Veritas NetBackup™ Release Notes

Release 8.3

Document Version 1

VERITAS™

Veritas NetBackup™ Release Notes

Last updated: 2020-07-30

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

About NetBackup 8.3

This chapter includes the following topics:

About the NetBackup 8.3 release

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

See "About new enhancements and changes in NetBackup" on page 11.

About EEBs and release content

NetBackup 8.3 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 8.3 can be found on the Veritas Operations Readiness Tools (SORT) website and in the .

See "About Veritas Services and Operations Readiness Tools" on page 62.

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 8.3 release" on page 9.

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

NetBackup 8.3 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 8.3 are grouped below by category. Select a link to read more information about the topic.

New features

- NetBackup provides data immutability and indelibility on WORM storage devices
- Database improvements reduce CPU load
- OpsCenter data collectors for PureDisk and NetBackup Deduplication Appliance are no longer supported
- OpsCenter 8.3 offers dynamic views
- Monitoring OpsCenter performance tuning using the OpsCenter web UI
- Enhancements to Universal Shares support
- RBAC enhancements
- Configure storage servers in the NetBackup web UI
- New link to Veritas SaaS Backup site added to the NetBackup web UI
- Notifications icon added to the NetBackup web UI
- About policy management in the NetBackup web UI
- Support for Single Sign-On in the NetBackup web UI
- Configuration settings added to NetBackup web UI
- Use NetBackup web UI to share images from an on-premises location to the cloud
- Audit events can be exported to system logs through the NetBackup web UI
- CALLHOME_PROXY_SERVER option for NetBackup master and media servers
- RESTful APIs included in NetBackup 8.3

Secure communication features, changes, and enhancements

- About NetBackup CA migration to a CA with key strength of 2048 bits and greater
- Support for external key management service (KMS) servers

- **Note:** Before you install or upgrade to NetBackup 8.3 from a release earlier than 8.1, make sure that you read and understand the *NetBackup Read This First for Secure Communications* document. NetBackup 8.1 includes many enhancements that improve the secure communications of NetBackup components. The *NetBackup Read This First for Secure Communications* document describes the features and benefits of these enhancements:

  NetBackup Read This First for Secure Communications

Support changes and enhancements

- NetBackup 8.3 support additions and changes
- Supported extended attributes and file types for granular restore on Linux and Windows
- NetBackup 8.3 licensing enhancements
- Performance improvement in the `nbdeployutil` utility
- Newer SuSE Linux compilers used with NetBackup 8.3
- Support for persistent robotic paths for Linux media servers
- Several shutdown commands to be deprecated in a future release

Installation, upgrade, and configuration changes and enhancements

- Move the NetBackup database from any btrfs file systems
- Optional installation of Java GUI and JRE
- Changes to user session default values

Cloud-related changes and enhancements

- Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 8.3
- New Asset Services APIs require conversion for Cloud assets
- About uploading deduplicated data to the cloud using MSDP cloud
- CloudPoint is available from the NetBackup web UI
- Support for Nutanix Files file shares

Virtualization changes and enhancements

- Update for RHV workload from NetBackup web UI

- Database changes require migration of VMware and RHV assets
- Build your own (BYO) support on RHEL for VMware Instant Access
- NetBackup install now includes the Nutanix Acropolis Hypervisor (AHV) plug-in for the Hypervisor policy

Database agent changes and enhancements

- Enhancements and changes for the Microsoft SQL Server agent
- Microsoft SQL Server Instant Access support
- Microsoft SQL Server stream handler introduced
- Support for Microsoft SQL standalone and Availability Group (AG) databases
- Enhancements for NetBackup for Oracle
- Oracle stream handler introduced
- NetBackup install now includes the MongoDB plug-in

Other announcements

- Changes in the legacy log folder structure
- Bare Metal Restore enhancements
- MSDP multi-domain support added
- Integration of Veritas Resiliency Platform with NetBackup
- Enhancements to NAS workloads

NetBackup provides data immutability and indelibility on WORM storage devices

NetBackup 8.3 provides the ability to write backups to WORM (Write Once Read Many) storage devices so that their data cannot be corrupted. Additionally, it lets you take advantage of advanced options available from your storage vendors to protect your backup data per applicable statutes.

NetBackup protects your data from being encrypted, modified, and deleted using WORM properties:

- Immutability
  This protection ensures that the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.
- Indelibility

This property protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

For more information, see *Configuring immutability and indelibility of data in NetBackup* in the NetBackup Administrator's Guide, Volume I.

Database improvements reduce CPU load

This release of NetBackup introduces improvements that significantly reduce the CPU load on NetBackup's datastore, an SAP SQL Adaptive Server Anywhere (ASA) relational database that runs on the master server. This release of NetBackup introduces improvements that significantly reduce the CPU load on a primary NetBackup datastore, the SAP SQL Adaptive Server Anywhere (ASA) relational database that runs on the master server.

These improvements reduce the load on the database by:

- Optimizing certain queries in `bpdbm` and `nbemm`.
- Caching more information in `bpjobd`.
- Keeping in-memory copies of some commonly accessed tables.
- Moving the Resource Broker (RB) and the Media and Device Selection (MDS) tables out of the NetBackup relational database on the master server.

Two new files now reside in the `/usr/openv/netbackup/db` directory: `rb.db` (Resource Broker) and `mds.db` (Media and Device Selection)

OpsCenter data collectors for PureDisk and NetBackup Deduplication Appliance are no longer supported

Starting with NetBackup OpsCenter 8.3, the data collectors (**Settings -> Configuration -> Agent -> Integrated Agent -> Create/Edit/Delete Data Collector**) to collect the data from “Veritas NetBackup PureDisk” and “Veritas NetBackup Deduplication Appliance” products are no longer supported.

If you have configured the data collectors for “Veritas NetBackup PureDisk” and “Veritas NetBackup Deduplication Appliance”, Veritas strongly recommends that you delete these data collectors manually as well as any previously collected data for policies, jobs, appliance hardware, and so on for these data collectors. The collected appliance hardware data for “Veritas NetBackup Deduplication Appliance” can be seen under **Monitor -> Appliance Hardware -> Deduplication**.

The data collected from these products in previous versions will not be deleted upon upgrade. The OpsCenter Agent Configuration UI screens for these data collectors now provide visual indications of the deprecated support for these products. These visual indications are provided primarily to inform you to delete

these data collectors manually as subsequent OpsCenter releases might remove the entire “Integrated Agent” (**Settings -> Configuration -> Agent -> Integrated Agent**) from OpsCenter.

Also, Veritas recommends that you delete any alert policies created for “Agent Server Communication Break” and “Appliance Hardware Failure” (if configured for a “Veritas NetBackup Deduplication Appliance”) failures and clear any previously generated alerts for this alert policy.

OpsCenter 8.3 offers dynamic views

OpsCenter views are logical groups of IT assets (master servers or clients) that are organized in a hierarchical manner. You can manually add objects to a view and such views are called static views.

In OpsCenter 8.3, you can also have dynamic views by creating filters and associating them to the views. Dynamic views are automatically updated when an object that matches the filter criteria is added or removed. OpsCenter View Builder does not support dynamic views.

For more information, refer to the NetBackup OpsCenter Administrator’s Guide.

Monitoring OpsCenter performance tuning using the OpsCenter web UI

The database size grows rapidly as you add more NetBackup master servers in OpsCenter. Therefore, to get the optimum OpsCenter performance, monitoring the database cache memory, the server and GUI heap memory, and its status is very important. Using the OpsCenter tuning feature, you can monitor the OpsCenter memory and the tuning status.

To monitor the OpsCenter tuning status:

1. In the OpsCenter console, click **Settings > OpsCenter Tuning**.

For more information, refer to the NetBackup OpsCenter Administrator’s Guide.

Enhancements to Universal Shares support

The following enhancements to the support of universal shares are new in NetBackup 8.3:

- Dedicated Universal Share policy - Configuring the Universal Share Protection Point is easier with a new Universal Share policy type.
- Central web UI configuration support - Configuring and managing the Universal Share can now be performed from the NetBackup web UI. Accessing two

separate interfaces is no longer required for Universal Share management. See *Create a Universal Share* in the NetBackup Web UI Administrator's Guide for more information.

- Quotas - This feature allows the NetBackup administrator the ability to limit the amount of data that is ingested into each individual share. In this way, the amount of storage within MSDP can be protected and managed. The quota limit is based on the front-end terabyte measure of the storage ingested into the share.
- Support for software-only NetBackup deployments - The Universal Share is fully supported in a NetBackup software-only (also know as Build Your Own or BYO) deployment scenario.
- Active Directory (AD) integration - User access to the Universal Share can be managed using Active Directory permissions.
- High Availability (HA) Appliance - The Universal Share is now fully supported with the NetBackup Appliance HA option. If a node fails in an HA configuration the Universal Share will automatically failover to the surviving node.
- Scalability enhancements - The Universal Share now supports up to 5 million files per share. The already fast Protection Point performance has been improved as well.
- New APIs - Besides an API for provisioning a Universal Share Projection Point, there is a new API that enable a Universal Share policy to be remotely initiated. This is especially handy for database administrators who want to script the Protection Point as part of their database dump script. Refer to the NetBackup 8.3 API reference documentation on SORT or on your master server:
  `https://<master_server>/api-docs/index.html`

For more information, see *About Universal Shares* in the NetBackup Administrator's Guide, Volume I.

RBAC enhancements

In NetBackup 8.3, role-based access control (RBAC) allows more granular permissions, improved flexibility, and greater control. The design of RBAC is based on Access Control Lists (ACLs) and it closely follows the ANSI INCITS 359-2004 standard. Earlier design of RBAC enforcement was dynamic in nature, whereas the new RBAC is static in its configuration.

By default, only the "Administrator" role is created, which has all privileges for RBAC. An "Administrator" must sign into the NetBackup web UI to configure any custom roles, such as a workload administrator or a backup administrator.

Note the following RBAC enhancements to NetBackup 8.3:

- The installation checks for pre-NetBackup 8.3 RBAC principals, roles, and object groups.
- Existing API key users must be assigned to a new RBAC role.
- Tools are available to migrate the **Backup administrator** role and create a new **Security administrator** role with the users that had the old RBAC **Security administrator** role. Other roles must be reconfigured manually.

More information about the RBAC tools is available:

- RBAC roles utility. Provides the latest role definitions for the new RBAC capabilities that are introduced in NetBackup 8.3.
  https://www.veritas.com/support/en_US/article.100047660
- User migration tool. Options include the ability to convert the **Backup administrator** role and to create a new **Security administrator** role and re-add any users that had the pre-8.3 **Security administrator** role.
  https://www.veritas.com/support/en_US/article.100047577

Configure storage servers in the NetBackup web UI

The NetBackup web UI lets you configure storage servers, disk pools, storage units, and universal shares. The types of storage servers available for configuration are: AdvancedDisk, Cloud storage, MSDP, and OpenStorage.

For more information, see the NetBackup 8.3 Web UI Administrator's Guide.

New link to Veritas SaaS Backup site added to the NetBackup web UI

The NetBackup web UI now includes a link to the Veritas SaaS Backup site. From the NetBackup web UI, select **Veritas SaaS Backup** on the left-side navigation to view information about this backup and recovery software-as-a-service (SaaS).

Notifications icon added to the NetBackup web UI

To make you aware of important system events, a **Notifications** icon is now located at the top right in the NetBackup web UI. If a number is displayed with the icon, it indicates how many unseen messages exist.

You can click the icon to open a **Notifications** window and view a list of the most recent notifications 10 at a time. From the window, you can choose to see a more comprehensive list of all notifications. You can sort, filter, and search the comprehensive list. You can also choose a specific notification and review details about it, including a full description as well as any appropriate extended attributes.

Note: Job events are not included with these notifications. See job details in the **Activity Monitor** for information about job events.

More information about notifications is available in the following guide:

NetBackup Web UI Backup Administrator's Guide

About policy management in the NetBackup web UI

The NetBackup web UI uses protection plans to protect the assets in your NetBackup environment. To manage classic policies you must use the NetBackup Administration Console. However, some policy types can also be managed in the NetBackup web UI:

- MS-Windows
- Standard
- Oracle
- MS-SQL-Server

See the following guides for details on these policies.

NetBackup Administrator's Guide, Volume I

NetBackup for Oracle Administrator's Guide

NetBackup for Microsoft SQL Server Administrator's Guide

Support for Single Sign-On in the NetBackup web UI

This release of NetBackup allows users to use Single Sign-On (SSO) to sign into the NetBackup web UI.

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only one AD or LDAP domain is supported for each master server domain. This feature is not available for local domain users.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.

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

Configuration settings added to NetBackup web UI

You can now configure the following settings in the NetBackup web UI:

- User session settings. These settings include session idle timeout, maximum concurrent sessions, user account lockout, and sign-in banner configuration.
- Trusted master servers.

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

Use NetBackup web UI to share images from an on-premises location to the cloud

Starting with NetBackup 8.3, you can use the NetBackup web UI to share images from an on-premises location to the cloud. You can set up a cloud recovery host on demand and share the images to that server.

This feature, which was earlier called automated disaster recovery, is now available from NetBackup web UI.

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

Audit events can be exported to system logs through the NetBackup web UI

You can now export NetBackup audit events to the system logs and view them in the system logs. For example, on a Windows system, use Windows Event Viewer to view the NetBackup audit events that you have exported. You can export the events of all or selected audit categories to the system logs. Use the **Audit event** settings option under **Security > Security events** in the NetBackupweb UI.

For more information, refer to the NetBackup Web UI Administrator’s Guide

CALLHOME_PROXY_SERVER option for NetBackup master and media servers

Veritas introduces the `CALLHOME_PROXY_SERVER` option for NetBackup master and media servers. The option lets you specify an unauthenticated proxy server that NetBackup uses to relay Smart Meter data to Veritas. At this time, NetBackup does not have a method to verify that the value is set correctly.

More information about this new option is available. See the NetBackup Administrator's Guide, Volume I and Smart Meter documentation.

RESTful APIs included in NetBackup 8.3

NetBackup 8.3 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 > 8.3
  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.

Note: The NetBackup APIs are not supported on environments where NetBackup Access Control (NBAC) is enabled.

NetBackup 8.3 includes these new and enhanced APIs:

- Access Control: Provides access to NetBackup role-based access control configuration.
- Asset Service: Provides access to NetBackup asset information.
- Cloud Buckets: Create and list cloud buckets for MSDP storage servers.
- Cloud Files & Folders Recovery: Recovers individual files and folders from cloud virtual machines.
- Cloud Recovery Targets: Lists the targets to which cloud assets can be recovered.

- Credential Management: Provides management of credentials used by NetBackup.
- Data Classifications: List data classifications defined in the system.
- Disk Volumes: Update disk volumes.
- Disk Volume Replication Targets: Provides ability to configuration replication targets for disk volumes.
- Event Log: Provides an insight of the activities and issues in the NetBackup environment. Also allows custom notifications with easy integration using event log messages and notifications APIs.
- Hosts: List hosts that are pending certificate renewal.
- Identity Providers: Manage identity provider configurations for single sign-on based authentication using SAML.
- Key Management Services: Provides access to key management service configuration.
- Media Servers: List media servers.
- NetBackup Certificate Authorities: Provides access to NetBackup certificate authority configuration.
- Policies: Make a copy of an existing policy and list unique clients associated with policies.
- Recovery Point Service: Query information on data that has been backed up based on workload.
- Security Domains: Manage AD/LDAP domains with Veritas NetBackup Authentication Service (AT).
- Snapshot Management Servers: Provides access to snapshot management server configuration.
- SQL Server Instant Access: Provides the Instant Acess capabilities for SQL Server backups.
- SQL Server Restore: Restore SQL Server from a single recovery point or a complete chain.
- SSO Login: Log in to the NetBackup web UI using single sign-on (SSO) authentication method.
- Trust Versions: List the trust versions based on NetBackup certificate authority migration.
- Trusted Master Servers: Provides access to trusted master server configuration.
- Universal Shares: Manage universal share storage on an MSDP storage server.

Deprecated APIs

The following APIs have been deprecated in NetBackup 8.3.

- Asset DB: The Asset DB APIs have been superseded by the Asset Service APIs.
- Role-Based Access Control: The APIs in the /rbac sub-context have been superseded by the /access-control sub-context. Any RBAC configuration data created using the APIs defined in the /rbac sub-context is now read-only. This data remains available to help create similar access control using the new APIs found in the /access-control sub-context.

Versioned APIs

The following APIs have been versioned in NetBackup 8.3. The previous version of these APIs is still supported if you specify the correct version.

- `GET /admin/jobs`

  The PolicyType enum was updated to be UPPERCASE_WITH_UNDERSCORES.

- `GET /admin/jobs/{jobId}`

  The PolicyType enum was updated to be UPPERCASE_WITH_UNDERSCORES.

- `POST /config/{workloadType}/access-hosts`

  Error code and response changed to 500 "client hostname could not be found", instead of a generic exception when an invalid access host is provided and cannot be validated.

- `GET /config/policies`

  Now returns more information than just each policy's name and has default pagination if called without pagination parameters.

- `POST /recovery/workloads/{workload}/scenarios/{scenarioType}/pre-recovery-check`

  Introduced 404 in pre-recovery check. This error is returned if an invalid vmserver is provided in the request.

- `GET /security/auditlogs`

  Now supports pagination, filtering, and sorting. This API now returns the audit details object.

- `GET /security/auditlogs/{auditId}`

  This API now returns the audit details object.

- `GET /security/cacert`

Now returns the latest trust-version along with the list of certificate authorities that need to be added or removed from the trust-store of the NetBackup host.

- `GET /security/logindetails`
  Now supports pagination, filtering, and sorting. This API now returns the audit login details object.
- `GET /security/logindetails/{auditId}`
  This API now returns the audit login details object.
- `GET /storage/disk-pools`
  No longer returns attributes related to size for CLOUD disk pools. Changed filter parameters from case insensitive to case sensitive.
- `POST /storage/disk-pools`
  No longer accepts kmsKeyPassphrase which was required for CLOUD disk pool.
- `POST /storage/storage-servers`
  Removed KMS attributes from input.
- `POST /storage/storage-servers/{storageServerId}/disk-volumes`
  Now supports creation of cloud disk volumes for MSDP storage servers.
- `GET /storage/storage-units`
  No longer returns attributes related to size for CLOUD storage unit.
- `GET /storage/storage-units/{storageUnitName}`
  No longer returns attributes related to size for CLOUD storage unit.
- `PATCH /storage/storage-units/{storageUnitName}`
  No longer returns attributes related to size for CLOUD storage unit.
- `GET /storage/storage-units/{storageUnitName}/replication-relationships`
  Updated resource type in the response.

Note: See the NetBackup 8.3 API Reference on SORT for more information. Make sure to review the *Versioning* topic and the *What's New* topic in the *Getting Started* section.

About NetBackup CA migration to a CA with key strength of 2048 bits and greater

In certain scenarios, you may need to migrate your existing NetBackup certificate authority (CA) hierarchy to a new one. NetBackup supports migrating the existing

NetBackup CA to a new one with the following key strengths: 2048 bits, 4096 bits, 8192 bits, and 16384 bits.

AfterNetBackup 8.3 installation or upgrade, new root CA with 2048-bits key strength is deployed.

The NetBackup CA migration process comprises the following stages:

1. Initiating NetBackup CA migration
2. Activating the new NetBackup CA
3. Completing NetBackup CA migration
4. Decommissioning the old NetBackup CA

Note: This process is an optional clean-up task.

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:

See "After initiating CA migration, connection errors may occur" on page 41.

See the NetBackup Security and Encryption Guide for more information on NetBackup CA migration.

Support for external key management service (KMS) servers

NetBackup supports external key management service (KMS) servers with certain configurations. Review the following prerequisites and important notes before you configure external KMS server in NetBackup:

- External KMS server should support Key Management Interoperability Protocol (KMIP).
- NetBackup supports KMIP versions 1.0, 1.1, 1.2, 1.3, 1.4 and 2.0. By default, NetBackup uses the highest version from this list that the external KMS supports.
- NetBackup master servers should be able to establish an outbound connection to the KMIP port (typically 5696) on the KMS.
- Symmetric keys from external KMS server are consumed for encryption and decryption.
- PEM-formatted certificates are used for authentication with external KMS server.

For more information about external KMS configuration, see the NetBackup Security and Encryption Guide.

NetBackup 8.3 support additions and changes

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

The following products and services are supported starting with NetBackup 8.3:

- Platforms
  - Red Hat Linux-s390x - client only. Media servers are no longer supported.
  - SUSE Linux-s390x - client only. Media servers are no longer supported.
  - Solaris 11.4 (x86-64) - client only.
- Databases
  - Microsoft SharePoint 2019
  - MongoDB 3.4, 3.6, 4.0 on CentOS 6/7/8
  - PSF - Hadoop 3.x on CentOS 7
  - PSF - Hadoop HDFS 3.1.x on Red Hat Enterprise Linux 7.7

Supported extended attributes and file types for granular restore on Linux and Windows

The following extended attributes and file types for granular restore are supported by NetBackup.

Supported Linux extended attributes and file types

- Attributes/metadata
  - User and group IDs (Basic ACLs)
  - File/folder mode, permissions and flags
  - Timestamps (modification and access time only)
- File types for restore
  - Regular file
  - Directory
  - Symbolic link
  - Hardlink
  - Sparse file

Supported Windows extended attributes and file types

- Attributes/metadata
  - Owner, Group, SCALs & DACLs
  - Basic, extended and inherited attributes
  - Timestamps (modification, access and creation time)
  - Advanced attributes like: compression, encryption, archive and index
  - Alternate Data Stream (ADS)
- File types for restore
  - Regular file
  - Compressed file
  - Encrypted file
  - Directory
  - File-Symlink
  - Directory Symlink
  - Directory Junction
  - Volume Junction
  - Hardlink
  - Sparse file

The following extended attributes and file types for granular restore are not supported by NetBackup.

Unsupported Linux extended attributes and file types

- Attributes/metadata
  - Extended ACL
  - Extended attributes (`xattrs`)
- File types for restore
  - Encrypted files or folders
  - Named pipe (FIFO)
  - UNIX sockets

Unsupported Linux extended attributes and file types

- Attributes/metadata
  - Unable to restore original DOS name
  - Restore previous file version
- File types for restore
  - Certain system and registry files or directories

NetBackup 8.3 licensing enhancements

NetBackup 8.3 includes these licensing enhancements:

- Flexible Licensing
  - Enhanced benefit: If a virtual machine is protected, irrespective of the policy type, it is treated as a virtual workload.
  - New license type string: For NetBackup 8.3 and later, set the license type in the `nbdeployutil` utility using `NETBACKUP_PLATFORM_BASE_COMPLETE_EDITION_FLEX` to enable the benefits of Flexible Licensing.

  For more information about Flexible Licensing, refer to the NetBackup Licensing Guide.

Performance improvement in the `nbdeployutil` utility

NetBackup has made improvements in the `nbdeployutil` utility that help to reduce overall run time of the utility. You must upgrade the master server to NetBackup 8.3 to see these improvements immediately for scheduled reports. If you are manually running the `nbdeployutil` utility, the improvements are observed 90 days after the upgrade to NetBackup 8.3.

In a multi-master server scenario, it is recommended that you upgrade all the master servers to see all the improvements.

For more information about `nbdeployutil`, refer to the NetBackup Commands Reference Guide.

Newer SuSE Linux compilers used with NetBackup 8.3

The following platforms now use SLES Linux 12, SP3:

- Linux SLES x86_64
- Linux zSeries SLES 64-bit

Note: NetBackup 8.3 cannot be installed on these systems if the OS kernel is older than 4.4.73. The client names are now `SuSE4.4.73` and `IBMzSeriesSuSE4.4.73`.

Support for persistent robotic paths for Linux media servers

NetBackup 8.3 introduces the ability to configure persistent robotic paths for Linux media servers.

To enable this functionality, you can download a Linux rules file from the Veritas Support Downloads Center. When the downloaded rules file is installed in the specified directory, NetBackup uses `/dev/tape/by-path` type paths that persist across SAN interruptions. If this rules file is not present, NetBackup continues to use the `/dev/sg` type paths.

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*.

Move the NetBackup database from any btrfs file systems

Veritas does not support the installation or upgrade of the NetBackup database on a btrfs file system. If the NetBackup database resides on a btrfs file system, move the database to a supported file system (such as ext4 or xfs) before you start the upgrade. The database files reside on the master server in the directories under `/usr/openv/db`. More information about moving the database before an upgrade is available in the NetBackup Upgrade Guide.

Optional installation of Java GUI and JRE

Starting with NetBackup 8.3, the Java GUI and the JRE packages are optional for UNIX, Linux, and Windows media servers and UNIX and Linux clients.

As with previous releases, the Java GUI and JRE packages are installed automatically on all master servers because they are required. The Java GUI and the JRE are not part of the default installation on Windows clients. Install the Java

Remote Administration Console if you require this functionality on your Windows clients.

Changes to user session default values

With NetBackup 8.3, the default values for two user session parameters have changed to increase security.

The default number of failed sign-in attempts allowed is 5. Previously, this value was 0.

- In the NetBackup web UI, go to **User sessions > User account settings > Number of failed sign-in attempts allowed**.
- In the NetBackup Administration Console, go to **NetBackup Management > Host Properties > Master Servers > server > User Account Settings > Account lockout > Number of failed log-in attempts allowed**
- With the CLI, use the `GUI_MAX_LOGIN_ATTEMPTS` parameter with commands. For example, `bpgetconfig -X GUI_MAX_LOGIN_ATTEMPTS`.

The default value for the account lockout duration is 15 minutes. Previously, this value was 1440 minutes (24 hours). (The user account is automatically unlocked after the lockout duration.)

- In the NetBackup web UI, go to **User sessions > User account settings > Unlock locked accounts**.
- In the NetBackup Administration Console, go to **NetBackup Management > Host Properties > Master Servers > server > User Account Settings > Account lockout duration**
- With the CLI, use the `GUI_ACCOUNT_LOCKOUT_DURATION` parameter with commands. For example, `bpgetconfig -X GUI_ACCOUNT_LOCKOUT_DURATION`.

By default, these user session settings are enabled. You can disable these settings with the NetBackup web UI, the NetBackup Administration Console, or the `bpsetconfig` command.

Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 8.3

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 8.3. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 8.3, 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 version 2.5.4 or newer. The following cloud support has been added to version 2.5.4 and later but was not included in the NetBackup 8.3 final build:

- Hitachi Vantara CloudScale (S3)
- Nutanix Objects (S3)
- Orange Business Systems Flexible Engine OBS (S3)
- SandStone MOS (S3)
- Amazon (S3) regions:
  - Africa (Cape Town)
  - Asia Pacific (Hong Kong)
  - Europe (Milan)
  - Europe (Stockholm)
  - Middle East (Bahrain)
- Google (S3) regions:
  - Asia East 2
  - Asia Northeast 2
  - Asia-South1
  - EU-North1
  - EU-West4
  - EU-West 6
  - NorthAmerica-Northeast1
  - SouthAmerica-East1
  - US-West2
- SwiftStack Object Storage (S3) buffer size changes

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

New Asset Services APIs require conversion for Cloud assets

As a result of database changes for Cloud assets, a migration of existing assets is required if you upgrade to a NetBackup 8.3 master server. This process is a one-time conversion that occurs after the upgrade.

Migration Steps:

- The migration process begins when the Cloud Asset service plug-in starts. (There is a 30-second delay.) A warning in the header of the API response indicates that migration is in progress. The warning is also displayed in the NetBackup web UI. During this process, the provided data may be inconsistent and incomplete.
- For every 10,000 cloud assets, migration takes approximately 10 minutes. Migration time may be affected if any jobs are running concurrently.
- Each asset is also registered with RBAC.

After migration:

- The previous AssetDB APIs will no longer function correctly. You must convert them to the new Asset Service APIs. For information about Asset Services APIs, refer to the API Reference documentation on SORT or to the YAML files on the master server: `https://<master_server>/api-docs/index.html`

About uploading deduplicated data to the cloud using MSDP cloud

NetBackup 8.3 introduces MSDP cloud, a new cloud solution with the deduplication technology. Data is stored directly to cloud targets with deduplication.

One MSDP storage server can support both local storage and multiple cloud storage targets. After you configure the MSDP storage server, you can add a cloud storage target to that storage server and then the MSDP storage server can store data to cloud target.

You can use the following types of NetBackup media servers to configure MSDP cloud:

NetBackup host	Version	Configuration information
NetBackup Appliance	Veritas NetBackup Appliance	NetBackup Appliance Documentation
NetBackup media server	NetBackup 8.3 on Red Hat Enterprise Linux or CentOS	NetBackup 8.3 Deduplication Guide

For information about the supported cloud vendors and features, refer to the NetBackup Master Compatibility Lists.

If your NetBackup setup contains one MSDP storage server, configure the MSDP storage server and add another cloud storage to that storage server. You can use the MSDP cloud feature in the following scenarios:

- Create a disk pool and a storage unit using the cloud storage and back up the data directly to that cloud storage.
- Create a disk pool and a storage unit using the cloud storage. Back up the data to the local MSDP storage server and then do an optimized deduplication to duplicate the data to the cloud storage.

For more information about configuration, administration, and troubleshooting, refer to the NetBackup 8.3 Deduplication Guide.

CloudPoint is available from the NetBackup web UI

Starting with NetBackup 8.3, you can add CloudPoint servers from the NetBackup web UI. You can manage CloudPoint and control discovery of assets from the NetBackup web UI, REST API, and CLI without interacting with the CloudPoint interfaces.

You can upgrade from CloudPoint 2.x and later. If you are using a standalone CloudPoint server and want to use it along with NetBackup, you can migrate your CloudPoint server. For more information, See the Veritas NetBackup CloudPoint Install and Upgrade Guide.

Support for Nutanix Files file shares

CloudPoint adds support for Nutanix storage arrays. You can configure the new CloudPoint plug-in for Nutanix Files to discover and protect NFS shares on Nutanix storage arrays.

For more details on the Nutanix Files plug-in, refer to the *Veritas NetBackup CloudPoint Install and Upgrade Guide*.

Granular restore of files, folders, and volumes on cloud virtual machines

NetBackup enables you to perform a granular restore of files and folders on cloud virtual machines. You can create snapshots and restore, at the same time you can also locate and restore individual files and folders. You can also restore volumes from virtual machines.

This process is known as granular restore in which each single file in the snapshot is considered as a granule or more commonly referred to as single file restore. NetBackup makes an inventory of all the files within a snapshot using an indexing

process. You can restore specific files from a snapshot only if that snapshot has been indexed by NetBackup. See the NetBackup Web UI Cloud Administrator's Guide for more information.

Update for RHV workload from NetBackup web UI

You can now configure the RHV access host from the NetBackup web UI. The access host lets your RHV environment communicate securely with NetBackup.

For more information, refer to the NetBackup Web UI RHV Administrator's User Guide.

Database changes require migration of VMware and RHV assets

As a result of database changes for VMware and RHV assets, a migration of existing assets is required if you upgrade to a NetBackup 8.3 master server. This process is a one-time conversion that occurs after the upgrade.

Migration Steps:

- The migration process begins when the VMware or RHV Asset service plug-in starts. (There is a 30-second delay.) A warning in the header of the API response indicates that migration is in progress. The warning is also displayed in the NetBackup web UI. During this process, the provided data may be inconsistent and incomplete.
- For every 10,000 assets, migration takes approximately 15 minutes. Migration time may be affected if any jobs are running concurrently.
- Each asset is also registered with RBAC.

After migration:

- The previous AssetDB APIs will no longer function correctly. You must convert them to the new Asset Service APIs. For information about Asset Services APIs, refer to the API Reference documentation on SORT or to the YAML files on the master server: `https://<master_server>/api-docs/index.html`

Build your own (BYO) support on RHEL for VMware Instant Access

NetBackup now supports VMware Instant Access Build Your Own (BYO). You can build your own storage server on a Red Hat Enterprise Linux (RHEL) operating system to support VMware instant access. For more information, see the following guide:

NetBackup Web UI VMware Administrator’s Guide

NetBackup install now includes the Nutanix Acropolis Hypervisor (AHV) plug-in for the Hypervisor policy

With NetBackup 8.3, the Nutanix Acropolis Hypervisor (AHV) plug-in for the **Hypervisor** policy is installed as part of the NetBackup installation.

The Hypervisor policy leverages several existing NetBackup features to protect the hypervisor and the virtualization workloads. For example, incremental backups and accelerator for hypervisors using the hypervisor change block tracking capabilities.

Hypervisor policy will also support the newer versions of Nutanix AHV.

Veritas recommends that you migrate your existing BigData policies to Hypervisor policy for protecting your Nutanix AHV VMs.

- Starting with NetBackup 8.3, you cannot create new **BigData** policies to protect your Nutanix AHV VMs. (You cannot create a **BigData** policy that has `Application_Type=Nutanix-AHV` value in the backup selection.)
  However, the existing **BigData** policies will work after the upgrade.
- From the next NetBackup release after version 8.3, the **BigData** policies for protecting Nutanix AHV VMs will not run.

For more information, refer to the NetBackup for Nutanix AHV Administrator's Guide.

Note: You can continue using the **BigData** policy to protect your Hadoop, HBase, and MongoDB data.

Restore of the Nutanix AHV VMs that were backed up using the BigData policy are supported.

Enhancements and changes for the Microsoft SQL Server agent

This release of NetBackup includes these enhancements and changes for the Microsoft SQL Server agent:

Support for the Microsoft SQL Server agent with the NetBackup web UI:

- Configure a classic policy to protect SQL Server.
- Configure protection plans to protect SQL Server.
- Manage SQL Server credentials.
- Support for immediate backups (Backup now) in the NetBackup web UI.
- The `nbsqladm` command can be enabled or disabled using the `ENABLE_NBSQLADM` option. For details see the NetBackup Administrator's Guide, Volume I and the NetBackup Commands Reference Guide.

- The `nbsqladm` command options `-new_host` and `-new_instance` are deprecated. To change an instance or a host name, delete the instance and use `-add_instance` to add the instance again.
- Retry attempts for failed backups attempt a retry of only the failed database backups instead of all the databases that were attempted for backup. This new retry behavior is supported for all objects: instances, availability groups, and clusters. This update only applies to intelligent policies and not to batch-file based policies.
- Improvements to make discovery of SQL Server instances, availability groups, and databases faster and more efficient.

Microsoft SQL Server Instant Access support

NetBackup now supports Instant Access for Microsoft SQL Server. You can use this feature with NetBackup Appliance or Build Your Own (BYO) storage server on a Red Hat Enterprise Linux (RHEL) operating system. For more information, see the following guide:

NetBackup Web UI Microsoft SQL Server Administrator's Guide

Microsoft SQL Server stream handler introduced

NetBackup 8.3 introduces the Microsoft SQL Server stream handler. You can apply the Microsoft SQL Server stream handler to all of the Microsoft SQL Server version and Azure SQL Server. You can use the **MS-SQL** policy or the **Standard** policy to enable this feature.

You can enable and disable the Microsoft SQL Server stream handler per policy or all policies at once using the `cacontrol` command line utility.

For more information, see the NetBackup Deduplication Guide.

Support for Microsoft SQL standalone and Availability Group (AG) databases

CloudPoint adds support for Microsoft SQL standalone databases and also the databases that are a part of a SQL Availability Group (AG). You can use the CloudPoint application plug-in for Microsoft SQL to discover and protect application instances and standalone and AG databases.

For more information about the SQL plug-in, refer to the *Veritas NetBackup CloudPoint Install and Upgrade Guide*.

Enhancements for NetBackup for Oracle

NetBackup 8.3 includes the following Oracle-related enhancements:

- In the **Specify maximum limits** section of the Oracle tab in the NetBackup web UI, you can specify **Section size** for all Oracle backups performed. This parameter enables RMAN's multisection backup.
- When an Oracle instance or an instance group needs to be registered, you can use **Oracle Wallet** as an option for credentials.
- NetBackup 8.3 provides full support of Oracle Real Application Clusters (RAC) when you set up an Oracle policy in the NetBackup web UI. However, the NetBackup Administration Console does not have support for Oracle RAC policy setup.
  The NetBackup Web UI Security Administrator's Guide contains the instructions to add an Oracle RAC.
  The NetBackup for Oracle Administrator's Guide contains all information for creating an Oracle RAC policy that applies to the policy creation in the web UI. Note that all setup information in Appendix A and Appendix B is deprecated as of NetBackup 8.3. The next NetBackup maintenance release removes the support for the setup that is described in these appendices. All OIP users should use the Oracle RAC feature in the web UI to protect any RAC setup.
- The NetBackup web UI also has the ability to load balance the RAC database during a backup. The NetBackup Web UI Security Administrator's Guide contains the information for load balancing.

Oracle stream handler introduced

NetBackup 8.3 introduces the Oracle stream handler. The Oracle stream handler is enabled by default for newly created Oracle policies after an upgrade to NetBackup 8.3. By default, the Oracle stream handler only supports stream-based backups. You can enable and disable the Oracle stream handler per policy or all policies at once using the `cacontrol` command line utility.

When the Oracle stream handler is used, the `FILESPERSET` variable is more flexible. You can set `FILESPERSET > 1` in the policy or the `bp.conf` without a large decrease in deduplication rates.

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

NetBackup install now includes the MongoDB plug-in

With NetBackup 8.3, the MongoDB plug-in is installed as part of the NetBackup installation. Use the MongoDB plug-in to protect your MongoDB data.

For more information, refer to the NetBackup MongoDB Administrator's User Guide.

Changes in the legacy 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.

More information is available:

See "If NetBackup 8.3 upgrade fails on Windows, revert to previous log folder structure" on page 41.

Bare Metal Restore enhancements

NetBackup 8.3 includes the following enhancements for NetBackup Bare Metal Restore (BMR):

- The BusyBox TPIP component is upgraded from 1.24.1 to 1.31.1 in 3PPCD. It is recommended that you download the latest 3.0 version of 3PPCD using the following link:
  https://www.veritas.com/content/support/en_US/downloads/update.UPD238422
- NetBackup BMR configurations are supported based on the operating system and the patch release. More information about the supported operating systems and patch levels for BMR configurations is available:
  https://www.veritas.com/content/support/en_US/article.100039356
- The following BMR boot server and client versions are supported on LDOM and LPAR:

Hypervisor Type and Version	OS Version on Guest VM Version
Solaris LDOM 11.3	Solaris SPARC 10.11, 11.0, 11.1, 11.2, and 11.3
AIX LPAR 7.2	AIX 6.1, 7.1, and 7.2

MSDP multi-domain support added

Previously, the NetBackup media servers and clients cannot directly use an MSDP storage server from another NetBackup domain. For example, NetBackup media servers or clients cannot backup data to an MSDP storage server from another NetBackup domain.

Starting with NetBackup 8.3, with the MSDP multi-domain support, one NetBackup domain can directly use the storage server from another NetBackup domain.

For more information about configuration, administration, and troubleshooting, refer to the NetBackup 8.3 Deduplication Guide.

Integration of Veritas Resiliency Platform with NetBackup

You can integrate NetBackup and Veritas Resiliency Platform to manage your disaster recovery operations. Veritas Resiliency Platform provides a single console from which you can proactively maintain business uptime across private, public, and hybrid clouds. Integrating NetBackup and Resiliency Platform lets you leverage the capabilities, such as complete automation, visualizing and monitoring DR-specific information for all resiliency operations for the virtual machines in your data center. You can add, edit, delete, or refresh a Resiliency Platform. You can add more than one Resiliency Platform in NetBackup. See the NetBackup Web UI Administrator's Guide for more information.

Enhancements to NAS workloads

- Dynamic data streaming for NAS workloads
  You can perform an off-host backup of NAS volumes, where a volume is backed up using multiple dynamic data streams. Dynamic streaming is built on the NetBackup client framework and uses the NASData- Protection policy type for snapshot and backup orchestration.
- Introducing new NAS-Data-Protection policy
  The NAS-Data-Protection policy supports storage lifecycle policy as policy storage, snapshot, and backup from snapshot as primary and secondary operations.
- Configuring dynamic data streaming with backup host pool
  Backup host pool is a group of master, media, or client servers that can be used for taking backups. The dynamic data streaming feature with backup host pool is supported for Linux and Windows master and media server only

For more information about these enhancements, see the NetBackup Snapshot Client Administrator's Guide.

Chapter 3

Operational notes

This chapter includes the following topics:

About NetBackup 8.3 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 8.3.

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 8.3 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 8.3 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 8.3 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

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

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

About support for HP-UX Itanium vPars SRP containers

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

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

NetBackup administration and general operational notes

NetBackup provides a complete, flexible data protection solution for a variety of platforms. The platforms include Windows, UNIX, and Linux systems. In addition to a standard set of data protection features, NetBackup can also utilize several other licensed and non-licensed components to better protect a variety of different systems and environments. This topic contains some of the general operational notes and known issues that are associated with the administration of NetBackup 8.3.

Backups for workloads that use the BigData policy may fail

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

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

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

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

Images can be expired from NetBackup catalog even if still WORM-locked on storage

Commands to immediately expire images do not check whether an image is WORM-locked and result in the removal of images from the NetBackup catalog as it would for non-WORM images. If the images are still WORM-locked on storage, image cleanup jobs show `error 2060069 unable to delete indelible image`. NetBackup continues to try to delete these images until either it is successful (for example, once the WORM indelible time has elapsed) or until `nbdelete -purge_deletion_list` is used to remove the images from the cleanup worklist.

Workaround: Re-import such images if they were removed from NetBackup catalog by mistake.

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

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

Workaround:

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

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

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

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

To renew the web server certificate using the new CA

1. Verify if the `nbatd` service has successfully migrated the NetBackup CA using the following steps:
   - Check the migration summary status. The status should be 'INITIATED'.
   - Run the `nbseccmd -nbcamigrate -summary` command to check the CA migration status.
   - The new key pair with the desired key size should be present in the NetBackup web server keystore. Check the keystore at the following location:
     On Windows:
     <INSTALL_PATH>`/var/global/vxss/tomcatcreds/nbwebsvc/.VRTSat/profile/certstore/keystore`
     On UNIX:
     <INSTALL_PATH>`/var/global/vxss/tomcatcreds/nbwebsvc/.VRTSat/profile/certstore/keystore`
2. After you have verified that the `nbatd` service has successfully migrated the NetBackup CA, run the following command to renew the NetBackup web server certificate:

   ```
   nbseccmd -nbcamigrate -syncMigrationDB
   ```

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

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

Workaround:

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

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

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

Workaround:

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

2. Trigger a manual backup.

Under unusual circumstances, SLP copies are incorrectly expired

Under unusual circumstances, SLP copies are incorrectly expired.

During SLP duplication the `bpduplicate` process can lose connection with its child `bpdm` process. If that happens, the first duplication attempt fails. SLP duplications are resilient to failures and retry until all specified copies have been created. If the duplication retry occurs and completes promptly, the orphaned `bpdm` process can expire the duplicate.

After `bpdm` tries to update its disconnected `bpduplicate` parent process, the orphaned `bpdm` process attempts to add metadata for the duplicate copy the SLP was asked to create. The `bpdbm` daemon responds that the copy already exists, and in response, the orphaned `bpdm` requests that the image be deleted.

See the following tech note for more information:

https://www.veritas.com/support/en_US/article.100047236

Granular restores require adequate available space on target

If the space available on the target restore file system is not enough, the granular restore operation fails.

Workaround: Ensure that enough space is available on the target restore file system.

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 limitations when using IPv6 address as client name or image name

The following NetBackup limitations can occur if an IPv6 address is used as a client name or an image name:

- Using IPv6 addresses as client names in a policy do not work with Instant recovery (IR) snapshots on Windows systems. That can cause a backup to fail. Specify a host name instead of an IPv6 address.

  Image names are created automatically in NetBackup, and consist of a combination of the client name and a timestamp. If the client name is configured in the policy as the IPv6 address, the result is an image name (in the image catalog) that includes the IPv6 address. That causes the backup to fail.

- Using IPv6 addresses as image names under the catalog do not work with Instant Recovery (IR) snapshots on Windows systems.

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 8.3.

For more information about the specific NetBackup administration interfaces, refer to the *NetBackup Administrator's Guide, Volume I*. For information about how to install the interfaces, refer to the *NetBackup Installation Guide*. For information about platform compatibility with the administration consoles, refer to the various NetBackup compatibility lists available on the Veritas Support website.

See “About NetBackup compatibility lists and information” on page 77.

Screen resolution of 1280x1024 or higher recommended for NetBackup web UI

When you use the NetBackup web UI, Veritas recommends that you use a screen resolution of 1280x1024 or higher. Lower screen resolutions have known problems on some of the web UI screens.

NetBackup web UI policies list may temporarily display out-of-date policy details

The web UI policies list may temporarily display out-of-date policy details and some options that are not supported in the web UI. This issue may occur if the policy is created or modified outside of the web UI, such as the Java GUI or CLI. Communication between the web UI and other clients is not instantaneous. The communication process can take up to one minute after the policy’s most recent change.

Workaround: If you see the issue, refresh the web UI policy list one minute after the policy’s most recent change. Or, you can view the policy’s details page immediately for up-to-date details.

Search limitations for security events lists in the NetBackup web UI

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

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

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

Terminating a NetBackup Administration Console session from the web UI does not log the user out

When a user logs into the NetBackup Administration Console, NetBackup creates a session. That session appears in the **Active sessions** tab of the NetBackup web UI and can be terminated. However, if that session is terminated from the web UI, the user is not logged out of the NetBackup Administration Console completely. Instead, some functionality in the NetBackup Administration Console may not work properly. Users may receive a message such as `Status Code: 117. Web service`

```
authentication failed. You may have to log in to the NetBackup
Administrator Console again.
```

Note: Veritas recommends that you do not terminate these sessions from the **Active sessions** tab of the NetBackup web UI.

Workaround: If a session is terminated from the web UI, the user must log in again to the NetBackup Administration Console to regain full functionality.

Access control methods supported in NetBackup 8.3

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. You cannot use the web UI if you have NetBackup Access Control (NBAC) enabled.

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

"Operation timed out" message appears when policies are accessed from the Remote Administration Console

When you access policies from the NetBackup Remote Administration Console, a warning message is displayed:

```
The operation timed out. The operation has exceeded the time out
limit, though service or daemon may still be processing the request.
```

The warning appears because the `NBJAVA_CORBA_DEFAULT_TIMEOUT` default value is less than required. However, the policies still can be accessed after you click **OK**.

Workaround: Modify the `NBJAVA_CORBA_DEFAULT_TIMEOUT` value:

- From:
  `SET NBJAVA_CORBA_DEFAULT_TIMEOUT=60`
- To:
  `SET NBJAVA_CORBA_DEFAULT_TIMEOUT=300`

After completing the changes, restart the NetBackup Remote Administration Console. The policies are loaded within maximum 5 minutes (300 seconds).

For more information about setting configuration options for the NetBackup Remote Administration Console, see the NetBackup Administrator's Guide, Volume I for NetBackup 8.3.

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.

Reduced functionality during the initialization of the NetBackup Administration Console

The following issues occur if one or more of the NetBackup services or daemons on the host that is specified in the logon dialog is not running:

- Reduced functionality (for example, only the Backup, Archive, and Restore component is available).
- **Cannot Connect** errors occur during initialization of the NetBackup Administration Console

NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later

The NetBackup Administration Console may encounter a core dump issue when the Simplified Chinese UTF-8 locale is used on a Solaris SPARC 64-bit system

with Solaris 10 Update 2 and later installed. For more information, refer to Bug ID 6901233 at the following URL on the Oracle Technology Network website:

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6901233

If you encounter this issue, apply the appropriate Solaris patches or upgrades that Oracle provides for this issue.

NetBackup Bare Metal Restore operational notes

NetBackup Bare Metal Restore (BMR) automates and streamlines the server recovery process, making it unnecessary to reinstall operating systems or configure hardware manually. This topic contains some of the operational notes and known issues that are associated with BMR in NetBackup 8.3.

After upgrading the NetBackup master server to 8.3, BMR backup jobs may report failure

After upgrading the NetBackup master server to 8.3, the upgrade will be successful, however, you may see failure for BMR backup jobs with the error message `The NetBackup client version is incompatible with the master server.`

Refer to the following Veritas Support article for more information:

https://www.veritas.com/docs/100048124

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

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

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

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

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

NetBackup 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 8.3.

Before you configure 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.

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.
```

Snapshots on t2.type instances created from AWS Amazon Linux AMIs are not supported

Snapshots on t2.type instances created from AWS Amazon Linux AMIs are not supported.

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.

Indexing error may occur for Micorosft Azure cloud assets

For Microsoft Azure cloud assets, the indexing operation fails sometimes with the following error:

```
No available slots to attach disk.
```

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 8.3.

Image clean-up may fail for Microsoft Azure workloads

For Microsoft Azure workloads, image clean-up fails with following error:

```
30464: invalid error code .
```

Workaround: This error is related to Veritas CloudPoint. Refer to the Veritas CloudPoint release notes for incidents 7253 and 8030.

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
```

MongoDB create snapshot job may freeze

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

```
flexsnap-coordinator: "Jun 18 22:31:51 11f5b9b5977c
flexsnap-coordinator[1] Thread-4037029 flexsnap.coordinator:
 WARNING - post_snapshot failed for child

<asset_id: eg:fs-lnxnative-ext4-74d0ad4b-d81e-4819-9a68-
 bda6b3750b8e-33280449d30c2bb766721379375a1130>
 with exc <Exception details>.
```

Workaround:

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

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

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

Replica retention value is not honored even if it is longer than the snapshot retention value

Amazon AWS cloud snapshot replica retention is not honored when it is different from the primary snapshot retention.

Workaround:

1. Use the following command to get a list of all the cloud images along with other image information:

   ```
   <install_path>/bpimagelist -L -pt Cloud
   ```

   To get images for specific a client:

   ```
   <install_path>/bpimagelist -L -client <client_name>
   ```

2. Use the following command to check images that have a replica copy:

   ```
   <install_path>/bpimagelist -L -pt Cloud -backupid <backup_id>
   ```

   Search for the keyword "number of copies" and if the `number_of_copies` value is greater than 1 then it implies that image has replica copies.

3. Use one of the following commands to update expiry time for each replica copy:

   ```
   <install_path>/bpexpdate -recalculate -backupid <backup_id> -ret
   <retention_level> -copy <copy_number>
   ```

```
<install_path>/bpexpdate -backupid <backup_id> -d <date_in_format
mm/dd/yy hh:mm:ss> -copy <copy_number>
```

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

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

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

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

Permission denied error occurs if both user and password are updated

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

Workaround:

To avoid this issue:

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

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

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

Workaround:

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

Broken files system detected

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

NetBackup database and application agent operational notes

NetBackup offers several methods of protecting various database and application technologies This topic contains some of the operational notes and known issues that are associated with the protection of database technologies in NetBackup 8.3.

NetBackup for Microsoft SQL Server operational notes

NetBackup for SQL Server extends the capabilities of NetBackup for Windows to include backups and restores of SQL Server databases. These capabilities are provided for a Windows client using either a UNIX or Windows NetBackup master server. This topic contains some of the operational notes and known issues that are associated with NetBackup for Microsoft SQL Server in NetBackup 8.3.

Notes and restrictions for Microsoft SQL Server agent

- Note the following for the protection status of an asset:
  - The NetBackup web UI does not indicate if a classic policy protects an instance or an availability group. Use the NetBackup Administration Console to see how classic policies are used to protect instances or availability groups.
  - If a backup image does not exist for an asset, the web UI indicates that it is “Not protected”.
- Databases only appear on the **Databases** tabs in the NetBackup web UI if they meet one of the following criteria: A backup exists of the database, the database instance has validated credentials, or a manual discovery of databases was performed.
- The discovery process displays two messages. First, when a request to start discovery is initiated for the databases or availability groups the web UI displays, “Starting the discovery of…”. The discovery doesn’t begin until the second message displays, “Successfully started the discovery of ... Click Refresh to update the list.”
- NetBackup discovers and displays failover cluster instances (FCIs) under the cluster name and the physical node names. For example, instance `FCI` is

enumerated with both its physical nodes `hostvm10` and `hostvm11` and with its cluster name `sql-fci`. Databases are also enumerated with the node names and the cluster name.

- You must have the Microsoft SQL Server Native Client version 11.0.7462 ODBC driver or later installed on the availability group replicas to be able to discover and to browse databases on a read-scale availability group. Exit status 114 is received in the NetBackup Administration Console when you browse for databases from a SQL Server intelligent policy. In the web UI, a read-scale availability group is not discovered, but no error message is given.

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 8.3.

Support for localized environments in database and application agents

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

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

- VMWare:
  Username, Password, VM display name, DataCenter, Folder, Datastore, Resource pool, VApp, Network name, VM disk path

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

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

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

NetBackup for NDMP operational notes

NetBackup for NDMP is an optional NetBackup application. It enables NetBackup to use the Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems. This topic

contains some of the operational notes and known issues that are associated with NetBackup for NDMP in NetBackup 8.3.

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

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

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

NetBackup Snapshot Client operational notes

NetBackup Snapshot Client provides a variety of snapshot-based features for NetBackup. It supports clients on UNIX, Linux, and Windows platforms, on Fibre Channel networks (SANs) or traditional LANs. Each snapshot method relies on the snapshot technology that is built into the storage subsystem where the data is stored. This topic contains some of the operational notes and known issues that are associated with Snapshot Client in NetBackup 8.3.

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 8.3.

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 8.3.

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

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

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

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

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

Consider the following scenario:

- NetBackup is enabled to support NAT clients.
- An STU is created using the NetBackup Administration Console.
- You create a protection plan for VMware backup using the NetBackup web UI.
- You provide a backup host that has access to virtualization server.
- You assign the protection plan to a VMware asset.
- You check the policy that is created as part of the subscription.
- The correct VMware backup host appears on the **VMware** tab in the NetBackup Administration Console, but the **Clients > NetBackup host to perform automatic virtual machine selection** option is set to **Backup Media Server**. The media server cannot access the virtualization server, and the backup fails with status code 200.

Workaround:

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

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

Recommended SORT procedures for new installations

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

Table A-1

Procedure	Details
Create a Veritas Account on the SORT webpage	See "To create a Veritas Account on the SORT page" on page 64.
Create generic installation reports	See "To create a generic installation checklist" on page 64.
Create system-specific installation reports	See "To create a system-specific installation report for Windows" on page 65. See "To create a system-specific installation report for UNIX or Linux" on page 66.

To create a Veritas Account on the SORT page

1. In your web browser, navigate to:

   https://sort.veritas.com/netbackup

2. In the upper right corner, click **Login**, then click **Register now**.
3. Enter the requested login and contact information:

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

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

To create a generic installation checklist

1. In your web browser, navigate to:

   https://sort.veritas.com/netbackup

2. Find and select the **Installation and Upgrade Checklist** widget.

3 Specify the requested information

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

4 Click **Generate Checklist**.

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

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

To create a system-specific installation report for Windows

1 Go to the SORT website:

https://sort.veritas.com/netbackup

2 In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.

3 Select the **Data Collectors** tab

4 Select the radio button for **Graphical user interface** and download the correct data collector for your platform.

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

5 Launch the data collector after it finishes downloading.

6 On the **Welcome** screen, select **NetBackup** from the product family section and click **Next**.

7 On the **System Selection** screen, add all computers you want analyzed. Click **Browse** to see a list of computers you can add to the analysis. Veritas recommends starting the tool with an administrator or a root account.

8 When all systems are selected, review the **System names** section and click **Next**.

9 In the **Validation Options** screen, under **Validation options**, select the version to which you plan to upgrade.

10 Click **Next** to continue

11 The utility performs the requested checks and displays the results. You can upload the report to My SORT, print the results, or save them. Veritas recommends that you upload the results to the My SORT website for ease of centralized analysis. Click **Upload** and enter your My SORT login information to upload the data to My SORT.

12 When you are finished, click **Finish** to close the utility.

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

1 Go to the SORT website:

https://sort.veritas.com/netbackup

2 In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.

3 Select the **Data Collector** tab.

4 Download the appropriate data collector for your platform.

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

5 Change to directory that contains downloaded utility.

6 Run `./sortdc`

The utility performs checks to confirm the latest version of the utility is installed. In addition, the utility checks to see it has the latest data. The utility then lists the location of the log file for this session.

7 If requested, press **Enter** to continue.

8 Select the **NetBackup Family** at the **Main Menu**.

9 Select **Installation/Upgrade report** when prompted **What task do you want to accomplish?**

You can select multiple options by separating your response with commas.

10 Specify the system or systems you want included in the report.

If you previously ran a report on the specified system, you may be prompted to run the report again. Select **Yes** to re-run the report.

The utility again lists the location of the log files for the session.

The progress of the utility is displayed to the screen.

11 Specify **NetBackup** when prompted for the product you want installation or upgrade reports.

12 Enter the number that corresponds to the version of NetBackup you want to install.

The utility again lists the location of the log files for the session.

The progress of the utility is displayed to the screen.

13 The utility prompts you to upload the report to the SORT website if you want to review the report online. The online report provides more detailed information than the text-based on-system report.

14 When your tasks are finished, you can exit the utility. You have the option to provide feedback on the tool, which Veritas uses to make improvements to the tool.

Recommended SORT procedures for upgrades

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

Table A-2

Procedure	Details
Create a Veritas Account on the SORT webpage	See "To create a Veritas Account on the SORT page" on page 64.

Table A-2 *(continued)*

Procedure	Details
Create a system-specific upgrade report	See "To create a system-specific installation report for Windows" on page 65. See "To create a system-specific installation report for UNIX or Linux" on page 66.
Review the future platform and feature plans. Review the hot fix and emergency engineering binary release auditor information.	See "To review future platform changes and feature plans" on page 68. See "To review hot fix and emergency engineering binary information" on page 68.

To review future platform changes and feature plans

1. In your web browser, navigate to:

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

To review hot fix and emergency engineering binary information

1. In your web browser, navigate to:

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

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

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*, the *NetBackup Upgrade Guide*, and the *NetBackup Getting Started Guide*.

See "NetBackup installation and upgrade operational notes" on page 41.

- 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 8.3, 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.

- Master and media servers must have a minimum soft limit of 8000 file descriptors per process for NetBackup to run correctly.
  For more information about the effects of an insufficient number of file descriptors, refer to the following tech note on the Veritas Support website:
  http://www.veritas.com/docs/000013512
- To install NetBackup on Windows 2008/Vista/2008 R2/ UAC-enabled environments, you must log on as the official administrator. Users that are assigned to the Administrators Group and are not the official administrator cannot install NetBackup in UAC-enabled environments.
  To allow users in the Administrators Group to install NetBackup, disable UAC.
- NetBackup master and media servers exchange server version information at startup, and every 24 hours. This exchange occurs automatically. During startup after an upgrade, the upgraded media server uses the `vmd` service to push its version information to all of the servers that are listed in its server list.
- Veritas recommends that you have the master server services up and available during a media server upgrade.
- All compressed files are compressed using gzip. The installation of these files requires gunzip and gzip, so make sure that they are installed on the computer before you attempt to install NetBackup. For all UNIX platforms except HP-UX, the binaries are expected to be in `/bin` or `/usr/bin` and that directory is a part of the root user's `PATH` variable. On HP-UX systems, the `gzip` and `gunzip` commands are expected to be in `/usr/contrib/bin`. Installation scripts add that directory to the `PATH` variable. These commands must be present to have successful UNIX installations.

Required operating system patches and updates for NetBackup

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

The compatibility lists include information about the minimum OS level that is required to support a minimum NetBackup version in the latest major release line. In some cases, new releases of NetBackup may require specific vendor OS updates or patches. Table B-1 includes the OS updates and patches that are required for NetBackup 8.3. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 8.3 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 62.

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

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

Table B-1 Required operating system patches and updates for NetBackup 8.3

Operating system type and version	NetBackup role	Patch	Notes
AIX 6.1		AIX run-time libraries 9.0.0.3 or later	The run-time libraries need to be at 9.0.0.3 or later. You may need to restart after you change to version 9.0.0.3.
HP-UX		COMPLIBS.LIBM-PS32	If you install AT on an HP-UX platform, this patch is required.
HP-UX IA-64		Networking.NET-RUN: /usr/lib/libipv6.sl	
		Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.1	
		Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.sl	
		Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so	
		Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so.1	
		Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so	
		Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so.1	
		Networking.NET2-RUN: /usr/lib/libipv6.1	
Windows Vista x86-64	Client	KB936357	Microsoft microcode reliability update (suggested)
	Client	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Server 2008 x86-64	Client	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.

Table B-1 Required operating system patches and updates for NetBackup 8.3 *(continued)*

Operating system type and version	NetBackup role	Patch	Notes
Windows Server 2008 x86-64 (SP2)	Master, media, client	KB979612	Hot fix to improve TCP loopback latency and UDP latency
Windows Server 2008 x86-64 R2	Master, media, client	KB2265716	Hot fix for when a computer randomly stops responding. Note that this patch is also contained in Windows Server 2008 R2 SP1.
	Master, media, client	KB982383	Hot fix for a decrease in I/O performance under a heavy disk I/O load. Note that this patch is also contained in Windows Server 2008 R2 SP1.
	Master, media, client	KB983544	Update for the "Modified time" file attribute of a registry hive file. Note that this patch is also contained in Windows Server 2008 R2 SP1.
	Master, media, client	KB979612	Hot fix to improve TCP loopback latency and UDP latency Note that this patch is also contained in Windows Server 2008 R2 SP1.

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

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

NetBackup 8.3 binary sizes

Table B-2 contains the approximate binary sizes of the NetBackup 8.3 master server, media server, and client software for the various supported operating systems. These binary sizes indicate the amount of disk space occupied by the product after an initial installation. Note that for the sizes listed in the table, 1 MB equals 1024 KB.

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

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

See "About Veritas Services and Operations Readiness Tools" on page 62.

Table B-2 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
AIX	POWER		1681 MB	No longer supported	
Canonical Ubuntu	x86-64		1231 MB		
CentOS	x86-64		1236 MB	5848 MB	Media server or client compatibility only.
Debian GNU/Linux	x86-64		1231 MB		
HP-UX	IA-64		2141 MB	No longer supported	
Oracle Linux	x86-64		1237 MB	5877 MB	

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

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
Red Hat Enterprise Linux Server	POWER		313 MB		
Red Hat Enterprise Linux Server	x86-64		1237 MB	5850 MB	
Red Hat Enterprise Linux Server	z/Architecture		847 MB	No longer supported	Media server or client compatibility only.
Solaris	SPARC		1189 MB	5403 MB	
Solaris	x86-64		1213 MB	5750 MB	
SUSE Linux Enterprise Server	POWER		313 MB		
SUSE Linux Enterprise Server	x86-64		1070 MB	5158 MB	
SUSE Linux Enterprise Server	z/Architecture		859 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64		483 MB	2881 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 8.3.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Agent	Server	ViewBuilder
Oracle Linux	x86-64		772 MB	
Red Hat Enterprise Linux Server	x86-64		749 MB	
SUSE Linux Enterprise Server	x86-64		782 MB	
Windows Server	x86-64	261 MB	695 MB	230 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 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 62.

For NetBackup, SORT provides an Installation and Upgrade Checklist report as well as the ability to collect, analyze, and report on host configurations across your environments. In addition, you can determine which release contains the hot fixes or EEBs that you may have installed in your environment. You can use this data to assess whether your systems are ready to install or upgrade to a given release.

NetBackup compatibility lists

In addition to SORT, Veritas has made available a variety of compatibility lists to help customers quickly reference up-to-date compatibility information for NetBackup. These compatibility lists can be found on the Veritas Support website at the following location:

http://www.netbackup.com/compatibility

Note: For information about which versions of NetBackup are compatible with each other, select a **Software Compatibility List (SCL)**, and then select **Compatibility Between NetBackup Versions** from within the SCL.

About NetBackup end-of-life notifications

Veritas is committed to providing the best possible data protection experience for the widest variety of systems: platforms, operating systems, CPU architecture, databases, applications, and hardware. Veritas continuously reviews NetBackup system support. This review ensures that the proper balance is made between maintaining support for existing versions of products, while also introducing new support for the following:

- General availability releases
- Latest versions of new software and hardware
- New NetBackup features and functionality

While Veritas continually adds support for new features and systems, it may be necessary to improve, replace, or remove certain support in NetBackup. These support actions may affect older and lesser-used features and functionality. The affected features and functionality may include support for software, OS, databases, applications, hardware, and 3rd-party product integration. Other affected items may include the products that are no longer supported or nearing their end-of-support life with their manufacturer.

Veritas provides advance notification to better help its customers to plan for upcoming changes to the support status of the various features in NetBackup. Veritas intends to list older product functionality, features, systems, and the 3rd-party software products that are no longer supported in the next release of NetBackup. Veritas makes these support listings available as soon as possible with a minimum of 6 months where feasible before major releases.

Using SORT

Advance notification of future platform and feature support including end-of-life (EOL) information is available through a widget on the Veritas Services and Operations Readiness Tools (SORT) for NetBackup home page. The NetBackup Future Platform and Feature Plans widget on the SORT for NetBackup home page can be found directly at the following location:

https://sort.veritas.com/nbufutureplans

NetBackup end-of-support-life (EOSL) information is also available at the following location:

https://sort.veritas.com/eosl/show_matrix

See “About Veritas Services and Operations Readiness Tools” on page 62.

About changes in platform compatibility

The NetBackup 8.3 release may contain changes in support for various systems. In addition to using SORT, you should make sure to review the *NetBackup Release Notes* document and the NetBackup compatibility lists before installing or upgrading NetBackup software.

See “About new enhancements and changes in NetBackup” on page 11.

http://www.netbackup.com/compatibility

Appendix D

Other NetBackup documentation and related documents

This appendix includes the following topics:

About related NetBackup documents

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

Veritas releases various guides that relate to NetBackup software. 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 8.3. In these cases, refer to the latest version of the guide that is available. Unless otherwise specified, all NetBackup documents can be downloaded in PDF format or viewed in HTML format from the following location:

http://www.veritas.com/docs/000003214

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

Documentation published with NetBackup 8.3

Release notes and general administration guides:

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

Installation and configuration guides:

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

NetBackup Web UI guides:

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

NetBackup options guides:

- *NetBackup Add-in for Microsoft SCVMM Console Guide*
- *NetBackup Cloud Administrator's Guide*
- *NetBackup CloudPoint Installation Guide*
- *NetBackup Deduplication Guide*
- *NetBackup for Hadoop Administrator's Guide*
- *NetBackup for NDMP Administrator's Guide*
- *NetBackup for Nutanix Acropolis Hypervisor (AHV) Administrator's Guide*
- *NetBackup for VMware Administrator's Guide*
- *NetBackup Logging Reference Guide*
- *NetBackup OpenStorage Solutions Guide for Disk*
- *NetBackup OpsCenter Administrator's Guide*
- *NetBackup Plug-in for VMware vSphere Web Client*
- *NetBackup Plug-in for VMware vSphere Client (HTML5)*
- *NetBackup SAN Client and Fibre Transport Guide*
- *NetBackup Snapshot Client Administrator's Guide*

- *WebSocket Service (NBWSS) Reference Guide*

Database agent guides:

- *NetBackup for DB2 Administrator's Guide*
- *NetBackup for Hbase Administrator's Guide*
- *NetBackup for MariaDB Administrator's Guide*
- *NetBackup for Microsoft SQL Server Administrator's Guide*
- *NetBackup for MongoDB Administrator's Guide*
- *NetBackup for MySQL Administrator's Guide*
- *NetBackup for Oracle Administrator's Guide*
- *NetBackup for OpenStack Administrator's Guide*
- *NetBackup for PostgreSQL Administrator's Guide*
- *NetBackup for SQLite Administrator's Guide*

Troubleshooting guides:

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

Other reference guides:

- *NetBackup Commands Reference Guide*
- *NetBackup Emergency Engineering Binary Guide*
- *NetBackup in Highly Available Environments Guide*
- *NetBackup Network Ports Reference Guide*
- *NetBackup Security and Encryption Guide*
- *NetBackup Self Service Configuration Guide*
- *NetBackup Self Service Installation Guide*
- *NetBackup Self Service Release Notes*
- *NetBackup Third-party Legal Notices*