NetBackup™ Release Notes

Release 10.0

Document Version 1

VERITAS™

NetBackup™ Release Notes

Last updated: 2022-03-25

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1 About NetBackup 10.0 9

About the NetBackup 10.0 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 10.0 new features, changes, and enhancements 12
Changes in Veritas terminology 14
RESTful APIs included in NetBackup 10.0 14
Improvements to Activity monitor in the NetBackup web UI 18
Veritas announces NetBackup SaaS Protection (NSP) integration with web UI 19
NetBackup MSDP catalog shadow copy duplicates on data volumes 20
Malware detection in NetBackup 20
Accessing NetBackup Flex Scale from the NetBackup web UI 21
Non-root users with the required access can access CLIs 21
A new host ID-based certificate in NetBackup 10.0 cannot have a key size greater than 4096 22
Configure smart card or certificate user authentication without AD or LDAP domain validation 22
EOL for support of BMR clients on HP-UX 22
Last release for NetBackup OpsCenter and OpsCenter Analytics 22
NetBackup 10.0 support additions and changes 23
Workloads supported in the FIPS-compliant mode 24
Support for data-in-transit encryption (DTE) 24
NetBackup 10.0 removes support for direct backup to storage units (non-SLP) in ISM policies 25
BMR now supports ADK 10 for Windows restores 25
MSDP disk pool creation in the web UI supports AWS SSE-CMK 25

MSDP cloud immutable storage support for S3-compatible platforms and Azure 25
NetBackup for OpenStack supports OpenStack-Ansible 26
Guided Recovery for Oracle is no longer supported in OpsCenter 26
Several shutdown commands to be deprecated in a future release 26
Snapshot and Recovery of Windows VMs residing on the Google Cloud Platform 26
Support for configuring license types in the NetBackup web UI 27
Change in accessibility of the legacy logs 27
Notifications, Messages, and Resiliency configuration information are not upgraded 27
CloudPoint 8.3.x servers require upgrade to NetBackup 9.1.x before upgrading to version 10.0 27
Changes in vCenter plug-in support 28
Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.0 29
File path changes for CloudProvider.xml and cacert.pem 30
Upcoming changes for Oracle instance groups and commands 30
NetBackup Copilot for Oracle with instant access and universal share 30
NetBackup for Oracle and NetBackup for DB2 prevent the direct expiration of backup images 30
Plug-in to store the RMAN backups to MSDP storage directly 31
Backup and restore of Cassandra clusters 31
Recovery Vault for NetBackup 31
NetBackup Bare Metal Restore (BMR) operations in the NetBackup web UI 32

Chapter 3 Operational notes 33

About NetBackup 10.0 operational notes 33
NetBackup installation and upgrade operational notes 34
If NetBackup 10.0 upgrade fails on Windows, revert to previous log folder structure 34
Native installation requirements 34
NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952 35
About support for HP-UX Itanium vPars SRP containers 35

NetBackup administration and general operational notes 36
Permissions necessary for redirected restores with non-root service user accounts 36
Restore of the Root ("/") folder for NAS-Data-Protection policy fails 36
Stale devices shown on the device tree 36
Temporary devices listed as file system assets 37
NetBackup administration interface operational notes 37
Certain NetBackup web UI nodes do not work when NBAC is configured in the 'Required' or 'Automatic' mode 38
Some columns in the web UI are not searchable 38
Delay in NetBackup web UI when adding or removing columns in Catalog area 38
Job actions not available for workload administrators with limited RBAC permissions on assets 38
Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms 39
Intermittent issues with X forwarding of NetBackup Administration Console 40
NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later 40
NetBackup Cloud operational notes 40
Provider configuration for Azure Stack Hub fails with error “Authentication failed: invalid_instance” 40
Restore of cloud VM backup images replicated with AIR fails Pre-recovery check 41
Error in calculating the snapshot size in smart metering for Cloud workloads 41
Configuring a cloud recovery host on RHEL 8 42
NetBackup with Veritas CloudPoint operational notes 42
Offline VM backup fails with status code 156 42
Restoring a VM (with a Read-only disk) from an app-consistent snapshot fails 42
Editing a query with special characters in tag names is not supported for the intelligent Cloud groups 43
Starting or restarting the CloudPoint services may fail if a stale IP address entry is retained in the Podamn layer on RHEL 8.3 environment 43
VM disks not displayed due to discovery level 44
Granular restore fails if target path is deleted and recreated 44
Public cloud not supported with gov cloud or China region 45

Indexing not supported on instances created from AWS Marketplaces AMIs 45
Consistent host snapshot might fail 45
Configuring AWS plug-in with IAM role showed that the Authentication Method field is blank 45
Permission denied error occurs if both user and password are updated 46
Different source and target zones for Google Cloud Platform are not supported 46
Broken files system detected 46
NetBackup for NDMP operational notes 47
Parent directories in the path of a file may not be present in an NDMP incremental image 47
NetBackup for OpenStack operational notes 47
CentOS repository mirror URL is updated 47
NetBackup for OpenStack Datamover API (NBOSDMAPI) service times out in the haproxy connection 47
Policy schedule start time on the Horizon UI is different than configured in the policy 48
Instance volumes in the incremental backups cannot be mounted 48
NetBackup primary server does not re-issue the token if NetBackup VM is a 3-node cluster 48
NetBackup version is displayed as 'NetBackupforOpenStack_10.0.1Beta1' instead of 'NetBackup-CentOS3.10.0 9.0' on the Web UI 48
Success message appears along with the error message when you delete the policy that has snapshots 49
Unable to connect to NetBackup primary server using NBCA 49
Excluded Ceph Volume after restore is not mountable or formattable 49
Restored VMs have blank metadata config_drive attached 49
NBOSVM reconfig fails when you add new NetBackup VM to the cluster 50
Database does not sync after NetBackup cluster gets new nodes 50
Data on boot disk gets backed up despite exclusion 50
After reinitialization and import, OpenStack certificates are missing 50
CLI import changes scheduler trust value to disabled 50
Unable to get node details after you reinitialize the NetBackup Appliance 51

Snapshots fails with "object is not subscriptable" for many policy jobs at the exact same time 51
No operation is permitted in insecure way for SSL-enabled Keystone URL 51
NetBackup internationalization and localization operational notes 51
Support for localized environments in database and application agents 52
Certain NetBackup user-defined strings must not contain non-US ASCII characters 52
NetBackup Snapshot Client operational notes 53
Snapshot job fails with status code 927 53
HPE 3PAR array snapshot import fails with status code 4213 54
Snapshots are deleted after point-in-time rollbacks 54
Index from Snapshot operation does not populate contents of the snapshot accurately in the catalog 54
NetBackup virtualization operational notes 54
NetBackup for VMware operational notes 55

Appendix A About SORT for NetBackup Users 56

About Veritas Services and Operations Readiness Tools 56

Appendix B NetBackup installation requirements 58

About NetBackup installation requirements 58
Required operating system patches and updates for NetBackup 59
NetBackup 10.0 binary sizes 62

Appendix C NetBackup compatibility requirements 65

About compatibility between NetBackup versions 65
About NetBackup compatibility lists and information 66
About NetBackup end-of-life notifications 66

Appendix D Other NetBackup documentation and related documents 68

About related NetBackup documents 68

Chapter 1

About NetBackup 10.0

This chapter includes the following topics:

- About the NetBackup 10.0 release
- About NetBackup Late Breaking News
- About NetBackup third-party legal notices

About the NetBackup 10.0 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 10.0 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 10.0 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 56.

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

Chapter 2

New features, enhancements, and changes

This chapter includes the following topics:

- About new enhancements and changes in NetBackup
- NetBackup 10.0 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 10.0 release" on page 9.

See "About NetBackup compatibility lists and information" on page 66.

NetBackup 10.0 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 10.0 are grouped below by category. Select a link to read more information about the topic.

New features

- Changes in Veritas terminology
- RESTful APIs included in NetBackup 10.0
- Improvements to Activity monitor in the NetBackup web UI
- Veritas announces NetBackup SaaS Protection (NSP) integration with web UI
- NetBackup MSDP catalog shadow copy duplicates on data volumes
- Malware detection in NetBackup
- Accessing NetBackup Flex Scale from the NetBackup web UI

Secure communication features, changes, and enhancements

- Non-root users with the required access can access CLIs
- A new host ID-based certificate in NetBackup 10.0 cannot have a key size greater than 4096
- Configure smart card or certificate user authentication without AD or LDAP domain validation

---

- **Note:** Before you install or upgrade to NetBackup 10.0 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

- EOL for support of BMR clients on HP-UX
- Last release for NetBackup OpsCenter and OpsCenter Analytics
- NetBackup 10.0 support additions and changes

- Workloads supported in the FIPS-compliant mode
- Support for data-in-transit encryption (DTE)
- NetBackup 10.0 removes support for direct backup to storage units (non-SLP) in ISM policies
- BMR now supports ADK 10 for Windows restores
- MSDP disk pool creation in the web UI supports AWS SSE-CMK
- MSDP cloud immutable storage support for S3-compatible platforms and Azure
- NetBackup for OpenStack supports OpenStack-Ansible
- Guided Recovery for Oracle is no longer supported in OpsCenter
- Several shutdown commands to be deprecated in a future release
- Snapshot and Recovery of Windows VMs residing on the Google Cloud Platform
- Support for configuring license types in the NetBackup web UI

Installation, upgrade, and configuration changes and enhancements

- Change in accessibility of the legacy logs
- Notifications, Messages, and Resiliency configuration information are not upgraded

Cloud-related changes and enhancements

- Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.0
- File path changes for CloudProvider.xml and cacert.pem
- CloudPoint 8.3.x servers require upgrade to NetBackup 9.1.x before upgrading to version 10.0

Virtualization changes and enhancements

- Changes in vCenter plug-in support

Database agent changes and enhancements

- Upcoming changes for Oracle instance groups and commands
- NetBackup Copilot for Oracle with instant access and universal share
- NetBackup for Oracle and NetBackup for DB2 prevent the direct expiration of backup images
- Plug-in to store the RMAN backups to MSDP storage directly

- Backup and restore of Cassandra clusters

Other announcements

- Recovery Vault for NetBackup
- NetBackup Bare Metal Restore (BMR) operations in the NetBackup web UI

Changes in Veritas terminology

To modernize our terminology, Veritas has begun to replace certain outdated terms with more current terms.

Note: As Veritas continues to update its terminology, the deprecated terms and the new terms may be used interchangeably.

Deprecated term	New term
Master	Primary
Slave	Secondary or media server
Whitelist or white list	Allowed list
Blacklist or black list	Blocked list
White hat	Ethical
Black hat	Unethical

RESTful APIs included in NetBackup 10.0

NetBackup 10.0 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.

API documentation

You can find documentation for the NetBackup APIs in on SORT and on your primary server. Make sure to review the *Versioning* topic and the *What's New* topic in the *Getting Started* section.

- On your primary server:
  APIs are stored in YAML files on the primary server:
  `https://<primary_server>/api-docs/index.html`
  The APIs are documented in Swagger format. This format lets you review the code and test the functionality by making actual calls with the APIs. You must

have the appropriate security permissions to access the primary server and APIs to use the Swagger APIs.

Caution: Veritas recommends that you test APIs only in a development environment. Because you can make actual API calls from the Swagger files, you should not test the APIs in a production environment.

- On SORT:
  NetBackup API documentation is also available on SORT:
  HOME > KNOWLEDGE BASE > Documents > Product Version > 10.0
  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 10.0 includes these new and enhanced APIs:

- API Keys: Reissue and revoke existing API keys.
- Bare Metal Restore: Manage BMR clients, configurations, and VM conversions.
- Catalog Images: An image can be updated to modify its DTE mode.
- Continuous Data Protection: Manage CDP hosts.
- Data Classifications: Update data classifications.
- Host Properties: Manage the following types of host properties:
  - globalAttributes
  - universalSettings
  - fibreTransport
  - restoreFailover
  - generalServer
  - portRanges
  - timeouts
  - clientAttributes
  - distributedApplicationRestoreMappings
  - firewallAttributes
  - logging

    - cleanup
    - accessControl
    - networkSettings
    - credentialAccess
    - defaultJobPriorities
    - enterpriseVaultHosts
    - networkBandwidth
    - preferredNetworks
    - resilientNetworks
    - scalableStorage
    - clientName
    - encryption
    - windowsClientSettings
    - clientExcludeLists
    - clientNetwork
    - clientLotusNotes
    - clientExchange
    - clientSharePoint
    - clientActiveDirectory
    - clientEnterpriseVault
    - unixClientSettings
    - clientBusyFileSettings
- Malware: Manage scan hosts and initiate scans.
- Media Servers: A media server can be updated to modify its DTE mode.
- Recovery:
    - Instant access of files and folders from Standard and MS-Windows backup images.
    - Instant access for Oracle Copilot.
- Recovery Point Service: List provider protected recovery points.
- Retention Levels:

- Security Anomalies: Manage records of detected security anomalies and report generation.
- Server Lists: Manage the server lists for a host.
- Service Principals: Manage API access for principals other than NetBackup hosts or users, such as a Kubernetes controller.

Versioned APIs

These APIs that have been versioned in NetBackup 10.0 due to breaking changes. The previous version of these APIs is still supported by specifying the correct version. See the *Versioning* section in the **API Reference** on SORT for more details.

- Kubernetes Recovery Points:
  `GET /recovery-point-service/workloads/{workload}/recovery-points/{recoveryPointId}` has changed the datatype of the `instances` attribute of the `optionalKubernetesRecoveryPointInfo` response object from a list of strings to a list of objects.
- Host Properties:
  `GET /config/data-classifications` has changed from a collection of individual resource objects to a single resource object containing an array of data classifications.
- Universal Share Instant Access:
  `POST /recovery/workloads/universal-share/instant-access-mounts` has changed the type value. The `targetServer` attribute has also been renamed to `clients` and changed to an array of strings.
- Catalog Images:
  `GET /catalog/images` and `GET /catalog/images/{backupId}`
  The attribute `dteMode` has been renamed to `imageDteMode` in image response for v7.0.
  The `copyDteMode` attribute and the `hierarchicalDteMode` attribute were added to the `fragments` attribute in image response for v7.0.

See the *Versioned APIs* section of the **API Reference** on SORT for API v4.0-6.0 and API v7.0 examples.

API filter behavior changes

These APIs have changed in terms of filtering for the `nbuVersion` and `nbuReleaseVersion` fields. There are no behavior changes for other fields.

Note: This behavior will only affect the binary operators (for example, `gt`, `lt`, `le`, and so on) from filter expression.

- Listing Media Servers:
  `GET `/config/media-servers``
- Listing Hosts:
  The `/config/hosts` API behavior is the same as `/config/media-servers`, however, the filterable field is `nbuReleaseVersion`.

See the *API Filter Behaviour Changes* section of the **API Reference** on SORT for examples.

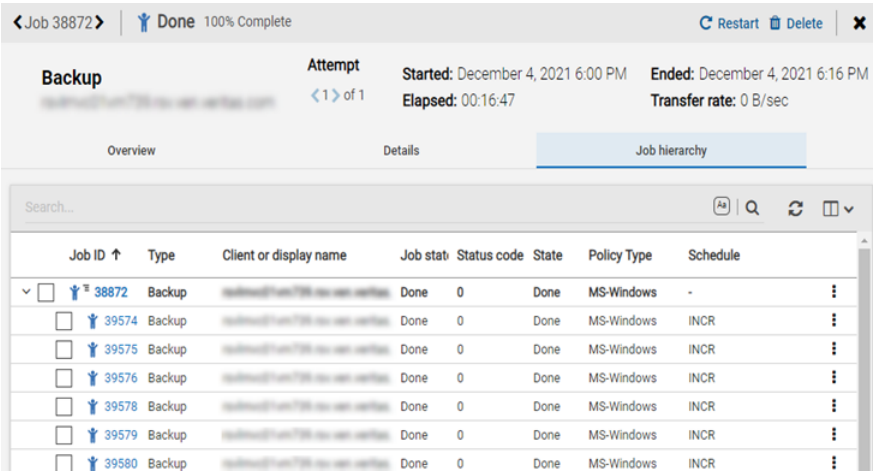
Improvements to Activity monitor in the NetBackup web UI

This version of NetBackup includes improvements to the display of jobs in the Activity monitor.

- A faster display of jobs.
- The addition of a jobs hierarchy view in the **Jobs** tab.
  Note: If you have an RBAC role that allows access to jobs, you can see the jobs list in the job hierarchy view. For example, the Default VMware Administrator role lets you see VMware jobs in the hierarchy view. However, if you only have access to one or more VMs (asset-level access), no jobs display in the job hierarchy view.
  The job hierarchy view displays the jobs so you can see the complete hierarchy of the jobs. This view includes the top-level job (or root job) and its child jobs (if applicable). A child job can, in turn, be a parent of additional child jobs.
  In the **Jobs** tab, click the **Hierarchy view** and **List view** buttons to switch between the job views.

- When you open the job details, a new **Job hierarchy** tab displays the job hierarchy for that job.



- Ability to create job filters.
  The previous job filters are removed. You can now create specific filters based on one or more query criteria. For example, you can create a filter that displays jobs for any clients that have a name that starts with “a” and have the job type “Restore”.
- A **Display density** that provides a more compact listing of jobs.
- Sorting is now case-insensitive for the following user-defined fields: **Storage unit**, **Policy name**, **Schedule**, and **Client or display name**.
- For an individual job, you can click on the link for the **Policy name** and the **Storage unit** to see details for the policy or the storage unit.
- Any changes to the column widths and column order are retained for the user.

Veritas announces NetBackup SaaS Protection (NSP) integration with web UI

NetBackup SaaS Protection (NSP) is a cloud-based, data protection and management solution that is deployed on Microsoft Azure:

- Integration with NetBackup web UI:
  NetBackup 10.0 lets you connect to and monitor NSP using the NetBackup web UI. With the web UI, you can launch NSP with Single Sign On (SSO).
- Role-based access control (RBAC):
  You can configure user access and delegate asset management and credentials access for NSP.

- Credential management:
  You can add the NSP credentials in the NetBackup credential management database.
- Automatic asset discovery:
  NetBackup runs an automatic resource discovery process to get all SaaS applications that are configured in NSP. This process updates the current state of NSP in NetBackup.

Limitations:

- The API response from NSP to NetBackup does not yet support localization.
- NSP supports IPv4 only. It does not support IPv6.

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

For more details about NetBackup SaaS Protection, refer to the *NetBackup SaaS Protection Administrator's Guide*.

NetBackup MSDP catalog shadow copy duplicates on data volumes

MSDP lets you store two additional duplicates of the catalog shadow copies on separate data volumes. The storage of the duplicates allows for better metadata resiliency.

This functionality uses the `cacontrol` command to add or delete a volume to store the duplicate.

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

Malware detection in NetBackup

NetBackup now supports scanning of backup images of Standard and MS-Windows policy type backups that are stored on an MSDP storage unit for occurrence of malware.

You can select one or more backup images of the supported policy types for an on-demand scan using a predefined list of scan hosts. Malware scanning is done by supported third-party scanners such as MS Defender, Symantec Protection Engine, and the NetBackup Malware Scanner, which needs to be preinstalled and configured on the scan host. If malware is detected during the scan, notification is generated in the NetBackup web UI. A list of on-going and completed scans is also shown in the NetBackup web UI. You are warned about recovery from the impacted image. A new command line tool `bpcleanrestore` is available on primary servers to restore only the clean files from the scanned backups.

The NetBackup Instant Access feature is used for mounting the MSDP backup images on the scan host either as SMB or NFS shares. For more information on the malware detection, refer to the *NetBackup Security and Encryption Guide*.

Accessing NetBackup Flex Scale from the NetBackup web UI

The Flex Scale appliance administrator (**appadmin**) can monitor and manage their cluster nodes and disks from the Flex Scale infrastructure page in the NetBackup web UI. The **appadmin** has the **Default Security Administrator** role for the NetBackup web UI and can also manage all of NetBackup.

For full instructions on managing NetBackup Flex Scale, see the following resources.

NetBackup Flex Scale Installation and Configuration Guide

NetBackup Flex Scale Administrator's Guide

Table 2-1 Accessing Flex Scale and NetBackup

Interface and URL	Access to Flex Scale or NetBackup
NetBackup web UI https://*primaryserver*/webui/login	To open Flex Scale, click the **Appliance management** node. This action opens the NetBackup Flex Scale infrastructure management console in a new browser tab.
Flex Scale infrastructure management console IPv4: https://*ManagementServerIPorFQDN*:14161/ IPv6: https://*ManagementServerIP*:14161/	To open NetBackup, click the **NetBackup** node. This action launches the NetBackup Flex Scale UI in the same browser tab. To access the Flex Scale infrastructure management console again, click **Cluster Monitor > Infrastructure** and then **Cluster Dashboard**.
Flex Scale UI https://ManagementServerIPorFQDN	To view the Flex Scale infrastructure, on the left click **Cluster Monitor > Infrastructure**. From that page you can also open the Flex Scale UI infrastructure management console. Click **Cluster Dashboard** at the top right.

Non-root users with the required access can access CLIs

Starting with NetBackup 10.0, non-root users with the required access can also administer NetBackup using certain administrator commands, for example `bperror`.

You need to authenticate yourself through the web UI. You need to generate an access code through the command-line interface, get the access request approved from the administrator, and then access the command. A new RBAC role called NetBackup Command Line (CLI) Administrator is created. It has all the permissions that are necessary to manage NetBackup using the CLI.

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

A new host ID-based certificate in NetBackup 10.0 cannot have a key size greater than 4096

Because of a technical limitation in NetBackup 10.0, you cannot generate or renew a host ID-based certificate to have a key size greater than 4096. Therefore, you must not migrate the NetBackup CA to have a key size greater than 4096. If the CA migration with a key size greater than 4096 is already in progress, you must complete the migration before you upgrade to NetBackup 10.0.

This technical limitation does not have any effect on the operations related to external CA-signed certificates.

Configure smart card or certificate user authentication without AD or LDAP domain validation

Starting with NetBackup 10.0, you can configure smart card or certificate user authentication without validating the users with AD or LDAP domain. This configuration does not support user groups. For more details, refer to the *NetBackup Security and Encryption Guide*.

EOL for support of BMR clients on HP-UX

With NetBackup 10.0, Veritas announces end-of-life (EOL) for support for NetBackup Bare Metal Restore (BMR) clients running on Hewlett-Packard Enterprise HP-UX. This operating system is no longer a supported platform for BMR clients. Support will continue on older versions of NetBackup and follow the published Veritas Product End of Life policy guidelines.

Last release for NetBackup OpsCenter and OpsCenter Analytics

NetBackup 10.0 is the last NetBackup version to include NetBackup OpsCenter and OpsCenter Analytics. OpsCenter 10.0 EoSL (End of Support Life) will align with the NetBackup 10.0 EoSL date. (See https://sort.veritas.com/eosl for product EoSL information.)

NetBackup IT Analytics (formerly APTARE) is the solution for NetBackup reporting and analytics.

NetBackup 10.0 support additions and changes

Note: This information is subject to change. See the NetBackup Compatibility List for all Versions for the most recent product and services support additions and changes.

The following products and services are supported starting with NetBackup 10.0:

- Windows 2022 on primary servers, media servers, and clients
- NetBackup plug-in for vSphere Client (HTML5) Version on NetBackup primary servers with vSphere Client (HTML5) 6.7 update 1 and later.
- Virtual systems:
  - VMware VDK 7.03
  - vSphere:
    vSphere 7.0, 7.0 U1, 7.0 U2, 7.0 U3
    vSphere 6.7, 6.7 U1, 6.7 U2, 6.7 U3
    vSphere 6.5, 6.5 U1, 6.5 U2, 6.5 U3
    VMware vSAN 6.5, 6.6, 6.6.1, 6.7, 6.7 U1, 6.7 U2, 6.7 U3
    VMware vSAN 7.0 , 7.0 U1, 7.0 U2, 7.0 U3
  - vCloud Director:
    Service provider versions: 9.0, 9.1, 9.5, 9.7, 10, 10.1, 10.2, 10.3
  - Backup and restore host:
    Windows Server 2019, 2016, 2012 R2, 2012
    Red Hat Enterprise Linux (RHEL) 7.7, 8.0
    SUSE Linux Enterprise Server (SLES) 12SP5, 15SP1
    CentOS 7.7
- Kubernetes cluster services:
  Azure Kubernetes Service on Kubernetes 1.21.x and later
- Veritas CloudPoint support additions:
  - Platform-as-a-service (PaaS) - Azure SQL:
    Restore to Original Location is supported. Restore to Alternate Location and In-place Restore are not supported.
  - Platform-as-a-service (PaaS) - Azure SQL Managed Instance:
    Restore to original location and Restore to Alternate Location are supported. In-place Restore is not supported.
  - Azure Gen2 Linux on Ubuntu 18.04 and 20.04, RHEL 8.4, and RHEL 7.8

- Azure Gen2 Windows on Windows 19

Workloads supported in the FIPS-compliant mode

Starting with NetBackup 10.0, the following workloads are supported in the FIPS-compliant mode:

- Veritas CloudPoint
- Oracle
- MS-SQL
- SAP HANA
- DB2
- VMware
- Hyper-V
- RHV
- Nutanix
- DynamicNAS
- MongoDB
- MySQL
- PostgreSQL
- SQLite
- MariaDB
- SharePoint

The support for the MSDP and NetBackup KMS (NBKMS) components to run in the FIPS mode was added earlier. The FIPS mode configuration that is introduced in 10.0 does not affect the earlier implementation. NBKMS continues to run in the FIPS mode, by default.

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

Support for data-in-transit encryption (DTE)

Starting with version 10.0, NetBackup supports data-in-transit encryption (DTE).

You can configure the DTE mode at various levels: global level (primary server-level) and client level.

After you configure the required DTE modes, data-in-transit is encrypted during communication between NetBackup hosts - primary servers, media servers, and clients. The TLS 1.2 or a later protocol is used for data encryption.

To achieve an end-to-end encryption of data within the NetBackup boundary, all NetBackup hosts must be upgraded to 10.0 or later. For more information about configuring data-in-transit encryption, see the *NetBackup Security and Encryption Guide*.

NetBackup 10.0 removes support for direct backup to storage units (non-SLP) in ISM policies

Starting with NetBackup 10.0, support for direct backup to non-SLP storage units in Integrated Storage Manager (ISM) policies has been removed.

ISM backups fail with a 1630 status code if an ISM policy attempts to use non-SLP storage as a backup destination. Before upgrading to NetBackup 10.0, switch all your existing ISM policies to use SLPs instead.

BMR now supports ADK 10 for Windows restores

With this release of NetBackup, Bare Metal Restore (BMR) supports Assessment and Deployment Kit (ADK) 10 for Windows restores.

MSDP disk pool creation in the web UI supports AWS SSE-CMK

The Media Server Deduplication Pool (MSDP) disk pool creation in the NetBackup web UI now supports AWS SSE-CMK (Server-Side Encryption with Customer-Managed Keys).

MSDP cloud immutable storage support for S3-compatible platforms and Azure

NetBackup 10.0 adds the support for the following cloud immutable storage on Red Hat Linux operating system:

- AWS S3-compatible platforms
- Azure blob storage

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

NetBackup for OpenStack supports OpenStack-Ansible

NetBackup 10.0 adds the support for another OpenStack distribution, OpenStack-Ansible. For more information, see *NetBackup for OpenStack Administrator's Guide*.

Guided Recovery for Oracle is no longer supported in OpsCenter

NetBackup 10.0 no longer supports Guided Recovery in OpsCenter. If a client has `ORACLE_METADATA=YES` set on a back-level client, then the backup jobs on that client end with a status code 1.

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*.

Snapshot and Recovery of Windows VMs residing on the Google Cloud Platform

You can now use CloudPoint to discover, snapshot, and recover the Windows VM assets running on the Google Cloud Platform (GCP). The support is introduced for the Windows on-host agent, and the agentless feature.

- The Windows agent (on-host or agentless) can discover the attached disks to be able to support file system and application consistent snapshots on GCP.
- You can back up the discovered assets and recover them using granular file/folder restore (GRT) or parameterized restore options from the snapshot recovery points.
- The MSSQL applications can be recovered to the original location or alternate locations.

Supported:

- Windows platforms - Windows server 2012 R2, 2016, and 2019
- Instance types - General purpose, Compute optimized, Memory optimized, GPU.

- MSSQL Server - SQL 2014, SQL 2016, SQL 2017, SQL 2019

Support for configuring license types in the NetBackup web UI

NetBackup 10.0 lets you configure the license types in the web UI for scheduled usage reports that are generated by `netbackup_deployment_insights`. You can also view the notifications that are related to the start and completion of the scheduled runs of `netbackup_deployment_insights`.

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

Change in accessibility of the legacy logs

NetBackup 10.0 sets the permissions on the legacy log directories to a more restrictive but configurable level. This change is designed to prevent unauthorized access to the NetBackup logs, which may contain sensitive information. You can configure the accessibility of the logs as world-readable or non-world-readable. Only the administrative level users or the owner of the logs can view the non-world-readable logs. For more information, see the *NetBackup Logging Reference Guide*.

Notifications, Messages, and Resiliency configuration information are not upgraded

During the upgrade from a pre-NetBackup 10.0 environment to NetBackup 10.0 and later, previous notifications, messages, and Resiliency configuration information is not migrated. Any previously added Resiliency Domains are no longer present on the **Resiliency** tab in the NetBackup web interface.

You must reconfigure after the upgrade completes to rediscover the resiliency domain data. Refer to the referenced tech note for additional information on how to reconfigure VRP after upgrading NetBackup to 10.0.

https://www.veritas.com/support/en_US/article.100052464

For more information, see the *NetBackup 10.0 Upgrade Guide*.

CloudPoint 8.3.x servers require upgrade to NetBackup 9.1.x before upgrading to version 10.0

If your NetBackup 8.3.x server has CloudPoint, you must first upgrade CloudPoint to NetBackup 9.1.x before you upgrade to NetBackup 10.0. Then you can proceed to upgrade NetBackup 8.3.x to NetBackup 10.0. The process for upgrade is as shown:

The process for this upgrade is:

1. Disable the CloudPoint server for maintenance in the NetBackup web UI.
2. Upgrade the CloudPoint server from NetBackup 8.3.x to NetBackup 9.1.x.
3. Upgrade the CloudPoint server from NetBackup 9.1.x to NetBackup 10.0.
4. Enable the CloudPoint server in the NetBackup web UI.
5. Upgrade the NetBackup server from 8.3.x directly to 10.0.

Changes in vCenter plug-in support

Note the following changes and features for the vCenter plug-in:

- The plug-in is installed on the NetBackup server itself and is registered with the desired vCenter.
- This plug-in is based on the new Remote Plug-in Architecture that is provided by VMware version 6.7 U1 and later. Therefore, NetBackup 10.0 is supported from vCenter with version 6.7 U1 and later.
- The plug-in must be registered with each NetBackup primary server which is to be monitored for backups of virtual machines that vCenter servers manage.
- For vCenter 7.0 onwards, registration of multiple primary servers is possible. For versions from 6.7 U1 up to 7.0, it is only possible to register one primary server. Therefore, starting with vCenter 7.0, multiple NetBackup servers can be available for selection during plug-in login.
- It is mandatory to explicitly log in to the plug-in. The user needs to have valid NetBackup user credentials.

  Note: Login is required only when managing recovery and instant recovery. However, it is not needed for monitoring purposes.

- To access and manage the backup and recovery of the virtual machines performed by a specific NetBackup server, you must select the same NetBackup server while logging in to the plug-in.
- The plug-in supports registration only from the primary servers and not the media servers.
- If you have a NetBackup version earlier than version 10.0, continue to use the earlier version of the plug-in along with the new 10.0 version. Otherwise, it is recommended to uninstall the earlier version of the plug-in.
- Version 10.0 of the plug-in is supported for NetBackup 10.0 onwards. Earlier versions of the plug-in do not support NetBackup 10.0 onwards.

- Template-based VM recovery and discovery is not supported by the plug-in.
  Recovery and discovery of VMs created with VMware templates is not supported by the plug-in.
- NetBackup Appliance with vCenter 6.7 is not supported by the plug-in.
  Starting with NetBackup 10.0, the plug-in does not support NetBackup Appliance with vCenter 6.7 U1, U2 and U3. However it supports the NetBackup Appliance with vCenter 7.0.

Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 10.0

If you use cloud storage in your NetBackup environment, you may need to update your cloud configuration file on the NetBackup primary server immediately after you install or upgrade to NetBackup 10.0. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 10.0, 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 2.8.6.

The following cloud support has been added to version 2.8.7 and later but was not included in the NetBackup 10.0 final build:

- Amazon Glacier Instant Retrieval (IR)
- Amazon GovCloud - Glacier Instant Retrieval (IR)- Amazon (S3)
- Asia Pacific (Jakarta) region
- Google (S3) - Asia South2 (Delhi) region
- Google (S3) - Australia-Southeast2 (Melbourne) region
- Google (S3) - North America Northeast2 (Toronto) region
- Quantum Active Archive and ActiveScale Systems - Standard (S3)
- Quantum Active Archive and ActiveScale Systems - Glacier (S3)
- Wasabi (S3) - EU-West-2 (Paris) region

For the latest cloud configuration package, see the following article:

https://www.veritas.com/content/support/en_US/downloads/update.UPD971796

For additional information on adding cloud storage configuration files, refer to the following tech note:

http://www.veritas.com/docs/100039095

File path changes for CloudProvider.xml and cacert.pem

The location of the cloud configuration files, `CloudProvider.xmlfile` and `cacert.pem`, is changed in this release.

You do not need to take any action for this change. Install or upgrade processes for NetBackup 10.0 handle the change to the new paths.

The new file paths are as follows:

- For Windows:
  <installation-path>\NetBackup\var\global\cloud
- For UNIX:
  /usr/openv/var/global/cloud/

Note: Make sure that you do not change the file permission and ownership.

Refer to the *NetBackup Cloud Administrator's Guide* for more details.

Upcoming changes for Oracle instance groups and commands

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 `nboraadm` command with options in the web UI and APIs.

NetBackup Copilot for Oracle with instant access and universal share

You can use universal share to configure the NetBackup Copilot for Oracle (also known as Oracle Copilot) backup, both on appliance and BYO server. You can also create an instant access mount from a specific recovery point and access the backup data directly. An instant access Oracle database can be configured from the web UI or with a REST API.

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

NetBackup for Oracle and NetBackup for DB2 prevent the direct expiration of backup images

Catalog maintenance operations on Oracle and DB2 databases send requests into NetBackup to synchronize the database catalog with the NetBackup catalog. As part of the catalog synchronization, the database may initiate an image expiration (delete) request to the NetBackup catalog. These requests may also come from

the DBA when command-line options are used. For compliance reasons, you may want to prevent the expiration of images in the NetBackup catalog from a database request by using a bp.conf entry on the primary server.

To prevent the expiration of backup images, use the following `bp.conf` entry on the primary server:

```
PREVENT_ORACLE_DIRECT_EXPIRE
PREVENT_DB2_DIRECT_EXPIRE
```

In a clustered primary server environment, these settings should be set and match in all the primary server `bp.conf` files.

For more information, see the *NetBackup for Oracle Administrator's Guide* and the *NetBackup for DB2 Administrator's Guide*.

Plug-in to store the RMAN backups to MSDP storage directly

NetBackup Deduplication Direct for Oracle is a lightweight plug-in that you can use to store the RMAN backups to MSDP storage directly. The Oracle database administrator can control the whole protection and life-cycle stages without NetBackup client. It also enables client-side deduplication to minimize network traffic and improves overall backup speed. For more information, see *NetBackup for Oracle Administrator's Guide*.

Backup and restore of Cassandra clusters

NetBackup 10.0 enables backup and restore of Cassandra clusters with the following supported features:

- Full and differential incremental backups
- Backing up from a geographically co-located data center
- Semantic data deduplication, saving backup storage space
- Granular recovery at the keyspace and column family level
- Alternate recovery to a different cluster or keyspace or column family
- CLI support for backup and restore

For more information, see the *NetBackup 10.0 Cassandra Administrator's Guide*.

Recovery Vault for NetBackup

Recovery Vault for NetBackup provides a public, cloud-based secondary storage as a service (SaaS). Recovery Vault offers a single, flexible repository for on-premises to your public cloud workloads. It is supported on MSDP Cloud and

not supported for native cloud. However, NetBackup lists these providers during native cloud storage server creation.

In NetBackup 10.0, your options for Recovery Vault are:

- NetBackup Recovery Vault Amazon
- NetBackup Recovery Vault Amazon Government
- NetBackup Recovery Vault Azure
- NetBackup Recovery Vault Azure Government
- NetBackup Recovery Vault Seagate Lyve Cloud

Recovery Vault requires its own license. It is a subscription-based license. Contact your account manager or sales team to learn more and get started with Recovery Vault.

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

NetBackup 10.0 includes the following capabilities for Bare Metal Restore in the NetBackup web UI:

- View and manage the clients that are backed up for VM conversion.
- Convert BMR-enabled backups to a virtual machine using the Virtual Machine Conversion wizard.
- Create point-in-time configurations.
- View and manage VM conversion tasks.

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

Chapter 3

Operational notes

This chapter includes the following topics:

- About NetBackup 10.0 operational notes
- NetBackup installation and upgrade operational notes
- NetBackup administration and general operational notes
- NetBackup administration interface operational notes
- NetBackup Cloud operational notes
- NetBackup with Veritas CloudPoint 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 10.0 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 10.0.

If NetBackup 10.0 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 10.0 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 VRTSpbx.rpm VRTSnbclt.rpm VRTSpddea.rpm
```

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

Starting with NetBackup 8.0, all NetBackup server names must use a host name that is complaint with RFC 1123 ("Requirements for Internet Hosts - Application and Support") and RFC 952 ("DOD Internet Host Table Specification") standards. These standards include the supported and unsupported characters that can be used in a host name. For example, the underscore character (_) is not a supported character for host names.

More information is available about these standards and about this issue:

RFC 952

RFC 1123

http://www.veritas.com/docs/000125019

These standards should be applied to all computing hosts, including all NetBackup hosts. To accommodate legacy environments and functionality, features of NetBackup that were implemented before 2010 continue to allow some non-compliant characters. But newer features, as well as more recently integrated 3rd-party components, are not tested with nor expected to be compatible with host names that do not adhere to the industry standards.

In some situations, it may be possible to configure name services with a network hostname alias that is standards-compliant, and then use the alias when you configure NetBackup. But using host names that are standards-compliant is the only way to ensure compatibility with all features.

About support for HP-UX Itanium vPars SRP containers

Hewlett Packard Enterprise (HPE) introduced a new type of container for HP-UX Virtual Partitions (vPars)-enabled servers called Secure Resource Partitions (SRPs). As part of the security changes introduced by SRPs, native HP-UX install tools such as `swinstall` and `swremove` are disabled from being 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 10.0.

Permissions necessary for redirected restores with non-root service user accounts

If you use a non-root service user account, specific access must be allowed for that user when you add files to the `/usr/openv/netbackup/db/altnames` directory. The service user account must have full access to these files through the ownership or group and the permissions. For example, if the service user is `svcname` and its group is `srvgrp`, the file can have permissions of `400`. If the file owner is for a different user and group, the file permissions must allow access to the service user. For example, `777`. Equivalent permission settings must be used in a Windows environment.

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.

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 10.0.

For more information about the specific NetBackup administration interfaces, refer to the NetBackup Web UI Administrator's Guide or the NetBackup Administrator's Guide, Volume I.

For information about how to install the interfaces, refer to the NetBackup Installation Guide. For information about platform compatibility with the administration consoles, refer to the various NetBackup compatibility lists available on the Veritas Support website.

See “About NetBackup compatibility lists and information” on page 66.

Certain NetBackup web UI nodes do not work when NBAC is configured in the 'Required' or 'Automatic' mode

If the NetBackup Access Control (NBAC) is configured in the 'Required' or 'Automatic' mode in your NetBackup environment, the following nodes in the NetBackup web UI do not work as expected:

- Bare Metal Restore
- Catalog Management
- Host Properties

Some columns in the web UI are not searchable

Some columns in tables throughout the NetBackup web UI are not searchable. For example in **Hosts > Host properties**, the **Host type** column is not searchable. If you enter *Client* in the search field, the web UI returns the message *No data to display*, even though Client may appear in the table as a Host type. (Some other columns, such as **Host** are searchable.)

Delay in NetBackup web UI when adding or removing columns in Catalog area

In the **Catalog** area of the web UI, you can add or remove columns from the table of images. The more images that are displayed, the longer it takes to for the interface to refresh if you add or remove columns. This issue will be fixed in an upcoming release.

Job actions not available for workload administrators with limited RBAC permissions on assets

Note following issues for view and managing jobs with the NetBackup web UI:

- A job does not receive an asset ID until it runs, which means a queued job does not have an asset ID. Users that have roles with more granular asset permissions for a workload are not able to view or cancel queued jobs.
  This behavior does not affect users with an RBAC role that has full job permissions or a role that can manage all assets for a particular workload.
- A job does not receive an asset ID if the asset is not yet discovered. Users that have roles with more granular asset permissions for a workload are not able to cancel or restart a job for the asset.
  This behavior does not affect users with an RBAC role that has full job permissions or a role that can manage all assets for a particular workload.

Example 1 - VMware administrator with limited asset permissions cannot cancel any queued jobs

Consider a user that has RBAC permissions only for a VMware vCenter or one or more VMs.

- The user cannot see queued jobs for the vCenter or for the VMs.
- Similarly, the user is not able to cancel any queued jobs for the vCenter or for the VMs.

Example 2 - VMware or RHV administrator with limited asset permissions cannot cancel or restart jobs for undiscovered assets

Consider a user that has RBAC permissions only for a VMware vCenter or an RHV server. This user also has one or more job permissions for these assets, but does not have job permissions for all workload assets.

- A new asset is added to the environment, but the discovery process hasn't run yet.
- An existing intelligent group is configured so it includes the new asset.
- When the backup runs, it includes the new asset in the backup.
- The user is not able to cancel or restart a job for the new asset.

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 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 10.0.

Provider configuration for Azure Stack Hub fails with error “Authentication failed: invalid_instance”

Provider configuration for Azure Stack Hub fails if the Authentication type is AAD and the optional parameter `Authentication Resource URL` is provided. The configuration fails with the error message: `Authentication failed: invalid_instance`.

This issue is a known issue with the Azure Stack Hub API. It is expected to be fixed in the near future.

Workaround:

Do not use the optional parameter `Authentication Resource URL` while configuring provider for Azure Stack Hub.

Restore of cloud VM backup images replicated with AIR fails Pre-recovery check

Restore of cloud VM backup images replicated to another NetBackup domain using Auto Image Replication (AIR) with a NetBackup version earlier than 10.0 fails during Pre-recovery check with the error `exception: Illegal xml request string!.`

AIR is supported for cloud VM backup images from NetBackup version 10.0 onwards. As this feature is new, AIR backup images of cloud virtual machines replicated to an earlier version of NetBackup domain such as 9.1 is not supported. The NetBackup domain primary server version should be 10.0 or higher. You might encounter the error if the primary server version of the NetBackup target domain is earlier than 10.0.

Workaround:

Make sure that the target NetBackup domain primary server version is 10.0 or higher.

Error in calculating the snapshot size in smart metering for Cloud workloads

Errors can be observed in calculating the snapshot size for cloud workloads due to which the NbDeployutil Capacity Report might report the total volume size as the snapshot size, instead of the actual used size. Refer to the log to identify the warning message.

This situation can happen due to the following reasons:

- Insufficient permissions to obtain the snapshot size in case of AWS, Azure, or Azure Stack Hub plug-ins. Check to see if the following permissions are added in the plug-in configurations:
  For AWS:

  ```
  "ebs:ListSnapshotBlocks",
  ```

  For Azure and Azure Stack Hub:

  ```
  "Microsoft.Compute/snapshots/beginGetAccess/action",
  "Microsoft.Compute/snapshots/endGetAccess/action",
  ```

- Maximum requests limit is reached for the cloud API's that are used for calculating the snapshot size.
- Maximum retries were exceeded for connecting with the network.

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 10.0.

Offline VM backup fails with status code 156

Offline backup of a virtual machine VM fails with status code 156 if the credentials are added for agentless file and folder recovery.

This behavior occurs because NetBackup tries to take an application-consistent snapshot of the VM, which fails because the VM is offline and CloudPoint cannot connect to the agent.

Restoring a VM (with a Read-only disk) from an app-consistent snapshot fails

For a Windows VM, the snapshot fails with a VSS error, like the following; hence the VM cannot be restored.

```
Failure: flexsnap.GenericError: Failed to take snapshot(error:Failed
to create VSS snapshot of the selected volumes.)"
```

For a Linux VM, the snapshot may or may not be successful for a VM under which the disk is discovered, but it will fail for other VMs due to the missing dependencies.

Error example:

```
linear_flow.Flow: create snapshot(test-win) of host
linux-1(len=4)'requires['snap_google-gcepd-us-west2-b-7534340043132122994']

but no other entity produces said requirements\n MissingDependencies
```

In the above case, if a snapshot is successful for a Linux VM, a Read-only disk is restored in a Read/write mode.

Editing a query with special characters in tag names is not supported for the intelligent Cloud groups

While you create an intelligent Cloud group, if you specify a query that has the asset tag names (referenced from your cloud provider) containing spaces or special characters such as `(, ), &, \, /, ", ‘, [, ],{,` or `}`, you cannot later edit the query to modify any parameters.

This does not prevent you from successfully creating the intelligent group and applying the protection plan to it. Only the **Edit query** functionality is affected with this limitation.

Workaround:

To avoid this issue, ensure that the tag names do not contain the specified special characters and then create a new query with the new tag names.

Starting or restarting the CloudPoint services may fail if a stale IP address entry is retained in the Podamn layer on RHEL 8.3 environment

Sometimes the following error may be encountered when the CloudPoint service containers restart.

```
Error adding network: failed to allocate for
 range 0: 10.89.0.140 has been allocated to
 02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc,
 duplicate allocation is not allowed
ERRO[0000] Error while adding pod to CNI network
 "flexsnap-network": failed to allocate for
 range 0: 10.89.0.140 has been allocated to
 02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc,
 duplicate allocation is not allowed
Error: error configuring network namespace for container
 02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc:
 failed to allocate for range 0:
 10.89.0.140 has been allocated to
 02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc,
 duplicate allocation is not allowed"
```

The issue exists in the Podman subsystem which fails to remove the existing IP allocated for the container from dir `/var/lib/cni/networks/flexsnap-network/`, when the container is stopped.

Workaround:

1. Find the stale IP address, which is retained when the containers are stopped. For example 10.89.0.140 in the above error.
2. Run the following command to delete the stale entry from`dir /var/lib/cni/networks/flexsnap-network/`:

   ```
   # rm /var/lib/cni/networks/flexsnap-network/10.89.0.140
   ```

3. Start the service:

   ```
   # podman start <service-name>
   ```

VM disks not displayed due to discovery level

After you restore a VM from backup copy, the VM disks are not displayed in the **Volumes** tab of the **Virtual machine** details page. The CloudPoint server's level discovery is not able to map the virtual machine disks with the virtual machine because it requires deep discovery at the configuration level.

Workaround:

Run deep discovery manually. Select a configuration for the provider and click **Discover**. Alternatively, you can wait for a periodic autodiscovery to run, which performs deep discovery.

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

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 for NDMP operational notes

NetBackup for NDMP is an optional NetBackup application. It enables NetBackup to use the Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems. This topic contains some of the operational notes and known issues that are associated with NetBackup for NDMP in NetBackup 10.0.

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 for OpenStack operational notes

NetBackup for OpenStack is an optional NetBackup application. This topic contains some of the operational notes and known issues that are associated with NetBackup for OpenStack in NetBackup 10.0.

CentOS repository mirror URL is updated

The CentOS repository mirror URL is updated to `vault.centos.org` from `mirror.centos.org`. You must update it in all Yum repository files located at `/etc/yum.repos.d/CentOS-*`.

On compute node, you must make the `CentOS-OpenStack-ussuri.repo` file immutable during the deployment. Run the following command to make the file immutable:

```
chattr +i /etc/yum.repos.d/CentOS-OpenStack-ussuri.repo
```

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

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

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

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

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

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

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

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

Instance volumes in the incremental backups cannot be mounted

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

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

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

Workaround:

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

NetBackup version is displayed as 'NetBackupforOpenStack_10.0.1Beta1' instead of 'NetBackup-CentOS3.10.0 9.0' on the Web UI

On NetBackup VM, version **NetBackup-CentOS3.10.0 9.0** is displayed under `/usr/openv/netbackup/bin/version`. NetBackup Web UI does not display the same version and displays **NetBackupforOpenStack_10.0.1Beta1** 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 policy contains snapshots. Please delete all snapshots and try again.`
- `Success: Deleted: <policy name>`

Unable to connect to NetBackup primary server using NBCA

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

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

Workaround:

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

For more information, see the following Support article:

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

Excluded Ceph Volume after restore is not mountable or formattable

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

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

Restored VMs have blank metadata config_drive attached

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

Workaround:

Delete metadata `config_drive` or set the desired value.

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

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

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

Workaround:

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

Database does not sync after NetBackup cluster gets new nodes

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

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

Workaround:

Run the policy import from CLI.

Data on boot disk gets backed up despite exclusion

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

After reinitialization and import, OpenStack certificates are missing

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

Workaround:

Upload the certificates again.

CLI import changes scheduler trust value to disabled

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

Workaround:

Configure NetBackup with import option from UI after reinitialization.

Unable to get node details after you reinitialize the NetBackup Appliance

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

Workaround:

Restart `nbosjm-policies` and `nbosjm-cron` services on NetBackup nodes.

```
systemctl restart nbosjm-policies
```

```
systemctl restart nbosjm-cron
```

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

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

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

Workaround:

Contact Veritas Support to implement a known workaround.

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

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

Workaround:

Configure the NetBackup appliance with OpenStack CA provided.

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

NetBackup internationalization and localization operational notes

This topic contains some of the operational notes and known issues that are associated with internationalization, localization, and non-English locales in NetBackup 10.0.

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 (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 10.0.

Snapshot job fails with status code 927

Snapshot job fails with status code 927: No backup host from configured backup host pool is available for job execution.

This issue appears when you do not upgrade at least one backup host from the pool, along with primary server upgrade from NetBackup 8.3 to NetBackup 9.1. This situation fails the accelerator-enabled DNAS policy for NAS.

Workaround:

Upgrade the primary server along with at least one of the backup hosts from the backup host pool from NetBackup 8.3 to NetBackup 9.1. Then run the accelerator-enabled DNAS policy for NAS.

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 10.0.

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 10.0.

Discovery fails for policies with queries that contain "&" in VM displayName values

VM discovery fails for VMware policies with queries that contain `&` (ampersand characters) in the VM `displayName` value. This behavior occurs when you use the NetBackup web UI to create a VMware Intelligent Policy with the Query Builder.

Workaround:

To configure a VMware Intelligent Policy that uses `&` in the VM `displayName` value, use the NetBackup Administration Console. Alternatively, you can create a policy that specifies the particular VMware VM rather than using the Intelligent Policy method.

Backup of a virtual machine fails with status code 11

A backup of a VMware virtual machine (VM) may fail with status code 11 if an associated `fstab` file entry is longer than 90 characters.

Workaround:

Make sure that entries in the `fstab` file are limited to 90 characters or less.

Appendix A

About SORT for NetBackup Users

This appendix includes the following topics:

- About Veritas Services and Operations Readiness Tools

About Veritas Services and Operations Readiness Tools

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

Access SORT from the following webpage:

https://sort.veritas.com/netbackup

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

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

- **Custom Reports**
  Use this tool to get recommendations for your system and Veritas enterprise products.
- **NetBackup Future Platform and Feature Plans**
  Use this tool to get information about what items Veritas intends to replace with newer and improved functionality. The tool also provides insight about what items Veritas intends to discontinue without replacement. Some of these items include certain NetBackup features, functionality, 3rd-party product integration, Veritas product integration, applications, databases, and the OS platforms.

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

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

Appendix B

NetBackup installation requirements

This appendix includes the following topics:

- About NetBackup installation requirements
- Required operating system patches and updates for NetBackup
- NetBackup 10.0 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 and the NetBackup Upgrade Guide.

See "NetBackup installation and upgrade operational notes" on page 34.

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- Database rebuilds are likely to occur in each major, minor (single-dot), and release update (double-dot) version of NetBackup. Therefore, before upgrading to NetBackup 10.0, 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/openv/db/data` (UNIX) or `<install_path>\Veritas\NetBackupDB\data` (Windows) directories. If you have changed the location of some of the files in either of these directories, free

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

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

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

Required operating system patches and updates for NetBackup

NetBackup server and client installations are only supported on a defined set of operating systems (OSs) that are listed in the NetBackup compatibility lists. Most OS vendors provide patches, updates, and service packs (SPs) for their products. The best practice of NetBackup Quality Engineering is to test with the latest SP or update level of the OS when a platform is tested. Therefore, NetBackup is supported on all vendor GA updates (n.1, n.2, and so on) or SPs (SP1, SP2, and so on). However, if a known compatibility issue exists on a specific SP or updated OS level, this information is identified in the compatibility lists. If no such compatibility issues

are noted, Veritas recommends that you install the latest OS updates on your servers and clients before you install or upgrade NetBackup.

The 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 10.0. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 10.0 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 66.

See "About Veritas Services and Operations Readiness Tools" on page 56.

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 primary servers and media servers to ensure proper client functionality.

Table B-1 Required operating system patches and updates for NetBackup 10.0

Operating system type and version	NetBackup role	Patch	Notes
Beijing Linx Software Corp Linx OS	Primary, media, client	Kernel 2.6.32.26 or later	
CentOS 6.x	Primary, media, client	Kernel 2.6.32-608.el6 or later	
CentOS 7.x	Primary, media, client	Kernel 3.10.0-241.el7 or later	
Debian 8	Primary, 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 10.0 *(continued)*

Operating system type and version	NetBackup role	Patch	Notes
HP-UX IA-64	Client only	Networking.NET-RUN: /usr/lib/libipv6.sl	
	Client only	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.1	
	Client only	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.sl	
	Client only	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so	
	Client only	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so.1	
	Client only	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so	
	Client only	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so.1	
	Client only	Networking.NET2-RUN: /usr/lib/libipv6.1	
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	Primary, 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	Primary, 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 10.0 *(continued)*

Operating system type and version	NetBackup role	Patch	Notes
SUSE Linux 12	Primary, 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 10.0 binary sizes

Table B-2 contains the approximate binary sizes of the NetBackup 10.0 primary server, media server, and client software for the various supported operating systems. These binary sizes indicate the amount of disk space occupied by the product after an initial installation. Note that for the sizes listed in the table, 1 MB equals 1024 KB.

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

Note: Table B-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 Compatibility List for all Versions.

Table B-2 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	64-bit client	64-bit server	Notes
AIX	POWER	1853 MB	No longer supported	
Canonical Ubuntu	x86-64	1521 MB		

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

OS	CPU Architecture	64-bit client	64-bit server	Notes
CentOS	x86-64	1521 MB	7052 MB	
Debian GNU/Linux	x86-64	1521 MB		
HP-UX	IA-64	2389 MB	No longer supported	
Oracle Linux	x86-64	1521 MB	7052 MB	
Red Hat Enterprise Linux Server	POWER	307 MB		
Red Hat Enterprise Linux Server	x86-64	1521 MB	7052 MB	
Red Hat Enterprise Linux Server	z/Architecture	1023 MB	No longer supported	Media server or client compatibility only.
Rocky Linux client		1521 MB		
Solaris	SPARC	1377 MB	No longer supported	
Solaris	x86-64	1370 MB	No longer supported	
SUSE Linux Enterprise Server	POWER	309 MB		
SUSE Linux Enterprise Server	x86-64	1288 MB	5474 MB	
SUSE Linux Enterprise Server	z/Architecture	1037 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64	514 MB	3899 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 Server and **ViewBuilder** for the various operating systems that are compatible with NetBackup OpsCenter 10.0.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Server	ViewBuilder
Oracle Linux	x86-64	716 MB	
Red Hat Enterprise Linux Server	x86-64	715 MB	
SUSE Linux Enterprise Server	x86-64	729 MB	
Windows Server	x86-64	669 MB	225 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.

Appendix C

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: 10.0 OpsCenter server > 9.0 primary server > 8.3 media server > 7.7.3 client.

All NetBackup versions are four digits long. The NetBackup 10.0 release is the 10.0.0.0 release. Likewise, the NetBackup 9.1 release is the NetBackup 9.1.0.0 release. For the purposes of supportability, the fourth digit is ignored. A 9.1 primary server supports a 9.1.0.1 media server. Likewise, a 9.1.0.1 primary supports a 9.1 OpsCenter server. An example of what is not supported is a 9.1 OpsCenter server with a 10.0 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 56.

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 56.

About changes in platform compatibility

The NetBackup 10.0 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

Appendix D

Other NetBackup documentation and related documents

This appendix includes the following topics:

- About related NetBackup documents

About related NetBackup documents

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

Not all documents are published with each new release of NetBackup. In the guides, you may see references to other documents that were not published for NetBackup 10.0. 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.
