

Veritas NetBackup™ Release Notes

Release 9.0.0.1

Veritas NetBackup™ Release Notes

Last updated: 2021-07-23

Legal Notice

Copyright © 2021 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 9.0.0.1	8
	About the NetBackup 9.0.0.1 release	8
	About NetBackup Late Breaking News	9
	About NetBackup third-party legal notices	9
Chapter 2	New features, enhancements, and changes	10
	About new enhancements and changes in NetBackup	10
	NetBackup 9.0.0.1 new features, changes, and enhancements	11
	Supercharged functionality for OpenStack workloads	11
	NetBackup support for vCloud Director 9.0, 9.1, and 9.5 reaching EOL	12
	Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 9.0.0.1	12
Chapter 3	Operational notes	14
	About NetBackup 9.0.0.1 operational notes	14
	NetBackup installation and upgrade operational notes	15
	After initiating CA migration, connection errors may occur	15
	If NetBackup 9.0.0.1 upgrade fails on Windows, revert to previous log folder structure	15
	Native installation requirements	16
	NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952	16
	Do not install from the menu that appears when the installation DVD is inserted	16
	About support for HP-UX Itanium vPars SRP containers	17
	NetBackup administration and general operational notes	17
	Starting NetBackup services may generate a warning on Solaris platforms	17
	NetBackup Messaging Broker (mqbroker) not listed in services lists even if it is running	18
	Backup fails with the Status Code 2074 "Disk volume is down"	18

Restore of the Root ("/") folder for NAS-Data-Protection policy fails	19
Backups for workloads that use the BigData policy may fail	19
Child backup jobs may enter a queued state for workloads that use BigData policy	19
Errors are shown in the jobs detail when NetBackup attempts to expire images from non-WORM capable storage	20
NetBackup web server certificate renewal failure during initiation of NetBackup CA migration or upgrade	20
Microsoft Azure backup fails if the resource group name contains a period (.)	21
Stale devices shown on the device tree	21
Temporary devices listed as file system assets	22
NetBackup administration interface operational notes	22
Search limitations for security events lists in the NetBackup web UI	22
Access control methods supported in NetBackup 9.0.0.1	22
Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms	23
Intermittent issues with X forwarding of NetBackup Administration Console	23
NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later	23
NetBackup Bare Metal Restore operational notes	23
BMR restore may take significant amount of time for formatting and volume creation step	24
NetBackup with Veritas CloudPoint operational notes	24
Snapshot jobs fail due to exceptions	24
Deleted snapshots still visible in the NetBackup web UI	24
Granular restore fails if target path is deleted and recreated	25
Public cloud not supported with gov cloud or China region	25
Indexing not supported on instances created from AWS Marketplaces AMIs	25
Consistent host snapshot might fail	25
Configuring AWS plug-in with IAM role showed that the Authentication Method field is blank	26
MongoDB create snapshot job may freeze	26
Updating a cloud plug-in while a job runs causes job failure	26
Permission denied error occurs if both user and password are updated	27
Different source and target zones for Google Cloud Platform are not supported	27

Broken files system detected	27
NetBackup deduplication operational notes	28
Backup jobs fail with "Storage server is down ..." for WORM storage servers in multi-domain environments	28
Backup job fails after media server with MSDP on Solaris 10 is upgraded to NetBackup 9.0.0.1	29
Configuring MSDP storage server on Solaris 10 fails	29
The ampersand character (&) not allowed in NetBackup deduplication engine credentials	29
NetBackup for NDMP operational notes	30
Parent directories in the path of a file may not be present in an NDMP incremental image	30
NetBackup for OpenStack operational notes	30
Instance volumes in the incremental backups cannot be mounted	30
NetBackup master server does not re-issue the token if NetBackup for OpenStack VM is a 3-node cluster	30
NetBackup version is displayed as 'Netbackup_9001_beta1' instead of 'NetBackup-CentOS3.10.0 9.0' on the Web UI	31
Success message appears along with the error message when you delete the policy that has snapshots	31
Unable to connect to NetBackup master server using NBICA	31
Excluded Ceph Volume after restore is not mountable or formattable	32
Restored VMs have blank metadata config_drive attached	32
NBOSVM reconfig fails when you add new NetBackup for OpenStack VM to the cluster	32
Database does not sync after NetBackup for OpenStack cluster gets new nodes	32
Data on boot disk gets backed up despite exclusion	32
After reinitialization and import, OpenStack certificates are missing	33
CLI import changes scheduler trust value to disabled	33
Unable to get node details after you reinitialize the NetBackup for OpenStack Appliance	33
Snapshots fails with "object is not subscriptable" for many policy jobs at the exact same time	33
No operation is permitted in insecure way for SSL-enabled Keystone URL	33
NetBackup internationalization and localization operational notes	34
Support for localized environments in database and application agents	34

	Certain NetBackup user-defined strings must not contain non-US ASCII characters	35
	NetBackup Snapshot Client operational notes	35
	HPE 3PAR array snapshot import fails with status code 4213	36
	Snapshots are deleted after point-in-time rollbacks	36
	Index from Snapshot operation does not populate contents of the snapshot accurately in the catalog	36
	NetBackup virtualization operational notes	36
	NetBackup for VMware operational notes	37
Appendix A	About SORT for NetBackup Users	39
	About Veritas Services and Operations Readiness Tools	39
Appendix B	NetBackup installation requirements	41
	About NetBackup installation requirements	41
	Required operating system patches and updates for NetBackup	42
	NetBackup 9.0.0.1 binary sizes	45
Appendix C	NetBackup compatibility requirements	48
	About compatibility between NetBackup versions	48
	About NetBackup compatibility lists and information	49
	About NetBackup end-of-life notifications	49
Appendix D	Other NetBackup documentation and related documents	51
	About related NetBackup documents	51

About NetBackup 9.0.0.1

This chapter includes the following topics:

- [About the NetBackup 9.0.0.1 release](#)
- [About NetBackup Late Breaking News](#)
- [About NetBackup third-party legal notices](#)

About the NetBackup 9.0.0.1 release

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

See [“About new enhancements and changes in NetBackup”](#) on page 10.

About EEBs and release content

NetBackup 9.0.0.1 incorporates fixes to many of the known issues that affected customers in previous versions of NetBackup. Some of these fixes are associated with the customer-specific issues. Several of the customer-related fixes that were incorporated into this release were also made available as emergency engineering binaries (EEBs).

Listings of the EEBs and Etracks that document the known issues that have been fixed in NetBackup 9.0.0.1 can be found on the Veritas Operations Readiness Tools (SORT) website and in the [NetBackup Emergency Engineering Binary Guide](#).

See [“About Veritas Services and Operations Readiness Tools”](#) on page 39.

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

About new enhancements and changes in NetBackup

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

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

See [“About the NetBackup 9.0.0.1 release”](#) on page 8.

See [“About NetBackup compatibility lists and information”](#) on page 49.

NetBackup 9.0.0.1 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 9.0.0.1 are grouped below by category. Select a link to read more information about the topic.

Note: For NetBackup 9.0 features, changes, and enhancements, see the following document:

[NetBackup 9.0 Release Notes](#)

New features

- [Supercharged functionality for OpenStack workloads](#)
- [NetBackup support for vCloud Director 9.0, 9.1, and 9.5 reaching EOL](#)

Secure communication features, changes, and enhancements

-
- **Note:** Before you install or upgrade to NetBackup 9.0.0.1 from a release earlier than 8.1, make sure that you read and understand the *NetBackup Read This First for Secure Communications* document. NetBackup 8.1 includes many enhancements that improve the secure communications of NetBackup components. The *NetBackup Read This First for Secure Communications* document describes the features and benefits of these enhancements:

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

Cloud-related changes and enhancements

- [Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 9.0.0.1](#)

Supercharged functionality for OpenStack workloads

With NetBackup 9.0.0.1, we have added significant capability for the protection of OpenStack environments. The following new key features are now available:

- Incremental backup
- Role-based access control with keystone integration
- Quota integration to protect system capacities
- Backup to Universal Shares, NFS, and S3

- Integration with NetBackup WebUI and Horizon UI
- Application consistency for MySQL, SQL server, Oracle, MariaDB, Sybase, and SharePoint
- Tenant-level self-service protection
- Resource Throttling
- Backup or recovery of individual volumes
- One-Click Restore of the entire OpenStack cloud, DR migration to a new cloud, Instant mount, and Single File Restore
- Charge back for tenant usage, consumption

For more information, see the [NetBackup for OpenStack 9.0.0.1 Administrator's Guide](#).

NetBackup support for vCloud Director 9.0, 9.1, and 9.5 reaching EOL

VMware Cloud Director versions 9.0, 9.1, and 9.5 will no longer be supported starting with the next release of NetBackup.

More information about the end-of-life notifications is available:

See [“About NetBackup end-of-life notifications”](#) on page 49.

Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 9.0.0.1

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 9.0.0.1. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 9.0.0.1, related operations fail.

Veritas continuously adds new cloud support to the cloud configuration files between releases. Updating your cloud configuration files is necessary only if your cloud storage provider was added to the cloud configuration package after version 2.7.2. The following cloud support has been added to version 2.8.1 and later but was not included in the NetBackup 9.0.0.1 final build:

- Amazon (S3) - AP Osaka region
- Dell EMC Isilon PowerScale (S3)
- Google (S3) - US-West3 (Salt Lake City) region

- Google (S3) - US-West4 (Las Vegas) region
- IBM (S3) - AP Australia region
- IBM (S3) - AP Tokyo region
- Seagate - Lyve Cloud (S3)
- Tencent Cloud - Cloud Object Storage (COS) (S3)
- XSKY Enterprise Object Storage (S3)

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>

Operational notes

This chapter includes the following topics:

- [About NetBackup 9.0.0.1 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 with Veritas CloudPoint operational notes](#)
- [NetBackup deduplication operational notes](#)
- [NetBackup for NDMP operational notes](#)
- [NetBackup for OpenStack operational notes](#)
- [NetBackup internationalization and localization operational notes](#)
- [NetBackup Snapshot Client operational notes](#)
- [NetBackup virtualization operational notes](#)

About NetBackup 9.0.0.1 operational notes

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

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

[NetBackup Release Notes, Administration, Installation, Troubleshooting, Getting Started, and Solutions Guides](#)

NetBackup installation and upgrade operational notes

NetBackup can be installed and upgraded in heterogeneous environments using a variety of methods. NetBackup is also compatible with a mixture of servers and clients that are at various release levels in the same environment. This topic contains some of the operational notes and known issues that are associated with the installation, upgrade, and software packaging of NetBackup 9.0.0.1.

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 9.0.0.1 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 9.0.0.1 upgrade fails on Windows, revert to previous log folder structure

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

For Windows, if the upgrade to NetBackup 9.0.0.1 fails and rollback occurs, run the following command to continue working on an earlier NetBackup version:

```
mklogdir.bat -fixFolderPerm
```

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

Native installation requirements

In NetBackup 8.2, a change was made to initial installs such that the answer file is now required. This change may have some negative effect on users who want to use the native packages to create VM templates or otherwise install the NetBackup packages without configuring the product. On Linux, one possible way of obtaining the previous behavior is with the `--noscripts` option of the RPM Package Manager. Providing this option when installing the `VRTSnbpcck` 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 VRTSnbpcck.rpm
rpm -U VRTSnbpcck.rpm VRTSnbclt.rpm VRTSnbdea.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 run within the SRP environment. The `swinstall` and `swremove` tools can only be called from the global host running vPars, which then pushes the native packages to the SRP containers.

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

NetBackup administration and general operational notes

NetBackup provides a complete, flexible data protection solution for a variety of platforms. The platforms include Windows, UNIX, and Linux systems. In addition to a standard set of data protection features, NetBackup can also utilize several other licensed and non-licensed components to better protect a variety of different systems and environments. This topic contains some of the general operational notes and known issues that are associated with the administration of NetBackup 9.0.0.1.

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:

```
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 9.0.0.1 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 (OCS) restart. After a restart, the OCS 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 133 (invalid request).

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 -backup_id` 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/nbwebsec/.VRTSat/profile/certstore/keystore
```

On UNIX:

```
<INSTALL_PATH>/var/global/vxss/tomcatcreds/nbwebsec/.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.

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 9.0.0.1.

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 49.

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 9.0.0.1

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 9.0.0.1.

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 `bmrrst` logs:

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

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

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 9.0.0.1.

Snapshot jobs fail due to exceptions

A high memory pressure on the CloudPoint VM causes the Flexsnap-MongoDB container and the Flexsnap-Rabbitmq container 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 the CloudPoint OnHost agent or the 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 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 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 9.0.0.1.

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 9.0.0.1

After you upgrade media server with MSDP to NetBackup 9.0.0.1 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 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 9.0.0.1.

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

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

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

NetBackup for OpenStack operational notes

NetBackup for OpenStack is an optional NetBackup application. This topic contains some of the operational notes and known issues that are associated with NetBackup for OpenStack in NetBackup 9.0.0.1.

Instance volumes in the incremental backups cannot be mounted

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

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

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

Workaround:

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

NetBackup version is displayed as 'Netbackup_9001_beta1' instead of 'NetBackup-CentOS3.10.0 9.0' on the Web UI

On NetBackup for OpenStack VM, version **NetBackup-CentOS3.10.0 9.0** is displayed under `/usr/opensv/netbackup/bin/version`. NetBackup Web UI does not display the same version and displays **Netbackup_9001_beta1** instead.

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

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

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

Unable to connect to NetBackup master server using NBCA

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

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

Workaround:

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

For more information, see the following Support article:

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

Excluded Ceph Volume after restore is not mountable or formattable

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

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

Restored VMs have blank metadata `config_drive` attached

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

Workaround:

Delete metadata `config_drive` or set the desired value.

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

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

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

Workaround:

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

Database does not sync after NetBackup for OpenStack cluster gets new nodes

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

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

Workaround:

Run the policy import from CLI.

Data on boot disk gets backed up despite exclusion

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

After reinitialization and import, OpenStack certificates are missing

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

Workaround:

Upload the certificates again.

CLI import changes scheduler trust value to disabled

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

Workaround:

Configure NetBackup with import option from UI after reinitialization.

Unable to get node details after you reinitialize the NetBackup for OpenStack Appliance

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

Workaround:

Restart `wlm-workloads` and `wlm-cron` services on NetBackup for OpenStack nodes.

```
systemctl restart wlm-workloads
```

```
systemctl restart wlm-cron
```

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

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

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

Workaround:

Contact Veritas Support to implement a known workaround.

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

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

Workaround:

Configure the NetBackup for OpenStack appliance with OpenStack CA provided.

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

NetBackup internationalization and localization operational notes

This topic contains some of the operational notes and known issues that are associated with internationalization, localization, and non-English locales in NetBackup 9.0.0.1.

Support for localized environments in database and application agents

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

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

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

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

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

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 9.0.0.1.

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/opensv` 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 9.0.0.1.

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 9.0.0.1.

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](#)

About Veritas Services and Operations Readiness Tools

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

Access SORT from the following webpage:

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

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

- **Installation and Upgrade Checklist**
Use this tool to create a checklist to see if your system is ready for a NetBackup installation or an upgrade. This report contains all the software and the hardware compatibility information specific to the information provided. The report also includes product installation or upgrade instructions, as well as links to other references.
- **Hot fix and EEB Release Auditor**
Use this tool to find out whether a release that you plan to install contains the hot fixes that you need.

- **Custom Reports**

Use this tool to get recommendations for your system and Veritas enterprise products.

- **NetBackup Future Platform and Feature Plans**

Use this tool to get information about what items Veritas intends to replace with newer and improved functionality. The tool also provides insight about what items Veritas intends to discontinue without replacement. Some of these items include certain NetBackup features, functionality, 3rd-party product integration, Veritas product integration, applications, databases, and the OS platforms.

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

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

NetBackup installation requirements

This appendix includes the following topics:

- [About NetBackup installation requirements](#)
- [Required operating system patches and updates for NetBackup](#)
- [NetBackup 9.0.0.1 binary sizes](#)

About NetBackup installation requirements

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

See “[NetBackup installation and upgrade operational notes](#)” on page 15.

- 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 9.0.0.1, you must ensure that you have an amount of free disk space available that is equal to or greater than the size of the NetBackup database. That means for default installations, you are required to have that amount of free space on the file system containing the `/usr/opensv/db/data` (UNIX) or `<install_path>\Veritas\NetBackupDB\data` (Windows) directories. If you have changed the location of some of the files in either of these directories,

free space is required in those locations equal to or greater than the size of the files in those locations. Refer to the [NetBackup Administrator's Guide, Volume I](#) for more information about storing NBDB database files in alternate locations.

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

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

Required operating system patches and updates for NetBackup

NetBackup server and client installations are only supported on a defined set of operating systems (OSs) that are listed in the [NetBackup compatibility lists](#). 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 9.0.0.1. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 9.0.0.1 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 49.

See [“About Veritas Services and Operations Readiness Tools”](#) on page 39.

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 9.0.0.1

Operating system type and version	NetBackup role	Patch	Notes
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	
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

Table B-1 Required operating system patches and updates for NetBackup 9.0.0.1 (*continued*)

Operating system type and version	NetBackup role	Patch	Notes
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 7	Media, client	Kernel 3.10.0-229.7.1 or later	More information is available: Kernel security and bug fix update
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

Table B-1 Required operating system patches and updates for NetBackup 9.0.0.1 (*continued*)

Operating system type and version	NetBackup role	Patch	Notes
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

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

- Symantec AntiVirus. Update to latest version and latest update (required).
- The `Symevent` driver updates (required). Update to latest driver version.

NetBackup 9.0.0.1 binary sizes

[Table B-2](#) contains the approximate binary sizes of the NetBackup 9.0.0.1 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		1835 MB	No longer supported	

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

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
Canonical Ubuntu	x86-64		1486 MB		
CentOS	x86-64		1492 MB	7084 MB	
Debian GNU/Linux	x86-64		1486 MB		
HP-UX	IA-64		2313 MB	No longer supported	
Oracle Linux	x86-64		1493 MB	7073 MB	
Red Hat Enterprise Linux Server	POWER		315 MB		
Red Hat Enterprise Linux Server	x86-64		1493 MB	6963 MB	
Red Hat Enterprise Linux Server	z/Architecture		1028 MB	No longer supported	Media server or client compatibility only.
Solaris	SPARC		1381 MB	5937 MB	
Solaris	x86-64		1406 MB	6295 MB	
SUSE Linux Enterprise Server	POWER		314 MB		
SUSE Linux Enterprise Server	x86-64		1255 MB	6287 MB	
SUSE Linux Enterprise Server	z/Architecture		1039 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64		482 MB	3122 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 9.0.0.1.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Agent	Server	ViewBuilder
Oracle Linux	x86-64		748 MB	
Red Hat Enterprise Linux Server	x86-64		750 MB	
SUSE Linux Enterprise Server	x86-64		763 MB	
Windows Server	x86-64	No longer supported as of NetBackup 9.0.0.1	688 MB	231 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 compatibility between NetBackup versions](#)
- [About NetBackup compatibility lists and information](#)
- [About NetBackup end-of-life notifications](#)

About compatibility between NetBackup versions

You can run mixed versions of NetBackup between primary servers, media servers, and clients. This back-level support lets you upgrade NetBackup one server at a time, which minimizes the effect on overall system performance.

Veritas supports only certain combinations of servers and clients. In mixed version environments, certain computers must be the highest version. Specifically, the version order is: OpsCenter server, primary server, media server, and then clients. For example, the scenario that is shown is supported: 9.0 OpsCenter server > 8.3.0.1 primary server > 8.3 media server > 8.0 client.

All NetBackup versions are four digits long. The NetBackup 9.0 release is the 9.0.0.0 release. Likewise, the NetBackup 8.3 release is the NetBackup 8.3.0.0 release. For the purposes of supportability, the fourth digit is ignored. An 8.3 primary server supports an 8.3.0.1 media server. Likewise, an 8.3.0.1 primary supports an 8.3 OpsCenter server. An example of what is not supported is an 8.3 OpsCenter server with a 9.0 primary server.

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

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

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

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

About NetBackup compatibility lists and information

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

See [“About Veritas Services and Operations Readiness Tools”](#) on page 39.

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 39.

About changes in platform compatibility

The NetBackup 9.0.0.1 release may contain changes in support for various systems. In addition to using SORT, you should make sure to review the *NetBackup Release Notes* document and the NetBackup compatibility lists before installing or upgrading NetBackup software.

See “[About new enhancements and changes in NetBackup](#)” on page 10.

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

Other NetBackup documentation and related documents

This appendix includes the following topics:

- [About related NetBackup documents](#)

About related NetBackup documents

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

Not all documents are published with each new release of NetBackup. In the guides, you may see references to other documents that were not published for NetBackup 9.0.0.1. In these cases, refer to the latest available version of the guide.

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

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

Documentation published with NetBackup 9.0.0.1

- *NetBackup Release Notes*
- *NetBackup Emergency Engineering Binary Guide*
- *NetBackup Installation Guide*
- *NetBackup Quick-Start Upgrade Guide*

- *NetBackup Upgrade Guide*
- *NetBackup Administrator's Guide, Volume I*
- *NetBackup CloudPoint Installation Guide*
- *NetBackup for OpenStack Administrator's Guide*
- *NetBackup OpsCenter Administrator's Guide*
- *NetBackup OpsCenter Reporting Guide*
- *NetBackup OpsCenter Performance and Tuning Guide*
- *NetBackup Status Codes Reference Guide*