command might not list the NetBackup Messaging Broker (mqbroker) service despite the service being in a running state. It may lead to the wrong interpretation that the NetBackup Messaging Broker service is not running.

You can verify this situation with the following steps.

1. Check the output of the following command:

2. `bpps | grep mqbroker output`

It may not list mqbroker.

3. Check the output of the following command:

```
ps -ef | grep usr | grep openv | grep mqbroker | grep beam.smp
```

It lists mqbroker if the NetBackup Messaging Broker service is in a running state.

Workaround:

1. Run the following command:

```
/usr/openv/mqbroker/bin/nbmqroker stop
```

2. Wait for few seconds and then run the `bp.start_all` command, located in `/usr/openv/netbackup/bin/bp.start_all`.

3. Check the output of the following command:

```
ps -ef | grep usr | grep openv | grep mqbroker | grep beam.smp
```

4. Run the following command:

```
/usr/openv/netbackup/bin/bpps
```

It should list the NetBackup Messaging Broker service.

Backup fails with the Status Code 2074 “Disk volume is down”

Some backup jobs may fail with the Status Code 2074 “Disk volume is down”. This issue occurs when a backup job is started after an Open Cloud Storage Daemon (OCSD) restart. After a restart, the OCSD in-memory information is clean, and it does not have the required data under the storage configuration structure. As a result, the calls to retrieve cloud LSU (or disk volume) details fail.

Workaround:

Perform the following procedure on the media server:

1. Stop all MSDP services:

```
<install_path>/pdde/pdconfigure/pdde stop
```

2. Start all MSDP services:

```
<install_path>/pdde/pdconfigure/pdde start
```

3. Verify disk volume status using the following command. The disk volume status should be UP.

```
<install_path>/netbackup/bin/admincmd/bpstsinfo -lsuinfo -stype  
PureDisk -lsuname <disk-volume-name>
```

4. Start a new backup job.

Restore of the Root ("/") folder for NAS-Data-Protection policy fails

While restoring from a snapshot image for NAS-Data-Protection policy, if you select "/" as the restore pattern, the restore fails with the error 2823.

Workaround:

Do not select "/" for restore. Instead, expand the "/" tree structure, and select the items individually that you want to restore.

Backups for workloads that use the BigData policy may fail

If you have a NetBackup client as a backup host for protecting the workloads that use the BigData policy, and this backup host is shared between two master servers, then the backups fail.

During backup, NetBackup client scans the `bp.conf` file. If the master server is in the second position, the backup fails, and the following error is displayed:

```
(6654) Unable to retrieve the credentials for the server.
```

Workaround: Ensure that the master server entry is the first entry as a server name in the `bp.conf` file.

Child backup jobs may enter a queued state for workloads that use BigData policy

In NetBackup Appliance environments with multiple backup hosts where the BigData policy is used, one of the child backup jobs may go into a queued state if the media server goes into an inactive state. This scenario applies to Hadoop, HBase, and MongoDB workloads.

Workaround:

From the **Media and Device Management > Devices > Media servers** menu in NetBackup Administration Console, right-click the inactive media server and change the status from **Deactivated** to **Activate**.

Errors are shown in the jobs detail when NetBackup attempts to expire images from non-WORM capable storage

NetBackup routinely attempts to remove expired backups from the catalog and subsequently on storage. In cases where backups are WORM-locked on storage beyond the catalog expiration time, attempts to delete the data from storage causes the job to complete with partial-success. The job completes with a status (1) with a per-image error code of 2060069 reported in the job details. Each cleanup cycle attempts to remove the backup until storage successfully allows the deletion of the WORM-locked images.

Workaround:

To remove the WORM images from the cleanup cycle, perform one of the following as appropriate:

- Run a manual import to get the WORM images back into catalog.
- Use the `nbdelete -purge_deletion_list -backupid` command to remove the WORM image backup IDs from deletion worklist. This command does not delete these images from storage, so you have to delete the images manually from storage.

NetBackup web server certificate renewal failure during initiation of NetBackup CA migration or upgrade

If the initiation of NetBackup CA migration fails because of the NetBackup web service time out, renewal of the NetBackup web server certificate fails.

To renew the web server certificate using the new CA

- 1 Verify if the `nbatd` service has successfully migrated the NetBackup CA using the following steps:
 - Check the migration summary status. The status should be 'INITIATED'.
 - Run the `nbseccmd -nbcamigrate -summary` command to check the CA migration status.
 - The new key pair with the desired key size should be present in the NetBackup web server keystore. Check the keystore at the following location:

On Windows:

```
<INSTALL_PATH>/var/global/vxss/tomcatcreds/nbwebsvc/.VRTSat/profile/certstore/keystore
```

On UNIX:

```
<INSTALL_PATH>/var/global/vxss/tomcatcreds/nbwebsvc/.VRTSat/profile/certstore/keystore
```

- 2 After you have verified that the `nbatd` service has successfully migrated the NetBackup CA, run the following command to renew the NetBackup web server certificate:

```
nbseccmd -nbcamigrate -syncMigrationDB
```

Microsoft Azure backup fails if the resource group name contains a period (.)

For a VM or a disk snapshot, if the disk name or the asset resource group name contains a period, the backup job fails.

Workaround:

- If the resource group name contains a period, move the disks to a resource group without the period.
- If the disk name contains a period rename the disk.

SLP does not retry multistreaming backup if child job fails or is canceled

While a multistreaming backup job is running, if one child job is complete but another child job fails or is canceled, the storage lifecycle policy (SLP) does not retry the backup job.

Workaround:

1. Run the `nbstlutil cancel -backupid <backup identifier>` command to cancel the backup job and clean up the pending jobs.
2. Trigger a manual backup.

Stale devices shown on the device tree

During the indexing or restore process, sometimes the stale devices that are present in the volume are not cleaned up and are displayed in the device tree.

Workaround:

1. Unmount any file systems that mounted the device. (If required use `force unmount`)

2. If any of the partitions belongs to LVM, then remove the volume group from disk using the `vgreduce` command and then the `pvremove` command.
3. Execute the `blockdev -flushbufs` command to remove any outstanding reference to that device.
4. Remove the device references from the device tree. For example, whole/partition disks `/dev/xvdf`, `/dev/disk/by-path`, `by-id`, `by-label`, `by-partuuid` and `by-uuid`
5. Use the following command to remove the device from sysfs:
6.

```
echo 1 > /sys/block/device-name/device/delete
```

Where device-name might be `xvdf`.
7. Reboot the host to resolve this issue.

Temporary devices listed as file system assets

If the discovery process and restore process are running at the same time, for the duration of the restore process, sometimes the temporary devices are discovered and listed as a files system asset. After the restore process is complete, the temporary devices are no longer listed as file system assets during the subsequent discovery.

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 9.0.

For more information about the specific NetBackup administration interfaces, refer to 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 63.

Global NDMP credentials option is unavailable from the NetBackup web UI

The NetBackup web UI does not include the option **Use global NDMP credentials for this NDMP host**.

Workaround:

Access the **Use global NDMP credentials for this NDMP host** option from the NetBackup Administration Console rather than the NetBackup web UI. For more information, see *Authorizing NetBackup access to a NAS (NDMP) host* in the [NetBackup for NDMP Administrator's Guide](#) and *NDMP Global Credentials properties* in the [NetBackup Administrator's Guide, Volume I](#) and the NetBackup Help.

Username

Differences exist between browsers in functionality of the NetBackup web UI

The NetBackup web UI may behave differently for different browsers. Some functionality, for example a date picker, may not be available on all browsers. These inconsistencies are due to the capabilities of the browser and not because of a limitation with NetBackup.

Search limitations for security events lists in the NetBackup web UI

For the following NetBackup web UI features, the Search functionality is available only for the **User name** and **Domain name** fields:

- **Security > Security Events > Access History**
- **Security > Security Events > Audit Events**

The Search functionality is not available for **Description**, **Reason**, or other columns in these table listings. You can use filters to view events of a specific audit category for example, Login, Job, Policy and so on.

Access control methods supported in NetBackup 9.0

Role-based access control (RBAC) in NetBackup is available only for the web UI and the APIs. Other access control methods for NetBackup are not supported for the web UI and APIs, with the exception of Enhanced Auditing (EA). Users that are configured with EA have full permissions for the web UI and APIs.

For more information, see the [NetBackup Web UI Security Administrator's Guide](#).

Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms

Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms, particularly Red Hat Enterprise Linux 6.0 (RHEL 6.0) on VMware. The issue is a result of incompatibilities between the default GNU C Library (`glibc`) and Advanced Vector Extensions (AVX) on newer hardware. The issue should be fixed in a future release of `glibc`.

Workaround: Run the `export LD_BIND_NOW=1` command before you execute `runInstaller`.

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 9.0.

BMR boot server not supported on a NetBackup appliance or a Flex appliance

A Bare Metal Restore (BMR) boot server cannot be configured on a NetBackup appliance or a Flex appliance.

BMR restore may take significant amount of time for formatting and volume creation step

Due to operating system changes, a Bare Metal Restore (BMR) restore may take significant time during the formatting step when there are logical volumes in the system being restore. Red Hat Enterprise Linux 8 has introduced some changes for LVM2 which causes scanning of the udev database. This scanning takes a significant amount of time for LVM-related operations.

When you perform a BMR restore, you may see the following message in the `bmrrest` logs:

```
WARNING: Device * not initialized in udev database even after waiting
10000000 microseconds.
```

The BMR restore still succeeds, despite the longer restore time.

NetBackup Cloud operational notes

NetBackup Cloud Storage enables you to back up and restore data from cloud Storage as a Service (STaaS) vendors. This topic contains some of the operational notes and known issues that are associated with the NetBackup Cloud in NetBackup 9.0.

Configuring a cloud recovery host on RHEL 8

Before you run `ims_system_config.py` to configure the cloud recovery host on RHEL 8, install Python 2 and create a soft link from Python 2 to Python. The `ims_system_config.py` script uses Python 2.

NetBackup with Veritas CloudPoint operational notes

This topic contains some of the operational notes and known issues that are associated with the Veritas CloudPoint and NetBackup 9.0.

CloudPoint CFT upgrade

After you upgrade NetBackup CloudPoint from version 8.3 to version 9.0 using CFT upgrade, you must delete the old stack. The elastic IP for the new instance in the upgraded stack is also disassociated when you delete the old stack.

Workaround:

Associate the elastic IP to the new instance in the upgraded stack.

Defunct processes continue on the CloudPoint host

The CloudPoint on-host agent container might produce defunct process (mount.ntfs) after the indexing job on the Windows host is complete. Number of defunct processes depends on the number of supported file systems on the host. If the host contains 4 file systems, the number of defunct process increases by 4. This function has no functional effect on the indexing job but gradually, the defunct processes fill the system process ID table.

Workaround:

The defunct processes consume an entry in the process table. However, this process doesn't hold any system resources, such as CPU cycles or memory. To resolve this issue, restart the on-host agent container. Use the following command:

```
docker restart <container_name>
```

Snapshot jobs fail due to exceptions

A high memory pressure on CloudPoint VM causes the Flexsnap-MongoDB and Flexsnap-Rabbitmq containers to restart. After the container restarts, the Off-Host Agent service container cannot establish a communication with Rabbitmq. This issue might occur with any agent service, such as CloudPoint OnHost agent or CloudPoint Off Host agent.

Workaround:

Restart the corresponding Flexsnap-agent container. Use the following command:

```
docker restart <container_name>
```

Deleted snapshots still visible in the NetBackup web UI

Although the stale snapshots are deleted from the Amazon Web Services (AWS) console, the deleted snapshots are still visible in the NetBackup web UI.

Granular restore fails if target path is deleted and recreated

On protected VM assets, if you recreate a filesystem and mount it to the same drive or path, then subsequent discovery updates the CloudPoint asset database for newly created filesystems. Also, the old filesystem assets that are mounted on same drive or mount point are marked for deletion but not removed from asset database. This is because the retention period is of 1 day if there is no snapshot associated to the older filesystem asset. In this case, if you initiate the granular restore with the same drive or mount path as a target, then the operation might fail with an error. This issue doesn't occur if you try granular restore after 1 day on the such drives or mount paths. This problem also exists if you unmount the existing disk from the drive or mount path and mount another file-system to same drive or mount path.

Workaround:

Do not use a filesystem as granular restore target destination that was recreated from an existing filesystem or newly created filesystem on last discovered mount point or drive.

Public cloud not supported with gov cloud or China region

If you try to a configure a public cloud region plug-in with a gov cloud or China region cloud, the following error occurs:

```
Plug-in authentication failed. Credentials are invalid.
```

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.
```

Consistent host snapshot might fail

Sometimes the consistent host snapshot might fail with the following error:

The host level snapshot of `<host_nam>` cannot be performed as asset hierarchy is incomplete.

This issue occurs due to the following reasons:

- Granular restore is performed on the host in the last 10 minutes.
- A new disk is attached to the host and the discovery of required assets is not completed.

Configuring AWS plug-in with IAM role showed that the Authentication Method field is blank

If you attach an IAM role to a CloudPoint server that is already added to NetBackup, the role is not assigned in NetBackup.

Workaround:

You must sync NetBackup with CloudPoint by using the following command:

```
/usr/opensv/volmgr/bin/tpconfig -update -cloudpoint_server <ip/name  
which CP is registered in NBU> -cloudpoint_server_user_id admin  
-manage_workload CLOUD
```

MongoDB create snapshot job may freeze

If CloudPoint is unable to unfreeze the file system during a snapshot, the subsequent MongoDB snapshot freezes. Status of the previous snapshot job is successful, but the following errors are recorded in the logs:

```
flexsnap-coordinator: "Jun 18 22:31:51 11f5b9b5977c  
flexsnap-coordinator[1] Thread-4037029 flexsnap.coordinator:  
WARNING - post_snapshot failed for child  
  
<asset_id: eg:fs-lnxnative-ext4-74d0ad4b-d81e-4819-9a68-  
bda6b3750b8e-33280449d30c2bb766721379375a1130>  
with exc <Exception details>.
```

Workaround:

You can use the following command to unfreeze the file system:

```
fsfreeze -u <mount_point>
```

In the case of an Oracle application, if CloudPoint fails to unfreeze the file system, the next snapshot job fails.

Updating a cloud plug-in while a job runs causes job failure

If you edit the Azure plug-in configuration when a snapshot, restore, replication or any job is in progress, the job fails with the following error:

```
Request failed unexpectedly: 'AzurePlugin' object has no attribute 'aops'.
```

Workaround: Update the Azure plugin configuration only when no operations on assets managed by that configuration are in progress.

Permission denied error occurs if both user and password are updated

An issue might occur if you try to update the CloudPoint Server agentless connection credentials with a non-standard user. If you create a new user on a specific VM, then the user should be a part of the sudoers file, or the connection fails. The new user must have the permission to perform any root operation using the `sudo` command without a password.

Workaround:

To avoid this issue:

- Ensure that the `sudo` command without password is configured. Check the user entry in the `/etc/sudoers` file.
- Ensure that the binary `flexsnap-agentless` and plug-ins are not created with the old user. If they are created with the old user, delete the files.

Different source and target zones for Google Cloud Platform are not supported

Although Google Cloud Platform allows the restore snapshot across all zones, the CloudPoint server does not allow the source location and target location of the restore to be in different zones across plug-in configurations. This issue occurs because the zones are managed by configuration and so the restore to zones which is not part of config is not supported.

Workaround:

Ensure that the source location and the target locations are in the same zones as plug-in configurations.

Broken files system detected

Sometimes, a broken file system is detected on CloudPoint server during the restore process. In this case, the mount fails with the following error: Invalid super block or structure needs cleaning.

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 9.0.

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 UNIX or Windows NetBackup master server. This topic contains some of the operational notes and known issues that are associated with NetBackup for Microsoft SQL Server in NetBackup 9.0.

Notes and restrictions for Microsoft SQL Server agent

NetBackup does not support the Configure instant access option with file stream-enabled databases. Microsoft requires that the file stream files and filegroups are restored to a local file system location.

To restore file stream-enabled databases, use one of the following options:

- Configure instant access for the entire VM.
See the section *Create an instant access VM* in the [NetBackup Web UI VMware Administrator's Guide](#).
- Restore the database from a snapshot backup (without instant access). Make sure that the file stream files and filegroups are restored to the local file system. See the section *Perform a complete database recovery* in the [NetBackup Web UI Microsoft SQL Server Administrator Guide](#).

NetBackup deduplication operational notes

NetBackup provides several deduplication options that let you deduplicate data everywhere, as close to the source of data as you require. Deduplication everywhere lets you choose at which point in the backup process to perform deduplication.

NetBackup can manage the deduplication of environments that use the NetBackup Deduplication Engine. This topic contains some of the operational notes and known issues that are associated with the NetBackup Deduplication Engine in NetBackup 9.0.

For the most up-to-date compatibility information for MSDP, see the [NetBackup Enterprise Server and Server OS Software Compatibility List](#).

Backup jobs fail with "Storage server is down ..." for WORM storage servers in multi-domain environments

A problem occurs in a multi-domain environment, where two domains (both NetBackup master servers) share an MSDP user name.

If Domain 1 and Domain 2 have the same MSDP user name, and Domain 1 has created a NetBackup WORM Storage Server, and Domain 2 is configured to connect to the WORM Storage Server, backup jobs fail with the error `Storage Server is down or unavailable`.

Workaround:

1. Create a new user for Domain 2. On the NetBackup WORM Storage Server, run the following command to create the MSDP user:

```
setting MSDP-user add-MSDP-user username=user_name
```

2. On Domain 2, run the following NetBackup command to update the NetBackup WORM Storage Server to use the new user:

```
tpconfig -add -stype PureDisk -storage_server <storageserver>  
-sts_user_id <user id> -password <password>
```

3. On the NetBackup WORM Storage Server, stop and then restart the NetBackup Deduplication Manager (spad):

```
dedupe MSDP stop  
  
dedupe MSDP start
```

Backup job fails after media server with MSDP on Solaris 10 is upgraded to NetBackup 9.0

After you upgrade media server with MSDP to NetBackup 9.0 on Solaris 10, **spad** and **spoold** services in MSDP do not start. If you run the `bpps` command to check NetBackup processes, no MSDP processes are found.

Workaround:

1. On Solaris 10, after you upgrade the media server, change the first line from `#!/bin/sh` to `#!/bin/bash` in the following scripts:
 - `/usr/opensv/pdde/pdconfigure/scripts/installers/PDDE_initConfig.sh`
 - `/usr/opensv/pdde/pdconfigure/pdde`
 - `/usr/opensv/pdde/pdconfigure/etc/init.d/Solaris/pdde`
 - `/usr/opensv/pdde/pdconfigure/etc/init.d/Solaris/pdservice`
2. Run the following commands to restart all NetBackup services in media server with MSDP:

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

Configuring MSDP storage server on Solaris 10 fails

When you set up a new MSDP storage server on Solaris 10, the MSDP storage server cannot be configured successfully.

Workaround:

On Solaris 10, before you configure the MSDP storage server, change the first line from `#!/bin/sh` to `#!/bin/bash` in the following scripts:

- `/usr/opensv/pdde/pdconfigure/scripts/installers/PDDE_initConfig.sh`
- `/usr/opensv/pdde/pdconfigure/pdde`
- `/usr/opensv/pdde/pdconfigure/etc/init.d/Solaris/pdde`
- `/usr/opensv/pdde/pdconfigure/etc/init.d/Solaris/pdservice`

The ampersand character (&) not allowed in NetBackup deduplication engine credentials

Do not use an ampersand character (&) in NetBackup deduplication engine credentials.

The deduplication components use the credentials when they communicate with the NetBackup deduplication engine. You enter the NetBackup deduplication engine credentials when you configure the storage server.

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 9.0.

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 (master server, media server, Enterprise Media Manager (EMM) server, volume database host, media host, client)
- 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

NetBackup for NDMP operational notes

NetBackup for NDMP is an optional NetBackup application. It enables NetBackup to use the Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems. This topic contains some of the operational notes and known issues that are associated with NetBackup for NDMP in NetBackup 9.0.

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

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

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

NetBackup Snapshot Client operational notes

NetBackup Snapshot Client provides a variety of snapshot-based features for NetBackup. It supports clients on UNIX, Linux, and Windows platforms, on Fibre Channel networks (SANs) or traditional LANs. Each snapshot method relies on the snapshot technology that is built into the storage subsystem where the data is stored. This topic contains some of the operational notes and known issues that are associated with Snapshot Client in NetBackup 9.0.

HPE 3PAR array snapshot import fails with status code 4213

An HPE 3PAR array snapshot import fails with status code 4213. Currently, CloudPoint does not support the snapshot type Clone for the VSO (virtual server owner) snapshot method.

Workaround: Reconfigure the policy using the snapshot type COW (copy-on-write).

Snapshots are deleted after point-in-time rollbacks

In the case of the VSO FIM snapshot method for Network Attached Storage (NAS), when you perform a point-in-time rollback from an older copy, the snapshots on the storage array after that point are deleted. This operation renders the NetBackup image inconsistent, thus the image is deleted.

Similarly, when you perform a point-in-time rollback of an older snapshot from one of the mountpoints, only the snapshot that is associated with that mount point is deleted. Also, the images are deleted because they become inconsistent. However, the other snapshots belonging to other mountpoints would still reside on the storage array and you need to manually clean them up.

Index from Snapshot operation does not populate contents of the snapshot accurately in the catalog

Note: This issue is specific to on-premises workloads and UNIX platforms.

In the case of the Index from Snapshot operation, if the `/usr/openv` directory on the snapshot mount host is linked to a different path, the contents of the snapshot is not indexed accurately in the catalog.

Workaround: Reconfigure the storage lifecycle policy to have only the snapshot operation and remove the index from snapshot operation.

NetBackup virtualization operational notes

NetBackup offers several methods of protecting virtual environments. The two primary virtualization technologies that NetBackup can protect are VMware and Hyper-V, although NetBackup can protect other virtualization technologies as well. This topic contains some of the operational notes and known issues that are associated with the protection of virtualization technologies in NetBackup 9.0.

NetBackup for VMware operational notes

NetBackup for VMware provides backup and restore of the VMware virtual machines that run on VMware ESX servers. Additionally, the NetBackup plug-in for VMware vCenter (vCenter plug-in) allows the vSphere Client to monitor virtual machine backups and recover a virtual machine from a backup. This topic contains some of the operational notes and known issues that are associated with NetBackup for VMware and the vCenter plug-in in NetBackup 9.0.

VMware protection plan creation can fail when automatic scheduling and WORM storage are used

The protection plan creation does not work for the VMware workload when you select the following options:

- All schedule frequencies are set to less than one week.
- The WORM storage has a valid **Lock Maximum Duration** that is less than one week greater than the requested retention period.

Workaround: If you use a protection plan to protect VMware with WORM capable storage, set the WORM storage **Lock Maximum Duration** to greater than one week. Or, explicitly select the schedule type in the protection plan.

Media servers cannot access the virtualization server, fails with status code 200

Consider the following scenario:

- NetBackup is enabled to support NAT clients.
- An STU is created using the NetBackup Administration Console.
- You create a protection plan for VMware backup using the NetBackup web UI.
- You provide a backup host that has access to virtualization server.
- You assign the protection plan to a VMware asset.
- You check the policy that is created as part of the subscription.

- The correct VMware backup host appears on the **VMware** tab in the NetBackup Administration Console, but the **Clients > NetBackup host to perform automatic virtual machine selection** option is set to **Backup Media Server**. The media server cannot access the virtualization server, and the backup fails with status code 200.

Workaround:

- 1** Go to the **NetBackup Administration Console > NetBackup Management > Policies**.
- 2** Select the appropriate policy in the right pane.
- 3** In the **Change Policy** dialog box, select the **Clients** tab.
- 4** Click the **Select automatically through VMware Intelligent Policy** query option.
- 5** Select the required backup host from the **NetBackup host to perform automatic virtual machine selection** drop-down list.
- 6** Click **OK**.

About SORT for NetBackup Users

This appendix includes the following topics:

- [About Veritas Services and Operations Readiness Tools](#)
- [Recommended SORT procedures for new installations](#)
- [Recommended SORT procedures for upgrades](#)

About Veritas Services and Operations Readiness Tools

Veritas Services and Operations Readiness Tools (SORT) is a robust set of standalone and web-based tools that support Veritas enterprise products. For NetBackup, SORT provides the ability to collect, analyze, and report on host configurations across UNIX/Linux or Windows environments. This data is invaluable when you want to assess if your systems are ready for an initial NetBackup installation or for an upgrade.

Access SORT from the following webpage:

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

Once you get to the SORT page, more information is available as follows:

- **Installation and Upgrade Checklist**

Use this tool to create a checklist to see if your system is ready for a NetBackup installation or an upgrade. This report contains all the software and the hardware compatibility information specific to the information provided. The report also includes product installation or upgrade instructions, as well as links to other references.

- **Hot fix and EEB Release Auditor**
 Use this tool to find out whether a release that you plan to install contains the hot fixes that you need.
- **Custom Reports**
 Use this tool to get recommendations for your system and Veritas enterprise products.
- **NetBackup Future Platform and Feature Plans**
 Use this tool to get information about what items Veritas intends to replace with newer and improved functionality. The tool also provides insight about what items Veritas intends to discontinue without replacement. Some of these items include certain NetBackup features, functionality, 3rd-party product integration, Veritas product integration, applications, databases, and the OS platforms.

Help for the SORT tools is available. Click **Help** in the upper right corner of the SORT home page. You have the option to:

- Page through the contents of the help similar to a book
- Look for topics in the index
- Search the help with the search option

Recommended SORT procedures for new installations

Veritas recommends new NetBackup users perform the three procedures that are listed for an initial introduction to SORT. The tool has many other features and functions, but these serve as a good introduction to SORT. In addition, the procedures provide a helpful base of knowledge for other SORT functionality.

Table A-1

Procedure	Details
Create a Veritas Account on the SORT webpage	See “To create a Veritas Account on the SORT page” on page 50.
Create generic installation reports	See “To create a generic installation checklist” on page 50.
Create system-specific installation reports	See “To create a system-specific installation report for Windows” on page 51. See “To create a system-specific installation report for UNIX or Linux” on page 52.

To create a Veritas Account on the SORT page

- 1 In your web browser, navigate to:
<https://sort.veritas.com/netbackup>
- 2 In the upper right corner, click **Login**, then click **Register now**.
- 3 Enter the requested login and contact information:

Email address	Enter and verify your email address
Password	Enter and verify your password
First name	Enter your first name
Last name	Enter your last name
Company name	Enter your company name
Country	Enter your country
Preferred language	Select your preferred language
CAPTCHA text	Enter the displayed CAPTCHA text. If necessary, refresh the image.

- 4 Click **Submit**.
- 5 When you receive your login information, you can log into SORT and begin uploading your customized information.

To create a generic installation checklist

- 1 In your web browser, navigate to:
<https://sort.veritas.com/netbackup>
- 2 Find and select the **Installation and Upgrade Checklist** widget.

3 Specify the requested information

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

4 Click **Generate Checklist**.

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

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

To create a system-specific installation report for Windows

- 1 Go to the SORT website:
<https://sort.veritas.com/netbackup>
- 2 In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.
- 3 Select the **Data Collectors** tab
- 4 Select the radio button for **Graphical user interface** and download the correct data collector for your platform.

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.

- 5 Launch the data collector after it finishes downloading.

- 6 On the **Welcome** screen, select **NetBackup** from the product family section and click **Next**.
- 7 On the **System Selection** screen, add all computers you want analyzed. Click **Browse** to see a list of computers you can add to the analysis. Veritas recommends starting the tool with an administrator or a root account.
- 8 When all systems are selected, review the **System names** section and click **Next**.
- 9 In the **Validation Options** screen, under **Validation options**, select the version to which you plan to upgrade.
- 10 Click **Next** to continue
- 11 The utility performs the requested checks and displays the results. You can upload the report to My SORT, print the results, or save them. Veritas recommends that you upload the results to the My SORT website for ease of centralized analysis. Click **Upload** and enter your My SORT login information to upload the data to My SORT.
- 12 When you are finished, click **Finish** to close the utility.

To create a system-specific installation report for UNIX or Linux

- 1 Go to the SORT website:
<https://sort.veritas.com/netbackup>
- 2 In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.
- 3 Select the **Data Collector** tab.
- 4 Download the appropriate data collector for your platform.

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.
- 5 Change to directory that contains downloaded utility.
- 6 Run `./sortdc`

The utility performs checks to confirm the latest version of the utility is installed. In addition, the utility checks to see it has the latest data. The utility then lists the location of the log file for this session.
- 7 If requested, press **Enter** to continue.
- 8 Select the **NetBackup Family** at the **Main Menu**.

- 9** Select **Installation/Upgrade report** when prompted **What task do you want to accomplish?**
 You can select multiple options by separating your response with commas.
- 10** Specify the system or systems you want included in the report.
 If you previously ran a report on the specified system, you may be prompted to run the report again. Select **Yes** to re-run the report.
 The utility again lists the location of the log files for the session.
 The progress of the utility is displayed to the screen.
- 11** Specify **NetBackup** when prompted for the product you want installation or upgrade reports.
- 12** Enter the number that corresponds to the version of NetBackup you want to install.
 The utility again lists the location of the log files for the session.
 The progress of the utility is displayed to the screen.
- 13** The utility prompts you to upload the report to the SORT website if you want to review the report online. The online report provides more detailed information than the text-based on-system report.
- 14** When your tasks are finished, you can exit the utility. You have the option to provide feedback on the tool, which Veritas uses to make improvements to the tool.

Recommended SORT procedures for upgrades

Veritas recommends current NetBackup users perform the three procedures that are listed for an initial introduction to SORT. The tool has many other features and functions, but these serve as a good introduction to SORT for users who already use NetBackup. In addition, the procedures provide a helpful base of knowledge for other SORT functionality.

Table A-2

Procedure	Details
Create a Veritas Account on the SORT webpage	See "To create a Veritas Account on the SORT page" on page 50.

Table A-2 (continued)

Procedure	Details
Create a system-specific upgrade report	See "To create a system-specific installation report for Windows" on page 51. See "To create a system-specific installation report for UNIX or Linux" on page 52.
Review the future platform and feature plans. Review the hot fix and emergency engineering binary release auditor information.	See "To review future platform changes and feature plans" on page 54. See "To review hot fix and emergency engineering binary information" on page 54.

To review future platform changes and feature plans

- 1 In your web browser, navigate to:
<https://sort.veritas.com/netbackup>
- 2 Find and select the **NetBackup Future Platform and Feature Plans** widget.
- 3 Select **Display Information**.
- 4 Review the information provided
- 5 Optional - sign in to create notification - Click **Sign in and create notification**.

To review hot fix and emergency engineering binary information

- 1 In your web browser, navigate to:
<https://sort.veritas.com/netbackup>
- 2 Find and select the **NetBackup Hot Fix and EEB Release Auditor** widget.
- 3 Enter the hot fix or emergency engineering binary (EEB) information.
- 4 Click **Search**.
- 5 The new page shows a table with the following columns:

Hot fix of EEB Identifier	Shows the hot fix or EEB number that was entered on the previous screen.
Description	Displays a description of the problem that is associated with the hot fix or EEB.
Resolved in Versions	Provides the version of NetBackup where this issue is resolved.

NetBackup installation requirements

This appendix includes the following topics:

- [About NetBackup installation requirements](#)
- [Required operating system patches and updates for NetBackup](#)
- [NetBackup 9.0 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*, the *NetBackup Upgrade Guide*, and the *NetBackup Getting Started Guide*.

See [“NetBackup installation and upgrade operational notes”](#) on page 25.

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- Database rebuilds are likely to occur in each major, minor (single-dot), and release update (double-dot) version of NetBackup. Therefore, before upgrading to NetBackup 9.0, you must ensure that you have an amount of free disk space available that is equal to or greater than the size of the NetBackup database. That means for default installations, you are required to have that amount of free space on the file system containing the `/usr/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.

- Master 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 tech note on the Veritas Support website:
<http://www.veritas.com/docs/000013512>
- NetBackup master 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 master 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](#). 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, etc.) 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 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. [Table B-1](#) includes the OS updates and patches that are required for NetBackup 9.0. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 9.0 and other NetBackup releases can be found on the [Veritas Services and Operational Readiness Tools \(SORT\) website](#) and in the [NetBackup compatibility lists](#).

See [“About NetBackup compatibility lists and information”](#) on page 63.

See [“About Veritas Services and Operations Readiness Tools”](#) on page 48.

Note: An OS vendor may have released a more recent update or patch that supersedes or replaces a patch that is listed in [Table B-1](#). The OS patches that are listed here and in SORT should be considered at the minimum patch level that is required to install and run NetBackup. Any OS updates, patches, or patch bundles that supersede or replace those listed in [Table B-1](#) are supported unless otherwise specified. Veritas recommends that you visit the Support website of your particular OS vendor for their latest patch information.

Note: Any required patch that is listed in [Table B-1](#) for the NetBackup client should also be installed on your master servers and media servers to ensure proper client functionality.

Table B-1 Required operating system patches and updates for NetBackup 9.0

Operating system type and version	NetBackup role	Patch	Notes
AIX 6.1		AIX run-time libraries 9.0.0.3 or later	The run-time libraries need to be at 9.0.0.3 or later. You may need to restart after you change to version 9.0.0.3.
Beijing Linx Software Corp Linx OS	Master, media, client	Kernel 2.6.32.26 or later	
CentOS 6.x	Master, media, client	Kernel 2.6.32-608.el6 or later	

Table B-1 Required operating system patches and updates for NetBackup 9.0 (continued)

Operating system type and version	NetBackup role	Patch	Notes
CentOS 7.x	Master, media, client	Kernel 3.10.0-241.el7 or later	
Debian 8	Master, media, client	Kernel 3.16.7-1 or later	More information is available: Debian 8 release notes
HP-UX	Client only	COMPLIBS.LIBM-PS32	If you install AT on an HP-UX platform, this patch is required.
HP-UX IA-64	Client only	Networking.NET-RUN: /usr/lib/libip6.sl	
	Client only	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.1	
	Client only	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.sl	
	Client only	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so	
	Client only	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so.1	
	Client only	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so	
	Client only	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so.1	
	Client only	Networking.NET2-RUN: /usr/lib/libip6.1	
HP-UX 11.31	Media	QPK1131 (B.11.31.1003.347a) patch bundle	This patch bundle is required for NetBackup media server support. It is an HP-UX March 2010 patch bundle.
Oracle Linux 6	Media, client	Kernel 2.6.32-504.14.1 or later	More information is available: Kernel security and bug fix update
Oracle Linux 7	Media, client	Kernel 3.10.0-229.7.1 or later	More information is available: Kernel security and bug fix update

Table B-1 Required operating system patches and updates for NetBackup 9.0 (continued)

Operating system type and version	NetBackup role	Patch	Notes
Red Hat Enterprise Linux 6	Master, media, client	Kernel 2.6.32-504.16.2.el6 or later	More information is available: Red Hat tech note RHSA-2015:0864 - Security Advisory
Red Hat Enterprise Linux 7	Master, media, client	Kernel 3.10.0-229.7.2.el7 or later	More information is available: Red Hat tech note RHSA-2015:1137 - Security Advisory
SUSE Linux 11	Master, media, client	SUSE Linux Enterprise 11 Service Pack 3 or later	More information is available: Security update for Linux kernel:SUSE-SU-2014:1695-1
SUSE Linux 12	Master, media, client	Kernel 3.12.31 or later	More information is available: Security update for the Linux Kernel: SUSE-SU-2015:0068-1
	Client	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.

Veritas recommends the following updates when you run NetBackup on Windows operating systems:

- Microsoft `storport` hot fix. This fix applies to Windows x86 and x64, on both SP1 and SP2: (required) <http://support.microsoft.com/?id=932755>
- Symantec AntiVirus. Update to latest version and latest update (required).
- The `Symevent` driver updates (required). Update to latest driver version.

NetBackup 9.0 binary sizes

[Table B-2](#) contains the approximate binary sizes of the NetBackup 9.0 master server, media server, and client software for the various supported operating systems. These binary sizes indicate the amount of disk space occupied by the product after an initial installation. Note that for the sizes listed in the table, 1 MB equals 1024 KB.

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

Note: [Table B-2](#) and [Table B-3](#) only list 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 Operating System Compatibility List* document at <http://www.netbackup.com/compatibility>.

Table B-2 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
AIX	POWER		1776 MB	No longer supported	
Canonical Ubuntu	x86-64		1424 MB		
CentOS	x86-64		1428 MB	6698 MB	Media server or client compatibility only.
Debian GNU/Linux	x86-64		1424 MB		
HP-UX	IA-64		2260 MB	No longer supported	
Oracle Linux	x86-64		1429 MB	6731 MB	
Red Hat Enterprise Linux Server	POWER		315 MB		
Red Hat Enterprise Linux Server	x86-64		1429 MB	6857 MB	
Red Hat Enterprise Linux Server	z/Architecture		969 MB	No longer supported	Media server or client compatibility only.
Solaris	SPARC		1320 MB	5749 MB	

Table B-2 NetBackup binary sizes for compatible platforms (*continued*)

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
Solaris	x86-64		1346 MB	6108 MB	
SUSE Linux Enterprise Server	POWER		314 MB		
SUSE Linux Enterprise Server	x86-64		1195 MB	5982 MB	
SUSE Linux Enterprise Server	z/Architecture		981 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64		484 MB	3008 MB	Covers all compatible Windows x64 platforms.

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

- If you install NetBackup in a custom location on a Windows system, some portions of the software are installed on the system drive regardless of the primary application folder location. The space that is required on the system drive generally accounts for 40 to 50 percent of the total binary size that is listed in [Table B-2](#).
- If you install NetBackup server on a Windows cluster, some portions of the software are installed on the cluster shared disk. Note, the space that is required on the cluster shared disk is in addition to the binary size that is listed in [Table B-2](#). The additional required space is equivalent to 15 to 20 percent of the total binary size.

NetBackup OpsCenter

[Table B-3](#) contains the approximate binary sizes of the OpsCenter Agent, Server, and **ViewBuilder** for the various operating systems that are compatible with NetBackup OpsCenter 9.0.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Agent	Server	ViewBuilder
Oracle Linux	x86-64		757 MB	

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms
(continued)

OS	CPU Architecture	Agent	Server	ViewBuilder
Red Hat Enterprise Linux Server	x86-64		769 MB	
SUSE Linux Enterprise Server	x86-64		769 MB	
Windows Server	x86-64	263 MB	701 MB	263 MB

NetBackup plug-ins

Disk space requirements for the NetBackup vCenter Web Client Plug-in and the NetBackup System Center Virtual Machine Manager Add-in can be found in the *NetBackup Plug-in for VMware vSphere Web Client Guide* and the *NetBackup Add-in for Microsoft SCVMM Console Guide*, respectively.

NetBackup compatibility requirements

This appendix includes the following topics:

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

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 48.

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. These compatibility lists can be found on the Veritas Support website at the following location:

<http://www.netbackup.com/compatibility>

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 48.

About changes in platform compatibility

The NetBackup 9.0 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 11.

<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 9.0. 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.

Documentation published with NetBackup 9.0

Release notes and general administration guides:

- *NetBackup Release Notes*
- *NetBackup Administrator's Guide, Volume I*
- *NetBackup Administrator's Guide, Volume II*

Installation and configuration guides:

- *NetBackup Installation Guide*
- *NetBackup Quick-Start Upgrade Guide*
- *NetBackup Upgrade Guide*
- *NetBackup Device Configuration Guide*

NetBackup Web UI guides:

- *NetBackup Web UI Administrator's Guide*
- *NetBackup Web UI Cloud Administrator's Guide*
- *NetBackup Web UI Microsoft SQL Server Administrator's Guide*
- *NetBackup Web UI Oracle Administrator's Guide*
- *NetBackup Web UI RHV Administrator's Guide*
- *NetBackup Web UI VMware Administrator's Guide*

NetBackup options guides:

- *NetBackup Add-in for Microsoft SCVMM Console Guide*
- *NetBackup AdvancedDisk Storage Solutions Guide*
- *NetBackup Bare Metal Restore Administrator's Guide*
- *NetBackup Cloud Administrator's Guide*
- *NetBackup CloudPoint Installation Guide*
- *NetBackup DataStore SDK Programmer's Guide for XBSA*
- *NetBackup Deduplication Guide*
- *NetBackup for Microsoft Azure Stack Administrator's Guide*
- *NetBackup for Hadoop Administrator's Guide*
- *NetBackup for Hyper-V Administrator's Guide*
- *NetBackup for NDMP Administrator's Guide*
- *NetBackup for Nutanix Acropolis Hypervisor (AHV) Administrator's Guide*
- *NetBackup for VMware Administrator's Guide*
- *NetBackup Logging Reference Guide*
- *NetBackup OpenStorage Solutions Guide for Disk*
- *NetBackup OpsCenter Administrator's Guide*
- *NetBackup OpsCenter Reporting Guide*

- *NetBackup OpsCenter Performance and Tuning Guide*
- *NetBackup Plug-in for VMware vSphere Web Client*
- *NetBackup Plug-in for VMware vSphere Client (HTML5)*
- *NetBackup Replication Director Solutions Guide*
- *NetBackup SAN Client and Fibre Transport Guide*
- *NetBackup Snapshot Client Administrator's Guide*
- *NetBackup Vault Administrator's Guide*
- *NetBackup Vault Operator's Guide*
- *NetBackup WebSocket Service (NBWSS) Reference Guide*

Database agent guides:

- *NetBackup for DB2 Administrator's Guide*
- *NetBackup for Enterprise Vault Agent Administrator's Guide*
- *NetBackup for Informix Administrator's Guide*
- *NetBackup for Lotus Notes Administrator's Guide*
- *NetBackup for Hbase Administrator's Guide*
- *NetBackup for MariaDB Administrator's Guide*
- *NetBackup for Microsoft Exchange Server Administrator's Guide*
- *NetBackup for Microsoft SharePoint Server Administrator's Guide*
- *NetBackup for Microsoft SQL Server Administrator's Guide*
- *NetBackup for MongoDB Administrator's Guide*
- *NetBackup for MySQL Administrator's Guide*
- *NetBackup for Oracle Administrator's Guide*
- *NetBackup for OpenStack Administrator's Guide*
- *NetBackup for PostgreSQL Administrator's Guide*
- *NetBackup for SAP Administrator's Guide*
- *NetBackup for SQLite Administrator's Guide*
- *NetBackup for Sybase Administrator's Guide*

Troubleshooting guides:

- *NetBackup Status Codes Reference Guide*
- *NetBackup Troubleshooting Guide*

Other reference guides:

- *NetBackup Backup, Archive, and Restore Getting Started Guide*
- *NetBackup Commands Reference Guide*
- *NetBackup Emergency Engineering Binary Guide*
- *NetBackup Clustered Master Server Administrator's Guide*
- *NetBackup in Highly Available Environments Guide*
- *NetBackup Network Ports Reference Guide*
- *NetBackup Security and Encryption Guide*
- *NetBackup Self Service Configuration Guide*
- *NetBackup Self Service Installation Guide*
- *NetBackup Self Service Release Notes*
- *NetBackup Third-party Legal Notices*