

Veritas NetBackup™ Release Notes

Release 8.2

Document Version 5



Veritas NetBackup™ Release Notes

Last updated: 2019-11-07

Legal Notice

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

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

<https://www.veritas.com/support>

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

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

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1	About NetBackup 8.2	9
	About the NetBackup 8.2 release	9
	About NetBackup Late Breaking News	10
	About NetBackup third-party legal notices	10
Chapter 2	New features, enhancements, and changes	11
	About new enhancements and changes in NetBackup	11
	NetBackup 8.2 new features, changes, and enhancements	12
	External certificate authority certificates supported by NetBackup 8.2	14
	Configure external security certificates from the NetBackup Administration Console	14
	NetBackup supports file-based certificates and Windows certificate store as external certificate sources	15
	Support for NetBackup web UI sign-in with a smart card or software certificate	15
	More backup jobs can start per second	15
	Compression rates and deduplication rates are now reported separately for MSDP storage	15
	RESTful APIs included in NetBackup 8.2	15
	New API keys feature provides user authentication to APIs and commands	18
	NetBackup 8.2 support additions and changes	18
	NetBackup licensing enhancements	20
	About NAT support in NetBackup	21
	BMR client restores from NetBackup 8.2 servers require NetBackup CA-signed certificates	21
	The update_clients script is no longer available for client pushes	21
	Several shutdown commands to be deprecated in a future release	21
	OpenStack workloads protected with BigData policies	22
	New pre-installation checks added	22
	Assign RBAC roles during UNIX installations	22
	Media server install and upgrade improvements	23

VxUpdate support for upgrading media servers	23
Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 8.2	23
Certificate validation for cloud providers against Certificate Revocation List (CRL)	24
Configure custom object chunk size for new cloud storage	24
Change in NetBackup Cloud configuration service	24
New parameter (<code>CSSC_ALLOW_LEGACY_AUTH</code>) added to support older cloud storage media servers	25
Backup data to cloud using NetBackup with Amazon Snowball and Amazon Snowball Edge	25
Auto Image Replication (AIR) and target AIR now support CloudCatalyst storage server	25
Integrated snapshot management enhancements	26
New option (<code>reinitialize</code>) added to the <code>csconfig</code> command utility	27
NetBackup enhancements for VMware	27
NetBackup protection for Red Hat Virtualization (RHV)	28
New Instant Access features	28
Changes to global resource limits for VMware, RHV, and Hyper-V resources	29
Enhanced recovery process for Nutanix AHV virtual machines	29
NetBackup introduces Accelerator support for Nutanix AHV through the upcoming Nutanix AHV plug-in	29
Enhancements for the Microsoft SQL Server agent	30

Chapter 3	Operational notes	31
	About NetBackup 8.2 operational notes	31
	NetBackup installation and upgrade operational notes	32
	Linux daemon shutdown issues	32
	Native installation requirements	32
	NetBackup 8.2 and SUSE 15 installation issue	33
	NetBackup 8.2 and RHEL 8 installation issue	33
	NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952	33
	Do not install from the menu that appears when the installation DVD is inserted	34
	About support for HP-UX Itanium vPars SRP containers	34
	NetBackup administration and general operational notes	34
	NetBackup master server is not supported on a btrfs file system	35

Non-administrator users in environments with NBAC cannot read or update resource limits	35
Media servers and backup host must use the same NetBackup version for BigData policies	35
Backups for workloads that use the BigData policy may fail	35
OpenStack restore jobs successful even when instance recreation fails	36
NetBackup limitations when using IPv6 address as client name or image name	36
NetBackup administration interface operational notes	36
Terminating a NetBackup Administration Console session from the web UI does not log the user out	37
Terminating a NetBackup web UI session does not log the user out immediately	37
Access control methods supported in NetBackup 8.2	37
"Operation timed out" message appears when policies are accessed from the Remote Administration Console	38
Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms	38
Intermittent issues with X forwarding of NetBackup Administration Console	38
Reduced functionality during the initialization of the NetBackup Administration Console	39
NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later	39
NetBackup API operational notes	39
NetBackup APIs must be called with percent-encoded URLs	40
If a restarted backup or snapshot job fails, the job initiator ID no longer appears in the NetBackup Jobs API response	40
NetBackup Cloud operational notes	40
OpenStack backup job fails with error 6619	40
Automated Disaster Recovery recovers VMs with AWS VM import prerequisites	40
Import and recoverec2 jobs may fail on automated DR servers	41
Unable to obtain the administrator password to use an AWS EC2 instance that has a Windows OS	41
Certificate Revocation check using CRL not supported with Veritas Access cloud storage	42
Storage server may display incorrect value of CRL if SSL is off	42
NetBackup with Veritas CloudPoint operational notes	42

CloudPoint 2.x messages are in English for ISM	42
Image clean-up may fail for Microsoft Azure workloads	43
NetBackup database and application agent operational notes	43
NetBackup for Hadoop operational notes	43
NetBackup deduplication operational notes	43
Dialog box might become unresponsive when you configure MSDP	
KMS encryption	44
NetBackup internationalization and localization operational notes	44
Support for localized environments in database and application	
agents	45
Certain NetBackup user-defined strings must not contain non-US	
ASCII characters	45
NetBackup for NDMP operational notes	46
Parent directories in the path of a file may not be present in an	
NDMP incremental image	46
NetBackup SAN Client and Fibre Transport operational notes	46
Unable to stop the nbftclnt process on the NetBackup client	47
NetBackup Snapshot Client operational notes	47
HPE 3PAR array snapshot import fails with status code 4213	
.....	47
Snapshots are deleted after point-in-time rollbacks	47
Index from Snapshot operation does not populate contents of the	
snapshot accurately in the catalog	48
NetBackup virtualization operational notes	48
NetBackup for VMware operational notes	48
NetBackup for Hyper-V operational notes	50
 Appendix A	
About SORT for NetBackup Users	51
About Veritas Services and Operations Readiness Tools	51
Recommended SORT procedures for new installations	52
Recommended SORT procedures for upgrades	56
 Appendix B	
NetBackup installation requirements	58
About NetBackup installation requirements	58
Required operating system patches and updates for NetBackup	60
NetBackup 8.2 binary sizes	64
 Appendix C	
NetBackup compatibility requirements	67
About NetBackup compatibility lists and information	67
About NetBackup end-of-life notifications	68

Appendix D	Other NetBackup documentation and related documents	70
	About related NetBackup documents	70

About NetBackup 8.2

This chapter includes the following topics:

- [About the NetBackup 8.2 release](#)
- [About NetBackup Late Breaking News](#)
- [About NetBackup third-party legal notices](#)

About the NetBackup 8.2 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 8.2 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 8.2 can be found on the Veritas Operations Readiness Tools (SORT) website and in the [NetBackup Emergency Engineering Binary Guide](#).

See [“About Veritas Services and Operations Readiness Tools”](#) on page 51.

About NetBackup appliance releases

The NetBackup appliances run a software package that includes a preconfigured version of NetBackup. When a new appliance software release is developed, the

latest version of NetBackup is used as a basis on which the appliance code is built. For example, NetBackup Appliance 3.1 is based on NetBackup 8.1. This development model ensures that all applicable features, enhancements, and fixes that were released within NetBackup are included in the latest release of the appliance.

The NetBackup appliance software is released at the same time as the NetBackup release upon which it is based, or soon thereafter. If you are a NetBackup appliance customer, make sure to review the *NetBackup Release Notes* that correspond to the NetBackup appliance version that you plan to run.

Appliance-specific documentation is available at the following location:

<http://www.veritas.com/docs/000002217>

About NetBackup Late Breaking News

For the most recent NetBackup news and announcements, visit the NetBackup Late Breaking News website at the following location:

<http://www.veritas.com/docs/000040237>

Other NetBackup-specific information can be found at the following location:

https://www.veritas.com/support/en_US/15143.html

About NetBackup third-party legal notices

NetBackup products may contain third-party software for which Veritas is required to provide attribution. Some of the third-party programs are available under open source or free software licenses. The license agreement accompanying NetBackup does not alter any rights or obligations that you may have under those open source or free software licenses.

The proprietary notices and the licenses for these third-party programs are documented in the *NetBackup Third-party Legal Notices* document, which is available at the following website:

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

New features, enhancements, and changes

This chapter includes the following topics:

- [About new enhancements and changes in NetBackup](#)
- [NetBackup 8.2 new features, changes, and enhancements](#)

About new enhancements and changes in NetBackup

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

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

See [“About the NetBackup 8.2 release”](#) on page 9.

See [“About NetBackup compatibility lists and information”](#) on page 67.

NetBackup 8.2 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 8.2 are grouped below by category. Select a link to read more information about the topic.

New features

- [External certificate authority certificates supported by NetBackup 8.2](#)
- [Configure external security certificates from the NetBackup Administration Console](#)
- [NetBackup supports file-based certificates and Windows certificate store as external certificate sources](#)
- [Support for NetBackup web UI sign-in with a smart card or software certificate](#)
- [More backup jobs can start per second](#)
- [Compression rates and deduplication rates are now reported separately for MSDP storage](#)
- [RESTful APIs included in NetBackup 8.2](#)
- [New API keys feature provides user authentication to APIs and commands](#)

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 8.2 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 8.2 support additions and changes](#)
- [NetBackup licensing enhancements](#)
- [About NAT support in NetBackup](#)
- [BMR client restores from NetBackup 8.2 servers require NetBackup CA-signed certificates](#)

- The `update_clients` script is no longer available for client pushes
- Several shutdown commands to be deprecated in a future release
- OpenStack workloads protected with BigData policies

Installation, upgrade, and configuration changes and enhancements

- New pre-installation checks added
- Assign RBAC roles during UNIX installations
- Media server install and upgrade improvements
- VxUpdate support for upgrading media servers

Cloud-related changes and enhancements

- Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 8.2
- Certificate validation for cloud providers against Certificate Revocation List (CRL)
- Configure custom object chunk size for new cloud storage
- Change in NetBackup Cloud configuration service
- New parameter (`CSSC_ALLOW_LEGACY_AUTH`) added to support older cloud storage media servers
- Backup data to cloud using NetBackup with Amazon Snowball and Amazon Snowball Edge
- Auto Image Replication (AIR) and target AIR now support CloudCatalyst storage server
- Integrated snapshot management enhancements
- New option (`reinitialize`) added to the `csconfig` command utility

Virtualization changes and enhancements

- NetBackup enhancements for VMware
- NetBackup protection for Red Hat Virtualization (RHV)
- New Instant Access features
- Changes to global resource limits for VMware, RHV, and Hyper-V resources
- Enhanced recovery process for Nutanix AHV virtual machines
- NetBackup introduces Accelerator support for Nutanix AHV through the upcoming Nutanix AHV plug-in

Database agent changes and enhancements

- [Enhancements for the Microsoft SQL Server agent](#)

External certificate authority certificates supported by NetBackup 8.2

Veritas introduces support for external certificate authority certificates. This change provides an alternative to the NetBackup Certificate Authority for providing host verification and security. It supports certificates in PEM, DER, and P7B formats.

For more information about external CA support in NetBackup and external CA-signed certificates, see the following resources:

- Video: [Using External Certificate authority \(CA\)-signed certificates with NetBackup](#)
- [NetBackup Security and Encryption Guide](#).

External certificate authority limitations in NetBackup 8.2

- **External certificate authority specifications containing UNC paths or mapped network drives fail for Windows hosts that use a remote installation method**

You cannot use UNC paths and mapped network drives for external CA certificate specifications on Windows hosts performing remote installations. Remote installation methods include VxUpdate and the setup wizard push installation option. If you attempt to use a UNC path or mapped network drive, the precheck and the installation operations fail due to inaccessible paths.

Configure external security certificates from the NetBackup Administration Console

You can now configure external CA-signed certificates when you add a new deployment policy or modify an existing deployment policy from the NetBackup Administration Console. External CA-signed certificates are signed by a CA other than the NetBackup CA. The **Change Deployment Policy** dialog box contains a new **Security** tab that lets you configure the security certificates.

For more information, refer to the [NetBackup Administrator's Guide, Volume 1](#).

NetBackup supports file-based certificates and Windows certificate store as external certificate sources

With NetBackup 8.2, you can use X.509 certificates that your trusted certificate authority (CA) has issued. NetBackup supports file-based certificates and Windows certificate store as external certificate sources.

In a clustered master server setup, a Windows certificate store as an external certificate source is not supported.

For more information, refer to the "About external CA support in NetBackup" chapter from the [NetBackup Security and Encryption Guide](#)

Support for NetBackup web UI sign-in with a smart card or software certificate

Security administrators can allow NetBackup web UI users to sign in with a Common Access Card (CAC), personal identity verification (PIV) card, or a digital certificate.

More backup jobs can start per second

NetBackup can now start more than one backup job per second across a master server domain. For any one client, the limit of starting only one job per second still holds. However, multiple jobs from different clients can now be started within the same second. Depending on the configuration involved, significantly more backup jobs can be started within any fixed time period, which may change the performance behavior of the system. In some environments, you may need to change some configuration settings to achieve the optimum performance behavior.

Compression rates and deduplication rates are now reported separately for MSDP storage

NetBackup now supports the reporting of compression rates and deduplication rates separately for the MSDP storage consumption.

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

RESTful APIs included in NetBackup 8.2

NetBackup 8.2 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 > 8.2](#)

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 8.2 includes these new and enhanced APIs:

- Jobs API: Includes progress logs and individual try logs
- Discover Now: Provides the ability to manually initiate discovery on a vCenter or RHV managers
- Images API: Provides the ability to browse content, manage expiration, change primary copy, fast import for CloudCatalyst
- VM Server Credential Management: Provides the ability to verify and delete credentials
- VM Server Configuration Management: Includes resource limits and proxy host configuration
- Common Access Card (CAC) and Personal Identity Verification (PIV): Provides the ability to authenticate by user certificate
- User Session Management: Compliant with Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)
- API Keys: API authentication management

- **Storage Management:** Create, read, update, and delete (CRUD) operations on disk and cloud STUs, disk pools, cloud storage pools, and MSDP replication topology management
- **NetBackup Configuration Management:** Lists running processes and daemons. Also read and update configuration, similar to `bpgetconfig` and `bpsetconfig`
- **Manual Backup:** Performs `bpbackup` operations on existing policies

Versioned APIs

The following APIs have been versioned in NetBackup 8.2. The previous version of these APIs is still supported if you specify the correct version.

```
GET /admin/jobs
GET /admin/jobs/{jobId}
GET /admin/jobs/{jobId}/try-logs
POST /config/slps
PATCH /config/slps/{slpName}
GET /config/snapshotproviders/supportedplugins
GET /config/snapshotproviders/supportedplugins/{pluginType}
POST /config/snapshotproviders/configuredplugins/{pluginType}/
    instances
PUT /config/snapshotproviders/configuredplugins/{pluginType}/
    instances/{instanceName}
GET /config/hosts
POST /preview-asset-group
POST /recovery/workloads/vmware/instant-access-mounts
GET /recovery/workloads/vmware/instant-access-mounts
GET /recovery/workloads/vmware/instant-access-mounts/{mountId}
POST /recovery/workloads/vmware/instant-access-mounts/{mountId}/
    restore
POST /recovery/workloads/vmware/instant-access-vms
GET /recovery/workloads/vmware/instant-access-vms
GET /recovery/workloads/vmware/instant-access-vms/{mountId}
POST /servicecatalog/slos
GET /servicecatalog/slos
GET /servicecatalog/slos/{sloId}
PUT /servicecatalog/slos/{sloId}
PATCH /servicecatalog/slos/{sloId}
DELETE /servicecatalog/slos/{sloId}
GET /storage/storage-units
GET /storage/storage-units/{storageUnitName}
```

Note: See the [NetBackup 8.2 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.

New API keys feature provides user authentication to APIs and commands

NetBackup now supports user authentication through API keys. A NetBackup API key is a pre-authenticated token that lets a NetBackup user run NetBackup commands, such as `nbcertcmd -createToken` or `nbcertcmd -revokeCertificate`, or access NetBackup RESTful APIs.

Unlike a password, an API key can exist for a long time and you can configure its expiration. Therefore, any operations that need authentication can run for a long time using API keys.

NetBackup 8.2 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 8.2:

- Platforms
 - Red Hat Enterprise Linux 8.0 (Power) - client
 - Red Hat Enterprise Linux 8.0 (x86-64) - master server, client
 - SUSE Linux Enterprise Server 15 (POWER) - client
 - SUSE Linux Enterprise Server 15 (x86-64) - master server, media server, client
 - SUSE Linux Enterprise Server 15 (z/Architecture) - media server, client
 - Windows Server 2019 (x86-64) - master server, media server
- Virtualization
 - Nutanix support
 - AOS version 5.10
 - VMware support
 - vCloud Director 9.1, 9.5 New features, enhancements, and changes 18
 NetBackup 8.2 new features, changes, and enhancements

- VDDK 6.7 U2
- Guest OS support for Hyper-V on Windows Server 2016
 - SUSE Linux Enterprise Server 15
- Databases
 - Apache Hadoop HDFS 3.x
 - Microsoft Exchange Server 2019
 - Microsoft Exchange Server 2019 CU1
 - Oracle Database 18.4 (18c)
 - Guest OS support for Hyper-V on Windows Server 2016
- BMR support
 - BMR client and BMR boot server
 - Oracle Enterprise Linux 6.10 (x86-64)
 - Red Hat Enterprise Linux 6.10 (x86-64)
 - Red Hat Enterprise Linux 7.6 (x86-64)
 - Solaris 11.2 (SPARC)
 - Solaris 11.3 (SPARC)
 - Windows Server 2019
 - BMR server
 - Red Hat Enterprise Linux 6.10 (x86-64)
 - Windows Server 2019

Cloud provider changes and enhancements

This release of NetBackup includes these Cloud provider changes and enhancements:

- Support for the following cloud providers is discontinued with NetBackup 8.2. However, NetBackup OpsCenter reports job data for these providers for the media servers that use an older version.
 - AT&T
 - Rackspace
 - Atmos
- The following Amazon S3 cloud providers are supported:

- Kingsoft Standard Storage Service
- Veritas Cognitive Object Storage
- Support is added for the following Amazon S3 regions:
 - Amazon EU (Paris) and CN: Ningxia
 - Amazon GovCloud US-East region
- Support is added for the Amazon AWS IAM Roles for stream-based backup operations.
- Support is added for Azure Germany region.
- Backing up data to the Microsoft Azure Archive tier is supported.
- Support is added for Glacier Deep Archive storage class for Amazon and AmazonGov.
- For backups to Glacier, the zero the lifecycle policy is changed to direct uploads.
- NetBackup CloudCatalyst now supports Amazon S3 Glacier.

For more information about cloud vendor support, see the [NetBackup Cloud Administrator's Guide](#) .

NetBackup licensing enhancements

NetBackup 8.2 includes these licensing enhancements:

- NEVC licensing support for `nbdeployutil`
 Smart Meter supports the NetBackup Enterprise Virtual Client (NEVC) licensing model only for customers who have NetBackup 8.2 master servers at this time. NEVC licensing is based on the total number of CPU sockets of a hypervisor. When you set the license type as NEVC, `nbdeployutil` captures NEVC usage information and generates a licensing report during its automated or scheduled run. This NEVC information is sent to Smart Meter. For more information about NEVC licensing, refer to the NetBackup licensing guide.

- Traditional, NEVC, Capacity – NDMP and BigData, and NetBackup Platform Base Complete Edition with Flex Licensing support in Smart Meter

Smart Meter supports these licensing platforms:

- NetBackup Traditional Licensing Model Edition
- NetBackup Enterprise Virtual Client Edition (NEVC)
- NetBackup Platform Base BigData Workload Edition
- NetBackup Platform Base NDMP Edition

- NetBackup Platform Base Complete Edition with Flexible Licensing

The `nbdeployutil` utility sends usage information for these licensing types that are displayed on the Smart Meter portal.

The `nbdeployutil` utility does not support Complete Edition with Flexible Licensing at this time, and `nbdeployutil` does not create flex reports or a JSON file. NetBackup sends the NetBackup Platform Base Complete Edition usage information to Smart Meter which is further converted to Flex licensing support usage. Smart Meter displays both the actual usage of the customer and the converted usage for Complete Edition with Flexible Licensing.

About NAT support in NetBackup

NetBackup now supports NetBackup clients in a private network that are connected to NetBackup servers in a public network through a device that performs network address translation (NAT). Such NetBackup clients are referred to as NAT clients.

For information on enabling support for NAT clients in NetBackup, see the [NetBackup Administrator's Guide, Volume I](#).

BMR client restores from NetBackup 8.2 servers require NetBackup CA-signed certificates

Bare Metal Restore (BMR) restores use NetBackup CA-signed certificates or host ID-based certificates. Therefore, the NetBackup 8.2 master and media servers that contain backup images for BMR clients must have NetBackup CA-signed certificates for successful BMR restores.

For more information on the BMR workflows that are supported in NetBackup 8.2, refer to the following article:

https://www.veritas.com/support/en_US/article.100044534

The `update_clients` script is no longer available for client pushes

Be aware you cannot use the `update_clients` installation script to push NetBackup 8.2 or later clients. You must use `VxUpdate`. For more information on `VxUpdate`, see the [NetBackup Upgrade Guide](#).

Several shutdown commands to be deprecated in a future release

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

- `bp.kill_all`

- `bpdown`
- `bpclusterkill`

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

OpenStack workloads protected with BigData policies

The NetBackup BigData policy now protects OpenStack workloads.

For detailed information about using the BigData policy for OpenStack, refer to the *NetBackup for OpenStack Administrator's Guide*.

New pre-installation checks added

NetBackup uses a pre-installation program that performs checks at the beginning of installations or upgrades to try to make sure that the operation will be successful before proceeding. The checks that are performed were developed from customer input on previous problems that were encountered during installations and upgrades.

Ten new networking and configuration checks were added for NetBackup 8.2. Veritas can update the checker whenever new customer feedback is received. Refreshes are not dependent on a NetBackup release. If your server can connect to telemetry.veritas.com, NetBackup automatically updates the checker with the latest version when the installation or the upgrade starts.

Video: [The NetBackup 8.2 Upgrade Experience](#)

Assign RBAC roles during UNIX installations

RBAC bootstrapping lets you assign role-based access control (RBAC) permissions to a user or a user group during NetBackup installation or upgrade on UNIX platforms. The UNIX installer uses the `bpbaz -AddRBACPrincipal` CLI to grant both security administrator and backup administrator permissions to the user or the user group that you specify in the `/tmp/NBInstallAnswer.conf` file.

Note: RBAC bootstrapping provides access to all objects for the specified user or user group, even if previously the user or the user group had restricted access to certain objects. For example, the existing user Tester1 was assigned the backup administrator role with access to only some object groups. If Tester 1 is specified for RBAC bootstrapping, Tester1 is assigned both the backup administrator and the security administrator roles with access to all objects.

After installation or upgrade, you can run the `bpbaz -AddRBACPrincipal` CLI standalone on both Windows and UNIX platforms to assign RBAC permissions. The CLI is available only on the master server.

For more information, refer to the following guides:

- *NetBackup Installation Guide*
- *NetBackup Upgrade Guide*
- *NetBackup Commands Reference Guide*
- *NetBackup Web UI Security Administrator's Guide*

Media server install and upgrade improvements

In NetBackup 8.2, the ability to install and upgrade NetBackup media servers using native operating system commands has been added. Similar to the native packages for clients feature, the configuration is driven by an answer file.

For more information, see the appropriate sections in the following guides:

- [NetBackup Installation Guide](#)
- [NetBackup Upgrade Guide](#)

VxUpdate support for upgrading media servers

In NetBackup 8.2, the ability to upgrade media servers using VxUpdate has been added. Media server running NetBackup versions 7.7 and later can be upgraded using this method. The ability to apply EEBs to NetBackup 8.2 media servers has also been added.

Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 8.2

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 8.2. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 8.2, related operations fail.

Veritas continuously adds new cloud support to the cloud configuration files between releases. The cloud storage support in the NetBackup 8.2 final build matches that which is contained in the cloud configuration package version 2.6.0.

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 8.2 final build:

- Nutanix Buckets (S3)

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

<http://www.veritas.com/docs/100033434>

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

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

Certificate validation for cloud providers against Certificate Revocation List (CRL)

For all the cloud providers, NetBackup provides a capability to verify the SSL certificates against the CRL (Certificate Revocation List). If SSL is enabled and the CRL option is enabled, each non-self-signed SSL certificate is verified against the CRL. If the certificate is revoked, NetBackup does not connect to the cloud provider. For more information, see the *NetBackup Cloud Administrator's Guide*.

Configure custom object chunk size for new cloud storage

For new cloud storage, you can specify a custom object chunk size to enhance the performance of backup and restore operations. For more information, see the *NetBackup Cloud Administrator's Guide*.

Change in NetBackup Cloud configuration service

The NetBackup CloudStore Service Container (`nbcssc`) service is a web-based service that is used for cloud configuration on the media servers that are configured for cloud storage. Starting with NetBackup release 8.2, the `nbcssc` service is no longer being deployed.

The operations that `nbcssc` performed are now taken over by two existing NetBackup services. The NetBackup Web Management Console (`nbwmc`) service now handles the cloud configuration operations and the NetBackup Service Layer (`nbsl`) service handles the throttling service and the metering data collector service functions.

However, NetBackup does provide support for the older media servers that are configured for cloud storage. Media server versions 7.7.x to 8.1.2 are supported. The older media servers that host the `nbcssc` service can work seamlessly with a master server that is upgraded to the latest version. The master server uses port 5637 to communicate with the `nbcssc` service running on older media servers.

This back-level media support sets up a smoother transition path for your existing NetBackup deployment wherein you can plan rolling upgrades for the older media servers without disrupting your existing cloud storage production workflow.

Refer to the *Veritas NetBackup Cloud Administrator's Guide* for more information about cloud configuration. Refer to the *Veritas NetBackup Network Ports Reference Guide* for more information on the ports that NetBackup uses.

New parameter (CSSC_ALLOW_LEGACY_AUTH) added to support older cloud storage media servers

All the NetBackup cloud storage configuration parameter settings are defined in the `cloudstore.conf` configuration file. To enable communication with the older media servers that are configured for cloud storage, NetBackup 8.2 introduces a new parameter named `CSSC_ALLOW_LEGACY_AUTH`. You can use this parameter to enable or disable master server communication with legacy cloud storage media servers.

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

Backup data to cloud using NetBackup with Amazon Snowball and Amazon Snowball Edge

Amazon Snowball and Amazon Snowball Edge devices can be configured with NetBackup and CloudCatalyst to backup data to cloud.

For more information, see *Protecting data with Amazon Snowball and Amazon Snowball Edge* in the [NetBackup Cloud Administrator's Guide](#).

Auto Image Replication (AIR) and target AIR now support CloudCatalyst storage server

CloudCatalyst storage server can be the source or the target server for AIR and targeted AIR. When the source storage is CloudCatalyst storage server, the target storage must be MSDP or CloudCatalyst storage server. When the target storage is CloudCatalyst storage server, the source storage can be MSDP or CloudCatalyst storage server.

Note: AIR and target AIR operations require a trust relationship before you configure the CloudCatalyst storage server as a target storage. You must select CloudCatalyst storage server as the target for AIR from the drop-down list of a trusted master server.

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

Integrated snapshot management enhancements

On-premises enhancements

NetBackup 8.2 includes the following enhancements for SAN:

- Application-consistent snapshot is supported for Oracle and DB2 workloads.
- XFS file system and Linux volume manager is supported on NetBackup clients of RHEL and SUSE platforms.
- Backups from Snapshot, Index Snapshot, Live Browse, Single File Restore are supported for the following NetBackup client platforms: Red Hat Linux, SUSE, Solaris, AIX, HP-UX, Windows.
- Point-in-time rollback restores of Windows workloads that use hardware snapshots now use VSS resync capabilities.
- The following storage arrays are supported: NetApp FAS, HP-3PAR, Pure Storage, and EMC Unity.

NetBackup 8.2 includes the following enhancements for NAS:

- Snapshot of NAS shares over Network File System (NFS) is supported.
- Backups from Snapshot, Index Snapshot, Live Browse, and Single File Restore are supported.
- Point-in-time rollback restores of Windows workloads that use hardware snapshots now use VSS resync capabilities
- The following storage array is supported: NetApp cDOT.

In-cloud enhancements

This release of NetBackup includes the following enhancements for protecting in-cloud assets using NetBackup and CloudPoint (version 2.2 or later) integration:

- You can take application consistent (point-in-time) snapshots of the applications that are deployed on virtual machines in cloud. This enhancement also lets you perform point-in-time rollback restores of applications. For supported applications, see the [NetBackup Master Compatibility Lists](#).
- If CloudPoint (Snapshot Management Server in NetBackup) is deployed in AWS Cloud, then you can configure AWS plug-ins using AWS IAM Role
- You can perform a rollback recovery of cloud assets. The rollback recovery of a cloud asset overwrites the existing data on the original asset. Unlike original or alternate location restore, a new copy is not created of the restored image, but the existing data on the source is replaced

- You can choose to replicate snapshots of cloud assets from the primary location to a remote or a secondary location. This capability is available only for AWS Cloud assets. The snapshot management servers (CloudPoint) support cross-region and cross-account replication in AWS

For more information on these enhancements, see the [NetBackup Web UI Cloud Administrator's Guide](#).

New option (`reinitialize`) added to the `csconfig` command utility

When you make any updates to the cloud storage configuration settings, a service restart is required for the changes to take effect. For NetBackup 8.2 and later releases, you have to restart the NetBackup Web Management Console (`nbwmc`) web service. For releases before NetBackup 8.2, you have to restart the NetBackup CloudStore Service Container (`nbcssc`) service. To avoid a service restart, NetBackup 8.2 introduces a new option (`reinitialize`) for the `csconfig` command utility. The `csconfig reinitialize` option reinitializes the CloudStore service container components in the `nbwmc` web service. This command reloads the updated configuration settings automatically and a service restart is no longer required.

Refer to the *Veritas NetBackup Commands Reference Guide* for more information.

NetBackup enhancements for VMware

NetBackup 8.2 offers more enhancements to VMware Discovery, Recover, Backup, and Configuration capabilities through the NetBackup web UI and NetBackup APIs:

- A user can now manually trigger the discovery of a VMware server on demand. A user can also get the benefits of autodiscovery whenever virtual server credentials are added or updated.
- The recovery workflow in the NetBackup web UI supports a datastore cluster as a recovery target.
- Options are available for users to specify the copy of interest for restore purposes along with the ability to specify an alternate VMware recovery host.
- New permissions help to prevent destructive recovery of VMware assets.
- New NetBackup APIs provide the capability to manage granular resource limits, VMware server credentials, and access hosts for VMware and other workloads like Red Hat Virtualization (RHV).
- Users can now edit, delete, and validate server credentials in the NetBackup web UI.
- During protection plan creation, the backup administrator can now select VMware backup options.

- VMware agentless restore lets you restore individual files and folders to virtual machines where the NetBackup client is not installed. By using VxUpdate, NetBackup can deploy the recovery tool to the virtual machines, restore files and folders, and perform the required cleanup. NetBackup does not require a connection to the destination virtual machine to recover the files. All recovery is handled through the ESX server using APIs.

See these resources for more information about these enhancements:

- Video: [NetBackup VMware Agentless Restore](#)
- [NetBackup API Reference on SORT](#)
- [NetBackup Web UI VMware Administrator's Guide](#)

NetBackup protection for Red Hat Virtualization (RHV)

NetBackup 8.2 enables protection of the virtual machines that are part of the Red Hat Virtualization (RHV) platform. NetBackup 8.2 web UI lets you manage, protect, and recover the Red Hat Virtualization workload. NetBackup integrates with oVirt APIs to provide VM-level protection in the RHV environment with the RHV manager.

Note: Users must be root user or an administrator or have a role that is configured for them in NetBackup RBAC.

For more information, see one of the following guides:

- [NetBackup Web UI RHV Administrator's Guide](#)
- [NetBackup Web UI Backup Administrator's Guide](#)
- [NetBackup Web UI Security Administrator's Guide](#)

New Instant Access features

NetBackup 8.2 includes the following new features related to Instant Access:

- Restore and download files and folders using the Instant Access feature.
NetBackup supports restore and download of multiple files and folders using the Instant Access feature. This feature enables increased accessibility of data to users.
- Create virtual machine using the Instant Access feature.
NetBackup supports vMotion when you create a virtual machine using the Instant Access feature. You can migrate an instant access virtual machine automatically and release resources from a storage appliance.
- Protect Universal Share data.

NetBackup protects your data on a Universal Share by backing up the data and managing the backups. You can instantly access the backups with NetBackup Instant Access APIs. For information about NetBackup APIs, see the following website:

[NetBackup API Reference on SORT](#)

Changes to global resource limits for VMware, RHV, and Hyper-V resources

The following limitations apply to setting global limits on the use of VMware, Red Hat Virtualization (RHV), and Hyper-V resources:

- New and changed resource limits may not take effect immediately. It can take a couple of jobs before the resource limit updates are in effect.
- In NetBackup 8.2, you can set global limits for VMware, Red Hat Virtualization (RHV), and Hyper-V resources only through the NetBackup Administration Console or the NetBackup Configuration API. You cannot set these resource limits with the NetBackup web UI. For more information about the Configuration API, see the [NetBackup API Reference on SORT](#). For more information about VMware resource limits, see the [NetBackup 8.2 for VMware Administrator's Guide](#). For more information about RHV resource limits, see the [NetBackup Web UI RHV Administrator's Guide](#). For more information about Hyper-V resource limits, see the [NetBackup 8.1.1 for Hyper-V Administrator's Guide](#).

Enhanced recovery process for Nutanix AHV virtual machines

NetBackup 8.2 introduces an enhanced experience for the recovery of Nutanix AHV VMs that are protected using the BigData policy. The Administration Console's Backup, Archive, and Restore page or the command line options can be used to plan the complete VM recovery in a user-friendly manner.

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

NetBackup introduces Accelerator support for Nutanix AHV through the upcoming Nutanix AHV plug-in

Starting with the 8.2 version, NetBackup introduces a new policy type called Hypervisor. The Hypervisor policy type lets you protect hyper converged systems and hypervisors like Nutanix Acropolis Hypervisor (AHV) or Red Hat Virtualization (RHV).

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

You can use the Hypervisor policy for Nutanix AHV along with accelerator support with the upcoming plug-in.

You can get more information through the upcoming *NetBackup for AHV Administrator's Guide*. The plug-in and the guide will be available shortly after the release of NetBackup 8.2.

Enhancements for the Microsoft SQL Server agent

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

- Support for availability groups with the SQL Server Intelligent Policy
Support was added for the advanced, basic, and read-scale availability databases with the SQL Server Intelligent Policy.
- Restore performance improvements
To the NetBackup MS SQL Client user interface, the ability to filter backup images by database name was added. Also, general performance improvements were made to the restore interface. Together, these enhancements significantly improve the speed for browsing and selecting backup images for the recovery of a known database.
- Transaction log backups while incremental or full backups are active
Scheduling algorithms now allow the administrator to schedule concurrent transaction log backups with full or differential backups. This change eliminates the need to create separate policies for transaction log and full or differential backups, and it simplifies recovery.

See the *NetBackup for Microsoft SQL Server Administrator's Guide* for more details.

Operational notes

This chapter includes the following topics:

- [About NetBackup 8.2 operational notes](#)
- [NetBackup installation and upgrade operational notes](#)
- [NetBackup administration and general operational notes](#)
- [NetBackup administration interface operational notes](#)
- [NetBackup API operational notes](#)
- [NetBackup Cloud operational notes](#)
- [NetBackup with Veritas CloudPoint operational notes](#)
- [NetBackup database and application agent operational notes](#)
- [NetBackup deduplication operational notes](#)
- [NetBackup internationalization and localization operational notes](#)
- [NetBackup for NDMP operational notes](#)
- [NetBackup SAN Client and Fibre Transport operational notes](#)
- [NetBackup Snapshot Client operational notes](#)
- [NetBackup virtualization operational notes](#)

About NetBackup 8.2 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](#)

See [“About related NetBackup documents”](#) on page 70.

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 8.2.

Linux daemon shutdown issues

During a client install or upgrade (all methods) and a media server native install or an upgrade, NetBackup daemons are started as part of the last NetBackup RPM package that is installed. (VRTSnbcfg for clients and VRTSnetbp for media servers.) When the version of the native `rpm` command on the system is 4.14.0 or newer, you may experience issues shutting down NetBackup daemons the first time after an install or an upgrade. All subsequent shutdown attempts will behave as expected.

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 impact 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 VRTSnbpc package will avoid 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 client or media server. For example:

```
echo "MACHINE_ROLE=CLIENT" > /tmp/NBInstallAnswer.conf
rpm -U --noscripts VRTSnbpck.rpm
rpm -U VRTSspb.x.rpm VRTSnbclt.rpm VRTSpddea.rpm
```

NetBackup 8.2 and SUSE 15 installation issue

After you install NetBackup on a SUSE 15 server, the NetBackup services do not start. This issue is the result of changes to the SUSE packages.

To resolve this installation issue, do one of the following:

- 1 Before NetBackup installation, install the `insserv-compat` package from the SuSE15 ISO.
- 2 If NetBackup is already installed:
 - Install the `insserv-compat` package from SuSE15 ISO.
 - Run the `insserv netbackup` command.
 - Run the `chkconfig netbackup` command. The output should be `netbackup on`.

NetBackup 8.2 and RHEL 8 installation issue

After you provide the NetBackup license key during the NetBackup 8.2 installation on RHEL 8, you receive the error shown:

```
/usr/opensv/netbackup/bin/admincmd/bpminlicense: error while loading
shared libraries: libnsl.so.1: cannot open shared object file: No
such file or directory (127)
```

This issue results from the upgrade of the `libnsl.so.1` library by Red Hat. To resolve this installation issue, do one of the following:

- 1 Before you start the NetBackup installation, log into the RHEL 8 server with root credentials and install the `libnsl` library.
- 2 Log into the RHEL 8 server with root credentials and install the `libnsl` library. Then reinstall NetBackup.

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

Starting with NetBackup 8.0, all NetBackup server names must use a host name that is compliant with RFC 1123 ("Requirements for Internet Hosts - Application and Support") and RFC 952 ("DOD Internet Host Table Specification") standards. These standards include the supported and unsupported characters that can be

used in a host name. For example, the underscore character (_) is not a supported character for host names.

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

[RFC 952](#)

[RFC 1123](#)

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

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

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

About support for HP-UX Itanium vPars SRP containers

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

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

NetBackup administration and general operational notes

NetBackup provides a complete, flexible data protection solution for a variety of platforms. The platforms include Windows, UNIX, and Linux systems. In addition to a standard set of data protection features, NetBackup can also utilize several other licensed and non-licensed components to better protect a variety of different systems and environments. This topic contains some of the general operational notes and known issues that are associated with the administration of NetBackup 8.2.

NetBackup master server is not supported on a btrfs file system

On UNIX platforms, the NetBackup Sybase database files reside on the master server in the directories at the following location: `/usr/opensv/db`.

NetBackup does not support the database if it is installed or upgraded on a `btrfs` file system. For successful NetBackup operations, ensure that the NetBackup database directories are on a file system other than `btrfs`, for example `ext4` or `xfs`.

Non-administrator users in environments with NBAC cannot read or update resource limits

A non-root or non-administrator user in a NBAC-configured environment is not able to read or update the resource limit values. This issue applies for all supported workloads.

Workaround: Add the non-root or non-administrator user to the `auth.conf` file with appropriate permissions to enable access to the resource limit functionality in the NetBackup Administration Console.

For more information about resource limits, see the [NetBackup Administrator's Guide, Volume I](#).

Media servers and backup host must use the same NetBackup version for BigData policies

For BigData policies, the media server and the backup hosts must use the same NetBackup version. If the media server on which the storage unit resides is on an older NetBackup version, the backup jobs fails with error 20.

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.

OpenStack restore jobs successful even when instance recreation fails

In an OpenStack environment, restore jobs are successful even when an attempt to recreate an instance from recovered data fails.

To troubleshoot, verify the issue through the OpenStack dashboard.

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 8.2.

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 67.

- NetBackup Web User Interface (UI)
- NetBackup Administration Console
- Remote Administration Console

- Character-based, menu interfaces for device management
- Command line

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.

Terminating a NetBackup web UI session does not log the user out immediately

If an administrator terminates a user's active web UI session, that user is not logged out of the session immediately. Instead, the user is logged out only after navigating to a different page or after the session reaches the idle session time-out period.

Access control methods supported in NetBackup 8.2

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 8.2.

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 API operational notes

NetBackup includes RESTful application programming interfaces (APIs). These APIs provide a web-service-based interface that lets you configure and administer NetBackup in your environments. This topic contains some of the operational notes and known issues that are associated with NetBackup APIs in NetBackup 8.2.

See the *NetBackup API Reference* documentation on SORT for more information. This HTML document is a reference tool that describes each API and its options.

NetBackup APIs must be called with percent-encoded URLs

NetBackup APIs must be called with percent-encoded URLs in accordance with the Internet Engineering Task Force (IETF) standard [RFC 3986](#). Clients that are not compliant to the specification may fail to get a valid response.

If a restarted backup or snapshot job fails, the job initiator ID no longer appears in the NetBackup Jobs API response

If a backup job or snapshot job is restarted and then fails, the NetBackup Jobs API does not return the initiator ID of the job.

If you attempt to view the list of jobs by initiator ID, the restarted jobs that failed do not appear.

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 8.2.

OpenStack backup job fails with error 6619

OpenStack backup job fails with error 6619 in the following scenarios:

- The OpenStack services go down during the backup.
- The OpenStack is not responding or is slow in response.
- Connection is reset during the backup.

Workaround: Restart the OpenStack service and reinitiate the backup.

Automated Disaster Recovery recovers VMs with AWS VM import prerequisites

The Automated Disaster Recovery feature can recover virtual machines that satisfy the Amazon Web Services VM import prerequisites.

For more information about the prerequisites, refer to the following article:

https://docs.aws.amazon.com/vm-import/latest/userguide/vmie_prereqs.html

Import and recoverec2 jobs may fail on automated DR servers

The import job fails or `recoverec2` job fails on the automated DR server. The following error message is seen in the logs:

```
Critical bpdm (pid=29453) sts_open_server failed: error 2060018 file not found
```

The issue might occur when the `NBU_PD_SERVER` path object is marked as corrupted in the deduplication catalog. This scenario might be a genuine corruption.

Workaround:

Try to use the following steps to resolve the issue or contact the Veritas Technical Support Team:

1. Stop the NetBackup service monitor using the following command:

```
/usr/opensv/netbackup/bin/nbsvcmon -terminate
```

2. Stop MSDP using the following command:

```
/usr/opensv/pdde/pdconfigure/pdde stop
```

3. Delete the PODB files that have `NBU_PD_SERVER` using the following commands:

```
rm -f /storage/storage/databases/catalog/2/po.db
rm -f /storage/storage/databases/catalog/2/ul.db
rm -f /storage/storage/databases/catalogshadow/2/podb.*
rm -f /storage/storage/databases/catalogshadow/2/uldb.*
rm -f /storage/storage/databases/catalogshadow/2/.chksum*
```

4. Start MSDP using the following command:

```
/usr/opensv/pdde/pdconfigure/pdde start
```

5. Start the NetBackup service monitor using the following command:

```
/usr/opensv/netbackup/bin/nbsvcmon
```

Unable to obtain the administrator password to use an AWS EC2 instance that has a Windows OS

This error occurs after the instance is launched from an AMI that is converted using automated disaster recovery.

The following error is displayed:

```
Password is not available. This instance was launched from a custom AMI, or the default password has changed. A password cannot be retrieved for this instance. If you have forgotten your password,
```

you can reset it using the Amazon EC2 configuration service. For more information, see [Passwords for a Windows Server Instance](#).

For more information, refer to the following articles:

- [Amazon Elastic Compute Cloud Common Messages](#)
- [How to migrate your on-premises domain to AWS Managed Microsoft AD using ADMT](#)

Certificate Revocation check using CRL not supported with Veritas Access cloud storage

The Certification Revocation check using a Certificate Revocation List (CRL) is not supported with Veritas Access cloud storage. After you upgrade NetBackup, if SSL is turned on, the Veritas Access storage server goes down. You must turn off the certification revocation check and bring up the server. For more information see, [NetBackup Cloud Administrator's Guide](#).

Storage server may display incorrect value of CRL if SSL is off

After you upgrade the CloudCatalyst storage server or the cloud storage servers, if SSL is off, the storage server displays incorrect an value of the Certificate Revocation List (CRL) (set to 1).

Workaround: Update the CRL value according to the SSL value. In this case, turn off the CRL flag. For more information, see the [NetBackup Cloud Administrator's Guide](#).

NetBackup with Veritas CloudPoint operational notes

Veritas CloudPoint is a flexible, snapshot-based enterprise cloud backup solution built specifically for dynamic multi-cloud environments. This topic contains some of the operational notes and known issues that are associated with the Veritas CloudPoint and NetBackup 8.2.

CloudPoint 2.x messages are in English for ISM

In the case of Integrated Snapshot Management (ISM, NetBackup-CloudPoint integration), the messages that are populated from CloudPoint 2.x are in English for all NetBackup locales.

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.

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 8.2.

NetBackup for Hadoop operational notes

Using the NetBackup Parallel Streaming Framework (PSF), Hadoop data can be protected using NetBackup. This topic contains some of the operational notes and known issues that are associated with NetBackup for Hadoop in NetBackup 8.2.

Hadoop with Kerberos restore job fails with error 2850

A Hadoop with Kerberos restore job fails with error 2850. This issue arises if the HDFS owner does not set ownership for files and directories or if there are issues with Kerberos configuration.

Workaround: Before restoring, ensure the following.

- Ensure that the HDFS owner user is used for Kerberos backup.
- Ensure that with the current Kerberos user, it is possible to set the owners/ACLs manually using HDFS commands, such as `chown` and `setfacl`.

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

NetBackup deduplication operational notes

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

issues that are associated with the NetBackup Deduplication Engine in NetBackup 8.2.

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

Dialog box might become unresponsive when you configure MSDP KMS encryption

When you configure MSDP KMS encryption and enter invalid characters, the dialog box might become unresponsive.

Workaround: You must configure MSDP encryption using valid ASCII characters. If you enter invalid characters and the dialog box becomes unresponsive, you can forcibly close the dialog box:

- Windows
Use the Task Manager to close the unresponsive NetBackup Administration Console.
- UNIX
Use the following command to get the process ID:

```
/usr/opensv/netbackup/bin/bpps | grep NBJAVA | grep -v nbwmc
```

Run the `kill` command.

Restart the NetBackup Administration Console, delete the storage server where the error occurred. Reconfigure MSDP KMS with valid characters.

For more information about the supported characters, refer to the About the NetBackup Deduplication Engine credentials topic in the [NetBackup Deduplication Guide](#).

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 8.2.

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 8.2.

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 SAN Client and Fibre Transport operational notes

SAN Client is a NetBackup optional feature that provides high-speed backups and restores of NetBackup clients.

Unable to stop the nbftclnt process on the NetBackup client

The `nbftclnt` process cannot be stopped using the `bp.kill_all` command and or the `kill -9 nbftclnt` command.

Workaround:

Use the `echo "1"` command on the `issue_lip` interface of the corresponding Fibre Channel port to reset the port.

For more information, refer to the following article:

[RHEL-storage_administration_guide/scanning-storage-interconnects](#)

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 8.2.

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 8.2.

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 8.2.

Some Pre-Recovery check validations may fail while restoring a VMware VM to an ESXi cluster through the web UI and API

When restoring a VMware VM to an ESXi cluster through the NetBackup web UI and API, some of the validations in the Pre-Recovery check fail with the following errors:

- For datacenter restores:
`Failed to validate datacenter path.`
- For datastore or datastore cluster restores:
`Datastore/datastore cluster name for configuration file not found.`
`nn megabytes requested on datastore name, 0 available`

Workaround: These error messages are inaccurate and can be ignored. The user is still able to recover the VM.

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**.

NetBackup and vCloud Director support

NetBackup 8.2 does not support vCloud Director versions before 9.0. If you have a pre-9.x vCloud Director version you must: upgrade to vCloud 9.0, 9.1, and 9.5 or use a NetBackup 8.1.2 or older server as the backup and the recovery host with the vCloud Director.

When building the VIP query for the VMware policy with a vCloud Director version the master does not support, do the following when creating the policy:

- 1 In the **NetBackup host to perform automatic virtual machine selection** drop-down on the **Clients** tab, specify a host with a NetBackup version that supports the vCloud Director version. A NetBackup 8.2 master server cannot enumerate possible values for pre-9.x vCloud fields.
- 2 In the **Query Builder**, you must manually enter the name of the VM requiring protection in the **Value(s)** field. Select the other values in the **Query Builder** as required for your policy.
- 3 Save the query and test it with the **Test Query** option.

When you restore VMs, ensure that you select a recovery host that supports the vCloud Director version for the VM that is restored.

NetBackup for Hyper-V operational notes

NetBackup for Hyper-V provides snapshot-based backup of the virtual machines that run on various versions of Windows Server. This topic contains some of the operational notes and known issues that are associated with NetBackup for Hyper-V in NetBackup 8.2.

Recovery wizard fails to browse for the selected Hyper-V server

The **NetBackup Hyper-V Add-In Recovery Wizard** fails to browse the restore location for the selected Hyper-V server on the **Restore Options** page.

The following error message might be seen:

```
Error Code : HostServerUnknown ; Message : Virtual machine host
<hostname> is not associated with this VMM management server. ;
Recommended Action : Check the virtual machine host name and then
try the operation again.
```

If the VM is configured to be highly-available, then the Hyper-V server name is set to the virtual cluster name during the backup. Browsing the virtual cluster name is not supported.

Workaround: In the **NetBackup Hyper-V Add-In Recovery Wizard** and **Recovery Options** page, click **Change** and select a valid node within the cluster instead of the virtual cluster name. You can then continue with the restore of the virtual machine to an alternate Hyper-V server.

About SORT for NetBackup Users

This appendix includes the following topics:

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

About Veritas Services and Operations Readiness Tools

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

Access SORT from the following webpage:

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

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

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

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

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

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

Recommended SORT procedures for new installations

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

Table A-1

Procedure	Details
Create a Veritas Account on the SORT webpage	See “To create a Veritas Account on the SORT page” on page 53.
Create generic installation reports	See “To create a generic installation checklist” on page 53.
Create system-specific installation reports	See “To create a system-specific installation report for Windows” on page 54. See “To create a system-specific installation report for UNIX or Linux” on page 55.

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 53.

Table A-2 (continued)

Procedure	Details
Create a system-specific upgrade report	See “To create a system-specific installation report for Windows” on page 54. See “To create a system-specific installation report for UNIX or Linux” on page 55.
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 57. See “To review hot fix and emergency engineering binary information” on page 57.

To review future platform changes and feature plans

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

To review hot fix and emergency engineering binary information

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

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

NetBackup installation requirements

This appendix includes the following topics:

- [About NetBackup installation requirements](#)
- [Required operating system patches and updates for NetBackup](#)
- [NetBackup 8.2 binary sizes](#)

About NetBackup installation requirements

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

See [“NetBackup installation and upgrade operational notes”](#) on page 32.

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

have changed the location of some of the files in either of these directories, free space is required in those locations equal to or greater than the size of the files in those locations. Refer to the *NetBackup Administrator's Guide, Volume I* for more information about storing NBDB database files in alternate locations.

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

- Master and media servers must have a minimum soft limit of 8000 file descriptors per process for NetBackup to run correctly.
 For more information about the effects of an insufficient number of file descriptors, refer to the following tech note on the Veritas Support website:
<http://www.veritas.com/docs/000013512>
- 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 8.2. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 8.2 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 67.

See [“About Veritas Services and Operations Readiness Tools”](#) on page 51.

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 8.2

Operating system type and version	NetBackup role	Patch	Notes
AIX 6.1	Client only	AIX run-time libraries 9.0.0.3 or later	The run-time libraries need to be at 9.0.0.3 or later. You may need to restart after you change to version 9.0.0.3.
Beijing Linx Software Corp Linx OS	Master, media, client	Kernel 2.6.32.26 or later	
CentOS 6.x	Master, media, client	Kernel 2.6.32-608.el6 or later	
CentOS 7.x	Master, media, client	Kernel 3.10.0-241.el7 or later	
Debian 8	Master, media, client	Kernel 3.16.7-1 or later	More information is available: Debian 8 release notes
HP-UX	Client only	COMPLIBS.LIBM-PS32	If you install AT on an HP-UX platform, this patch is required.
HP-UX IA-64	Client only	Networking.NET-RUN: /usr/lib/libip6.sl	
	Client only	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.1	
	Client only	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.sl	
	Client only	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so	
	Client only	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so.1	
	Client only	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so	
	Client only	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so.1	
	Client only	Networking.NET2-RUN: /usr/lib/libip6.1	

Table B-1 Required operating system patches and updates for NetBackup 8.2 (continued)

Operating system type and version	NetBackup role	Patch	Notes
HP-UX 11.31	Media	QPK1131 (B.11.31.1003.347a) patch bundle	This patch bundle is required for NetBackup media server support. It is an HP-UX March 2010 patch bundle.
Oracle Linux 6	Media, client	Kernel 2.6.32-504.14.1 or later	More information is available: Kernel security and bug fix update
Oracle Linux 7	Media, client	Kernel 3.10.0-229.7.1 or later	More information is available: Kernel security and bug fix update
Red Hat Enterprise Linux 6	Master, media, client	Kernel 2.6.32-504.16.2.el6 or later	More information is available: Red Hat tech note RHSA-2015:0864 - Security Advisory
Red Hat Enterprise Linux 7	Master, media, client	Kernel 3.10.0-229.7.2.el7 or later	More information is available: Red Hat tech note RHSA-2015:1137 - Security Advisory
SUSE Linux 11	Master, media, client	SUSE Linux Enterprise 11 Service Pack 3 or later	More information is available: Security update for Linux kernel:SUSE-SU-2014:1695-1
SUSE Linux 12	Master, media, client	Kernel 3.12.31 or later	More information is available: Security update for the Linux Kernel: SUSE-SU-2015:0068-1
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 8.2 (*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 8.2 binary sizes

[Table B-2](#) contains the approximate binary sizes of the NetBackup 8.2 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: [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 51.

Table B-2 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
AIX	POWER		1869 MB	No longer supported	
Canonical Ubuntu	x86-64		1339 MB		
CentOS	x86-64		1344 MB	5036 MB	Media server or client compatibility only.
Debian GNU/Linux	x86-64		1340 MB		
HP-UX	IA-64		2413 MB	No longer supported	
Oracle Linux	x86-64		1345 MB	5749 MB	
Red Hat Enterprise Linux Server	POWER		309 MB		
Red Hat Enterprise Linux Server	x86-64		1345 MB	5722 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	z/Architecture		1011 MB	2903 MB	Media server or client compatibility only.
Solaris	SPARC		1377 MB	4771 MB	
Solaris	x86-64		1376 MB	5794 MB	
SUSE Linux Enterprise Server	POWER		333 MB		
SUSE Linux Enterprise Server	x86-64		1224 MB	5468 MB	
SUSE Linux Enterprise Server	z/Architecture		1023 MB	2914 MB	Media server or client compatibility only.
Windows	x86-64		494 MB	2755 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 8.2.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Agent	Server	ViewBuilder
Oracle Linux	x86-64		745 MB	
Red Hat Enterprise Linux Server	x86-64		748 MB	
SUSE Linux Enterprise Server	x86-64		752 MB	
Windows Server	x86-64	261 MB	742 MB	234 MB

NetBackup plug-ins

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

NetBackup compatibility requirements

This appendix includes the following topics:

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

About NetBackup compatibility lists and information

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

See “[About Veritas Services and Operations Readiness Tools](#)” on page 51.

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 51.

About changes in platform compatibility

The NetBackup 8.2 release may contain changes in support for various systems. In addition to using SORT, you should make sure to review the *NetBackup Release Notes* document and the NetBackup compatibility lists before installing or upgrading NetBackup software.

See “[About new enhancements and changes in NetBackup](#)” on page 11.

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

Other NetBackup documentation and related documents

This appendix includes the following topics:

- [About related NetBackup documents](#)

About related NetBackup documents

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 8.2. 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 8.2

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 Backup Administrator's Guide*
- *NetBackup Web UI Cloud Administrator's Guide*
- *NetBackup Web UI RHV Administrator's Guide*
- *NetBackup Web UI Security 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 Deduplication Guide*
- *NetBackup for VMware Administrator's Guide*
- *NetBackup Plug-in for VMware vSphere Web Client*
- *NetBackup Plug-in for VMware vSphere Client (HTML5)*
- *NetBackup Snapshot Client Administrator's Guide*

Database agent guides:

- *NetBackup for MariaDB Administrator's Guide*
- *NetBackup for Microsoft SQL Server Administrator's Guide*
- *NetBackup for MySQL Administrator's Guide*
- *NetBackup for Oracle Administrator's Guide*
- *NetBackup for OpenStack Administrator's Guide*
- *NetBackup for Nutanix Acropolis Hypervisor (AHV) 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 Third-party Legal Notices*