Veritas NetBackup™ Release Notes

Release 8.1

Document Version 2

VERITAS™

Veritas NetBackup™ Release Notes

Last updated: 2017-10-17

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

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

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 8.1

This chapter includes the following topics:

About the NetBackup 8.1 release

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

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

About EEBs and release content

NetBackup 8.1 incorporates fixes to many of the known issues that affected customers in previous versions of NetBackup. Some of these fixes are associated with the customer-specific issues that have been documented in the form of Titan or Salesforce.com (SFDC) cases. 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 8.1 can be found on the Veritas Operations Readiness Tools (SORT) website and in the NetBackup Emergency Engineering Binary Guide.

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

About NetBackup appliance releases

The NetBackup appliances run a software package that includes a preconfigured version of NetBackup. When a new appliance software release is developed, the latest version of NetBackup is used as a basis on which the appliance code is built. For example, NetBackup Appliance 3.0 is based on NetBackup 8.0. 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

About NetBackup third-party components

The following table lists some of the most well-known third-party components which are installed by NetBackup 8.1:

Table 1-1 Third-party components in NetBackup 8.1

Third party	Version
Java Runtime Environment (JRE)	■ IBM AIX (rs6000) 8.0.4.2 ■ IBM zLinux 8.0.4.2 ■ HP-UX (hpia64) 8.0.0.9 ■ Linux (RedHat, SuSE) 8u131 ■ Solaris (sparc, x86) 8u131 ■ Microsoft Windows 8u131

Chapter 2

New features, enhancements, and changes

This chapter includes the following topics:

About new enhancements and changes in NetBackup

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

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

See "About the NetBackup 8.1 release" on page 9.

See "About NetBackup compatibility lists and information" on page 72.

NetBackup 8.1 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 8.1 are grouped below by category. Select a link to read more information about the topic.

Secure communication features, changes, and enhancements

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

- About secure communications in NetBackup
- Host ID to host name mapping
- Catalog recovery with secure communications
- Communication between a NetBackup 8.1 master server and an OpsCenter 8.1 master server
- NetBackup requirements for inter-host communication
- Two-way trust for adding trusted master server for Targeted Auto Image Replication
- Secure communication between a NetBackup client in a demilitarized zone and a master server

New features

- Introducing NetBackup CloudCatalyst to upload deduplicated data to the cloud
- Faster full backups for Isilon filers using NetBackup Accelerator
- Auto Image Replication (A.I.R.) import confirmation feature introduced to SLPs
- Accurate licensing feature and other updates with nbdeployutil
- NetBackup introduces a new BigData policy type

Support changes and enhancements

- End-of-life for multiple NetBackup products, features, and platforms

- NetBackup 8.1 support additions
- DHCP client support changes in NetBackup 8.1
- NetBackup BMR functionality not supported for restoring clients with NetBackup 8.1
- Support has ended for the SYMCquiesce utility for Linux virtual machines
- Several shutdown commands will be deprecated in a future release
- Localization support added for the csconfig command

System requirement changes and enhancements

- New minimum system requirements for NetBackup master servers
- NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952

Installation, upgrade, and configuration changes and enhancements

- Upgrade considerations regarding MSDP fingerprint algorithm changes
- SCCM and Chef deployment tools and documentation now available
- Changes to media server and SSO device configuration procedures

Cloud-related changes and enhancements

- **Note:** Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 8.1
- Changes to Amazon cloud storage server object sizes
- Additional cloud-related enhancements

Virtualization changes and enhancements

- New options to exclude disks from VMware backups
- Restore Virtual Machine Disks wizard for VMware
- Support for non-ASCII characters in VMware

Database agent changes and enhancements

- New requirements for clustered file systems, database clusters, and distributed database applications
- Configuring the Distributed Application Restore Mapping host properties

- Changes to policy and other configuration for SQL Server clusters and SQL Server AGs
- Registering authorized locations used by a NetBackup database script-based policy
- DB2 OPTIONS command update

Other announcements

- Late-breaking new status codes for NetBackup 8.1

About secure communications in NetBackup

NetBackup 8.1 hosts can communicate with each other only in secure mode.

Each host much establish trust with the CA, after which a CA certificate is added to the trust store. Each NetBackup 8.1 host must also have a host ID-based certificate in order to successfully communicate.

A host ID-based certificate is deployed on the host during NetBackup installation. If the certificate cannot be deployed during installation, the host cannot communicate with other hosts. In this case, you must manually deploy a host ID-based certificate on the host using the `nbcertcmd` command to start host communication after installation.

Note: If you have any NetBackup 8.0 or earlier in your environment, you can enable insecure communication by navigating to the NetBackup Administration Console, then to the `Security Management > Global Security > Secure Communication` tab. On this tab, select the `Enable insecure communication with NetBackup 8.0 and earlier hosts` option.

Host ID to host name mapping

To perform successful secure communication in NetBackup 8.1, you should map all associated host names to their respective host IDs. The NetBackup-configured client name of a host (or the primary name) is automatically mapped to its host ID during certificate deployment. Additional host names are discovered during communication and may be automatically mapped to their respective host IDs, or may appear in the `Mappings for Approval` list. You can perform this configuration in the `Host Management` properties on the master server.

Catalog recovery with secure communications

When you restore NetBackup 8.1 after a disaster, you must recover the host identity of any master servers. The host identity includes information such as certificate details and security settings. The master server cannot communicate with media servers and clients in the new NetBackup instance until the earlier host identity has been recovered.

The host identity resides in a disaster recovery package which is created during each catalog backup. Because the disaster recovery package contains sensitive data such as security certificates and security settings, it is encrypted with a passphrase. You must provide the passphrease when you install NetBackup in disaster recovery mode after a disaster. This passphrase is not recovered during a restore of the disaster recovery package or during catalog recovery.

You must set the passphrase again in the new NetBackup instance. To set a passphrase, use the `Security Management > Global Security Settings > Disaster Recovery` tab in the NetBackup Administration Console. If the disaster recovery package passphrase is not set in the new instance, catalog backups will fail. This is also applicable for upgrades to NetBackup 8.1. To avoid catalog backup failures, set the disaster recovery package passphrase immediately after the upgrade.

Communication between a NetBackup 8.1 master server and an OpsCenter 8.1 master server

In order to successfully collect data from a NetBackup 8.1 master server which uses OpsCenter 8.1 server, perform the following:

- Add the OpsCenter server name to the `OPS_CENTER_SERVER_NAME` configuration option in the NetBackup configuration file. On UNIX, this options is in the file `bp.conf`, while on Windows it is a registry key.
- Enable insecure communication in NetBackup. To enable insecure communication, perform the following:
  - In the NetBackup Administration Console on the master server host, navigate to the `Security Management > Global Security > Hosts` tab and select `Enable insecure communication with NetBackup 8.0 and earlier hosts option is selected`.
  - On the master server host, set the `nbseccmd -setsecurityconfig -insecurecommunication` command line option to "on".

NetBackup requirements for inter-host communication

Beginning with the 8.1 release, NetBackup inter-host communication requires the following:

- The NetBackup master server must be up and running.
- The NetBackup `vnetd` process and its proxy processes must be active on all NetBackup 8.1 and later hosts.
  For more information, see the `vnetd` process description in the 8.1 version of the *NetBackup Administrator's Guide, Volume I*. Also see the *NetBackup Troubleshooting Guide* for information about troubleshooting the `vnetd` proxy processes. The guides are available through the following URL:
  http://www.veritas.com/docs/DOC5332
- NetBackup 8.1 hosts no longer use the connect option settings for connections to other NetBackup hosts, including the daemon port setting. The PBX and `vnetd` ports must be open to the remote hosts.

Veritas recommends that you know about and accommodate the following when you upgrade to NetBackup 8.1:

- Each inter-host connection uses an intra-host connection on each of the hosts. The local connections consume additional TCP ports and TCP memory. NetBackup server hosts that are already at or near their resource limits may need to be tuned.
- The inter-host connections that carry control protocol information are encrypted. CPUs with AES/AES-NI or RDRAND/SecureKey features can offload this workload.

Two-way trust for adding trusted master server for Targeted Auto Image Replication

With Targeted Auto Image Replication, when establishing trust between the source and the remote target server, you need to establish trust in both the domains.

- In the source master server, add the target master server as a trusted server.
- In the target master server, add the source master server as a trusted server.

More secure mechanism would use certificates to establish trust, wherein:

- You need to validate SHA1 fingerprint of root certificate.
- You can use authorization token to establish trust.

This enhancement is available through the **NetBackup Administration Console** and the `nbseccmd` command. For more information, see the NetBackup Deduplication Guide.

Secure communication between a NetBackup client in a demilitarized zone and a master server

Starting with NetBackup 8.1, the media server creates an HTTP tunnel to enable secure web service communication between NetBackup clients that are in a demilitarized zone (restricted network) and the master server. After the web service communication is set up, the further communication uses Secure Sockets Layer (SSL). Secure web service communication between the NetBackup clients and the master server is important for deploying security certificates and overall NetBackup communication.

Introducing NetBackup CloudCatalyst to upload deduplicated data to the cloud

NetBackup 8.1 introduces NetBackup CloudCatalyst, which uses MSDP deduplication technology to upload deduplicated data to the cloud. The data is uploaded by a CloudCatalyst storage server, which first stores data in a local cache. This cloud storage server is a dedicated host that can be either a Veritas NetBackup CloudCatalyst Appliance or an MSDP media server that is configured for NetBackup CloudCatalyst.

Table 2-1 Types of media servers that can be used as NetBackup CloudCatalyst storage servers

Host	Version	Configuration information
NetBackup appliance	Veritas NetBackup CloudCatalyst Appliance	NetBackup Appliance documentation
NetBackup media server	Red Hat Enterprise Linux, 7.3 or later NetBackup 8.1 or later	NetBackup 8.1 Deduplication Guide

See the NetBackup Master Compatibility Lists for updated information about supported cloud vendors and feature support.

The following are examples of scenarios that use NetBackup CloudCatalyst:

- In this CloudCatalyst scenario, the NetBackup environment contains two media servers: one is an MSDP storage server and one is a CloudCatalyst storage server.

  An MSDP storage server deduplicates client data during the backups. This storage server is used for short-term data retention. Per a storage lifecycle policy, NetBackup copies the data to a CloudCatalyst storage server using optimized duplication. The cloud storage is used for long-term data retention.

- In this CloudCatalyst scenario, the NetBackup environment contains only a CloudCatalyst storage server. This scenario does not use an MSDP storage server. Instead, the CloudCatalyst storage server deduplicates the data and then uploads it directly to cloud storage.

See the NetBackup Deduplication Guide for CloudCatalyst configuration, administration, and troubleshooting information.

Faster full backups for Isilon filers using NetBackup Accelerator

NetBackup's Accelerator option makes NDMP backups for Isilon filers (OneFS 7.1, OneFS 7.2, and OneFS 8.0) run faster than normal NDMP backups. (Previously, the Accelerator for NDMP option was available only for NetApp filers.) NetBackup Accelerator increases the speed of full backups by using the filer's change detection techniques to identify the modifications that occurred since the last backup. After an initial full backup that protects all data from the filer, NetBackup Accelerator backs up only the changed data from the filer to the media server. The media server combines the changed data with any previous backup images to create a new full backup image. If a file is already in storage and has not been changed, the media server uses the copy in storage rather than reading it from the filer to complete the backup image. The end result is a faster NetBackup NDMP backup.

More information about Accelerator for NDMP is available in the following guide:

NetBackup for NDMP Administrator's Guide for Release 8.1

See the NetBackup Master Compatibility List for the most recent list of supported versions of each NAS vendor.

Auto Image Replication (A.I.R.) import confirmation feature introduced to SLPs

NetBackup 8.1 introduces a new import confirmation feature that is related to targeted A.I.R. operations. When using targeted A.I.R., storage lifecycle (SLP) processing of each replicated image is paused in the source domain until a message has been received from the target domain that confirms that the image has been imported successfully. This feature ensures that source domain images remain in place at least until those images have been safely imported in the target domain.

Note: A.I.R. operations require that a trust relationship be established before configuring and operating SLPs that perform targeted replication. In NetBackup 8.1, these operations include import confirmation messages that are sent from the target domain to the source domain. Security changes in NetBackup 8.1 require that this trust relationship be re-established before import confirmation can proceed.

Import confirmation operations are not enabled by default in NetBackup 8.1, regardless of whether the system is upgraded from a previous NetBackup release or an initial install is performed. Refer to the following tech note for information about enabling the A.I.R. import confirmation feature in NetBackup 8.1:

https://www.veritas.com/support/en_US/article.000127326

For more information about import confirmation, see the NetBackup Administrator's Guide, Volume I.

Accurate licensing feature and other updates with nbdeployutil

With NetBackup 8.1, `nbdeployutil` offers an accurate licensing feature for the capacity licensing option. The accurate licensing model uses a unique mechanism that gathers the front-end data size during a backup operation. The gathered data is used in the capacity licensing report.

The capacity licensing model also detects overlapping backup selection data from the backup policies and automatically adjusts the charged data size. The capacity licensing report now displays the volume of the front-end terabyte data that is processed using NetBackup CloudCatalyst.

For more information about accurate licensing, see the NetBackup licensing models and the `nbdeployutil` utility section in the NetBackup NetBackup Administrator's Guide Volume II for NetBackup 8.1.

NetBackup introduces a new BigData policy type

Starting with the 8.1 version, NetBackup introduces a new policy type called BigData. The BigData polity type lets you back up big data applications like Hadoop and hyper converged systems like Nutanix Acropolis Hypervisor (AHV).

You need the appropriate NetBackup license to use the BigData policy type:

- To granularly back up and recover a Hadoop file system, you need the Application and Database license pack.
- To back up and recover Nutanix AHV virtual machines, you need the Enterprise Client license.

For detailed information about using the BigData policy for Hadoop and Nutanix AHV, refer to the *NetBackup for Hadoop Administrator's Guide* and the *NetBackup for Acropolis Hypervisor Administrator's Guide*, respectively. These guides will be available shortly after the release of NetBackup 8.1:

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

End-of-life for multiple NetBackup products, features, and platforms

On February 1st, 2017, the following NetBackup products reached the end of their support life (EOSL):

- NetBackup OpsCenter (7.0 - 7.6.1.2)
- NetBackup Enterprise Server (7.0 - 7.6.1.2)
- NetBackup Server (7.0 - 7.6.1.2)
- NetBackup Media Server Encryption Option (7.0 - 7.6.1.2)

Additionally, with NetBackup 8.1, support is discontinued for the following features, functionality, and OS and database platforms:

- NetBackup Plug-in for VMware vCenter
- NetBackup High Availability (HA) Media Server
- Replication Director for EMC VNX
- Microsoft Exchange 2007
- Microsoft SharePoint 2007
- DB2 versions 9.1, 9.5, 9.7 & 10.1
- OpenVMS - Client (IA-64)
- Canonical Ubuntu 12.04 (x86-64)
- Canonical Ubuntu 14.04 (x86-64)
- Canonical Ubuntu 14.10 (x86-64)
- Canonical Ubuntu 15.04 (x86-64)
- CentOS 5 (x86-64)
- Red Hat Enterprise Linux (RHEL) 5
- Windows Server 2008 (x86-32)
- Windows Vista
- Preinstallation Environment Checker

The Veritas NetBackup installation wizard no longer includes the **Preinstallation Environment Checker**.

- Remote (push) installations of UNIX/Linux clients using RSH and FTP

  Note: Use the SSH or SFTP methods as the alternatives. Push installation from the administration console will use SSH as well.

- Remote (push) installations of a master server in a disaster recovery
- Cluster installations using RSH, RCP, and REMSH

  Note: Use the SSH/SCP method as an alternative.

This list is subject to change. Complete and up-to-date NetBackup end-of-life (EOL) information is available on SORT.

General information about end-of-life notifications is also available:

See "About NetBackup end-of-life notifications" on page 73.

NetBackup 8.1 support additions

The following products and services are supported starting with NetBackup 8.1:

- VMware VDDK 6.5.1
- MySQL version 5
- New backup/restore host support:
  - Windows 10
  - Red Hat Enterprise Linux (RHEL) 6.7, 6.8, 7.2, 7.3
  - SUSE Linux Enterprise Server (SLES) 11 SP4, 12 SP1

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

More information about supported products and services is available:

See "About NetBackup compatibility lists and information" on page 72.

NetBackup BMR functionality not supported for restoring clients with NetBackup 8.1

In this release, NetBackup Bare Metal Restore (BMR) functionality is not supported for restoring the clients with NetBackup version 8.1 installed. However, you can still use Bare Metal Restore for restoring the clients with NetBackup version 8.0 and earlier installed. While restoring 8.0 and earlier clients, Veritas recommends that you use Shared Resource Tree (SRT) having 8.0 and earlier client version.

DHCP client support changes in NetBackup 8.1

NetBackup 8.1 does not support 8.1 clients that are configured with the “Dynamic Address” option set to “yes”. Older clients can continue to use this feature. Additionally, NetBackup does not support 8.1 clients that have a non-zero value for the `DHCP_ANNOUNCE_INTERVAL` setting.

Support has ended for the SYMCquiesce utility for Linux virtual machines

Support for the SYMCquiesce utility for Linux virtual machines has been discontinued starting in this NetBackup release. Newer operating systems provide native support for a similar functionality. Please contact your operating system vendor and VMware for additional information.

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

See “About NetBackup end-of-life notifications” on page 73.

Several shutdown commands will 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*.

Localization support added for the csconfig command

The error messages and help content for the `csconfig` command supports localization in the following languages:

- Chinese
- French
- Japanese

New minimum system requirements for NetBackup master servers

Starting with this release of NetBackup, the NetBackup master server requires 4 cores and 16 GB of RAM. This requirement does not apply to OpsCenter servers, media servers, or clients.

More information about minimum system requirements is available in the NetBackup Installation Guide for version 8.1.

Upgrade considerations regarding MSDP fingerprint algorithm changes

Because of the changes in the fingerprint algorithm for MSDP in NetBackup 8.1, consider your MSDP environment as you plan your upgrade path. Any NetBackup 8.0 and older host cannot access the NetBackup 8.1 MSDP because of the new fingerprint algorithm. Failed NetBackup jobs can result from a failure to plan for this condition.

For more information, refer to the NetBackup Upgrade Guide for NetBackup 8.1.

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

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

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

RFC 952

RFC 1123

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

SCCM and Chef deployment tools and documentation now available

With the NetBackup 8.1 release, Veritas now supports the use of System Center Configuration Manager (SCCM) and Chef for NetBackup deployment. Veritas has tested and validated several different deployment paths. Documentation and templates for both SCCM and Chef are available. See SORT for additional details around the support and use of SCCM and Chef.

Changes to media server and SSO device configuration procedures

The following items describe changes to the procedures for adding a media server and for configuring Shared Storage Option (SSO) devices:

- When you add a media server to an existing environment by the NetBackup Administration Console, add the new media server to the **Media Servers List** of the master server without restarting any service on all servers. For more information, see “Adding a media server” in the *Veritas NetBackup Administrator’s Guide, Volume I*.
- You must restart the NetBackup Device Manager (`ltid`) on all the servers that share tape drives whenever you perform the following actions:
  - Configure the shared drives to a newly added media server.
  - Add or remove the shared drives paths.

  For more information, see “Configuring Shared Storage Option devices in NetBackup” in the *Veritas NetBackup Administrator’s Guide, Volume II*.

Update cloud configuration file on the master server immediately after install or upgrade to NetBackup 8.1

Note: If you use cloud storage in your NetBackup environment, you should update your cloud configuration file on the NetBackup master server immediately after you install or upgrade to NetBackup 8.1.

Veritas continuously adds new cloud support to the cloud configuration files between releases. In fact, new cloud support has been added since the NetBackup 8.1 final build. If you have updated your cloud configuration file since installing NetBackup 8.0, you must update your cloud configuration file because some recently-added cloud providers and enchantments may not be included in the cloud configuration file in the NetBackup 8.1 build. If a cloud provider or related enhancement is not available in the cloud configuration file after upgrading to NetBackup 8.1, related operations will fail.

Immediately after you upgrade to NetBackup 8.1, update to the latest cloud configuration package to take advantage of the most recent cloud provider additions and enhancements. See the following tech notes for more information:

https://www.veritas.com/docs/000125094

https://www.veritas.com/support/en_US/article.000126560

Refer to the following tech note for details of cloud providers and related enhancements that were available in NetBackup 8.0 (deployed using the cloud configuration packages) and are not available in the cloud configuration file that is shipped with NetBackup 8.1:

https://www.veritas.com/support/en_US/article.000127978

Changes to Amazon cloud storage server object sizes

Starting with NetBackup 8.1, the object size for Amazon (S3) and Amazon GovCloud storage servers has changed. This change affects the valid range for the read and write buffer size for these cloud storage servers.

You must update the read and write buffer size values for pre-NetBackup 8.1 servers using the NetBackup Administration Console on the master server. Update these settings for each cloud storage server that is associated with a media server.

For the valid range, see the `READ_BUFFER_SIZE` and `WRITE_BUFFER_SIZE` information in the NetBackup Cloud Administrator's Guide. For procedures on how to update the read or write buffer size, see the NetBackup Upgrade Guide.

Additional cloud-related enhancements

The following cloud-related enhancements are included in NetBackup 8.1.

- Configure NetBackup Cloud Storage with Selected Regions
  Now while configuring a cloud storage server, you can select specific regions. Only the selected regions are used for NetBackup cloud operations. This enhancement is available through the `csconfig` CLI.
  For more information, see the NetBackup Command Reference Guide.
- Proxy server enhancements
  With this release the following enhancements are available for configuring proxy servers:
  - Authentication types BASIC and NTLM are supported
  - Authentication is supported for S3, Azure, SWIFT API Types cloud connectors
  - Proxy HTTP tunneling is configurable

- Proxy server can be specified through IP address or host name
- Communication between NetBackup and the CAP (C2S Access Portal) uses proxy server

This enhancement is available through the **Cloud Storage Configuration Wizard** and the `csconfig` command.

For more information, see the NetBackup Cloud Administrator's Guide and the NetBackup Command Reference Guide.

- Support for Amazon Virtual Private Cloud

  Using NetBackup you can add a new cloud storage in an Amazon virtual private cloud (VPC) environment.

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

- New cloud vendor support

  Support is added for the following cloud vendors:

  - CMCC Cloud Storage v5.x(S3)
  - OpenStack Swift Identity v3 Authentication version
  - BM SoftLayer
  - Fujitsu Cloud Service K5
  - Microsoft Azure Government

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

New options to exclude disks from VMware backups

This release provides new options to support excluding disks from VMware backups. These new options are on the **Exclude Virtual Disks from Backup** panel of the **Backup Policy Configuration Wizard** and on the **Change Policy** dialog box **Exclude Disks** tab.

The existing exclude disk options are moved from the **VMware - Advanced Attributes** dialog to the new dialog box and wizard panel.

For more information, see the "Exclude Disks tab" topic in the 8.1 version of the NetBackup for VMware Administrator's Guide available through the following URL:

Alternatively, you can use the NetBackup `bpplinfo` command to configure backup policy attributes.

One of the new exclude disk options is to exclude by VMware Custom Attribute. To help you with that method of excluding disks, the NetBackup plug-in for VMware vSphere Web Client includes a **Virtual Disk Exclusion Wizard**. You can use it to add a Custom Attribute to a virtual machine or virtual machines. NetBackup then can exclude the virtual disks that are identified in that Attribute from backups. For

more information, see the NetBackup Plug-in for VMware vSphere Web Client Guide available through the following URL:

Restore Virtual Machine Disks wizard for VMware

The new **Restore Virtual Machine Disks** wizard lets you restore one or more individual virtual machine disks. Previously, individual virtual machine disk restore required that you use NetBackup commands. For more information, see “About VMware virtual machine disk restore” in the NetBackup for VMware Administrator's Guide for NetBackup 8.1.

Support for non-ASCII characters in VMware

NetBackup now supports non-ASCII characters for virtual machines, with certain restrictions for the names that you use to back up and restore the VMs. For information about the requirements and restrictions, see “NetBackup for VMware: notes and restrictions” in the NetBackup for VMware Administrator's Guide for NetBackup 8.1.

New requirements for clustered file systems, database clusters, and distributed database applications

For a file system or database that is clustered or for database applications that are distributed, NetBackup 8.1 requires that you review the auto-discovered mappings in Host Management. For NetBackup for SQL Server, this requirement also applies to availability groups (AGs). On the **Mappings for Approval** tab, approve each valid mapping that NetBackup discovered in your environment. This configuration ensures that the hosts in the cluster are recognized as secure hosts and can communicate with the master server. If you only install the NetBackup client on one node in the cluster, then this configuration is not required. Perform this configuration in the Host Management properties on the master server. See the NetBackup Security and Encryption Guide for more information.

The Exchange, SharePoint, and SQL Server agents may require that you configure host information in the **Distributed Application Restore Mapping** host property on the master server.

- When you upgrade your master server to NetBackup 8.1, security requirements now exist that may affect your previous configurations for backups and restores of complex workloads including Exchange Server, SharePoint Server, and SQL Server. For example, a complex workload includes the following:
  - Exchange DAGs
  - Exchange clusters

- SharePoint Server
- SharePoint Server with a clustered back-end SQL Server
- SQL Server clusters
- SQL Server availability groups (AGs)
- SQL Server AGs with a failover cluster instance (FCI)

Veritas recommends that you first attempt your database workload backups with your current configuration. If backups do not succeed, then configure the **Distributed Application Restore Mapping** host property on the master server. If restores do not succeed, configuring the **Distributed Application Restore Mapping** should also resolve these issues.
Note that if you chose to configure the **Distributed Application Restore Mapping** for SQL Server highly available environments, certain previous configuration steps are no longer needed. In this case, the SQL Server agent no longer requires a second policy that contains the cluster or AG node names. For a SQL Server cluster or AG, you also do not need to configure permissions for redirected restores for the cluster or AG nodes.

- For new installations of NetBackup 8.1, follow the instructions for your agent in the agent's administrators guide. You must configure the mappings for distributed application restores. You must also review the auto-discovered mappings for the hosts in your environment.

Configuring the Distributed Application Restore Mapping host properties

For NetBackup 8.1, certain SQL Server environments require that you configure host information in the Distributed Application Restore Mapping host properties on the master server. This configuration is required for restores of a SQL Server cluster or a SQL Server availability group (AG). For VMware backups, if you use a **Primary VM identifier** other than **VM hostname**, then you must map the **Primary VM identifier** to the host name of the VM.

Changes to policy and other configuration for SQL Server clusters and SQL Server AGs

For legacy SQL Server backups (using batch files), NetBackup no longer requires a second policy that contains the cluster or AG node names. To perform restores, you no longer need to configure permissions for redirected restores (altnames). The mappings in the **Distributed Application Restore Mapping** host properties replace these configuration steps.

If you are upgrading from an earlier version of NetBackup, you can still use both the second “node name” policy and the altnames permissions for successful backups and restores of SQL Server. However, Veritas recommends that you allow restores only to specific hosts. In NetBackup 8.1, the `No.Restrictions` file only allows a requesting client to perform a redirected restore if that client is known by the master server.

Registering authorized locations used by a NetBackup database script-based policy

During a backup, NetBackup checks for scripts in the default script location or the authorized location(s). The default, authorized script location for UNIX is `usr/openv/netbackup/ext/db_ext` and for Windows is *`install_path`*`\netbackup\dbext`. If the script is not in the default script location or an authorized location, then the policy job fails. You can move any script into the default script location or any additional authorized location and NetBackup recognizes the scripts. All scripts must be stored and run locally.

The following client agents are affected:

- DB2
- MSSQL server
- Sybase
- SAP
- Oracle
- Informix-On-BAR
- DataStore
- DataTool's SQL-BackTrack

The `NetBackup\bin\goodies` directory on master and media servers includes a tool called `db_script_discovery`. This tool lets you query the NetBackup environment for a list of policies with the `bppllist` command. It filters that list for the policies that run scripts on clients using the XBSA policies. It then lists the clients, policy names, policy types, script paths, and whether the policy is active.

For more information about registering authorized locations and scripts, review the knowledge base article:

http://www.veritas.com/docs/000126002

For more information about registering authorized locations and scripts, refer to your database agent manual for NetBackup 8.1.

DB2 OPTIONS command update

The `DB2 OPTIONS` command is updated to include the `DB2_CLIENT=<client_name>` and the `DB2_SERVER=<server>` options. The update allows a user to specify these options within the command line. See the NetBackup for DB2 Administrator's Guide for NetBackup 8.1 for more information about the `DB2 OPTIONS` command.

Late-breaking new status codes for NetBackup 8.1

Three status codes were recently added. However, information about these status codes is not available in the NetBackup Status Codes Reference Guide or on the Troubleshooter for NetBackup 8.1.

- Refer to the following article for the information on the status code 5976 (The passphrase must contain minimum 8 and maximum 20 characters):
  https://www.veritas.com/support/en_US/article.000127922
- Refer to the following article for the information on the status code 5977 (The existing and new passphrase must be different):
  https://www.veritas.com/support/en_US/article.000127923
- Refer to the following article for the information on the status code 24630 (The **NetBackup Administration Console** failed to establish a secure connection with the host.):
  https://www.veritas.com/support/en_US/article.000127910

Chapter 3

Operational notes

This chapter includes the following topics:

About NetBackup 8.1 operational notes

NetBackup operational notes describe and explain important aspects of various NetBackup operations that may not be documented elsewhere in the NetBackup documentation set or on the Veritas Support website. The operational notes can be found in the *NetBackup Release Notes* for each version of NetBackup. Typical

operational notes include known issues, compatibility notes, and additional information about installation and upgrade.

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

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

See "About related NetBackup documents" on page 75.

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 8.1.

Services cannot start or backup may fail if PBX version is not compatible with the NetBackup version

During a NetBackup upgrade, the Veritas Private Branch Exchange (PBX) is also upgraded. However, because of the following reasons, the PBX version and the NetBackup version may not be compatible after the NetBackup upgrade.

- The PBX upgrade is not successful.
- NetBackup software on one of the hosts is downgraded, but the PBX is not downgraded.
- Your backup environment consists of a Veritas product other than NetBackup. The other product is upgraded and that caused PBX upgrade.

Note: If the NetBackup version is 8.1, the PBX version must be v1.7.4.0 or later.

To check the current PBX version, run the following command:

- On Windows:

  install_path\VxPBX\bin\pbxcfg -v

- On UNIX:

  ```
  /opt/VRTSpbx/bin/pbxcfg -v
  ```

To resolve the issue:

- Contact the Veritas Technical Support team and get the PBX version installed that is compatible with the existing NetBackup version.

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

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

About support for HP-UX Itanium vPars SRP containers

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

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

A Java error can occur on AIX 7.1

On AIX 7.1, the following message may appear in the installer:

```
WARNING: Installation of Java LiveUpdate agent failed.
Refer to file /tmp/JLU-Log/JavaLiveUpdate-Install.log on bmraix57 for more information.
```

If you encounter the message, run the following Java command and verify the error output:

```
#  /usr/openv/java/jre/bin/java
Error: Port Library failed to initialize: -125
Error: Could not create the Java Virtual Machine.
Error: A fatal exception has occurred. Program will exit.
```

If this error output is generated, refer to the following IBM support article to resolve the issue:

http://www-01.ibm.com/support/docview.wss?uid=swg1IV12285

Note: Other errors can cause the warning message to appear. The output from the Java command can determine if the fix from IBM can resolve the issue.

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 8.1.

Connection with NBAC-enabled 8.0 or earlier master server may fail

In a NetBackup 8.1 setup, if you want to connect to NBAC-enabled 8.0 (or earlier) master server using 8.0 (or earlier) **NetBackup Administration Console** packaged with 8.1 installation, connection to NetBackup Service Layer (NBSL) cannot be established. The NetBackup login fails as the credentials that are required for secure connection cannot be located because of mismatch in the Authentication Service (AT) data directory.

The following warning message is displayed:

```
Connection to the NetBackup Service Layer (NBSL) could not be
established. You may not be able to perform the operations that
require the NBSL service to be running. Restart the NBSL service.
```

To resolve this issue, perform one of the following:

- Disable the `-Dvrtsat.donot.suffix.username` configuration option that causes the credentials to be created in appropriate folders, thereby eliminating any mismatch in the AT data directory.
  - Replace all occurrences of `-Dvrtsat.donot.suffix.username=1` with `-Dvrtsat.donot.suffix.username=0`.

  The `-Dvrtsat.donot.suffix.username` option is available in the following file:
  On Windows: `C:\Program Files\Veritas\Java\nbjava.bat`

On UNIX: `/usr/openv/java/jnbSA`

- Use the currently installed version of the **NetBackup Administration Console** to connect to its associated master or media server.

Host ID-to-host name mappings are not case-sensitive

The host ID-to-host name mappings are not case-sensitive and are always displayed in a lower case irrespective of the capitalization that you have used while adding the mappings.

Mappings are displayed in the NetBackup Administration Console in the **Mapped Host Names / IP Addresses** column on the **NetBackup Management > Host Properties > Clients > Clients** tab. They can also be listed using the `nbhostmgmt` command.

Issues with SUSE 11 running on kernel versions later than 2.6

Live browse and backup problems can occur on SUSE 11 operating systems that have a kernel version later than 2.6. The issues occur because the `nbfirescan` process in NetBackup 8.1 does not support kernel versions later than 2.6.

To work around this issue, revert to kernel version 2.6 and perform the snapshot.

NetBackup limitations when using IPv6 address as client name or image name

The following two 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 8.1.

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

See "About NetBackup compatibility lists and information" on page 72.

- NetBackup Administration Console
- Remote Administration Console
- Character-based, menu interfaces for device management
- Command line

Memory requirements to run the NetBackup Administration Console

Veritas recommends that you run the console (`jnbSA`, `jbpSA`, or the Remote Administration Console) on a computer with at least 1 gigabyte of physical memory and 256 megabytes of memory available to the application.

Multiple versions of the NetBackup administration interface

Administrative interfaces for the supported versions of NetBackup are included in the installation package. For this release, that includes 7.7 and later versions. If you need to administer or perform operations for NetBackup pre-7.7 servers or clients, you can also install the NetBackup 8.0 Remote Administration Console. For information about the supported versions of the NetBackup administrative interface, see https://sort.veritas.com/eosl.

"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 8.1.

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 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 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 Accelerator operational notes

NetBackup Accelerator increases the speed of full backups. The increase in speed is made possible by change detection techniques on the client. The client uses the change detection techniques and the client's current file system to identify the changes that occurred since the last backup. This topic contains some of the operational notes and known issues that are associated with NetBackup Accelerator in version 8.1.

Accelerator version requirements for master, media, client, and media servers

NetBackup Accelerator requires master servers, media servers, and client servers to be at NetBackup 7.5 or higher. NetBackup appliance media servers require NetBackup Appliance 2.5 or higher for Accelerator support.

NetBackup Bare Metal Restore operational notes

NetBackup Bare Metal Restore (BMR) automates and streamlines the server recovery process, making it unnecessary to reinstall operating systems or configure hardware manually. This topic contains some of the operational notes and known issues that are associated with BMR in NetBackup 8.1.

Shared Resource Tree (SRT) creation may fail using NetBackup 8.1 as the BMR boot server on AIX and HP-UX platforms with NetBackup 8.0 and earlier clients

If you attempt to create a Shared Resource Tree (SRT) using NetBackup 8.1 as the BMR boot server on AIX and HP-UX platforms with NetBackup 8.0 and earlier clients, the SRT creation operation fails with an error message.

Workaround: Veritas recommends that you not upgrade your BMR boot server on AIX and HP-UX platforms to NetBackup 8.1.

If the boot server has a base installation of Solaris 10 update 11, the creation of SRTs can fail

If the boot server has a base installation of Solaris 10 update 11, the creation of Bare Metal Restore (BMR) shared resource trees (SRTs) that have a lower OS update can fail due to a kernel patch ID check. The issue occurs because Solaris 10 update 11 has a kernel patch ID that is lower than the ID for previous Solaris 10 updates.

Workaround: Update the kernel patch on the Solaris 10 update 11 BMR boot server. You can update the kernel by applying any of the provided kernel bug fix patches from Oracle Solaris. The kernel bug fix patches to Solaris 10 update 11 correct this issue by modifying the patch number to be higher than the other patches.

Many services on Solaris 11 print warning messages during a system boot and during BMR first boot

After a BMR restore during first boot on Solaris 11 and newer, error messages that are related to several services are seen.

Many services (such as `sendmail`) print warning messages during a system boot and during BMR first boot, such as:

```
sendmail/filesys_update failed
```

These messages are also seen during normal operating system installation on the system and therefore can be ignored.

Another set of messages that is seen on the console during BMR first boot are related to `zpool` and the Solaris Zones reconfiguration. All of these messages are harmless and have no effect on System Restore, and the zpools and the zones coming to the correct state

These messages come from SMF services and have no effect on system recovery.

Solaris Zone recovery on Solaris 11 and newer takes time to reconfigure after a BMR restore during first boot

During first boot after a Bare Metal Restore (BMR) restore operation, BMR reconfigures the zones using detach-attach commands. These commands may take some time to run if there are a large number of zones that need to be configured. After the BMR first boot command execution completes, the zpool, zones, and ZFS configurations may take some time to settle down with the new configuration.

Wait about 10 minutes after first boot (more depending on the number of zones) so that the system returns to the correct configuration state. You should not restart the system or log into any zones until that time to ensure a complete recovery.

A Solaris BMR restore operation fails if the text-installer package is not present in the customized AI ISO

A Solaris Bare Metal Restore (BMR) restore operation fails if the text-installer package is not present in the customized Automated Installer (AI) ISO that was created using the distribution constructor.

For shared resource tree (SRT) creation, if you use a customized AI ISO that was created using distribution constructor, then the text-installer package should not be removed from the AI manifest file.

For Solaris x86, this text-installer package is mandatory because the BMR restore makes use of a file from that package.

The /boot partition must be on a separate partition for a multiple device-based OS configuration

If the client is configured as root (`/`) under a multi-device, then for a successful BMR restore, the `/boot` partition must be on a separate partition. That means, if `/` and `/boot` are on the same partition, they are not supported for a multiple device-based OS configuration.

Multiple error messages might be displayed during the first boot after the restoration of a client with ZFS storage pools

During the first boot after the restoration of a client with ZFS storage pools, multiple error messages might be displayed. The following is an example:

```
SUNW-MSG-ID: ZFS-8000-D3, TYPE: Fault, VER: 1, SEVERITY: Major
EVENT-TIME: Mon May 23 13:10:09 CDT 2011
PLATFORM: SUNW,Sun-Fire-V215, CSN: -, HOSTNAME: bmrsol101.vxindia.veritas.com
SOURCE: zfs-diagnosis, REV: 1.0
EVENT-ID: c257eb38-495e-cdb6-9a52-a4d9c2ae38be
DESC: A ZFS device failed.  Refer to http://sun.com/msg/ZFS-8000-D3 for more information.
AUTO-RESPONSE: No automated response will occur.
IMPACT: Fault tolerance of the pool may be compromised.
REC-ACTION: Run 'zpool status -x' and replace the bad device.
```

For each disk in the computer you may see the error message. However, when you log on and run the `zpool status -x` command, you see the following message:

```
all pools are healthy
```

That is because of the ZFS import operation that is done during the first boot sequence. Bare Metal Restore (BMR) restores storage pools and contents in the BMR restoration environment and later imports to the client environment during first boot. That can cause an error message or a warning message during the first boot operation.

These messages only occur during the first boot operation and you can safely ignore them.

BMR may not format or clear the ZFS metadata

If you opt for the creation of a ZFS storage pool on small number of disks during a dissimilar disk restore (DDR), Bare Metal Restore (BMR) does not format or clear the ZFS metadata on the disks that remain. Because of that, if you attempt to use those disks to create other storage pools, you may see an error message that states a disk is in use under the ZFS storage pool.

To work around this issue, use the `-f` option to create a new storage pool on those disks.

Specifying the short name of the client to protect with Auto Image Replication and BMR

You must specify the short name of the client when you install NetBackup client packages on the computer that you want to protect with Auto Image Replication and Bare Metal Restore (BMR). You must also specify the short name of the client in the backup policy that you created on the primary domain. That policy backs up all of the client's local drives and gathers the client configuration that BMR requires. The DNS of the secondary or the tertiary domain cannot resolve the fully qualified name during a BMR recovery of that client at the disaster recovery site.

A restore task may remain in a finalized state in the disaster recovery domain even after the client restores successfully

In the case of a dissimilar domain restore where the primary and the disaster recovery domain names are different, the restore task remains in a finalized state in the disaster recovery domain even after the client restores successfully. The Bare Metal Restore (BMR) restore is successful in the disaster recovery domain and only the restore task update fails.

The update fails because of an invalid network configuration in the client. This behavior is expected because the restore does not modify the configuration files that are related to the DNS of the disaster recovery domain.

You must manually modify the following network configuration files to back up and restore the client in a disaster recovery domain:

- Solaris:
  - `/etc/hosts`
  - `/etc/resolv.conf`
  - `/etc/nodename`
  - `/etc/bge0.hostname`
- AIX:
  Use `smitty` to modify the network configuration.
- HP-UX:
  Use the HP System Management home page (SMH) to modify network configuration.
- Linux:
  `/etc/hosts`
  `/etc/resolv.conf`
  `/etc/sysconfig/network-scripts/ifcfg-eth*`
- Windows:

See the following URLs to modify the domain name in Windows:

- http://windows.microsoft.com/en-US/windows7/Connect-your-computer-to-a-domain
- http://support.microsoft.com/kb/295017

IPv6 support for BMR

Bare Metal Restore (BMR) provides protection to clients that can communicate over an IPv4-only network, an IPv6-only network, or a dual stack IPv4-IPv6 network. BMR recovery is yet supported only over IPv4 network as many NW boot protocols are not supported over IPv6 channel. In addition, when you configure a BMR database with the `bmrsetupmaster` command, the BMR master server IPv4 address needs to be enabled and able to resolve with the master server host name. Once `bmrsetupmaster` runs successfully, you can bring the IPv4 address down if you only want to use the IPv6 address.

During the BMR restore time, the master server and the media servers need to have IPv4 addresses up.

Example

A `bmrsetupmaster` may fail while BMR resolves its master's IPv4 address during its record creation into BMR database. As the BMR database creation fails, the BMR master does not function.

To resolve this issue, make sure an IPv4-based IP of the master server is enabled and can be resolved using the NetBackup master server name before you run the `bmrsetupmaster` command.

Note, the BMR backup is supported on IPv6 network channel, however, the BMR restore works only with IPv4 channel.

Automatic boot may fail for HP-UX after a restore

Sometimes after a Bare Metal Restore (BMR) restore and during the first boot of the client computer, the operating system automatic boot may fail. The HP BIOS then fails to identify the boot drive.

To resolve this issue, use the **HPBIOS > EFI** shell and select a hard drive that you can boot from (for example, `fs0:`) by looking at the device mapping table.

Change the directory (`cd`) to `\EFI\HPUX\` and run **HP-UX** to boot the operating system manually.

Note: Refer to the HP EFI manuals for more details on how to handle the EFI shell.

Once the client computer comes up, log on to the computer as `root` and run the following command to enable auto-booting.

```
setboot -p <hardware_path_of_boot_harddrive>
```

Prepare to Restore may not work for a Solaris client

A Bare Metal Restore (BMR) prepare-to-restore of a Solaris client computer may not work because the BMR boot server failed to resolve the IPv4 address of the client computer.

To work around this issue, perform the following:

- Make sure the IPv4 address, `client_host_name` mapping entry exists first in `/etc/hosts` before the IPv6 mapping entry.
  On the Solaris BMR boot server, if the `/etc/hosts` directory contains the IPv6 address `client_host_name` entry first, then the BMR boot server fails to identify client IPv4 address.
- Run **Prepare to Restore** again.

NetBackup Cloud operational notes

NetBackup Cloud Storage enables you to back up and restore data from cloud Storage as a Service (STaaS) vendors. NetBackup Cloud Storage is integrated with Veritas OpenStorage. This topic contains some of the operational notes and known issues that are associated with the NetBackup Cloud in NetBackup 8.1.

Incorrect error message is displayed while creating a bucket using the nbcldutil utility for Amazon cloud provider

While creating a bucket using `nbcldutil`, if you enter an invalid character as the last character of the bucket name, then an incorrect error message is displayed. This incorrect error message is displayed only for if the last character of the bucket name is an invalid character and not the rest of the characters. For example, if you type the bucket name value as `amzbucket-`, then the following incorrect error message is displayed:

```
Couldn't resolve host name
```

Network connection issues may occur when the Rackspace plug-in is used on a host running Windows Server 2008 R2 with IPv6 enabled

When the Rackspace plug-in is used on a host running Windows Server 2008 R2 with IPv6 enabled, NetBackup may experience network connection issues. Veritas recommends that you disable IPv6 on Windows Server 2008 R2 hosts that use the Rackspace plug-in.

NetBackup cluster operational notes

Clusters provide high availability of applications and data to users. In a cluster, two or more servers (called nodes) are linked in a network. These servers run the cluster software that allows each node access to the shared disks. This topic contains some of the operational notes and known issues that are associated with cluster technologies in NetBackup 8.1.

NetBackup services may start on the same active node after resource failure in a Solaris cluster setup

In the case of a NetBackup clustered master server in a Solaris cluster setup, NetBackup services may restart on the same active cluster node after failure instead of failing over to another node. The cluster log contains the following log message:

```
SC[,VRTS.scnb,scnb-harg,scnb-hars,gethostnames]: [ID 758691
daemon.warning] Current setting of Retry_interval= 300, might prevent
failover on repeated probe failures. It is recommended that
Retry_interval be greater than or equal to [(Thorough_probe_interval
+ Probe_timeout) * 2 * Retry_count]. Current values are
(Thorough_probe_interval = 60,Retry_count = 2,Probe_timeout = 30).
```

To resolve the issue, perform the following steps:

1. Set the `Retry_interval` option for resource `scnb_hars` to more than 360 using the following command:

   ```
   #/usr/cluster/bin/clrs set -y Retry_interval=400 scnb-hars
   ```

2. Verify the updated value of the `Retry_interval` option using the following command:

   ```
   # /usr/cluster/bin/clrs show -y Retry_interval scnb-hars
   ```

NetBackup database and application agent operational notes

NetBackup offers several methods of protecting various database and application technologies, such as Oracle, Microsoft SQL Server, and Microsoft Exchange Server. This topic contains some of the operational notes and known issues that are associated with the protection of database technologies in NetBackup 8.1.

NetBackup for Exchange operational notes

NetBackup for Exchange Server extends the capabilities of NetBackup to include online backups and restores of Exchange databases. This topic contains some of the operational notes and known issues that are associated with NetBackup for Exchange in NetBackup 8.1.

The status of a DAG backup can be empty if the restore is initiated from a node in the DAG

When you restore databases or granular items of a database availability group (DAG) backup, the restore status may appear empty from the Backup, Archive, and Restore (BAR) interface. The status is empty if the restore is initiated from a node in the DAG. You should initiate the restore from the active DAG node or a NetBackup server to properly see the activity status.

User-initiated backups in a DAG environment fail if initiated from a node in the DAG that is not currently active

User-initiated backups in a database availability group (DAG) environment fail if initiated from a node in the DAG that is not currently active for the virtual DAG name.

Workaround: Initiate the user backup from the active DAG node, or manually start the backup from the NetBackup master to properly start the backup.

NetBackup for SharePoint operational notes

NetBackup for SharePoint Server extend the capabilities of NetBackup to include online backups and restores of SharePoint databases. This topic contains some of the operational notes and known issues that are associated with NetBackup for SharePoint in NetBackup 8.1.

SharePoint GRT restore can fail if the host names or IP addresses are not mapped with the host ID

If all the SharePoint front-end and back-end host names or IP addresses of a NetBackup host are not mapped to their corresponding host ID, a SharePoint Granular Recovery Technology (GRT) restore that is associated with the host can fail with status code 2804.

To resolve the issue, approve the pending host ID-to-host name mappings:

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Security Management > Host Management**.
2. In the details pane, click the **Mappings for Approval** tab.
3. Select the mapping that you want to approve and right-click.
4. On the right-click options, click **Approve**. The selected mapping is approved.

   Alternatively, click **Mapping Details** on the right-click options. Use the **Mapping Details** dialog box to approve the selected mapping.

Granular restores skip versioned documents or files that are checked out

The following known issues relate to the restore of a document or a file that is enabled for versioning and is checked out at the time of backup:

- For SharePoint 2010, the granular restore of such documents or files is skipped. The restore fails with the error: "Additions to this website have been blocked."
- For SharePoint 2016, an additional version is present after restore. If the parent list contains a column that has a validation formula that might fail, the restore job might fail but the file content and other valid metadata are restored. The "checked-out" tag is also removed from the item.

To work around this issue, you can restore a checked-out item and its versions by selecting a list as the restore target. However, note that in this case, the "checked-out" tag is removed from the item. For more information, refer to the *NetBackup for Microsoft SharePoint Server Administrator's Guide*.

Modified system files or ghosted files are not cataloged or restored during a site collection restore

Modified system files or modified ghosted files are neither cataloged nor restored during a site collection restore. This issue is observed in SharePoint 2013/2016.

To work around this issue, restore the SharePoint web application content database. For more information, refer to the *NetBackup for Microsoft SharePoint Server Administrator's Guide*.

Restored wiki pages may not be correct

When you use Granular Recovery Technology (GRT) to restore a page in the wiki site, the restored content may be incorrect.

To work around this issue, restore the SharePoint web application content database. For more information, refer to the *NetBackup for Microsoft SharePoint Server Administrator's Guide*.

When you use Granular Recovery Technology (GRT) to restore ghosted or uncustomized ASPX pages from any template of SharePoint 2016, the restore job is successful, but the restored pages appear with the default content when it was created. This issue is not seen if the ASPX pages are uploaded to SharePoint. Such pages are treated as customized pages.

To work around this issue, restore the SharePoint web application content database. See "Redirecting the restore of a SharePoint Server Web application content database to an alternate SQL instance" in the *NetBackup for Microsoft SharePoint Server Administrator's Guide*.

NetBackup for Oracle operational notes

NetBackup integrates the database backup and recovery capabilities of the Oracle Recovery Manager (RMAN) with the backup and recovery management capabilities of NetBackup. This topic contains some of the operational notes and known issues that are associated with NetBackup for Oracle in NetBackup 8.1.

Oracle Copilot mount path in the oradnfstab file on Windows clients must contain only ASCII characters

On Windows clients, when the `oradnfstab` file is used for Oracle Copilot backups, the mount path that is specified in the `oradnfstab` file must contain only ASCII characters. The mount path is not currently internationalized.

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 8.1.

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

Error message appears when you remove a trusted master server without updating the trust

After you upgrade to NetBackup 8.1, if you remove a trusted master server without updating the trust, the `nbseccmd` command displays the following error message:

```
User authentication failed. User name, domain, password or token is
incorrect(5601).
```

Workaround: The error message is inaccurate. You must update the trust and then remove the trusted master server. For more information, see the NetBackup Deduplication Guide.

Status code 6 message may be displayed when adding a trusted master server

As a part of adding a trusted master server, the remote master server version is also retrieved. If the source master server is unable to retrieve the remote master server version, the following error message is displayed:

```
Exit status 6: The backup failed to back up the requested files.
```

Workaround: The error message is inaccurate. Re-attempt to add the trusted master server. For more information, see the NetBackup Deduplication Guide.

Duplication of NDMP images may fail when NBAC is enabled

In the case of NetBackup Access Control or NBAC-enabled NetBackup setup, when an NDMP image is backed up on AdvancedDisk and is duplicated to an MSDP on the same host, duplication job fails with status code 116. The following error message is displayed:

```
VxSS authentication failed
```

Review the logs from the NetBackup master and media server hosts to find this log entry.

Additional restriction for restoring data that uses SHA-2 algorithm

NetBackup 8.1 MSDP introduces SHA-2 fingerprinting. As a result, there is a restriction when using client-direct restore on a pre-8.1 client.

You cannot use client-direct restore from a back-level client to restore data that is backed up to a media server or from a client that uses the new SHA-2 algorithm. However, you may choose to restore the data using a server that supports SHA-2.

This restriction is in addition to the other notes and restrictions that are listed in "About MSDP fingerprinting" in the NetBackup Deduplication Guide for NetBackup 8.1.

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 8.1.

Support for localized environments in database and application agents

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

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

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 8.1.

An error may occur when restoring from an Isilon NDMP backup to alternate paths

This error is associated with Isilon OneFS 8.0.0.1.

An error (status code 2813: NDMP policy restore error) may occur when you restore from an Isilon NDMP backup to an alternate path. The restore fails when the number of directories in the specified alternate path is less than the number of directories in the selected restore path.

Note: EMC Isilon plans to include a fix to this issue in a future release of Isilon OneFS. Check your Isilon documentation and the Dell EMC Isilon website for more details about the fix.

Workaround:

Change the alternate path specification for the restore so that it does not have a smaller number of directories than the selected restore path has.

For example:

- Assume that backup the policy was set up to back up `/ifs/User_1`. Therefore, the backup includes subdirectories such as `/ifs/User_1/0/000/000` in it.
- You select `/ifs/User_1/0/000/000` for restore.
  In this case, the selected restore path has three directories in it: `0/000/000`.
- Next, you set up the restore to an alternate path: `/ifs/User_1/restore/` and run the restore job.
  However, the Isilon filer seems to ignore the first element of the alternate path (`/ifs`) and recognizes only two directories: `User_1/restore`.
- The restore fails with status code 2813 because the number of directories in the alternate path is less than the number of directories in the selected restore path. In this case, there are two directories (`User_1/restore`) in the alternate path versus three directories (`0/000/000`) in the selected restore path.
- Next, you change the alternate path to `/ifs/User_1/restore/test`.

Isilon now recognizes three directories (`User_1/restore/test`) in the alternate path. This number matches the number of directories in the selected restore path.

- The restore now completes successfully.

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 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 8.1.

NetBackup for VMware operational notes

NetBackup for VMware provides backup and restore of the VMware virtual machines that run on VMware ESX servers. Additionally, the NetBackup plug-in for VMware vCenter (vCenter plug-in) allows the vSphere Client to monitor virtual machine backups and recover a virtual machine from a backup. This topic contains some of the operational notes and known issues that are associated with NetBackup for VMware and the vCenter plug-in in NetBackup 8.1.

The VM's swap files are not excluded from the backup if a volume on the VM contains multiple swap files

If a Linux VMware VM volume contains more than one swap file, the NetBackup policy option "Exclude swap and paging files" does not work. The swap files are included in the backup of the VM. This issue affects NetBackup 8.1 and NetBackup 8.0.

Using the NetBackup appliance to install the NetBackup plug-in for VMware vSphere Web Client

The following information on installing the NetBackup vSphere Web Client plug-in was omitted from the *NetBackup Plug-in for VMware vSphere Web Client Guide*.

To install the NetBackup plug-in from the NetBackup appliance as master server

- Log on to the appliance as a **NetBackupCLI** user and run the `vwcp_manage` command to install the plug-in.

  For example, to install the plug-in on `vcenter_server.example.com`:

  ```
  vwcp_manage --register -v vcenter_server.example.com -u
  vcenter_username -p password
  ```

  To uninstall the plug-in:

  ```
  vwcp_manage --unregister -v vcenter_server.example.com -u
  vcenter_username -p password
  ```

VMware block-level incremental backups expire when the previous full backup expires

NetBackup VMware block-level incremental backups of a virtual machine are dependent on the previous full backup of the same VM made by the same policy. When a full VMware backup expires, any later block-level incremental backups for the VM that are based on the full backup also expire and are deleted. The expiration occurs without regard to the retention period in the incremental schedule. This issue applies to all versions of NetBackup for VMware.

Note: This issue does not apply to NetBackup Accelerator backups.

A VM restore to a vCenter fails when NetBackup has credentials for a restore ESX server

NetBackup's **VMware Restore ESX Server** option (under **Media and Device Management > Credentials > Virtual Machine Servers**) allows a particular ESXi server to perform the data movement for a VM restore. If the destination for the restore is a vCenter (not the ESXi server), the restore fails with status 2820, "NetBackup VMware policy restore error." The VM is restored but NetBackup cannot revert to the VM snapshot and delete the snapshot.

A NetBackup 8.1 emergency engineering binary (EEB) is available that fixes this issue.

As a workaround, you can use the vSphere interface to revert to the restored VM's snapshot and then remove the snapshot.

To revert to and remove the VM snapshot

1. In vSphere Web Client 6.0, right-click on the restored VM and select **Snapshots > Revert to Latest Snapshot**.
2. Right-click on the VM again and select **Snapshots > Manage Snapshots**. Use the **Manage VM Snapshots** dialog to remove the snapshot.

For details on your version of vSphere and how to remove snapshots, refer to VMware documentation.

Appendix A

About SORT for NetBackup Users

This appendix includes the following topics:

About Veritas Services and Operations Readiness Tools

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

Access SORT from the following webpage:

https://sort.veritas.com/netbackup

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

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

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

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

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

Recommended SORT procedures for new installations

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

Table A-1

Procedure	Details
Create a Veritas Account on the SORT webpage	See "To create a Veritas Account on the SORT page" on page 58.
Create generic installation reports	See "To create a generic installation checklist" on page 58.
Create system-specific installation reports	See "To create a system-specific installation report for Windows" on page 59. See "To create a system-specific installation report for UNIX or Linux" on page 60.

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 58.

Table A-2 *(continued)*

Procedure	Details
Create a system-specific upgrade report	See "To create a system-specific installation report for Windows" on page 59. See "To create a system-specific installation report for UNIX or Linux" on page 60.
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 62. See "To review hot fix and emergency engineering binary information" on page 62.

To review future platform changes and feature plans

1. In your web browser, navigate to:

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

To review hot fix and emergency engineering binary information

1. In your web browser, navigate to:

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

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

Appendix B

NetBackup installation requirements

This appendix includes the following topics:

About NetBackup installation requirements

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

See "NetBackup installation and upgrade operational notes" on page 33.

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

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

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

- 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 8.1. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 8.1 and other NetBackup releases can be found on the Veritas Services and Operational Readiness Tools (SORT) website and in the NetBackup compatibility lists.

See "About NetBackup compatibility lists and information" on page 72.

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

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

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

Table B-1 Required operating system patches and updates for NetBackup 8.1

Operating system type and version	NetBackup role	Patch	Notes
AIX 6.1	Master, media, client	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	Master, media, client	COMPLIBS.LIBM-PS32	If you install AT on an HP-UX platform, this patch is required.
HP-UX IA-64	Master, media, client	Networking.NET-RUN: /usr/lib/libipv6.sl	
	Master, media, client	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.1	
	Master, media, client	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.sl	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so.1	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so.1	
	Master, media, client	Networking.NET2-RUN: /usr/lib/libipv6.1	

Table B-1 Required operating system patches and updates for NetBackup 8.1 *(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	Master, media, client	Kernel 2.6.32-504.14.1 or later	More information is available: Kernel security and bug fix update
Oracle Linux 7	Master, 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 8.1 *(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 8.1 binary sizes

Table B-2 contains the approximate binary sizes of the NetBackup 8.1 master server, media server, and client software for the various supported operating systems. These binary size indicate the amount of disk space occupied by the product after an initial installation.

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 Symantec 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 56.

Table B-2 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
AIX	POWER		1622 MB	8053 MB	
Canonical Ubuntu	x86-64		1595 MB		
CentOS	x86-64		1042 MB	6252 MB	Media server or client compatibility only.
Debian GNU/Linux	x86-64		1595 MB		
HP-UX	IA-64		2117 MB	9366 MB	
OpenVMS	IA-64		128 MB		The listed sizes are for the NetBackup 7.5 binaries. No NetBackup 8.1 binaries for OpenVMS are provided.
Oracle Linux	x86-64		1053 MB	6254 MB	
Red Hat Enterprise Linux Server	x86-64		1053 MB	6946 MB	
Red Hat Enterprise Linux Server	z/Architecture		840 MB	3661 MB	Media server or client compatibility only.

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

OS	CPU Architecture	32-bit client	64-bit client	64-bit server	Notes
Solaris	SPARC		1127 MB	6326 MB	
Solaris	x86-64		1129 MB	6451 MB	
SUSE Linux Enterprise Server	x86-64		1013 MB	6750 MB	
SUSE Linux Enterprise Server	z/Architecture		834 MB	3610 MB	Media server or client compatibility only.
Windows	x86-32	833 MB			Covers all compatible Windows x86 platforms
Windows	x86-64		646 MB	1343 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 8.1.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Agent	Server	ViewBuilder
Oracle Linux	x86-64		644 MB	
Red Hat Enterprise Linux Server	x86-64		644 MB	
SUSE Linux Enterprise Server	x86-64		734 MB	
Windows Server	x86-64	245 MB	666 MB	225 MB

NetBackup plug-ins

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

Appendix C

NetBackup compatibility requirements

This appendix includes the following topics:

About NetBackup compatibility lists and information

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

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

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

NetBackup compatibility lists

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

http://www.netbackup.com/compatibility

Note: Select "Compatibility Between NetBackup Versions" from the compatibility lists for information about which versions of NetBackup are compatible with each other.

About NetBackup end-of-life notifications

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

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

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

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

Using SORT

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

https://sort.veritas.com/nbufutureplans

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

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

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

About changes in platform compatibility

The NetBackup 8.1 release may contain changes in support for various systems. In addition to using SORT, you should make sure to review the *NetBackup Release Notes* document and the NetBackup compatibility lists before installing or upgrading NetBackup software.

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

http://www.netbackup.com/compatibility

Appendix D

Other NetBackup documentation and related documents

This appendix includes the following topics:

About related NetBackup documents

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

Veritas releases various guides and technical manuals that relate to NetBackup software. These documents are published for new versions of NetBackup based on release type.

Unless otherwise specified, the NetBackup documents can be downloaded in PDF 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.

About NetBackup release notes documents

The following release notes documents are published for NetBackup software:

- *NetBackup Release Notes*
  This document contains a great deal of assorted information about particular releases of NetBackup for both UNIX and Windows platforms. This information includes, but is not limited to, new features, platform compatibility changes, patch requirements, documentation corrections, and known issues. This document also contains any operational notes that may not be found elsewhere in the NetBackup manuals or the online Help.
- *NetBackup Emergency Engineering Binary Guide*
  This document contains listings of some of the known issues that were identified, fixed, and available to NetBackup customers in the form of an Emergency Engineering Binary (EEB). It also lists a certain number of the issues that were fixed in a given release, but that may not have resulted in an EEB.

About NetBackup administration documents

The following administrator guides are published for NetBackup software:

- *NetBackup Administrator's Guide, Volume I*
  This guide explains how to configure and manage NetBackup on a UNIX or Windows server. This guide describes the NetBackup interfaces and how to configure hosts, storage devices and media, storage lifecycle policies (SLPs), backups, replication, and monitoring and reporting.
- *NetBackup Administrator's Guide, Volume II*
  This guide explains additional configuration and interface options for NetBackup. This guide also contains reference topics and information about NetBackup licensing.

About administration of NetBackup options

The following administrator guides for NetBackup options are published for NetBackup software:

- *NetBackup AdvancedDisk Storage Solutions Guide*

This guide explains how to configure, manage, and troubleshoot the NetBackup AdvancedDisk storage option. This guide describes how to use the disk storage that is exposed to NetBackup as a file system for backups.

- *NetBackup Bare Metal Restore Administrator's Guide*
  This guide explains how to install, configure, and manage NetBackup Bare Metal Restore (BMR) boot servers and clients to automate and streamline the server recovery process.
- *NetBackup Cloud Administrator's Guide*
  This guide explains how to configure and manage NetBackup to back up and restore data from cloud Storage as a Service (STaaS) vendors through Veritas OpenStorage.
- *NetBackup DataStore SDK Programmer's Guide for XBSA*
  This guide explains how to set up and use the XBSA Application Programming Interface to create a backup or archive application that communicates with NetBackup.
- *NetBackup Deduplication Guide*
  This guide explains how to plan, configure, migrate, monitor, and manage data deduplication in a NetBackup environment using the NetBackup Media Server Deduplication Option.
- *NetBackup Logging Reference Guide*
  This guide explains the various NetBackup logs and reports which can help you troubleshoot any problems that you encounter, including how to run reports from the NetBackup Administration Console and where logs are stored on your system.
- *NetBackup OpenStorage Solutions Guide for Disk*
  This guide describes how to configure and use an intelligent disk appliance in NetBackup for backups.
- *NetBackup for VMware Administrator's Guide*
  This guide describes how to configure NetBackup to perform such functions as off-host backups of VMware virtual machines that run on VMware ESX servers.
- *NetBackup Plug-in for VMware vSphere Web Client*
  This guide describes how to install and troubleshoot the vSphere Web Client plug-in for NetBackup. The vSphere Web Client plug-in allows you to monitor backups of virtual machines which are managed by vCenter servers, recover virtual machines from backups, and monitor VM backup status and related messages.
- *NetBackup for Hyper-V Administrator's Guide*

This guide explains how to configure and manage snapshot-based backup policies for the virtual machines that run on Windows Hyper-V servers.

- *NetBackup Add-in for Microsoft SCVMM Console Guide*
  This guide describes how to install and troubleshoot the NetBackup Add-in for System Center Virtual Machine Manager (SCVMM), and how to use it to recover virtual machines from NetBackup backup images.
- *NetBackup for NDMP Administrator's Guide*
  This guide explains how to install, configure, and use NetBackup for Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems.
- *NetBackup Replication Director Solutions Guide*
  This guide describes how to implement NetBackup OpenStorage-managed snapshots and snapshot replication, where the snapshots are stored on the storage systems of partnering companies.
- *NetBackup SAN Client and Fibre Transport Guide*
  This guide describes how to set up, configure, and manage the NetBackup SAN Client feature to use the Fibre Transport method for high-speed client backups.
- *NetBackup Snapshot Client Administrator's Guide*
  This guide explains how to install, configure, and use NetBackup Snapshot Client to enable a variety of snapshot-based features, including integration with VMware, Hyper-V, and Replication Director.
- *NetBackup Vault Administrator's Guide*
  This guide explains how to install, configure, and use NetBackup Vault to automate selection and duplication of backup images for off-site media storage.
- *NetBackup Vault Operator's Guide*
  This guide explains how to use NetBackup Vault to vault media as part of two major task areas: Administration and operation. Some of the described tasks include procedures for sending tapes off site, receiving tapes on site, and running reports on off-site media and vault jobs.
- *NetBackup WebSocket Service (NBWSS) Reference Guide*
  This guide explains how to use the NetBackup WebSocket Service (NBWSS) for communication with a cloud application and how to configure WebSocket endpoints for NBWSS.
- *NetBackup OpsCenter Administrator's Guide*
  This document describes how to use the NetBackup OpsCenter user interface to provide reporting, monitoring, and alerts for NetBackup and its agents and options.
- *NetBackup OpsCenter Reporting Guide*

This guide explains how to use NetBackup OpsCenter to generate and use comprehensive business-level reports to track the effectiveness of data backup and archive operations.

- *NetBackup OpsCenter Performance and Tuning Guide*
  This performance and tuning guide is for administrators who want to analyze, evaluate, and tune OpsCenter performance. This document is intended to provide guidance on how to tune OpsCenter for maximum performance, which system configurations you should use for OpsCenter depending on your backup environment, and best practices to follow for increased OpsCenter performance.

About administration of NetBackup database agents

The following administrator guides for NetBackup database agents are published for NetBackup software:

- *NetBackup for DB2 Administrator's Guide*
  This guide explains how to install, configure, and use the NetBackup for DB2 database agent.
- *NetBackup for Enterprise Vault Agent Administrator's Guide*
  This guide explains how to install, configure, and use the NetBackup for Enterprise Vault agent to protect Veritas Enterprise Vault configuration information and archived data.
- *NetBackup for Informix Administrator's Guide*
  This guide explains how to install, configure, and use the NetBackup for Informix agent to back up and restore the Informix databases that are on a UNIX NetBackup client.
- *NetBackup for Lotus Notes Administrator's Guide*
  This guide explains how to configure and use the NetBackup for Lotus Notes agent to back up and restore Lotus Notes databases and transaction logs on NetBackup clients.
- *NetBackup for Microsoft Exchange Server Administrator's Guide*
  This guide explains how to configure and use the NetBackup for Exchange Server agent to perform online backups and restores of Microsoft Exchange Server.
- *NetBackup for Microsoft SQL Server Administrator's Guide*
  This guide explains how to configure and use the NetBackup for Microsoft SQL Server agent to back up and restore Microsoft SQL Server databases and transaction logs.
- *NetBackup for Microsoft SharePoint Server Administrator's Guide*

This guide explains how to configure and use the NetBackup for SharePoint Server agent to back up and restore the SharePoint databases that are on a Windows NetBackup client.

- *NetBackup for Oracle Administrator's Guide*
  This guide explains how to configure and use the NetBackup for Oracle agent to back up and restore the Oracle databases that are on a NetBackup client.
- *NetBackup for SAP Administrator's Guide*
  This guide explains how to configure and use the NetBackup for SAP agent to back up and restore SAP and SAP HANA databases that are on a NetBackup client.
- *NetBackup for Sybase Administrator's Guide*
  This guide explains how to configure and use the NetBackup for Sybase agent to back up and restore Sybase databases that are on a NetBackup client.

About NetBackup installation documents

The following installation documents are published for NetBackup software:

- *NetBackup Installation Guide*
  This guide explains how to install NetBackup server, client, and administrative software on UNIX and Windows platforms.
- *NetBackup LiveUpdate Guide*
  This guide explains how to set up a NetBackup LiveUpdate server to provide a policy-driven method of distributing NetBackup software releases within your environment.
- *NetBackup Upgrade Guide*
  This guide is provided to help assist you plan and accomplish your upgrade of NetBackup software. This guide is updated periodically to provide you with the most up-to-date information.
- *NetBackup Quick-Start Upgrade Guide*
  This guide is designed as a supplement to the *NetBackup Upgrade Guide* for the experienced user. The information in this guide assumes that you have already read and understand the upgrade prerequisites. (Use of this guide by novice or inexperienced NetBackup administrators is not recommended. These administrators should use the *NetBackup Upgrade Guide*.)

About NetBackup configuration documents

The following configuration guides for NetBackup options are published for NetBackup software:

- *NetBackup Device Configuration Guide*
  This guide describes how to set up and configure the operating systems of the storage device hosts you use for NetBackup servers.

About NetBackup troubleshooting documents

The following troubleshooting guides are published for NetBackup software:

- *NetBackup Troubleshooting Guide*
  This guide provides general troubleshooting information and explains the various troubleshooting methods that can be used for NetBackup products and features.
- *NetBackup Status Codes Reference Guide*
  This guide provides a complete list of the status codes for NetBackup, Media Manager, device configuration, device management, and robotic errors. Each status code listing includes an explanation and the recommended actions.

About other NetBackup documents

The following documents are published for NetBackup software:

- *NetBackup Commands Reference Guide*
  This guide contains detailed information on the commands that run on UNIX systems and Windows systems, including all of the NetBackup man page commands.
- *NetBackup Clustered Master Server Administrator's Guide*
  This guide provides information on how to install and configure a NetBackup master server in a cluster.
- *NetBackup in Highly Available Environments Guide*
  This guide discusses various methods for using NetBackup in highly available environments and provides guidelines for protecting NetBackup against single points of failure.
- *NetBackup Security and Encryption Guide*
  This guide provides information about on how to secure NetBackup using access control, enhanced authorization and authentication, and encryption.
- *NetBackup Network Ports Reference Guide*

This guide provides a reference to NetBackup network ports, including master server and media server ports, client ports, default ports, and other ports that NetBackup uses.

- *NetBackup Getting Started Guide*
  This guide provides a high-level description of preinstallation information that is related to this release of NetBackup. The guide also includes descriptions of the NetBackup media kit, the NetBackup Electronic Software Distribution (ESD) images, and the NetBackup license key requirements.
- *NetBackup Backup, Archive, and Restore Getting Started Guide*
  This guide provides basic information about backup and restore procedures for new users of NetBackup. These procedures include how to back up, archive, and restore files, folders or directories, and volumes or partitions that reside on a computer.
- *NetBackup Third-party Legal Notices*
  This document contains proprietary notices for the Third-Party Programs and the licenses for the Third-Party Programs, where applicable, that pertain to the Veritas NetBackup and OpsCenter products.