NetBackup™ Release Notes

Release 9.1

Document Version 4

VERITAS™

NetBackup™ Release Notes

Last updated: 2022-02-03

Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

About NetBackup 9.1

This chapter includes the following topics:

About the NetBackup 9.1 release

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

See "About new enhancements and changes in NetBackup" on page 12.

About EEBs and release content

NetBackup 9.1 incorporates fixes to many of the known issues that affected customers in previous versions of NetBackup. Some of these fixes are associated with the customer-specific issues. Several of the customer-related fixes that were incorporated into this release were also made available as emergency engineering binaries (EEBs).

Listings of the EEBs and Etracks that document the known issues that have been fixed in NetBackup 9.1 can be found on the Veritas Operations Readiness Tools (SORT) website and in the NetBackup Emergency Engineering Binary Guide.

See "About Veritas Services and Operations Readiness Tools" on page 67.

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

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

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

See "About the NetBackup 9.1 release" on page 10.

See "About NetBackup compatibility lists and information" on page 77.

NetBackup 9.1 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 9.1 are grouped below by category. Select a link to read more information about the topic.

New features

- Changes in Veritas terminology
- Backup and restore of Kubernetes applications
- Backup anomaly detection in NetBackup
- Non-privileged user or service user account to run NetBackup services
- Support for AD user groups in the `auth.conf` file
- 2 FA support for the NetBackup Administration Console through SAML-based Identity Provider or CAC/PIV smart cards or user certificates
- NetBackup Client Direct deduplication is now supported with WORM
- Case insensitivity for client names in a NetBackup policy
- RESTful APIs included in NetBackup 9.1
- API keys enhancements
- BMR enhancements
- NetBackup support for vCloud Director 9.0, 9.1, and 9.5 has ended
- nbdeployutil renamed to NetBackup Deployment Insights
- About the NetBackup Smart Diagnosis (`nbsmartdiag`) utility

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 9.1 from a release earlier than 8.1, make sure that you read and understand the *NetBackup Read This First for Secure Communications* document. NetBackup 8.1 includes many enhancements that improve the secure communications of NetBackup components. The *NetBackup Read This First for Secure Communications* document describes the features and benefits of these enhancements:

  NetBackup Read This First for Secure Communications

Support changes and enhancements

- EOL for support on RHEL 7.0 through 7.3
- EOL for CentOS 8 support
- NetBackup 9.1 support additions and changes
- Several shutdown commands to be deprecated in a future release

Installation, upgrade, and configuration changes and enhancements

- Windows compiler and security requirements for NetBackup 9.1 and later installation and upgrade

RBAC-related changes and enhancements

- New RBAC default roles
- Changes to the RBAC permissions for jobs

Cloud-related changes and enhancements

- Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 9.1
- EOL for CloudPoint version 2.x
- Automated asset protection with intelligent cloud groups
- Changes to Cloud protection policies
- CloudPoint extensions for scalable workflows
- New backup options for cloud workloads
- Backup from snapshot
- Parameterized restore
- Windows agentless support
- Support for Microsoft Azure Stack Hub
- Support for CloudPoint on an RHEL 8.3 Podman environment
- Support for CloudPoint on SUSE Linux Enterprise Server (SLES)
- Combined deployment of NetBackup family products
- Cloud enhancements for administrators

Virtualization changes and enhancements

- Continuous data protection (CDP) provides backup for VMware without stunning the VMs
- Instant rollback for VMs
- For VMware and RHV environments, reduce the size of the job database before upgrade
- Query options added for VMware intelligent policies
- Nutanix AHV enhancements

Database agent changes and enhancements

- Oracle Instance Management to be removed from NetBackup Administration Console
- NetBackup Oracle Intelligent Policy can be configured with options for Data Guard
- Oracle and DB2 policy templates are deprecated in the NetBackup 9.1 release
- NetBackup for Microsoft SQL Server agent enhancements
- New behavior for Oracle and Microsoft SQL Server intelligent policies

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.

In NetBackup 9.1, the following terms have been updated:

Deprecated term	New term
Master	Primary (only in the NetBackup web UI)
Slave	Secondary or media server
Whitelist or white list	Allowed list
Blacklist or black list	Blocked list
White hat	Ethical

Deprecated term	New term
Black hat	Unethical

Backup and restore of Kubernetes applications

NetBackup enables end-to-end workflow to enable backup and restore of Kubernetes applications in the form of namespaces.

- New, light-weight NetBackup Kubernetes Operator Service (NBUKops) to be deploy on the Kubernetes clusters.
- Configuration of Kubernetes cluster and secure credential management.
- Automatic and on-demand Kubernetes asset discovery.
- Kubernetes asset service plug-in.
- RBAC at the granularity of cluster and namespace level.
- Protection plan based backups at namespace level.
- Versatile recovery options, like complete namespace, an individual custom resource or an individual persistent volume.
- Image lifecycle management with customizable retention and cleanup.
- Resource throttling per Kubernetes cluster.
- Capacity licensing, integration with Veritas Usage Insight.

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

Backup anomaly detection in NetBackup

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

The following backup job metadata, attributes, or features are verified during backup anomaly detection:

- Backup image size
- Number of backup files
- Data that is transferred in KB
- Deduplication rate
- Backup job completion time

Any unusual deviation in these backup job attributes is considered to be an anomaly and is notified using the NetBackup web UI.

For more information on the anomaly detection, refer to the NetBackup Security and Encryption Guide.

Non-privileged user or service user account to run NetBackup services

Starting with NetBackup 9.1, most of the master server services can be run with a non-privileged user or non-root user, which is highly recommended. The non-privileged user is referred to as service user and is intended to run only NetBackup services.

For more information on the service user account, refer to the NetBackup Security and Encryption Guide.

Support for AD user groups in the `auth.conf` file

You can now add Active Directory (AD) groups in the `auth.conf` file. This support is added only for master servers.

User groups are defined using the `<GRP>` tag in the `auth.conf` file.

For more information on the feature, refer to the NetBackup Security and Encryption Guide.

2 FA support for the NetBackup Administration Console through SAML-based Identity Provider or CAC/PIV smart cards or user certificates

You can now log on to the NetBackup Administration Console using CAC/PIV, smart cards, or user certificates or SAML-based IDP providers.

NetBackup Client Direct deduplication is now supported with WORM

Starting with NetBackup 9.1, NetBackup Client Direct deduplication (client-side deduplication) is now supported with WORM if the client being used to perform the client-side deduplication is at version 9.1 or greater.

Case insensitivity for client names in a NetBackup policy

If you create a policy with "client_1" and "Client_1" as client names, NetBackup lets you save the policy.

Update the `bp.conf` file using the `bpsetconfig` command. Set `CASE_INSENSITIVE_HOSTNAME_VALIDATION = YES` to force NetBackup to select for different character case in client names. The check is performed before NetBackup saves the policy. The policy is not saved until the client name issue is fixed.

If policies exist containing client names, using a different character case, before the `CASE_INSENSITIVE_HOSTNAME_VALIDATION` setting is enabled, the client names are not flagged. Changes to these policies, which are made using the NetBackup Administration Console, are not flagged as errors unless the client names are modified.

RESTful APIs included in NetBackup 9.1

NetBackup 9.1 includes both updated and new RESTful application programming interfaces (APIs). These APIs provide a web-service-based interface that lets you configure and administer NetBackup in your environments.

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

- On your master server
  APIs are stored in YAML files on the master server:
  `https://<master_server>/api-docs/index.html`
  The APIs are documented in Swagger format. This format lets you review the code and test the functionality by making actual calls with the APIs. You must have the appropriate security permissions to access the master server and APIs to use the Swagger APIs.

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

- On SORT
  NetBackup API documentation is also available on SORT:
  HOME > KNOWLEDGE BASE > Documents > Product Version > 9.1
  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.

Access control on jobs

The current version of several jobs APIs have added, finer-grained access control based on workload assets. Access to jobs can still be configured globally granting

operations to all jobs by using the `|MANAGE|JOBS|` namespace. Now, access to jobs can be limited to specific workloads and even specific assets for which the jobs have been run. Object-level access to backup and restore jobs is enforced based on the access control ID (namespace) of the asset for which the job was created.

Previously, the permission to change the job state was controlled by a single update operation. Additional job-specific operations have been added to allow an administrator the ability to grant suspend, restart, resume and cancel jobs independently.

Previous versions of job APIs included the notion of "initiator-based" access control in which a user that initiates a backup job has full privilege on that job regardless of operations granted by an administrator. In this release, the initiator-based access has been removed in lieu of asset-based object-level access control.

New APIs

NetBackup 9.1 includes these new and enhanced APIs:

- Agentless Hosts: Manage agentless hosts.
- iSCSI Settings: Manage global iSCSI settings for AHV workloads.
- Policies: Support for VMware policy type and new snapshot configuration validation.
- SAML Certificates: Manage SAML certificates for single sign-on based authentication.
- SLP: Update and check for conflicts with storage lifecycle policies (SLP).
- SLP Settings: Manage the global storage lifecycle policy (SLP) settings.
- SLP Windows: Manage storage lifecycle policy (SLP) windows.
- Snapshot Management Server Extensions: Manage extensions registered with the CloudPoint server.
- Snapshot Providers - Azure Domains: Retrieves information about configured Azure domains.
- Recovery
  - Cloud: Pre-recovery check for cloud asset recovery.
  - Nutanix AHV: Full AHV VM recovery. Individual file and folder recovery both with NetBackup client and agentless.
  - Oracle: Complete Oracle database recovery.
  - Physical: Granular file and folder recovery from a physical system.

  - VMware: Instant-Sync VM recovery.
- User Certificate Login: Allows for client certificate authentication with an X.509 certificate.
- `GET /catalog/image-contents`
  This existing API has been augmented to support the request header `X-NetBackup-All-Copies`. This header is a boolean that indicates it should return all backups for each path in the date range rather than only the latest.

Versioned APIs

Jobs

The following attributes were removed from the job detail response in V6.0:

`initiatorId`

The following attributes were added to the job detail response in V6.0:

Attribute	Type
`dteMode`	String
`dedupSpaceRatio`	Float
`compressionSpaceRatio`	Float
`workloadDisplayName`	String

Other changes to Jobs APIs include:

- `GET:/admin/jobs`
  A new cursor-based pagination strategy has been implemented for the list jobs APIs.
  RBAC enforcement has been expanded to include object-level enforcement based on workload assets.
  A new operation, `|OPERATIONS|MANAGE|JOBS|VIEW|`, has been introduced to grant view permission on an asset-based job. This allows an administrator to delegate access to a job independently of the asset for which a job is run.
  Initiator-based enforcement has been removed. Object-level enforcement support has made the initiator-based enforcement redundant.
- `GET:/admin/jobs/{jobId}`
  `GET:/admin/jobs/{jobId}/progress-logs`
  `GET:/admin/jobs/{jobId}/try-logs`

`GET:/admin/jobs/{jobId}/try-logs/{attempt}`
`GET:/admin/jobs/{jobId}/file-lists`

RBAC enforcement has been expanded to include object-level enforcement based on workload assets.
A new operation, `|OPERATIONS|MANAGE|JOBS|VIEW|`, has been introduced to distinguish the ability to view a job and the asset for which jobs are run.
Initiator-based enforcement has been removed. Object-level enforcement support has made the initiator-based enforcement redundant.

- `GET:/admin/jobs/{jobId}/cancel`
  `GET:/admin/jobs/{jobId}/suspend`
  `GET:/admin/jobs/{jobId}/resume`
  `GET:/admin/jobs/{jobId}/restart`

  RBAC enforcement has been expanded to include object-level enforcement based on workload assets.
  The ability to cancel, suspend, resume and restart a job can now be granted independently at both the api-level and object-level.
  Initiator-based enforcement has been removed. Object-level enforcement support has made the initiator-based enforcement redundant.

API keys enhancements

This release of NetBackup allows both non-SAML and SAML users to create and delete their own keys and reissue expired keys. The administrator can also add a key for a SAML user and change the expiration date of the key.

BMR enhancements

NetBackup 9.1 includes the following enhancements for NetBackup Bare Metal Restore (BMR):

- BMR client - Support for iSCSI disk for Windows
- BMR client / Boot support for Red Hat Enterprise Linux 7.9
- BMR client / Boot support for Oracle Linux 7.9
- BMR client / Boot support for Red Hat Enterprise Linux 8.3
- BMR client / Boot support for Oracle Linux 8.3

More information about the supported operating systems and patch levels for BMR configurations is available:

NetBackup BMR support with different operating system and its patch releases

NetBackup support for vCloud Director 9.0, 9.1, and 9.5 has ended

VMware Cloud Director versions 9.0, 9.1, and 9.5 is longer supported starting with this release of NetBackup.

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

See "About NetBackup end-of-life notifications" on page 77.

nbdeployutil renamed to NetBackup Deployment Insights

With NetBackup 9.1, `nbdeployutil` is renamed to `netbackup_deployment_insights`. It is recommended to use the NetBackup Deployment Insights tool when you manually generate the license reports.

The tool contains fixes that address the accuracy and performance concerns related to usage reporting. You can continue to use the `nbdeployutil` command with the same options.

About the NetBackup Smart Diagnosis (`nbsmartdiag`) utility

NetBackup Smart Diagnosis (`nbsmartdiag`) utility detects performance issues, such as high CPU utilization, high memory usage, and deadlocks for the registered NetBackup processes. When `nbsmartdiag` utility detects an issue, the appropriate evidence is collected for further troubleshooting, without any user intervention. `nbsmartdiag` is a service (or a daemon) that can be deployed on a NetBackup master server, a media server, or a client. The `nbsmartdiag` service is supported only on Windows and Linux (RHEL and SUSE) platforms.

For more information, see the NetBackup Troubleshooting Guide.

EOL for support on RHEL 7.0 through 7.3

Veritas plans to end-of-life (EOL) NetBackup master servers, media servers, and clients running on Red Hat Enterprise Linux (RHEL) 7.0 through 7.3. These operating systems will no longer be supported platforms and the last release supporting these will be the NetBackup 9.1 release.

You will need to migrate to a supported version of RHEL before attempting to upgrade to later than the NetBackup 9.1 release. RHEL 7.0 through 7.3 master server, media server, and client will continue to be supported on older versions of NetBackup and follow the published Veritas Product End of Life policy guidelines.

EOL for CentOS 8 support

Veritas plans to end-of-life (EOL) support for NetBackup master servers, media servers, and clients running on CentOS 8. The operating system will no longer be a supported platform and the last release supporting these will be the NetBackup 9.1 release.

CentOS 8 will continue to be supported on older versions of NetBackup and follow the published Veritas Product End of Life policy guidelines.

NetBackup 9.1 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 9.1:

- Support for Azure Stack 2008 version for BigData policies
- Support for NetBackup Continuous Data Protection for VMWare workloads
  See "Continuous data protection (CDP) provides backup for VMware without stunning the VMs" on page 30.
- Support for vCloud Director 10.2
- Bare Metal Restore (BMR) support:
  - See "BMR enhancements" on page 21.

The following products and services will no longer be supported after NetBackup 9.1:

- NetBackup master servers, media servers, and clients running on Red Hat Enterprise Linux (RHEL) 7.0 through 7.3.
  See "EOL for support on RHEL 7.0 through 7.3" on page 22.
- NetBackup master servers, media servers, and clients running on CentOS 8.
  EOL for CentOS 8 support

Cloud provider support changes and enhancements

This release of NetBackup includes these cloud provider support changes and enhancements:

- The following cloud providers are now supported:
  - PowerScale (Isilon PowerScale S3 Storage)

- Tencent Cloud (Cloud Object Storage (COS))
- Seagate Lyve Cloud (An on-demand solution for mass capacity storage)
- XSKY (XSKY Enterprise Object Storage)

- These additions and changes apply to regional support for the following cloud providers:
  - Amazon (AWS) regions:
    - Added support for Asia Pacific (Osaka) (ap-northeast-3)
  - IBM COS regions:
    - Added support for Sydney, Australia (s3.au-syd.objectstorage.softlayer.net)
    - Added support for Tokyo, Japan (s3.jp-tok.objectstorage.softlayer.net)
    - Removed support for Melbourne, Australia (s3.mel01.objectstorage.softlayer.net)
    - A name change for EU United Kingdom (s3.eu-gb.objectstorage.softlayer.net)

For more information about cloud vendor support, see the NetBackup Cloud Administrator's Guide.

Several shutdown commands to be deprecated in a future release

A new, fully documented command for shutting down NetBackup processes and daemons will be provided in an upcoming release. At that point, the following commands will no longer be available:

- `bp.kill_all`
- `bpdown`
- `bpclusterkill`

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

Windows compiler and security requirements for NetBackup 9.1 and later installation and upgrade

NetBackup 9.1 and later for Windows uses the Visual Studio 2019 compiler and the Windows 10 Software Development Kit (SDK). The installation and the upgrade process use Microsoft redistributable utilities to install Visual Studio 2019 C++ run-time libraries on Windows hosts where they are not already installed. These

utilities can fail or behave unexpectedly on hosts without all the security updates in place. Windows hosts must have all security updates in place before you install or upgrade to NetBackup 9.1 or later.

More information on the Microsoft redistributable utilities is available:

https://visualstudio.microsoft.com/downloads/

For further information about this issue, see either the NetBackup 9.1 Installation Guide or the NetBackup 9.1 Upgrade Guide.

New RBAC default roles

NetBackup 9.1 includes additional preconfigured roles in RBAC:

- Default AHV Administrator
- Default Kubernetes Administrator
- Default NetBackup Kubernetes Operator Service

You can add users to these roles and use the preconfigured permissions. The name, description, and permissions for these roles cannot be changed. Or, you can create a new role based on one of the default roles and then customize the role permissions to fit your security needs.

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

See the NetBackup 9.1 Web UI Administrator's Guide for more information.

Changes to the RBAC permissions for jobs

The following changes were made to RBAC permissions for jobs in the NetBackup 9.1 release:

- The **Update** operation for jobs is expanded and replaced with the following operations: **Cancel**, **Suspend**, **Resume**, and **Restart**.
- The **Default RHV Administrator** and **Default VMware Administrator** roles include permissions to view, cancel, and restart jobs for RHV or for VMware assets. These roles no longer include the global permission to view all jobs for any asset.
- The previous APIs for VMware and RHV jobs supported an "initiatorId" for job operations. Users that were given jobs permissions in this way can no longer

view jobs after an upgrade to NetBackup 9.1. Update the RBAC roles for these users to include the new permissions for jobs.

- Any roles that you created from the **Default RHV Administrator** and **Default VMware Administrator** templates are not affected. To update a custom role that you created, make the following changes to the RBAC permissions for the role:
  - In **NetBackup management > Global > Jobs**, remove the **View** permission.
  - Depending on how you configured the role, edit the permissions for all the RHV, or VMware assets. Or, edit the permissions for the individual assets.
    - Open the RHV workload and select **RHV settings > Manage permissions**.
    - Open the VMware workload and select **VMware settings > Manage permissions**.
    - Open the asset and click on the **Permissions** tab.

Update cloud configuration file on the primary server immediately after install or upgrade to NetBackup 9.1

If you use cloud storage in your NetBackup environment, you may need to update your cloud configuration file on the NetBackup master server immediately after you install or upgrade to NetBackup 9.1. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 9.1, related operations fail.

Veritas continuously adds new cloud support to the cloud configuration files between releases. Updating your cloud configuration files is necessary only if your cloud storage provider was added to the cloud configuration package after version 2.8.3.

The following cloud support has been added to version 2.8.4 and later but was not included in the NetBackup 9.1 final build:

- Google (S3) - Asia-Northeast3 (Seoul) region
- Google (S3) - Asia-Southeast2 (Jakarta) region
- Google (S3) - Europe-Central2 (Warsaw) region
- IBM (S3) – Amsterdam, Netherlands EU region
- IBM (S3) – Chennai, India region
- IBM (S3) – Frankfurt, Germany EU region
- IBM (S3) – Hong Kong S.A.R. of the PRC region

- IBM (S3) – Mexico City, Mexico region
- IBM (S3) – Milan, Italy EU region
- IBM (S3) – Montréal, Canada region
- IBM (S3) – Osaka, Japan AP region
- IBM (S3) – Oslo, Norway EU region
- IBM (S3) – Paris, France EU region
- IBM (S3) – San Jose, US region
- IBM (S3) – São Paulo, Brazil region
- IBM (S3) – Seoul, South Korea region
- IBM (S3) – Singapore region

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

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

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

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

EOL for CloudPoint version 2.x

Veritas announces the end-of-life (EOL) and end-of-support-life (EOSL) for the standalone distribution of CloudPoint version 2.x and below as of December 31, 2021. CloudPoint features and capabilities have been included in the NetBackup releases beginning with NetBackup version 8.3, as NetBackup CloudPoint.

Automated asset protection with intelligent cloud groups

You can now create and protect a dynamic group of assets by defining the intelligent cloud asset groups based on the query filters. A query also supports identifying the assets based on the asset tags referenced from your cloud provider. An intelligent cloud group automatically reflects changes in the asset environment when the assets are added or removed.

Then when you apply a protection plan to an intelligent cloud group, all the assets satisfying the query conditions will automatically be protected if the asset environment changes in future.

See the NetBackup Web UI Cloud Administrator Guide for more information.

Changes to Cloud protection policies

When you upgrade from a pre-NetBackup 9.1 environment to a NetBackup 9.1 or later environment, changes are made to Cloud protection plans. If the pre-upgrade environment has one protection plan with multiple cloud assets from different cloud provider types, that plan is split into one protection plan per cloud provider type after upgrade. The assets are distributed among the new protection plans based on the cloud provider type. For example, if there was a **WeeklyBackups** protection plan that contained Amazon, Azure, and Google assets, it is split as shown:

- **WeeklyBackups**: Contains only the Amazon assets.
- **WeeklyBackups_azure**: Contains only the Azure assets.
- **WeeklyBackups_gcp**: Contains only the Google assets.

CloudPoint extensions for scalable workflows

With the CloudPoint extensions, you can now elastically scale out and scale in the compute infrastructure that can concurrently service larger number of jobs as required. The extension resources are provisioned and deprovisioned automatically depending on the requests that are made by the CloudPoint server. This enhances the capacity and performance of the CloudPoint server. You can also manually enable or disable or uninstall extensions.

These CloudPoint extension environments are supported:

- On-premises, VM-based extension
- On-cloud, managed Kubernetes cluster-based extension (currently supported for Azure)

See the NetBackup CloudPoint Install and Upgrade Guide for more information.

New backup options for cloud workloads

NetBackup 9.1 includes the following new backup options for cloud workload.

- For Google cloud:
  Enable the Regional Snapshot option to specify whether the snapshots should be stored in the same region in which the asset exists. You can take low-cost regional snapshots in GCP. These snapshots can be 23% cheaper without any significant loss in resiliency or availability and provides greater control for enterprise users.
- • For Azure and Azure Stack Hub:
  Specify a snapshot destination resource group to associate snapshots to a particular peer resource group in the same region in which the asset exists.

For more information, see the following guides:

- NetBackup Web UI Administrator's Guide
- NetBackup Web UI Cloud Administrator's Guide
- NetBackup CloudPoint Install and Upgrade Guide

Backup from snapshot

You can set up a storage lifecycle policy using snapshots. Make a backup copy in a storage-optimized format that is sent to any supported storage tier of the same cloud. You can designate alternative locations such as a different cloud, or back to their own data center.

For more information, see the following guides:

- NetBackup Web UI Administrator's Guide
- NetBackup Web UI Cloud Administrator's Guide

Parameterized restore

While restoring the VMs, you can now change certain parameters for Azure and Azure Stack workloads. Like restoring to a separate subscription ID, restoring to a separate resource group, change the power state after restoring, and so on.

For more information, see the following guide:

- NetBackup Web UI Cloud Administrator's Guide

Windows agentless support

You can now protect assets on Windows platform, using CloudPoint's agentless feature to reduce resource footprint on the protected machines.

For more information, see the following guide:

- NetBackup CloudPoint Install and Upgrade Guide

Support for Microsoft Azure Stack Hub

NetBackup can now discover and protect your assets residing within the Microsoft Azure Stack Hub 2008 environment. The Azure Stack Hub lets you create, delete, and restore snapshots at the virtual machine level and the managed disk level.

For more information, see the following guide:

- NetBackup CloudPoint Install and Upgrade Guide

Support for CloudPoint on an RHEL 8.3 Podman environment

You can now install CloudPoint on a Red Hat Enterprise Linux 8.3 system which runs a Podman container ecosystem. In case of upgrade, if your current CloudPoint server is installed on a RHEL7.x host, then you first need to migrate the CloudPoint server to an RHEL 8.3 host, and then perform the upgrade using the Podman commands provided in the documentation.

For more information, see the following guide:

- NetBackup CloudPoint Install and Upgrade Guide

Support for CloudPoint on SUSE Linux Enterprise Server (SLES)

You can now install CloudPoint on a system running the SUSE Linux Enterprise Server (SLES) OS. Supported version is SLES 15 SP2.

For more information, see the following guide:

- NetBackup CloudPoint Install and Upgrade Guide

Continuous data protection (CDP) provides backup for VMware without stunning the VMs

NetBackup 9.1 introduces continuous data protection (CDP) to provide backup for VMware without stunning the virtual machines (VMs). Here are some features:

- Continuous data protection for VMware VMs to provide low-RPO (up to 30 minutes) backup through the NetBackup web UI.
- CDP supports Accelerator backup for MSDP-based and OST-based storage in addition to agentless single file restore.
- Resource throttling based on CDP gateway.
- API and RBAC support for CDP and gateway management

For more information, see *Continuous data protection* in the NetBackup 9.1 Web UI VMware Administrator's Guide

Combined deployment of NetBackup family products

Now you can deploy NetBackup, CloudPoint, and Veritas Resiliency Platform, easily from the Cloud Marketplace. The Cloud Marketplace provides a digital catalog of software ready to deploy on public cloud platforms. You can easily find, test, buy, deploy, and manage software on cloud.

For more information, see the following guide:

- NetBackup CloudPoint Install and Upgrade Guide

Cloud enhancements for administrators

NetBackup 9.1 includes the following enhancements:

- The NetBackup Web UI Administrator can grant RBAC permissions for:
  - Managing intelligent cloud groups
  - Managing CloudPoint extensions
- The NetBackup Web UI Administrator can also assign assets at a cloud provider-level, allowing a custom role to manage the assets that are associated with a specific cloud provider.
- You can manually trigger the cloud asset discovery if required, using the Discover option for individual cloud provider configurations.

For more information, see the following guides:

- NetBackup Web UI Administrator's Guide
- NetBackup Web UI Cloud Administrator's Guide
- NetBackup CloudPoint Install and Upgrade Guide

Instant rollback for VMs

With NetBackup 9.1, you can roll back a VM instantly from a backup image. You can roll back a VM multiple times to any recovery point or select multiple VMs and perform rollback. This feature is supported for an Appliance, a Virtual Appliance, and a build-your-own (BYO) server.

For more information, see the NetBackup 9.1 Web UI Administrator's Guide

For VMware and RHV environments, reduce the size of the job database before upgrade

The job database is now cached in memory in web services. Following an upgrade, existing VMware and RHV jobs are assigned an asset namespace to enable access control at an asset level. This process may take some time. You should reduce the size of the jobs database before upgrade to minimize the amount of processing required to perform the association and minimize the effect on web services performance. Very large job databases may see an alert regarding high heap space usage. For details on reducing the size of the job database or increasing the maximum heap size for web services, see the following article:

The activity monitor job cache is using a large amount of heap space

Query options added for VMware intelligent policies

Additional query options have been added for creating VMware intelligent policies: annotation, connectionState, datacenterPath, guestOS, networkName, powerState, template, version, vmFolder, vmxDatastore, and vmxDatastoreType.

With NetBackup 9.1, you can use OData keywords when you build queries with the NetBackup web UI. However, you must continue to use VMware intelligent policy (VIP) keywords you build queries with the NetBackup Administration Console.

For more information, see the following guides:

NetBackup 9.1 for VMware Administrator's Guide

NetBackup 9.1 Web UI VMware Administrator's Guide

Nutanix AHV enhancements

NetBackup 9.1 includes state-of-art features for the protection of Nutanix AHV. NetBackup 9.1 provides following enterprise-level capabilities to protect Nutanix AHV using the NetBackup web UI:

- Integration with NetBackupweb UI:
  Nutanix AHV features are integrated with NetBackup web UI to provide ability to configure, protect, recover, and monitor Nutanix AHV resources from a web browser.
- Role Base Access Control (RBAC):
  Lets the administrator configure user access and delegate NetBackup tasks such as AHV Asset management, Credentials access, workload protection, VM Recovery, and Files and Folders Recovery.
- Credential Management:
  Nutanix AHV credentials are added in the NetBackup Credential Management database as named credentials. The owner can share named credentials with other users or administrators for reuse without revealing actual credentials.
- Automatic Asset Discovery:
  Once AHV cluster is added in NetBackup Asset, NetBackup runs automatic Resource Discovery process and adds all VMs in the NetBackup asset. After the initial run, the Resource Discovery process runs at a scheduled interval which is configurable. This option ensures that any newly added VMs are included in the NetBackup asset.
- Intelligent VM Group:
  You can create an intelligent VM group based on a set of filters called queries. You can then apply protection to the group. NetBackup automatically selects

virtual machines based on the queries and include them for the protection during the backup operation.

- Individual VM backup:
  You can also select individual VMs for protection from the list of VMs which are available through automatic discovery process.
- Backup Now:
  Lets you perform ad hoc backup outside the backup schedule.
- Virtual Machine Quiescing:
  This option lets you select application-consistent or crash-consistent snapshots leveraging suspending the operations for the options that are provided by Nutanix.
- Resource throttling:
  This option avoids overloading of Nutanix AHV resources during backup operations. It is done by controlling the number of simultaneous snapshots, backups that can be performed on a Nutanix AHV resource.
- Restore options using NetBackup web UI recovery wizard:
  - VM restore:
    Lets you restore the entire AHV VM to same or a different AHV cluster.
  - Agentless File and folder recovery:
    Lets you restore individual files and folders of protected AHV VM to any homogeneous platform target host. The target host can be a virtual machine that is hosted on AHV or other hypervisors or even a physical machine where the NetBackup client is not installed. If NetBackup client is found on the target host then Files and Folders Recovery automatically uses NetBackup client.
  - File and folder recovery using NetBackup client:
    Lets you restore individual files or folder of protected AHV VM to any homogeneous platform where a NetBackup client is configured. This can be a virtual machine that is hosted on AHV or other hypervisors or even a physical machine where the NetBackup client is installed.
- Windows backup hosts support:
  In addition to Linux based NetBackup Media server/Backup Hosts, you could now use Windows based NetBackup Media server/Backup Hosts to protect Nutanix AHV Cluster.
- iSCSI transport mode:
  NetBackup now supports iSCSI transport mode for Windows and Linux based NetBackup Media server/Backup Hosts. NFS transport is additionally supported for Linux based NetBackup Media server/Backup Hosts.

- Automatic media server selection:
  This lets NetBackup automatically pick up available Media server from the pool of media servers. It distributes backup jobs across multiple media servers which are available.
- NetBackup APIs:
  You can also use NetBackup APIs which are added for all the above features.

For details, refer to the NetBackup 9.1 Web UI Nutanix AHV Administrator's Guide.

Oracle Instance Management to be removed from NetBackup Administration Console

Oracle Instance Management will be removed from the NetBackup Administration Console in a future release. NetBackup provides management of Oracle assets through the NetBackup web UI and APIs. Additionally, review the previous announcement in the NetBackup for Oracle Administrator's Guide on the removal of `nboraadm` and Instance Groups from NetBackup.

NetBackup Oracle Intelligent Policy can be configured with options for Data Guard

The NetBackup Oracle Intelligent Policy is now Data Guard aware. This option lets you specify a policy to always back up the primary or a standby database. The new **Data Guard backup options** drop-down is in the **Oracle** tab when you create an Oracle policy.

The following options are available:

- **None**
- **Require primary**
- **Require standby**
- **Prefer standby**

For more information, review the Oracle tab section in the NetBackup for Oracle Administrator's Guide.

Oracle and DB2 policy templates are deprecated in the NetBackup 9.1 release

NetBackup for Oracle and NetBackup for DB2 policy templates are deprecated as of NetBackup 9.1.

- Oracle policies using templates should be converted to an Oracle Intelligent Policy (OIP).
- NetBackup for DB2 templates should be converted to DB2 scripts. NetBackup for DB2 policies using templates require the template name to be replaced with the fully qualified path to the script on the client.
- In the next release, NetBackup for Oracle and NetBackup for DB2 backup and restore functionality will no longer function in the BAR GUI.
- The `bpdbsbora` and `bpdbsbdb2` commands are removed in the next release.

NetBackup for Microsoft SQL Server agent enhancements

This release includes the following changes to the SQL Server agent:

- Fixed issues with the restores of file stream databases in the NetBackup web UI.
  File stream databases can be restored to a different database, to a different path, or files can be restored to different paths.
- Ability to recover from any copy.
  Clients must be at version 9.1 or later. If you perform recovery from a lower-level client, NetBackup uses the primary copy for recovery and ignores any other selected copy.
  The batch file options include a new keyword `RESTORECOPYNUM`.
- For VMware backups of SQL Server, you can only select the primary copy for recovery in the NetBackup web UI.
- For environments with many databases and frequent transaction log backups, improved the web UI performance and time to display the image copy details for a recovery point.
- Added support to preserve the change data capture settings when a database or log backup is recovered.
  Clients must be at NetBackup 9.1 and later. To support legacy policies with the NetBackup Administration Console, the batch file options include a new keyword `KEEPCDC`.
- Added support for any databases that are run in single-user mode.

New behavior for Oracle and Microsoft SQL Server intelligent policies

In NetBackup 9.1, there is new behavior for Oracle and Microsoft SQL Server intelligent policies. Now NetBackup allows child jobs to run on the appropriate schedule that is due for each instance or any instance groups.

Previously, when a policy had multiple instances, instance groups, and multiple schedules which ran at the same time, child jobs ran on the same schedule as the parent discovery job.

Note: Microsoft SQL Server TLOG schedules run independently of the automatic schedules.

Chapter 3

Operational notes

This chapter includes the following topics:

About NetBackup 9.1 operational notes

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

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

NetBackup Release Notes, Administration, Installation, Troubleshooting, Getting Started, and Solutions Guides

NetBackup installation and upgrade operational notes

NetBackup can be installed and upgraded in heterogeneous environments using a variety of methods. NetBackup is also compatible with a mixture of servers and clients that are at various release levels in the same environment. This topic contains some of the operational notes and known issues that are associated with the installation, upgrade, and software packaging of NetBackup 9.1.

After initiating CA migration, connection errors may occur

NetBackup now supports certificate authorities with the following key strengths: 2048 bits, 4096 bits, 8192 bits, and 16384 bits. After NetBackup 9.1 installation or upgrade, by default a new root CA with 2048-bits key strength is deployed.

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

If NetBackup 9.1 upgrade fails on Windows, revert to previous log folder structure

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

For Windows, if the upgrade to NetBackup 9.1 fails and rollback occurs, run the following command to continue working on an earlier NetBackup version:

```
mklogdir.bat -fixFolderPerm
```

For more information, refer to the `mklogdir` command from the Veritas NetBackup Commands Reference Guide.

Native installation requirements

In NetBackup 8.2, a change was made to initial installs such that the answer file is now required. This change may have some negative effect on users who want to use the native packages to create VM templates or otherwise install the NetBackup packages without configuring the product. On Linux, one possible way of obtaining the previous behavior is with the `-noscripts` option of the RPM Package Manager. Providing this option when installing the `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.

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

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

About support for HP-UX Itanium vPars SRP containers

Hewlett-Packard Enterprise (HPE) introduced a new type of container for HP-UX Virtual Partitions (vPars)-enabled servers called Secure Resource Partitions (SRPs). As part of the security changes introduced by SRPs, native HP-UX install tools such as `swinstall` and `swremove` are disabled from being run within the SRP environment. The `swinstall` and `swremove` tools can only be called from the global host running vPars, which then pushes the native packages to the SRP containers.

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

NetBackup administration and general operational notes

NetBackup provides a complete, flexible data protection solution for a variety of platforms. The platforms include Windows, UNIX, and Linux systems. In addition to a standard set of data protection features, NetBackup can also utilize several other licensed and non-licensed components to better protect a variety of different systems and environments. This topic contains some of the general operational notes and known issues that are associated with the administration of NetBackup 9.1.

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.

NetBackup anomaly detection management service may not start after a full catalog restore

The NetBackup anomaly detection management (`nbanomalymgmt`) service may not start after a full catalog restore. This is typically observed when the service is up and running during the full catalog restore.

You may see the following errors in the `nbanomalymgmt` service log:

```
14:27:13.807 [8100.9844] <16> nbanomalymgmt: Error occurred while
 gathering data
14:27:13.808 [8100.9844] <2> nbanomalymgmt: State:[3], ExitCode:[0],
 WaitHint:[300000], CheckPoint:[2]
14:27:13.808 [8100.9844] <8> WaitForChildProc: Process [DETECTION]
 event handle is NULL
14:27:13.808 [8100.9844] <2> nbanomalymgmt: State:[3], ExitCode:[0],
 WaitHint:[300000], CheckPoint:[3]
14:27:13.808 [8100.9844] <8> WaitForChildProc: Process [ALERT]
 event handle is NULL
14:27:13.809 [8100.23948] <4> nbanomalymgmt: Worker thread exited.
 So shutting down the service.
```

During a full catalog restore, the nbanomalymgmt service is running, the anomaly detection database (`NB_Anomaly.db`) may get corrupted, and that can cause the issue.

Workaround:

If the catalog restore is already complete with the `nbanomalymgmt` service in the running state and that has caused the database to be corrupted and in turn the service cannot start, you need to do the following as a workaround:

1. Stop the `nbanomalymgmt` service before you restore the catalog to an alternate location or during disaster recovery (DR).

   Run the following command:

   On Linux: `/usr/openv/netbackup/bin/nbanomalymgmt -stop`

   On Windows: *<install_path>*`\\NetBakcup\\bin\\nbanomalymgmt -stop`

   Or from the Windows Service Control Manager, Stop “NetBackup Anomaly Detection Management Service”.

2. Delete all files under the `anomaly_detection` folder. The location of the folder is as follows:

   On Linux: `/usr/openv/var/global/anomaly_detection`

   On Windows:
   `<install_path>\\NetBackup\\var\\global\\anomaly_detection`

3. Restore the catalog to an alternate location and copy all files under the `anomaly_detection` folder to the following locations.

   On Linux: `/usr/openv/var/global/anomaly_detection`

   On Windows:
   `<install_path>\\NetBackup\\var\\global\\anomaly_detection`

4. After the restore completes, start the `nbanomalymgmt` service using the following command:

   On Linux: `/usr/openv/netbackup/bin/nbanomalymgmt -start`

   On Windows: `<install_path>\\NetBakcup\\bin\\nbanomalymgmt -start`

   Alternatively, do the following: Go to Windows Service Control Manager and start NetBackup Anomaly Detection Management Service.

To avoid the anomaly detection database corruption during catalog restore:

1. Stop the `nbanomalymgmt` service before performing full catalog restore or disaster recovery. Run the following command:

   For Linux:`/usr/openv/netbackup/bin/nbanomalymgmt -stop`

   For Windows:`<NetBackup Install Location>\\NetBakcup\\bin\\nbanomalymgmt -stop`

   Alternatively, do the following: From the Windows Service Control Manager, stop NetBackup Anomaly Detection Management Service.

2. Delete all files under the `anomaly_detection` folder. The location of the folder is as follows:

   On Linux: `/usr/openv/var/global/anomaly_detection`

   On Windows:
   `<install_path>\\NetBackup\\var\\global\\anomaly_detection`

3. After the restore completes, start the `nbanomalymgmt` service using the following command:

   On Linux: `/usr/openv/netbackup/bin/nbanomalymgmt -start`

   On Windows: `<install_path>\\NetBakcup\\bin\\nbanomalymgmt -start`

Alternatively, do the following: Go to Windows Service Control Manager and start NetBackup Anomaly Detection Management Service.

Authorization check fails if you change the user after installation or upgrade in an NBAC-enabled setup

Authorization check fails if you change the user after NetBackup installation or upgrade in an NBAC-enabled setup.

For more information on the service user (non-privileged or non-root user), refer to the NetBackup Security and Encryption Guide.

The following error message is displayed during installation or upgrade:

```
bprd failed to grant authorization check permission to host
 'host1'
118-VxSS authorization failed: Please make sure NBAC-Authorization
 is properly configured and running and you have necessary
 permissions to do these operations.
```

The issue occurs because the new service user is not part of the Security Administrator group.

Workaround:

To resolve the issue, you should add the new service user to the Security Administrator group (or remove the older one) using one of the following scenarios.

Scenario 1

Authorization check fails in one of the following cases:

- The root (UNIX) or Local System (Windows) user is changed to a new service user using the `nbserviceusercmd -changeUser` command.
- The NetBackup 9.1 upgrade is performed with the service user other than the root or Local System user.

To resolve the authorization check failure:

1. After changing the user, ensure that all NetBackup services are up and running.
2. Run the following command to add the new service user to the Security Administrator group:

   ```
   vssaz addazgrpmember --azgrpname "Security Administrators"
   --prplinfo ATP,atdomain,new service user
   ```

   The directory path to the `vssaz` command is as follows:

   On UNIX: `/usr/openv/netbackup/sec/az/bin`

On Windows: `<install_path>\sec\az\bin`

Scenario 2

Authorization check fails when one service user is changed to another service user using the `nbserviceusercmd -changeUser` command.

To resolve the authorization check failure:

1. After changing the user, ensure that all NetBackup services are up and running.
2. Run the following command to remove the older service user principle from the Global Security Administrator group.

   ```
   vssaz removeazgrpmember --azgrpname "Security Administrators"
   --prplinfo ATP,atdomain,older user
   ```

3. Run the following command to add the new service user to the Security Administrator group:

   ```
   vssaz addazgrpmember --azgrpname "Security Administrators"
   --prplinfo ATP,atdomain,new service user
   ```

The directory path to the `vssaz` command is as follows:

On UNIX: `/usr/openv/netbackup/sec/az/bin`

On Windows: `<install_path>\sec\az\bin`

Scenario 3

If the service user is changed to the root (UNIX) or Local System (Windows) user using the `nbserviceusercmd -changeUser` command, for example, after the NetBackup 9.1 fresh installation. It's recommended to remove the old service user from the Security Administrator group for increased security.

To eliminate the security vulnerability that may be introduced because of the stale entry of the old service user in the group:

1. After changing the user, ensure that all NetBackup services are up and running.
2. Run the following command to remove the older service user principle from the Global Security Administrator group.

   ```
   vssaz removeazgrpmember --azgrpname "Security Administrators"
   --prplinfo ATP,atdomain,older user
   ```

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.

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

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

Workaround:

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

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

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

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

Workaround:

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

Stale devices shown on the device tree

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

Workaround:

1. Unmount any file systems that mounted the device. (If required use `force unmount`)
2. If any of the partitions belongs to LVM, then remove the volume group from disk using the `vgreduce` command and then the `pvremove` command.
3. Execute the `blockdev -flushbufs` command to remove any outstanding reference to that device.
4. Remove the device references from the device tree. For example, whole/partition disks /dev/xvdf, /dev/disk/by-path, by-id, by-label, by-partuuid and by-uuid
5. Use the following command to remove the device from sysfs:
6. `echo 1 > /sys/block/device-name/device/delete`

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

Temporary devices listed as file system assets

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

NetBackup administration interface operational notes

The NetBackup administrator has a choice of several interfaces to use to administer NetBackup. All of the interfaces have similar capabilities. This topic contains some of the operational notes and known issues that are associated with these interfaces in NetBackup 9.1.

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 77.

Access control methods supported in NetBackup 9.1

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

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

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.
- An asset ID is not set for a cloud convert job. Users that have roles with more granular permissions for VMware assets can't view these jobs.
  This behavior does not affect users with an RBAC role that has full job permissions or a role that can manage all VMware assets.

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 9.1.

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.

Pre-recovery check for VM restore fails on Windows-based NetBackup primary or media servers if the VM's display name contains multi-byte characters

Azure cloud supports VM display names with multi-byte characters if the image is of Windows OS. But if the NetBackup primary servers or media servers run the Windows OS, the following error may occur: `Failed to invoke pre-recovery-check request.`

Workaround:

Use a Linux primary server or media server for original location restores or parameter restores.

Configuring a cloud recovery host on RHEL 8

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

NetBackup with Veritas CloudPoint operational notes

This topic contains some of the operational notes and known issues that are associated with the Veritas CloudPoint and NetBackup 9.1.

Connection attempt fails for the VM that is in the unreachable or stopped state, and has the credentials associated with it

A VM that is connected using the credentials associated with it can go into an error state due to being stopped or being unreachable, or due to the VM password being changed.

Then when a reconnection attempt is made, the connection fails with a wrong error message which suggests that a VM is already connected.

Workaround:

Invoke the following NetBackup REST API to update the VM state with updated credentials in the `credential_name` parameter.

API Url:

```
https://{NetBackup_PRIMARY_SERVER}/netbackup/config/snapshotproviders/
 connected-virtual-machines/{assetId}
```

API Method:

PUT

API Headers:

```
Content-Type: application/vnd.netbackup+json;version=3.0
Accept:application/vnd.netbackup+json;version=6.0
Authorization: {NetBackup Token}
```

API Request Payload:

```
{
  "data": {
    "type": "vmconnect",
    "attributes": {
      "vmConnectionAttributesList": [
        {
          "name": "credentialName",
          "singlevalue": "<credential_name>"
        }
      ]
    }
  }
}
```

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>
   ```

CloudPoint discovery status shows as failed in the NetBackup web UI

When you create an asset and delete it, and then create another asset with the same name and same configurations in a different region, the CloudPoint discovery status shows as failed in the NetBackup web UI.

Workaround:

Before creating an asset that uses an existing name in a different region, delete the older asset and run deep discovery. This way, the asset is updated in the CloudPoint server.

New CloudPoint asset information may affect recovery

NetBackup 9.1 introduced additional asset information for CloudPoint servers. This information is required during recovery. As a part of normal operations, this new information is discovered and the appropriate databases are populated with that information. If you attempt a recovery before that information is populated, the recovery fails. Veritas has observed this failure in both Amazon Web Services and Google Cloud Platform, but not Microsoft Azure.

Workaround:

Use one of these methods to resolve this issue:

- Wait at least 2 hours after the upgrade finishes for the appropriate discovery processes to populate the servers with the new information.
- Alternatively, manually run the discovery for the server you need to recover. From the NetBackup web UI, select **Cloud > CloudPoint Servers**, select the specific CloudPoint server, then from the Action menu, select **Discover**.

After upgrade, assets are unsubscribed from protection plans with GRT option enabled

After you upgrade to NetBackup 9.1, some assets may not be automatically resubscribed to protection plans with the GRT option enabled. You will receive notifications for the assets that failed to resubscribe. For example:

```
The asset <asset name> is unsubscribed from protection plan
<protection plan name>
```

```
Failed to re-subscribe the <asset name> to protection plan <protection
plan name> after conversion to new format. Please re-subscribe the
asset manually.
```

Workaround: Resubscribe the asset to the protection plan again after discovery.

Backup now option may fail with the error

After you upgrade to NetBackup 9.1, the Backup now option fails with the error:

```
Cloud snapshot indexing is not supported for the specified asset.
```

Workaround:

Run discovery before a running Backup now for the asset.

Adding new regions requires a new cloud plug-in configuration

You cannot add a new region to an existing cloud plug-in configuration. The edit plug-in configuration function cannot accommodate the newly added regions in the CloudPoint database, where multiple threads operate on same plug-in configuration. If you edit the existing cloud plug-in configuration to add a new region, the new region is not listed in the restore from backup wizard.

Workaround:

Create a new configuration with the same account credentials as the existing configuration and include the new regions.

In backup and restore jobs, the number of files transferred is shown as 0

In backup and restore jobs, the number of files transferred is shown as 0, even though the job is successful, and bytes transferred reports the correct values.

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.

Snapshot jobs fail due to exceptions

A high memory pressure on the CloudPoint VM causes the Flexsnap-MongoDB container and the Flexsnap-Rabbitmq container to restart. After the container restarts, the Off-Host Agent service container cannot establish a communication

with Rabbitmq. This issue might occur with any agent service, such as the CloudPoint OnHost agent or the CloudPoint Off Host agent.

Workaround:

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

```
docker restart <container_name>
```

Deleted snapshots still visible in the NetBackup web UI

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

Granular restore fails if target path is deleted and recreated

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

Workaround:

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

Public cloud not supported with gov cloud or China region

If you try to 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
```

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

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

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

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

Permission denied error occurs if both user and password are updated

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

Workaround:

To avoid this issue:

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

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

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

Workaround:

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

Broken files system detected

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

NetBackup deduplication operational notes

NetBackup provides several deduplication options that let you deduplicate data everywhere, as close to the source of data as you require. Deduplication everywhere lets you choose at which point in the backup process to perform deduplication. NetBackup can manage the deduplication of environments that use the NetBackup Deduplication Engine. This topic contains some of the operational notes and known

issues that are associated with the NetBackup Deduplication Engine in NetBackup 9.1.

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

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

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

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

Workaround:

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

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

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

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

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

   ```
   dedupe MSDP stop
   ```

   ```
   dedupe MSDP start
   ```

NetBackup for NDMP operational notes

NetBackup for NDMP is an optional NetBackup application. It enables NetBackup to use the Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems. This topic contains some of the operational notes and known issues that are associated with NetBackup for NDMP in NetBackup 9.1.

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

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

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

NetBackup for OpenStack operational notes

NetBackup for OpenStack is an optional NetBackup application. This topic contains some of the operational notes and known issues that are associated with NetBackup for OpenStack in NetBackup 9.1.

Instance volumes in the incremental backups cannot be mounted

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

NetBackup master server does not re-issue the token if NetBackup 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 master 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 master server provides.

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

On NetBackup 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 **Netbackup_9001_beta1** instead.

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

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

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

Unable to connect to NetBackup master server using NBCA

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

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

Workaround:

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

For more information, see the following Support article:

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

Excluded Ceph Volume after restore is not mountable or formattable

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

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

Restored VMs have blank metadata config_drive attached

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

Workaround:

Delete metadata `config_drive` or set the desired value.

NBOSVM reconfig fails when you add new NetBackup 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 9.1.

Support for localized environments in database and application agents

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

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

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

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

- Host name (primary server, media server, Enterprise Media Manager (EMM) server, volume database host, media host, client, instance group)
- Policy name
- Policy KEYWORD (Windows only)
- Backup, Archive, and Restore KEYWORD (Windows only)
- Storage unit name
- Storage unit disk pathname (Windows only)

- Robot name
- Device name
- Schedule name
- Media ID
- Volume group name
- Volume pool name
- Media description
- Vault policy names
- Vault report names
- BMR Shared Resource Tree (SRT) name
- Token name

NetBackup Snapshot Client operational notes

NetBackup Snapshot Client provides a variety of snapshot-based features for NetBackup. It supports clients on UNIX, Linux, and Windows platforms, on Fibre Channel networks (SANs) or traditional LANs. Each snapshot method relies on the snapshot technology that is built into the storage subsystem where the data is stored. This topic contains some of the operational notes and known issues that are associated with Snapshot Client in NetBackup 9.1.

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 don’t upgrade at least one backup host from the pool, along with master server upgrade from NetBackup 8.3 to NetBackup 9.1. This situation fails the accelerator-enabled DNAS policy for NAS.

Workaround:

Upgrade the master 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 9.1.

NetBackup for VMware operational notes

NetBackup for VMware provides backup and restore of the VMware virtual machines that run on VMware ESX servers. Additionally, the NetBackup plug-in for VMware vCenter (vCenter plug-in) allows the vSphere Client to monitor virtual machine backups and recover a virtual machine from a backup. This topic contains some of the operational notes and known issues that are associated with NetBackup for VMware and the vCenter plug-in in NetBackup 9.1.

CDP-protected VM gets turned off

With heavy load of database transactions, CDP protected VMs on ESXi hosts might get turned off. This situation occurs mostly when the VM performs database schema drop or recreate operations. The subsequent backup jobs for this VM fail with the error `The VM to be backed up is disconnected from CDP gateway`.

Workaround:

A VM crash does not create data loss. Keep sufficient CPU and memory free to handle sudden IO burst on ESXi. When the VM is back online, NetBackup CDP catches up with the pending I/Os. For HA VM, the VM restarts automatically.

Backups may fail when data on CDP staging path is corrupted

VM data that is present on the CDP staging path may become corrupted before the VM has any recoverable images. This situation causes a full backup or a backup with forced rescan schedule to fail.

If the data is corrupted when there are no recoverable VM images present, it indicates that the VM full sync is yet to complete. Therefore, a backup with a forced rescan schedule does not work.

Workaround:

Unsubscribe the VM from the CDP gateway and then subscribe it again.

Remove CDP gateways before resubscribing VMs to storage policies

When you detach a storage policy from a VM and re-subscribe the VM to another CDP gateway before removing it from the previous gateway, removal of the VM from the previous gateway fails.

Workaround:

Unsubscribe the VM from the already subscribed CDP gateway before subscribing the VM to another CDP gateway.

Appendix A

About SORT for NetBackup Users

This appendix includes the following topics:

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

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 38.

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- Database rebuilds are likely to occur in each major, minor (single-dot), and release update (double-dot) version of NetBackup. Therefore, before upgrading to NetBackup 9.1, you must ensure that you have an amount of free disk space available that is equal to or greater than the size of the NetBackup database. That means for default installations, you are required to have that amount of free space on the file system containing the `/usr/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 9.1. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 9.1 and other NetBackup releases can be found on the Veritas Services and Operational Readiness Tools (SORT) website and in the NetBackup compatibility lists.

See "About NetBackup compatibility lists and information" on page 77.

See "About Veritas Services and Operations Readiness Tools" on page 67.

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 9.1

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 9.1 *(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 9.1 *(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 9.1 binary sizes

Table B-2 contains the approximate binary sizes of the NetBackup 9.1 master server, media server, and client software for the various supported operating systems. These binary sizes indicate the amount of disk space occupied by the product after an initial installation. Note that for the sizes listed in the table, 1 MB equals 1024 KB.

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

Note: Table B-2 and Table B-3 only list the supported operating systems. For up-to-date information about the specific operating system versions that NetBackup currently supports, check the Installation and Upgrade Checklist on the Services and Operations Readiness Tools (SORT) website, or the NetBackup Operating System Compatibility List.

Table B-2 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
AIX	POWER		1863 MB	No longer supported	

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

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
Canonical Ubuntu	x86-64		1360 MB		
CentOS	x86-64		1336 MB	7529 MB	
Debian GNU/Linux	x86-64		1359 MB		
HP-UX	IA-64		2356 MB	No longer supported	
Oracle Linux	x86-64		1336 MB	7354 MB	
Red Hat Enterprise Linux Server	POWER		298 MB		
Red Hat Enterprise Linux Server	x86-64		1336 MB	7430 MB	
Red Hat Enterprise Linux Server	z/Architecture		1049 MB	No longer supported	Media server or client compatibility only.
Solaris	SPARC		2104 MB	6326 MB	
Solaris	x86-64		1486 MB	6468 MB	
SUSE Linux Enterprise Server	POWER		297 MB		
SUSE Linux Enterprise Server	x86-64		1289 MB	6497 MB	
SUSE Linux Enterprise Server	z/Architecture		1059 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64		504 MB	3384 MB	Covers all compatible Windows x64 platforms.

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

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

NetBackup OpsCenter

Table B-3 contains the approximate binary sizes of the OpsCenter Agent, Server, and **ViewBuilder** for the various operating systems that are compatible with NetBackup OpsCenter 9.1.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Agent	Server	ViewBuilder
Oracle Linux	x86-64		715 MB	
Red Hat Enterprise Linux Server	x86-64		714 MB	
SUSE Linux Enterprise Server	x86-64		727 MB	
Windows Server	x86-64	263 MB	662 MB	222 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

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

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

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

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

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

For complete information about compatibility between NetBackup versions, refer to the Veritas SORT website.

Veritas recommends that you review the End of Support Life information available online.

About NetBackup compatibility lists and information

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

See "About Veritas Services and Operations Readiness Tools" on page 67.

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.

See "EOL for support on RHEL 7.0 through 7.3" on page 22.

See "EOL for CentOS 8 support" on page 23.

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 67.

About changes in platform compatibility

The NetBackup 9.1 release may contain changes in support for various systems. In addition to using SORT, you should make sure to review the *NetBackup Release Notes* document and the NetBackup compatibility lists before installing or upgrading NetBackup software.

See “About new enhancements and changes in NetBackup” on page 12.

http://www.netbackup.com/compatibility

Appendix D

Other NetBackup documentation and related documents

This appendix includes the following topics:

About related NetBackup documents

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

Not all documents are published with each new release of NetBackup. In the guides, you may see references to other documents that were not published for NetBackup 9.1. In these cases, refer to the latest available version of the guide.

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

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