Symantec NetBackup™ 7.6 Release Notes

Release 7.6 First Availability

Document Version 2

Symantec

Symantec NetBackup™ 7.6 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 7.6 First Availability

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a set of web-based tools that supports Symantec enterprise products. For NetBackup, SORT provides the ability to collect, analyze, and report on host configurations across UNIX/Linux or Windows environments. This data helps to assess whether your systems are ready for an initial NetBackup installation or for an upgrade from your current version.

To access SORT, go to the following webpage:

https://sort.symantec.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.

- **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 Symantec enterprise products, tips for risk assessment, and product license tracking.
- **NetBackup Future Platform and Feature Plans**
  Use this tool to get information about what items Symantec intends to replace with newer and improved functionality, and what items Symantec intends to discontinue without replacement. Some of these items include certain NetBackup features, functionality, 3rd-party product integration, Symantec product integration, applications, databases, and the OS platforms.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

New features and enhancements

This chapter includes the following topics:

About NetBackup 7.6 new features and enhancements

This release of NetBackup emphasizes availability and performance to protect mission-critical data and applications in physical and virtualized environments. The following sections in this chapter describe several new features and enhancements that are found in NetBackup and its components.

New platforms and proliferation

NetBackup 7.6 contains support for several new software and hardware platforms. Some of this information can be found in various sections of the *NetBackup 7.6 Release Notes*. However, for the most up-to-date compatibility information, see the various compatibility lists on the Symantec Support website:

http://www.symantec.com/docs/TECH59978

See "About server and client platform compatibility" on page 39.

See "Disaster recovery with BMR" on page 14.

General new features and enhancements

This section describes some of the new general enhancements that can be found in this release of NetBackup.

- In NetBackup 7.6, the Sybase SQL Anywhere database (NetBackup catalog) has been upgraded to version 12.0.1. This version prioritizes higher performance, but compared to earlier NetBackup releases, this version can consume higher CPU.

  Note: Support for remote-EMM and shared-EMM server configurations is withdrawn in NetBackup 7.6. In a remote- or shared-EMM server configuration, the NetBackup relational database (NBDB), the Enterprise Media Manager (EMM), and the Resource Broker (RB) are moved to a server that is not the master server. This configuration is not supported in NetBackup 7.6.

  Customers who currently use this configuration should contact Symantec Support who will engage Symantec Engineering to review the options to disengage this configuration from an environment.

- An option has been provided so that job failover to a LAN can be prohibited if a Fibre Transport failure occurs. Using this option results in job failure instead of unexpected or undesirable traffic on the LAN. To enable this setting, open the NetBackup Administration Console and go to **Fibre Transport** > **Settings**

> **Host Properties** and choose the **Fail** option. Alternatively, select the **Fail** option in the preferences section of the SAN Client page of the Device Configuration Wizard.
Please note that the default setting is to failover to LAN if Fibre Transport is not available.

- The new NetBackup status code 2111 has been added to this release with the following description:

  ```
  All storage units are configured with On Demand Only and are not
  eligible for jobs requesting ANY storage unit.
  ```

  This code applies to the situation which previously led to a general status code 213 “No storage units available for use.” The new status code provides more granular troubleshooting.

- Support for 64-bit NDMP devices:
  Support has been added for NDMP dump type backups of devices with 64-bit inode numbers.

- NetBackup utility enhancements:
  This release of NetBackup includes improvements to the `NBCC`, `NBCCA`, `NBCCR`, and `nbsu` utilities. The improvements to `NBCC`, `NBCCA`, and `NBCCR` include many enhancements and high-priority fixes that improve the end-user experience. These fixes assist the NetBackup Support organization to identify NetBackup catalog and database consistency issues. Enhancements to `nbsu` 1.7 include improvements to NetBackup diagnostic data collection and the diagnosis of issues with NetBackup.

- Hot fix / EEB preinstall checker
  Before an upgrade, the NetBackup server installer checks that the release to be installed contains a fix corresponding to every EEB that is already installed. For any such fix that is not included in the release, the user is given detailed information about the fix. The user is then given the opportunity to cancel the installation.

- OpenStorage client direct restores:
  Performance has been improved and network overhead has been decreased for NetBackup client restores from any NetBackup deduplication storage.

- Catalog enhancements

  This feature offers the following improvements:

  - Catalog backup performance
    Performance improvements have been made to decrease the run time for catalog backups.

    - Catalog compression enhancements
      NetBackup now has a built-in compression method to compress the image catalog, which provides better compression ratios than earlier methods. Catalog files that are compressed under earlier methods are transparently migrated to the newer method when they are accessed as part of NetBackup operations.

- Logging Assistant Feature:
  This feature allows the user to enable, collect, upload, and disable the NetBackup debug logging that Symantec Support typically requires to troubleshoot support cases.

Accelerator enhancements

This section describes some of the new features and enhancements that have been added to NetBackup Accelerator in this release of NetBackup.

- Accelerator for VMware:
  This feature offers fast VMware data protection with full support for granular restore technology with much lower resource consumption than an incremental backup. It also offers Accelerated application data protection in virtualized environments.
- The following support has been added for Accelerator in NetBackup 7.6:
  - Accelerator is fully supported with the ReFS file system.
  - Accelerator is fully supported with and without NTFS deduplication enabled.
  - SQL server support for VMware environments
  - SharePoint support for VMware environments
  - Exchange support for VMware environments

Database and application agent support enhancements

This section describes some of the new database agent and application support enhancements that can be found in this release of NetBackup.

The following database and application support has been added in this release:

- DB2 support for zLinux

The following list includes various database and application enhancements in this release:

- A new lookup table has been added to the NetBackup relational database for Oracle, SQL Server, and DB2 database backups.

  The lookup table provides a mapping between the NetBackup backup identifier and the application's backup identifier. When the application searches for the backup to perform crosschecks or restores, it uses the application's backup identifier. The application's identifier is now efficiently mapped to the NetBackup backup identifier by the lookup table resulting in faster crosschecks and restores.

About NetBackup for Microsoft Exchange

The following support has been added to the NetBackup Exchange Agent:

- Exchange 2013 support (database only). Granular Recovery Technology (GRT) and off-host backups are not supported with this release.
- Exchange 2010 SP3 support on Windows 2008 R2 and Windows Server 2012.
- The Exchange client host properties now includes a property called Exchange credentials. Provide the credentials for a unique Exchange mailbox that has sufficient roles or group memberships to perform backups and restores. This account must also have the right to "Replace a process level token".
- In this release, for NetBackup operations with Exchange 2010 or 2013 you can now use a minimal mailbox account that has local administrator rights rather than Exchange administrator rights. See the *NetBackup for Exchange Administrator's Guide* for details.

About NetBackup for Microsoft SharePoint

The following support has been added to the NetBackup SharePoint Agent:

- NetBackup 7.6 backs up SharePoint 2010 service application components that are included with the Office Web Applications 2010 add-on. However, NetBackup does not currently support restores of these components. These Shared Services include the following:
  - Microsoft SharePoint Resources:\Shared Services\Shared Services Applications\Power Point Service Application
  - Microsoft SharePoint Resources:\Shared Services\Shared Services Applications\Word Viewing Service
  - Microsoft SharePoint Resources:\Shared Services\Shared Services Applications\Excel Calculation Service
- SharePoint 2013 support (database only). Please note, Granular Recovery Technology (GRT) is not supported with this release.

- Redirection of a SharePoint Content database to another SQL instance is supported. Redirecting a content database to another SQL instance lets you take advantage of data recovery from an unattached content database.
- NetBackup Accelerator for VMware support has been added for SharePoint.
- Claims-based authentication (CBA) is now supported for Web application in SharePoint 2010 and later. The following providers are supported:
  - Windows Authentication (LDAP)
  - Facebook
  - LinkedIn
  - Live Id
  - Forms-based authentication (FBA) using SQL Server
  - Active Directory Federation Services (AD FS) 2.0

Disaster recovery with BMR

This section describes some of the new Bare Metal Restore (BMR) features and enhancements that can be found in this release of NetBackup.

BMR now supports the following platforms and proliferations in NetBackup 7.6:

- BMR Server on Windows Server 2012
- BMR Client/Boot Server for Oracle Solaris 11 SPARC and x86-64.
- BMR Client/Boot Server for Red Hat Enterprise Linux 6 through update 4, except update 2.
- BMR Client/Boot Server for Red Hat Enterprise Linux 5 through update 9.
- BMR Client/Boot Server for Oracle Linux 6 through update 4.
- BMR Client/Boot Server for Oracle Linux 5 through update 8, except update 5 and update 6.
- BMR direct virtual machine creation from client backup:
  BMR can create a client VMware-based virtual machine from its backup image by running a wizard or executing a single command from the command line. This feature is a very easy and a very fast disaster recovery option that you can use to perform disaster recovery compliance testing as well. This feature helps in lowering the operational expenditure (OpEx) by leveraging a virtual environment for client recovery.
  In NetBackup 7.6, the VM creation process is supported for the clients that are based on Windows 2003/2008/2008 R2/Windows 7 operating systems. A VM

conversion wizard is provided through the NetBackup Administration Console to guide you through the VM creation process. In addition, a command-line interface process is also available to start VM creation. VM creation can be done from full, incremental, or synthetic backups.

Media Server Deduplication Pool enhancements

For the 7.6 release, new Media Server Deduplication Pool (MSDP) features focus on better performance and increased reliability. Collectively, the improvements provide the following benefits:

- Higher job success rate under various usage scenarios, including heavy workloads.
- Robust deduplication storage with predictable behaviors for various operations such as backup, restore, replication, and housekeeping.
- Less downtime and better system availability.

For more information about these features and enhancements, see the *NetBackup Media Server Deduplication Pool Guide* for the 7.6 release.

The following items describe the new features and improvements:

- The history framework now keeps track of the lifecycle of various data objects such as path objects, data objects, segment objects, tasks, and database entries. They can be viewed in the Activity Monitor. Previously, the framework tracked only transaction queue processing. This change gives Symantec Support and Development much more information about data flow in MSDP, which can help to better diagnose issues on customer sites.
- Log messages have been enhanced to make error information more informative.
- Reduced storage server memory requirements. Most important, 64 TBs of storage no longer require 64 GBs of host memory.
- The new NetBackup Deduplication Multi-Threaded Agent improves backup performance for both client-side deduplication and media server deduplication.
- New inline processing during data storage reduces transactions in the MSDP queue, which results in improved reliability and less queue processing.
- Improved single CPU core performance for architectures other than Intel.
- Restore operations no longer require a fingerprint index.
- Improved start time and performance significantly for the NetBackup Deduplication Engine, as follows:

- The engine loads only a small percentage of fingerprints into the fingerprint index cache. Previously, all fingerprints were loaded.
  You can configure the cache loading behavior.
- The engine no longer loads the transaction queue when it starts.
  NetBackup now processes backup transactions during the backup, so they do not have to be written to the transaction queue.

- Replaced the `PostgresSQL` database application by a reference database (`refDB`) for the deduplication fingerprint information. The following are some of the benefits that the new reference database provides:
  - Removes the single-point-of-failure inherent in a central reference management table.
  - Improves the performance of MSDP operations.
  - Increases the scalability of MSDP operations. More backup images can be processed and more jobs can run concurrently.
  - Limits any database corruption: Any corruption is limited to a small subset of the database. Database corruption does not affect backups, restores, or house keeping processes. Database corruption does not prevent the NetBackup Deduplication Engine (`spoold`) from starting.
  - Self-healing database: NetBackup detects corruption and reconstructs the affected parts of the database at the next backup.
- NetBackup now can restore directly to a client that deduplicates its own data.
- Remote WAN backup resiliency:
  This feature is intended to make backups successful on the networks that reset idle socket connections within a given period of time. This feature, together with the NetBackup 7.5 WAN resiliency feature, improves job success rate for operations over WAN links with less reliable network connectivity. The success rate is also improved for operations over WAN links with intermediate firewalls and the appliances that aggressively reset idle socket connections.

Some of the improvements that have been made to MSDP may become noticeable directly after an upgrade to NetBackup 7.6. For example, due to improvements in how NetBackup uses MSDP storage, after an upgrade you may see an increase in available storage space. The Used Capacity of a disk pool may decrease and the Available Space may increase.

Alternatively, some of the performance improvements that the new features provide may not become evident immediately after the upgrade to NetBackup 7.6. However, all performance improvements should be observed for the second backups after the upgrade.

NetBackup OpsCenter enhancements

This section describes some of the new features and enhancements that have been added to NetBackup OpsCenter in this release.

NetBackup OpsCenter 7.6 now supports the following platforms and proliferations:

- OpsCenter Server and OpsCenter Managed Server support on Windows Server 2012
- OpsCenter Server and OpsCenter Managed Server support on Oracle Linux 5/6.
- Enhanced NetBackup and deduplication appliance awareness for OpsCenter
  - Multiple deduplication appliances and NetBackup appliances are now centrally monitored.
  - Deduplication and NetBackup appliances now both send hardware failure alerts.
  - Deduplication reporting capabilities have been improved with these newly added reports that provide additional value.
- Publishing OpsCenter database schema
  OpsCenter now provides access to detailed information about the OpsCenter database schema. This information can be helpful before any SQL query is run to generate reports. The reports can be created directly within OpsCenter or from the third party reporting tools with external ODBC access to the OpsCenter database.
  The OpsCenter database schema is available as a `.pdf` file directly within the OpsCenter console.
- Integrate external Active Directory and LDAP group support into OpsCenter's Role Based Access:
  OpsCenter can now be configured to integrate directly with an Active Directory (AD) or an LDAP directory server. This configuration provides both external Domain-based user-level access and now AD and LDAP Group-level access to the Role Based Access in OpsCenter. The user can easily configure external Groups in the Active Directory or the LDAP directory. The external Groups can then be mapped directly into OpsCenter to configure corresponding access to OpsCenter Views and Groups, down to an individual client level.
- A new OpsCenter Getting Started Wizard:
  The Getting Started Wizard guides the setup and configuration of OpsCenter for the first-time login. The wizard guides the user through the steps of adding NetBackup master servers to be monitored in OpsCenter. The wizard also helps

configure Views and Groups, and their Role-Based Access security to control access to specific areas of the NetBackup infrastructure.

Storage Lifecycle Policy (SLP) enhancements

Various SLP enhancements have been made that offer several improvements in the user experience when SLPs are used, with or without Replication Director.

You can find more information about the SLP enhancements that are specific to Replication Director in the following section:

See "Replication Director enhancements" on page 21.

SLP Windows

This feature enables you to specify in an SLP the window during which duplication, index, import, or replication jobs are supposed to run. Before this release, NetBackup processed those jobs as soon as the backups completed. This setup caused some duplication, import, or replication jobs to compete with backups for resources, which caused some backups to slip over the backup window. Now you can define a backup window that runs first, followed by a window for duplication, indexing, replication, or import jobs to be processed. For example, the user can define a backup window that runs from 6:00 P.M. to 4:00 A.M. the next day and duplication, indexing, replication, or import jobs to be processed from 4:00 A.M. to 10:00 A.M.

In addition, this feature offers the following improvements:

- It reduces the time that is required to initiate the jobs that storage lifecycle policies control.
- Advanced window close options allow control over how the duplication window behaves with respect to the operation.
- You can configure the deactivation of SLP secondary operations with an associated reactivation time.
- You can choose to defer duplication processing until the source image copy is about to expire.

Suspend and resume for classic duplication jobs

This feature implements suspend and resume commands for classic (`bpduplicate`) jobs. These commands are especially important when SLP Windows are used. When the duplication window closes, it is best to suspend the job and then resume it once the window reopens again. The suspend and resume commands for other types of SLP jobs (such as, NDMP duplication, Optimized Duplication, and replication) will be implemented in a future release.

SLP parameters in Host Properties

SLP parameter values are now stored in a new configuration file. Parameters are now defined and persisted using the `nbsetconfig` or `nbgetconfig` command line interfaces, or in the NetBackup Administration Console under SLP Host Properties. All parameter values that were previously stored in the LIFECYCLE_PARAMETERS file are automatically migrated to the new configuration file after the upgrade to NetBackup 7.6.

Duplication job progress in Activity Monitor

This feature implements a progress bar for various duplication jobs often executed from an SLP. The progress bar works for all types of duplication (Classic/Opt Dupe/NDMP), but not replication. The progress bar has always been visible in the Activity Monitor, but it went from **0** directly to **100** when the duplication job was completed. Now the bar shows continuous progress based on the data that is duplicated. The **Current kilobytes written** field is also updated to show percent completion.

Auto Image Replication enhancements

Targeted Auto Image Replication provides clear visibility into the target domain when you configure the source domain.

The following improvements are now available to you when you configure an SLP to use Targeted Auto Image Replication:

- Target a specific master server by name
- Target a specific SLP in that master server for import
- Validation that NetBackup has confirmed that the chosen replication topology works and provides the expected behavior

The new data classification `Any` may be used by Import SLP in the target domain. This data classification is capable of importing any data classification and preserving the source domain's data classification in the target domain.

By using Targeted Auto Image Replication functionality, you no longer need a matching SLP name or a matching data classification across all participating domains. In addition, when the source SLP is configured, its storage configuration is validated against the target domains for compatibility, which simplifies the configuration process.

Targeted Auto Image Replication provides the following benefits to users with one-to-many and many-to-many replication topologies:

- Select a subset of available targets for replication within any given SLP

- Each target that is chosen is allowed to use a different retention to satisfy different SLAs for different business needs (i.e. short to medium retention off-site “hot standby” and long-term DR, plus tes/dev domain, etc.)
- Allows unnecessary network traffic to be eliminated without the requirement of additional disk storage in the source domain

By using Targeted Auto Image Replication, you are given a way to add new target devices as the old devices are “aged” out of service. An example situation is when you replace a full target device with a newer generation of hardware with much higher capacity. The Targeted SLP lets you have both targets configured at the same time at the storage layer to drain “in-flight” replications and to start using the new device in parallel. This feature eliminates any interruption in service for routine maintenance scenarios.

Targeted Auto Image Replication now provides a notification capability from the target master server to its source master server in the event that the target master is unable to import an image. The existing import errors that are posted to the master server’s Problems Report are now duplicated to the source master server’s Problems Report. This additional notification provides continuous feedback to the source domain of any risk of failure to import, as well as any device configuration changes which may have broken the replication configuration

NetBackup for Oracle enhancements

Various Oracle enhancements have been made that offer several improvements in the user experience, with or without Replication Director.

You can find more information about the Oracle enhancements that are specific to Replication Director in the following sections:

See “Replication Director enhancements” on page 21.

See “Oracle support for physical server in Replication Director” on page 24.

Oracle Intelligent Policy

This feature improves the end-user experience for protecting Oracle environments with NetBackup. Typically NetBackup administrators are responsible for protecting Oracle environments but have little knowledge of Oracle internals. DBAs on the other hand have extensive knowledge of Oracle but little or no experience using NetBackup. That requires coordination between the NetBackup administrator and the DBA to configure NetBackup properly to protect their Oracle environment. A number of design deficiencies exist today in NetBackup that make this process difficult and prone to user error.

To address these issues, the following improvements have been implemented by Oracle Intelligent Policy:

- You can create a single policy to protect multiple Oracle instances that are spread over multiple clients.
- A new discovery service discovers Oracle instances throughout the NetBackup environment. The service polls the clients every four hours and sends the discovered instances to an instance repository available to you on the NetBackup Administration Console. You can also use the `nboraadm` command to manage the instances.
- The need for Oracle Recovery Manager (RMAN) scripts has been removed because the scripts are now automatically generated at run-time.
- The Job Details in the Activity Monitor lets you view the backup summary, database state, RMAN input, and RMAN output for the Oracle Intelligent Policy.
- Enhanced error codes enable faster identification, troubleshooting, and correction of problems. You can easily restart a failed job.
- Oracle policy schedules have been improved with the elimination of the need for an application backup schedule.
- You can manually back up any number of instances or all the instances.
- Oracle Intelligent Policy automatically selects parameter settings at run-time that enable optimal deduplication.
- You can create a new archived log schedule that backs up the archived redo logs in intervals of minutes.
- The database administrator can control all instance and instance group credentials, providing improved security throughout the system.

For more detailed information about NetBackup for Oracle, see the *NetBackup for Oracle Administrator's Guide*.

Replication Director enhancements

This section describes some of the new features and enhancements that have been added to Replication Director in this release of NetBackup.

In NetBackup 7.6, Replication Director adds support for SAN-connected storage and additional customer workloads that include the following:

- File services data on NetApp (iSCSI and FC) block-connected arrays
- VMware file and application data on NAS datastores
- Applications in VMware NAS datastores: Exchange and SQL Server

- Physical (non-virtualized) Oracle data on NFS storage

New Replication Director functionalities

- Policy configuration for Replication Director is easier with the new Use Replication Director option. Enable Use Replication Director on the policy Attributes tab to automatically select other options that Replication Director requires. This option is available for the following policy types: MS- Windows, Standard, Oracle, NDMP, and VMware.
- Storage server configuration for Replication Director is easier in the Storage Server Configuration Wizard. The available OpenStorage Replication Director partners are now available from a drop-down menu when you select the storage server type.
- SLP Windows: Ability to control when SLP operations are allowed
- More flexible NDMP backup selections: ALL_FILESYSTEM directive and wildcards
- Redesigned the Oracle backup policies to improve ease of configuration including snapshot functionality
- Policy validation logic to ensure what is configured runs at backup time
- Disambiguation of error code 156

VSS Support in Replication Director

VSS Support in Replication Director introduces the ability to support block or SAN-connected devices (Fibre Channel and iSCSI) on the Windows OS platform. On a Windows platform, snapshots are created using Microsoft's VSS framework.

This feature implements functionality in NetBackup that enables you to do the following:

- Create snapshots on primary arrays.
- Replicate snapshots on remote arrays.
- Protection for file system data on block arrays.
- Perform recovery from primary and replicated snapshots or backups. Recovery can be single file (browse with Backup, Archive, and Restore or search with OpsCenter) or all contents of a volume.

SAN support for NetApp in Replication Director

SAN support for NetApp in Replication Director introduces the ability to support block or SAN-connected devices (Fibre Channel and iSCSI) on the UNIX and Linux platforms. This feature implements functionality in NetBackup to:

- Create snapshots on primary arrays.
- Replicate snapshots on remote arrays.
- Protection for file system data on block arrays.
- Perform recovery from primary and replicated snapshots or backups. Recovery can be single file (browse with Backup, Archive, and Restore or search with OpsCenter) or all contents of a volume.

Replication Director support for VMware (NAS Datastores)

Replication Director support for VMware (NAS Datastores) provides the capability for NetBackup virtualization features to operate in a snapshot and replication environment. The primary capabilities provided by this feature are:

- Create and replicate array-based snapshots on VMware NFS datastores containing one or more virtual machines.
- Restore of a VMware Virtual Machine (VM) from its vmdk files that are in a snapshot.
- Restore of individual files from the VM vmdk files in a snapshot.
- Backup of selected Virtual Machines from the snapshots at primary and remote location (from Replicated snapshots).

Exchange VM support for Replication Director (NAS datastores)

Exchange VM Support for Replication Director builds upon the NetBackup Replication Director for VM feature by adding support for Exchange. From a Replication Director-managed snapshot that was taken during an Exchange-aware backup of a VMware guest, NetBackup can do the following:

- Restore an Exchange database.
- Browse an Exchange database for mailbox items.
- Restore mailbox items.

Snapshots can include:

- Local snapshots.
- Replicas that are made from local snapshots.

- Remote snapshots (replicated to a remote server).
- Replicas that are made from remote snapshots.

The following URL is to a website that provides additional information about Exchange in a virtualized environment.

http://technet.microsoft.com/en-us/library/jj126252.aspx

SQL Server VM support for Replication Director

SQL Server VM Support for Replication Director builds upon the NetBackup Replication Director for VM feature by adding support for SQL Server. From a Replication Director-managed snapshot that was taken during an SQL-aware backup of a VMware guest, NetBackup can do the following:

- Restore an SQL database.

Snapshots can include:

- Local snapshots.
- Replicas that are made from local snapshots.
- Remote snapshots (replicated to a remote server).
- Replicas that are made from remote snapshots.

Oracle support for physical server in Replication Director

Oracle support for Physical Server in Replication Director enables customers with physical (non-virtualized) Oracle servers running on NFS-connected storage to leverage Replication Director. The feature implements functionality to:

- Use application-consistent (quiesced) or crash-consistent (non-quiesced) snapshots.
- Create snapshots, replicate snapshots, back up from primary or replicated copy.
- Recover from any copy (snapshot or backup).
- Deal properly with archive redo log truncation.
- Full and granular recovery.

Validation of SLP topology

This feature reduces the number of run-time failures that are seen during the execution of Replication Director replication jobs. The most common cause of run-time failures is user error in configuring an SLP for use with Replication Director. Validation of SLP topology by the storage server at configuration time can help

correct errors well before the associated policies are executed. In addition, knowing the topology up-front also helps the storage server to effectively allocate resources for the associated policy job.

NDMP wildcard support

The NDMP wildcard support feature enables you to specify the backup selection for an NDMP policy using a directive (`ALL_FILESYSTEMS`) or a path with regular expression (/vol/vol?_archive_*). Both directives and regular expressions selection should work for streaming and non-streaming backup. It should also work for Replication Director. In this manner, defining what data an NDMP policy should protect is now much simpler. For example, you can configure all of the data within a given filer to be protected rather than specifying the path names to back up.

Disambiguation of status code 156

This feature introduces a new set of status codes that help identify the cause of Snapshot Client failures that were previously under status code 156. These status codes include numbers 4200-4222.

See the *Symantec NetBackup Status Codes Reference Guide*.

NetBackup Search enhancements

This section describes some of the new features and enhancements that have been added to the Search and Discovery feature in this release of NetBackup.

- Standalone indexing server:
  You are no longer required to install an indexing server on a NetBackup media server. You can now install an indexing server as a standalone entity on any computer regardless of whether it is running NetBackup.
  If you install an indexing server on a computer that does not have the NetBackup client software installed, the installation wizard prompts you to install the NetBackup client software before you proceed with the indexing server installation. For more information about installing and upgrading an indexing server, see the *NetBackup Search Administrator's guide*.
- Holds Traceability report:
  The Holds Traceability report is introduced in NetBackup Search 7.6 to help you identify the search results from which the hold was placed on a backup image. This downloadable report contains detailed information about the search results, search query, and backup image list that is associated with the hold.
- Retention management and restore:

- Occasionally the need arises to preserve data longer than the normal lifecycle of a backup image. This feature provides a way for NetBackup administrators to hold and un-hold specific data.
- This feature allows the Restore utility to restore data from all supported policy types (Windows, Standard, NDMP, FlashBackup, VMware, and Hyper-V) and UNIX platforms. The Restore utility has also received usability enhancements, which include standardized configuration, restore job throttling, and a reduction of input parameters.

Virtualization enhancements

This section describes some of the new virtualization features and enhancements that can be found in this release of NetBackup.

This release includes the following new features and enhancements for VMware:

- Support for the VMware backup host and backup media server has been added for the following platforms:
  - SUSE 10 SP4 x64
  - SUSE 11 x64
  - Red Hat Enterprise Linux 5.5 x64
  - Red Hat Enterprise Linux 6.3 x64
- The Accelerator for virtual machine backup.
- Symantec introduces the NetBackup plug-in for VMware vCenter. In the VMware vSphere Client interface, you can use the NetBackup plug-in to monitor the status of virtual machine backups and restore virtual machines.
- NetBackup now supports vSphere 5.1. Support for VMware vCloud Director 5.1 has also been added, along with the ability to back up vCloud environments and restore vApps back into vCloud.
- Replication Director for protecting virtual machines in a snapshot and replication environment (NAS datastores).
  See "Replication Director support for VMware (NAS Datastores)" on page 23.
- A new command, `nbrestorevm`, has been added to the command line interface for the recovery of virtual machines.
- An instant recovery of virtual machines can now be performed by means of a Windows backup host. NetBackup starts the virtual machine directly from the backup image and makes it accessible to users on the ESX host immediately.

- The job details log in the Activity Monitor has enhanced error reporting for several snapshot-related errors with status code 156 for VMware virtual machines. In each case, an additional message states the reason for the error.
- A browse and search feature has been added t\o the Backup, Archive, and Restore interface. When you search for a virtual machine to restore, this feature makes it easier to locate the virtual machine in a large, multi-layered virtual environment.

The following enhancements have been made to Hyper-V in this release:

- Support has been added for Hyper-V on Windows Server 2012.
- Command line interface support of the `nbrestorevm` command has been added for Hyper-V.

About new NetBackup commands and status codes

This release of NetBackup contains new commands, utilities, and status codes. For a description of each of the following commands, refer to the *NetBackup Commands Reference Guide*. For a list of the NetBackup status codes, refer to the *NetBackup Status Code Reference Guide*.

The following is a list of the new commands released in NetBackup 7.6:

- `bpplcatdrinfo`
  List, modify, or set disaster recovery policy.
- `nbgetconfig`
  This command is the client version of `bpgetconfig`. It lets you view the local configuration on a client.
- `nboraadm`
  This command manages the Oracle instances that are used in Oracle backup policies.
- `nbrestorevm`
  This command restores VMware virtual machines.
- `nbsetconfig`
  This command is the client version of `bpsetconfig`. It lets you edit the local configuration on a client.
- `nbseccmd`
  This command runs the NetBackup Security Configuration service utility. Used in all security-related operations, this command adds inter-domain trust across master servers.
- `configurePorts`

This command is used to configure the Web ports for the Web Services Layer (WSL) application on the master server.

Chapter 2

Installation requirements and platform compatibility

This chapter includes the following topics:

About upgrade paths to the NetBackup 7.6 line of releases

Note: If you do not plan to upgrade your NetBackup environment to version 7.6 within the first calendar quarter of 2014, you can safely ignore this section.

Upgrades to NetBackup 7.6 are supported from any release since NetBackup 6.0. However, some of the functionality that was introduced in NetBackup 7.5.0.6 and later is not present in the NetBackup 7.6 GA release. The difference in functionality is limited to bug fixes and a small set of features. The following list describes the various upgrade paths that Symantec recommends:

- If you are currently running NetBackup 7.5.0.5 or earlier, your upgrade path is to NetBackup 7.6 GA.
- If you are currently running NetBackup 7.5.0.6 and you do not use Amazon S3 cloud storage buckets in regions other than US Standard, your upgrade path is to 7.6 GA.
- If you are currently running NetBackup 7.5.0.6 with Amazon S3 cloud storage buckets in regions other than US Standard, your upgrade path is to a release in the NetBackup 7.6 maintenance line (triple-dot) available near the end of the first calendar quarter of 2014.

Upgrades from NetBackup 7.5.0.6

If your NetBackup environment relies on any of the following functionality that is found in version 7.5.0.6 and later, then your upgrade path is to a release in the NetBackup 7.6 maintenance line (triple-dot).

- Amazon S3 cloud storage buckets in regions other than US Standard
See "Cloud storage notes" on page 91.

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. This section contains the installation requirements for both UNIX and Windows that are found in the *NetBackup Getting Started Guide*.

- Check for available disk space before you upgrade to NetBackup 7.x
During an upgrade to NetBackup 7.x, it is necessary to have enough free disk space to accommodate three complete copies of the NetBackup database. That includes all transaction logs and database files in the data directory including BMR if it is configured and in use. This directory is typically `/usr/openv/db/data` for UNIX-based operating systems and `\Veritas\NetBackupDB\data` for Windows-based operating systems when you use default installation methods.
- Symantec 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 that gunzip, and gzip, be installed on the computer before NetBackup is installed. 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.

Installation requirements for UNIX and Linux systems

Table 2-1 describes the requirements to prepare your UNIX and Linux systems for NetBackup installation. Use this table as a checklist to address each item.

Table 2-1 NetBackup installation requirements for UNIX and Linux

Check	Requirements
	Operating system: ■ For a complete list of compatible UNIX and Linux operating systems, refer to the *NetBackup 7.x Operating System Compatbility List* at the following website: http://www.symantec.com/business/support/overview.jsp?pid=15143 In the section **Common Topics**, under **Compatibility List**, click **NetBackup 7.x Operating System**.
	Memory: ■ Master servers in a production environment should have a minimum of 8 GB of memory each. ■ Media servers in a production environment should have a minimum of 4 GB of memory each. ■ Any client in a production environment should have a minimum of 512 MB of memory. ■ For reasonable performance of the NetBackup-Java interfaces, you need 512 MB of RAM. Of that space, 256 MB must be available to the interface program (`jnbSA` or `jbpSA`). For additional information about memory requirements, refer to the *NetBackup Backup Planning and Performance Tuning Guide*. http://www.symantec.com/docs/DOC5332

Table 2-1 NetBackup installation requirements for UNIX and Linux *(continued)*

Check	Requirements
	Disk space: ■ The exact amount of space that is required depends on the hardware platform. More information about this topic is available. See Table 2-3 on page 35. ■ NetBackup catalogs contain information about your backups that become larger as you use the product. The disk space that the catalogs require depends primarily on the following aspects of your backup configuration: ■ The number of files that are backed up. ■ The frequency of your backups. ■ The amount of time that you set to retain your backup data. **Note:** The value for disk space is for initial installation only. The NetBackup catalog requires considerably more space once the master server is placed in a production environment. For additional information on sizing requirements for the NetBackup catalog, refer to the *NetBackup Backup Planning and Performance Tuning Guide*. http://www.symantec.com/docs/DOC5332
	`gzip` and `gunzip` commands: ■ Ensure that the `gzip` and the `gunzip` commands are installed on the local system. The directories where these commands are installed must be part of the root user's path environment variable setting.
	Clustered systems: ■ Ensure that each node in the NetBackup cluster can run the `ssh` command, the `rsh` command, or its equivalent (on HP-UX, the command is `remsh`). The root user must be able to perform a remote login to each node in the cluster without entering a password. This remote login is necessary for installation and configuration of the NetBackup server and any NetBackup agents and options. After installation and configuration are complete, it is no longer required. ■ You must install, configure, and start the cluster framework before you install NetBackup. ■ You must have defined a virtual name using DNS, NIS, or the `/etc/hosts` file. The IP address is defined at the same time. (The virtual name is a label for the IP address.) More information about cluster requirements is available. *Symantec NetBackup Clustered Master Server Administrator's Guide* http://www.symantec.com/docs/DOC5332

Installation requirements for Windows systems

Table 2-2 describes the requirements to prepare your Windows systems for NetBackup installation. Use this table as a checklist to address each item.

Table 2-2 NetBackup installation requirements for Windows

Check	Requirements
	Operating system: ■ For a complete list of compatible Windows operating systems, refer to the *NetBackup 7.x Operating System Compatbility List* at the following website: http://www.symantec.com/business/support/overview.jsp?pid=15143 In the section **Common Topics**, under **Compatibility List**, click **NetBackup 7.x Operating System**.
	Memory: ■ Master servers in a production environment should have a minimum of 8 GB of memory each. ■ Media servers in a production environment should have a minimum of 4 GB of memory each. For additional information about memory requirements, refer to the *NetBackup Backup Planning and Performance Tuning Guide*. http://www.symantec.com/docs/DOC5332
	An NTFS partition.

Table 2-2 NetBackup installation requirements for Windows *(continued)*

Check	Requirements
	Disk space: ■ The exact amount of space that is required to accommodate the server software and the NetBackup catalogs depends on the hardware platform. More information about this topic is available. See Table 2-3 on page 35. ■ NetBackup catalogs contain information about your backups that become larger as you use the product. The disk space that the catalogs require depends primarily on the following aspects of your backup configuration: ■ The number of files that are backed up. ■ The frequency of your backups. ■ The amount of time that you set to retain your backup data. ■ Symantec recommends that you have a minimum available disk space of 5% in any Disk Storage Unit volume or file system. **Note:** The value for disk space is for initial installation only. The NetBackup catalog requires considerably more space once the master server is placed in a production environment. For additional information on sizing requirements for the NetBackup catalog, refer to the *NetBackup Backup Planning and Performance Tuning Guide*. http://www.symantec.com/docs/DOC5332
	Clustered systems: ■ All nodes in the cluster must run the same operating system version, service pack level, and NetBackup version. You cannot mix versions of server operating systems. ■ The installation account must have administrator privileges on all remote systems or on all nodes in the cluster. More information about cluster requirements is available. *Symantec NetBackup Clustered Master Server Administrator's Guide* http://www.symantec.com/docs/DOC5332
	The services and port numbers: ■ NetBackup services and port numbers must be the same across the network. ■ Symantec suggests that you use the default port settings for NetBackup services and Internet service ports. If you modify the port numbers, they must be the same for all master servers, media servers, and clients. The port entries are in the following file: `%SYSTEMROOT%\system32\drivers\etc\services`. To change the default settings, you must perform a custom installation of NetBackup or manually edit the services file.

Table 2-2 NetBackup installation requirements for Windows *(continued)*

Check	Requirements
	Remote Administration Console host names: ■ You must provide the names of the Remote Administration Console hosts during master server installation.

NetBackup 7.6 binary sizes

The information in this section helps you determine if you have allocated the proper amount of disk space to your servers to safely and efficiently back up and restore all of the data in your NetBackup environment.

For the current information on operating system version support, consult the SORT *Installation and Upgrade Checklist* or the *NetBackup Enterprise Server and Server 7.x OS Software Compatibility List*.

https://sort.symantec.com/netbackup.

NetBackup Enterprise Server and Server 7.x OS Software Compatibility List

- http://www.symantec.com/docs/TECH76648

Table 2-3 shows the approximate binary size of the NetBackup master and media server software, and the NetBackup client software requirements for each operating system that is compatible with NetBackup.

Table 2-3 NetBackup binary sizes for compatible platforms

OS/Version	CPU Architecture	32-bit client	64-bit client	32-bit server	64-bit server	Notes
AIX 6.1, 7.1	POWER		2430MB		6880MB	
Asianux 3	x86-64		1580MB		6350MB	
Canonical Ubuntu 9.04, 9.10, 10.04, 11.10, 12.04	x86-64		1580MB			
CentOS 5	x86-64		1580MB		6350MB	Media server or client compatibility only.
CentOS 6	x86-64		1580MB		6350MB	Media server or client compatibility only.
Debian GNU/Linux 5, 6	x86-64		1580MB			
FreeBSD 6.1, 6.2, 6.3, 7.x, 8.x, 9.x	x86-32	290MB				

Table 2-3 NetBackup binary sizes for compatible platforms *(continued)*

OS/Version	CPU Architecture	32-bit client	64-bit client	32-bit server	64-bit server	Notes
FreeBSD 6.3, 7.x, 8.x, 9.x	x86-64	290MB				
HP-UX 11.11, 11.23, 11.31	PA-RISC		955MB		2395MB	Media server or client compatibility only.
HP-UX 11.31	IA-64		2460MB		6910MB	
Mac OS X 10.6	x86-32	272MB				
Mac OS X 10.6, 10.7, 10.8	x86-64	272MB				
Novell Open Enterprise Server 2	x86-64		1576MB		6352MB	
Novell Open Enterprise Server 11	x86-64		1576MB		6352MB	
OpenVMS 5.5, 6.2, 7.3	HP VAX	128MB				The listed sizes are for the NetBackup 7.5 binaries. No NetBackup 7.6 binaries for OpenVMS are provided.
OpenVMS 6.1, 6.2, 7.3, 8.2, 8.3, 8.4	HP Alpha		128MB			The listed sizes are for the NetBackup 7.5 binaries. No NetBackup 7.6 binaries for OpenVMS are provided.
OpenVMS 8.2, 8.3, 8.3-1H1, 8.4	HP IA64		128MB			The listed sizes are for the NetBackup 7.5 binaries. No NetBackup 7.6 binaries for OpenVMS are provided.
Oracle Linux 5	x86-64		1580MB		6350MB	
Oracle Linux 6	x86-64		1580MB		6350MB	
Red Flag Linux 5	x86-64		1580MB		6350MB	
Red Hat Enterprise Linux 5	x86-64		1580MB		6350MB	
Red Hat Enterprise Linux 6	x86-64		1580MB		6350MB	
Red Hat Enterprise Linux Desktop 5	x86-64		1580MB			
Red Hat Enterprise Linux 4	POWER		466MB			

Table 2-3 NetBackup binary sizes for compatible platforms *(continued)*

OS/Version	CPU Architecture	32-bit client	64-bit client	32-bit server	64-bit server	Notes
Red Hat Enterprise Linux 5	POWER		466MB			
Red Hat Enterprise Linux 5	z/Architecture		1070MB		4920MB	Media server or client compatibility only.
Red Hat Enterprise Linux 6	z/Architecture		1070MB		4920MB	Media server or client compatibility only.
Solaris 10	SPARC		1552MB		4623MB	
Solaris 11	SPARC		1552MB		4623MB	
Solaris 10	x86-64		1250MB		4510MB	
Solaris 11	x86-64		1250MB		4510MB	
SUSE Linux Enterprise Server 10 (SP2)	x86-64		1576MB		6352MB	
SUSE Linux Enterprise Server 11	x86-64		1576MB		6352MB	
SUSE Linux Enterprise Server 9	POWER		473MB			Compatible with client only.
SUSE Linux Enterprise Server 10 (SP2)	POWER		473MB			Compatible with client only.
SUSE Linux Enterprise Server 10 (SP2)	z/Architecture		1050MB		4911MB	Media server or client compatibility only.
SUSE Linux Enterprise Server 11	z/Architecture		1050MB		4911MB	Media server or client compatibility only.
Windows	x86-32	750MB				Covers all compatible Windows x86 platforms
Windows	x86-64		975MB		2375MB	Covers all compatible Windows x64 platforms

Note: Unless stated otherwise in the table above, NetBackup is supported on all editions (Advanced, Base, DC, etc.) and on all vendor GA updates (n.1, n.2, etc.) or service packs (SP1, SP2, etc.) for the following Linux platforms: Asianux, CentOS, Debian GNU/Linux, Novell Open Enterprise Server, Oracle Linux, Red Flag Linux, Red Hat, and SUSE.

Table 2-4 shows the approximate binary size and the OpsCenter Agent, Server, and ViewBuilder software requirements for each operating system that is compatible with OpsCenter.

Table 2-4 OpsCenter binary sizes for compatible platforms

OS/Version	CPU Architecture	Agent	Server	ViewBuilder
Red Hat Enterprise Linux Server 5 (Kernel 2.6.18+)	x86-64		855MB	
SUSE Linux Enterprise Server 10 (SP2) (Kernel 2.6.16+)	x86-64		855MB	
Solaris 10	SPARC	451MB	959MB	
Solaris 10	x86-64		985MB	
Windows Server 2008 R2	x86-64	268MB	777MB	172MB
Windows Server 2012	x86-64	268MB	777MB	172MB

Table 2-5 shows the approximate binary size and the NetBackup vCenter Plugin client software requirements for each operating system that is compatible with the NetBackup vCenter Plugin.

Table 2-5 NetBackup vCenter Plugin binary sizes for compatible platforms

OS/Version	CPU Architecture	32-bit client	64-bit client	32-bit server	64-bit server	Notes
SUSE Linux Enterprise Server 11 (SP1)	x86-64	N/A	N/A	N/A	2.6GB	Thin Provision OVA format only
SUSE Linux Enterprise Server 11 (SP1)	x86-64	N/A	N/A	N/A	20GB	Thick Provision OVA format only

About server and client platform compatibility

You can find the NetBackup platform compatibility information and other various compatibility lists on the Symantec Support website. These compatibility lists offer a variety of up-to-date information about the operating systems that are compatible with NetBackup and NetBackup features.

See "About NetBackup compatibility lists" on page 43.

This section also contains the following types of information:

- Operating system compatibility information
- NetBackup feature compatibility
- Descriptions of the dedicated compatibility lists and instructions on how to locate them on the Symantec Support website

---

Note: This section describes the platform and operating system support changes at the time of release. For the most up-to-date information about software and hardware compatibility, see the *NetBackup Master Compatibility List* on the Symantec Support website.

http://www.symantec.com/docs/TECH59978 - *NetBackup Master Compatibility List*

New and discontinued server and client operating system support for NetBackup 7.6

This release of NetBackup contains many changes and enhancements in the support of compatible platforms and operating systems. The following lists include some of the platform support changes that were made since the last single-dot release of NetBackup.

Note: For an up-to-date listing of NetBackup operating system support, see "Operating Systems No Longer Supported by NetBackup" in the *NetBackup Enterprise Server and Server OS Software Compatibility List* available from the following location:

http://www.symantec.com/docs/TECH59978

Symantec has migrated information about future platform support changes to the SORT website for NetBackup.

https://sort.symantec.com/netbackup

See "About future NetBackup end-of-life notifications" on page 151.

New operating system support

NetBackup 7.6 now supports the following operating systems on the defined CPU architecture:

- Windows Server 2012 x64
- Windows 8 x64 (client)
- Mac OS X 10.8 (client)
- FreeBSD 8.2, 8.3, and 9.0 (client)
- Solaris 11 SPARC and x64 (master)
- Solaris 11 (master) with support for Oracle SunCluster
- Canonical Ubuntu 12.04, 12.10, and 13.04 (client)
- Oracle Linux 6 (master)
- AIX 7.1 (SAN Client)

Discontinued operating system support

NetBackup 7.6 does not support the following operating systems on the defined CPU architecture:

- Windows x86 (master and media).

  Note: Windows x86 is still fully supported as a client.

- Solaris 11 Express
- AIX 5.3 64-bit POWER
- Solaris 9 SPARC
- SUSE Linux Enterprise Server IA64
- Red Hat Enterprise Linux IA64

Note: No new packages are provided for these platforms in this release. However these platforms are still supported using the packages that are provided for NetBackup 7.0, 7.1, and 7.5. These platforms will not be supported after the 7.x EOSL date.

All UNIX 32-bit system support has been discontinued, with the exception of FreeBSD and Mac OS X.

- To upgrade these unsupported systems to NetBackup 7.6, you must first migrate your current NetBackup 6.x catalogs and databases to a system with a compatible platform. Another option is to use 32-bit NetBackup 6.x media servers and clients with a 64-bit NetBackup 7.6 master server.

  See the NetBackup installation guides for more information about migrating NetBackup master servers from 32-bit to 64-bit.

  Any 32-bit media servers and clients that use NetBackup 6.x are compatible with the 64-bit master servers that use NetBackup 7.x.
- In addition, NetBackup requires OpenStorage vendor plug-ins to be 64-bit. When you upgrade a media server that is used for OpenStorage to NetBackup 7.6, you also must update the vendor plug-in to a 64-bit version.

Other operating system support notes

The following list includes miscellaneous support information for specific operating systems:

- NetBackup Java-applications are no longer available on HP PA-RISC operating systems for servers and clients.
- NetBackup 7.6 contains the 7.5 version of the OpenVMS client package. If you already have the OpenVMS 7.5 client package installed, you do not have to reinstall this package.

File system support

The following list includes some of the file system support changes in NetBackup 7.6:

- Storage Foundation 6 is now supported for NetBackup clients.
- The ReFS file system is supported, but installing the NetBackup package on an ReFS volume is not supported.
- Global File System 2 (GFS2) file system support on Red Hat Enterprise Linux (RHEL) 5

Database agent compatibility in NetBackup 7.6

This release of NetBackup contains many changes and enhancements in the support of compatible platforms and operating systems. This section describes the changes in support that were made in this release.

New database support

NetBackup 7.6 offers the following database and application support:

- Exchange 2013 support. Please note, Granular Recovery Technology (GRT) backups are not supported with this release.
- Exchange 2010 SP3 support on Windows 2008 R2 and Windows Server 2012.
- SharePoint 2013 support (database only). Please note, Granular Recovery Technology (GRT) backups are not supported with this release.
- Claims-based authentication (CBA) is now supported for Web application in SharePoint 2010 and later. The following providers are supported:
  - Windows Authentication (LDAP)
  - Facebook
  - LinkedIn
  - Live Id
  - Forms-based authentication (FBA) using SQL Server
  - Active Directory Federation Services (AD FS) 2.0
- DB2 support for zLinux

Discontinued database support

NetBackup 7.6 discontinues the following database and application support:

- NetBackup 7.6 for SQL Server no longer supports backups of SQL Server 2000. Restores and recoveries from existing backup images are still supported, but will be retired in the next major release of NetBackup.
- NetBackup 7.6 for Exchange Server no longer supports backups of Exchange Server 2003. Restores and recoveries from existing backup images are still supported, but will be retired in the next major release of NetBackup.

Platform compatibility for NetBackup Cloud

The NetBackup Cloud feature is supported on a select group of NetBackup media server platforms. Supported platforms include:

- AIX
- HP-UX IA64
- Red Hat Enterprise Linux x64
- Solaris SPARC
- SUSE Linux Enterprise Server x64
- Windows 2008R2 (64 bit)

The minimum requirements for each platform are the same as the minimum requirements for NetBackup 7.6 media server. More information is available about supported media servers on the Symantec Support website.

http://www.symantec.com/docs/TECH76648 - *NetBackup Enterprise Server and Server 7.x OS Software Compatibility List*

Platform compatibility with the NetBackup Administration Consoles for UNIX

The NetBackup Administration Console provides a graphical user interface through which the administrator can manage NetBackup. The interface can run on any NetBackup Java-capable system. For information on how to install the consoles, see the *NetBackup Installation Guide*. For information on how to use the NetBackup Administration Console, see the *NetBackup Administrator's Guide, Volume 1*.

To see a list of platforms that are compatible with the NetBackup-Java Administration Console, the Backup, Archive, and Restore user interface, and the NetBackup Remote Administration Console (MFC), see the *NetBackup Enterprise Server and Server 7.x OS Software Compatibility List* on the Symantec Support website:

http://www.symantec.com/docs/TECH59978 - *NetBackup Enterprise Server and Server 7.x OS Software Compatibility List*

Note: A NetBackup-Java Administration Console can be supported on all Windows platforms to connect to remote servers.

Note: Beginning with NetBackup 7.6, all Windows client selections are referred to as **Windows**, instead of as their release versions, such as Windows 2003/2008/2012.

About NetBackup compatibility lists

The most up-to-date compatibility information on platforms, peripherals, drives, and libraries is located in various compatibility lists on the Symantec Support website. You can use the following methods to locate these lists and information:

- Symantec recommends that you use Symantec Operations Readiness Tools (SORT) to help you locate the latest platforms, peripherals, drives, and libraries. To access SORT, go to the following Web page:
  https://sort.symantec.com/netbackup
  For NetBackup, SORT provides an Installation and Upgrade Checklist report as well as the ability to collect, analyze, and report on host configurations across

UNIX/Linux or Windows environments. In addition, you can determine in what release whether any hot fixes or EEBs you have installed are fixed. You can use this data to assess whether your systems are ready to install or upgrade to this release.

- If you want to view a specific compatibility list, you can find links to each list that is posted on the Symantec Support website:
  http://www.symantec.com/docs/TECH59978 - *NetBackup Master Compatibility List*

  The following items describe each of the compatibility lists that are available.

  - *NetBackup Enterprise Server and Server 7.x OS Software Compatibility List*
    This list contains information about the operating system (OS) level and the version that is required to be compatible with a NetBackup master or media server. It also describes the OS level and the version that is required to be compatible with a NetBackup client. Predecessors and successors to the documented operating system levels may function without difficulty, as long as the release provides binary compatibility with the documented operating system.

    This list contains compatibility information about several NetBackup Enterprise features, including the following:

    - NetBackup Enterprise server and client
    - Bare Metal Restore (BMR)
    - NetBackup Access Control (NBAC)
    - Network Data Management Protocol (NDMP)
    - NetBackup OpsCenter
    - NetBackup SAN media server and SAN client
    - FT media server
    - NetBackup Media Server Deduplication Option
    - File system compatibility
    - NetBackup virtual system compatibility
    - NetBackup Media Server Encryption Option (MSEO)

    NetBackup compatibility for a platform or OS version requires platform vendor support for that product. The platform compatibility lists that NetBackup maintains are subject to change as vendors add and drop platforms or OS versions.

  - *NetBackup Enterprise Server and Server 7.x Hardware Compatibility List*

This list includes information for compatible drives, libraries, virtual tape devices, robot-types, fibre-channel HBAs, switches, routers, bridges, iSCSI configurations, and encryption devices. Other compatibility information includes the following:

- NetBackup Appliances
- AdvancedDisk arrays
- OpenStorage (OST) solutions
- Tape drives
- Fibre Transport media server host bus adapters (HBAs)
- Virtual tape libraries (VTLs)
- Network Data Management Protocol (NDMP) devices
- Tape libraries
- Encryption and security solutions

- *NetBackup 7.x Database and Application Agent Compatibility List*
  This list contains the most current compatibility information for the database agents and application agents that are supported on specific operating systems and CPU architectures.
- *NetBackup 7.x Snapshot Client Compatibility List*
  This list contains the most current server and client snapshot compatibility information that is sorted by arrays, agents, operating systems, and VSS providers.
- *NetBackup 7.x Cluster Compatibility List*
  This list contains the most current compatibility information for the cluster types and versions that are supported on specific operating systems and CPU architectures.
- *Statement of support for the importing of Backup Exec images in NetBackup 7.x using the Backup Exec Tape Reader*
- *Support for NetBackup 7.x in virtual environments*
  This list contains the most current compatibility information for NetBackup in virtual environments.

About software release types

Symantec maintains a policy by which NetBackup can deliver various levels of releases to accommodate customer needs. The following list defines the various release types and the version number schemes that are associated with each type.

The NetBackup family of software and appliance products use these release types and number schemes.

- A major release is the first in a series of releases. This type of release contains new features, new supported platforms, and a complete set of the latest product documentation.
- A minor release is a single-dot release that follows a major release, for example 2.6 or 7.6. This release type contains much of the same requirements as a major release. It contains a smaller set of new features and enhancements, any platform proliferation, and a complete set of updated documentation.
- A software release update is a double-dot release, for example 2.6.1 or 7.6.1. This release type may contain a few new features and enhancements as well as many product fixes. Only those documents that are applicable to the new features or enhancements are updated and republished.
- A maintenance release update is a triple-dot release, for example 2.6.0.1 or 7.6.0.1. This release type is primarily comprised of a number of fixes that are developed to address issues in major, minor, and software update releases. This release type may also include a small number of new features, enhancements, and platform or application proliferations. The only documentation that is provided is an online Readme and a release notes document that is available on the Symantec Support website.

Note: NetBackup versions 2.6.0.1, 2.6.1, 7.6.0.1, and 7.6.1 are used in this topic as examples. These versions of NetBackup do not exist at the time of this document's publication.

About compatibility with NetBackup 7.6

Symantec NetBackup has always maintained that the master server within an environment must be at a version level that is equal to or greater than the version levels of the media servers and clients within that environment. Symantec recommends that you keep your entire NetBackup environment up-to-date with the latest maintenance (triple-dot) releases. However, NetBackup offers the flexibility of an environment where the clients and the media servers are running a different triple-dot release than the master server. For example you can upgrade a media server or client to Version 7.6.0.1 in an environment where the master server is running Version 7.6. This same scenario applies to single-dot releases, for example Version 7.6.1.1.

Since the NetBackup catalog resides on the master server, the master server is considered to be the client for a catalog backup. If your NetBackup configuration includes a media server, it must use the same NetBackup version as the master

server to perform a catalog backup. See the *NetBackup Installation Guide* for information about mixed version support.

See "About software release types" on page 45.

For information about NetBackup compatibility with the NetBackup appliances, see the following Technote on the Symantec Support website.

http://www.symantec.com/docs/TECH136970

Symantec NetBackup does not support any scenario where a minor release or software release update is at a higher version level than the parent server. For instance, the following examples apply:

- If a master server is at 7.6, then the media servers and clients cannot be at a single-dot version level that is higher than 7.6, such as 7.7.
- If a master server is at 7.6, then the media servers and client servers cannot be at a double-dot version level that is higher than 7.6, such as 7.6.1.
- If a master server is at 7.6.1, then the media servers and clients cannot be at a double-dot version level that is higher than 7.6.1, such as 7.6.2.

Note: NetBackup versions 7.6.0.1, 7.6.1, 7.6.1.1, 7.6.2, and 7.7 are used in this topic as examples. These versions of NetBackup do not exist at the time of this document's publication.

The following table shows the various compatibility schemes that are supported with the current NetBackup 7.6 product line.

Table 2-6 Release compatibility for the NetBackup 7.6 product line

NetBackup master server	NetBackup media server	NetBackup client
7.6	7.0	7.0
7.6	7.0.1	7.0, 7.0.1
7.6	7.0.2	7.0, 7.0.1, 7.0.2
7.6	7.1	7.0, 7.0.x, 7.1, 7.1.0.x
7.6	7.1.0.1	7.0, 7.0.x, 7.1, 7.1.0.x
7.6	7.1.0.2	7.0, 7.0.x, 7.1, 7.1.0.x
7.6	7.1.0.3	7.0, 7.0.x, 7.1, 7.1.0.x
7.6	7.1.0.4	7.0, 7.0.x, 7.1, 7.1.0.x

Table 2-6 Release compatibility for the NetBackup 7.6 product line *(continued)*

NetBackup master server	NetBackup media server	NetBackup client
7.6	7.5	7.0, 7.0.x, 7.1, 7.1.0.x, 7.5
7.6	7.5.0.1	7.0, 7.0.x, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6	7.5.0.3	7.0, 7.0.x, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6	7.5.0.4	7.0, 7.0.x, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6	7.5.0.5	7.0, 7.0.x, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6	7.5.0.6	7.0, 7.0.x, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6	7.6	7.0, 7.0.x, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6

Note: Support for the NetBackup 6.x product line has ended as of October, 2012.

Auto Image Replication support

In NetBackup 7.6, Auto Image Replication is supported for the servers that run version 7.5.0.3 or higher. For lower versions to accept replications from 7.6, an Emergency Engineering Binary (EEB) for the 7.1 master server is required.

Auto Image Replication is supported between the servers that run versions 7.1.0.x and 7.5.0.x. An exception occurs in certain versions, in which the replication of catalog backups may fail.

For more information, refer to the following Technote:

http://www.symantec.com/docs/TECH191964

NetBackup compatibility

NetBackup is compatible with a mixture of NetBackup servers that are at various release levels in the same environment. However, Symantec validates only certain combinations of servers and clients within a NetBackup environment that must provide backward compatibility.

See “About compatibility with NetBackup 7.6” on page 46.

Note: The statements that are made in this topic do not override Symantec's standard End of Life policies. Once a NetBackup version reaches its end-of-life, no version of that product is supported. That includes backward-compatible versions.

Please review the following end-of-life technote on the Symantec Support website for more information:

http://www.symantec.com/docs/TECH74757

Another useful tool that you can use to create a checklist to see if your system is ready for a NetBackup installation or an upgrade is the Installation and Upgrade Checklist tool. This tool is one in a set of Web-based tools that support Symantec Enterprise products. You can locate this tool and others on the Symantec Operations Readiness Tools (SORT) web page.

The following is a list of best-practice rules that you should consider for a mixed-server environment:

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- During an upgrade to NetBackup 7.6, it is necessary to have enough free disk space to accommodate three complete copies of the NetBackup database. That includes all transaction logs and database files in the data directory including BMR if it is configured and in use. This directory is typically `/usr/openv/db/data` for UNIX-based operating systems and `\Veritas\NetBackupDB\data` for Windows-based operating systems when you use default installation methods.
- In a mixed-server environment, the master server must run the highest version of NetBackup in use in that configuration with the exception of Maintenance Releases.
  See "About compatibility with NetBackup 7.6" on page 46.
- A master server can inter-operate with a media server that is running a level of NetBackup that is one major release lower.
- A media server cannot have a numerically higher version than the master server. (Each media server must run equal or lower levels of NetBackup than the master server with which it is associated.)
- All NetBackup components (server, client, and console) on an individual system must be at the same version.
- The backup images that are created under an older version of NetBackup are recoverable with a newer version of NetBackup.
- Master and media servers should have a minimum soft limit of 8000 file descriptors per process.

For more information about the effects of an insufficient number of file descriptors, see the following Technotes on the Symantec Support website.
http://www.symantec.com/docs/TECH168846

- The NetBackup accelerator feature requires configured media servers to be at a NetBackup 7.5 version level. At the time of this release, the NetBackup appliances do not run on a version level that is equivalent to NetBackup 7.5. Therefore, NetBackup accelerator backups do not work on NetBackup appliance media servers.
- NetBackup master and media servers exchange NetBackup server version information at startup, and every 24 hours. This exchange occurs automatically. After an upgrade, at startup, an upgraded media server uses the `vmd` service to push its version information to all of the servers that are listed in its server list.
- To install NetBackup on Windows 2008/Vista/2008 R2/7 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.

For additional information about NetBackup version compatibility, see the following Technote on the Symantec Support website.

http://www.symantec.com/docs/TECH29677

About platform life cycles

NetBackup software is compatible with an ever-changing set of platforms. And NetBackup must be flexible enough to handle platform life cycle issues such as adding and removing a platform from its compatibility list.

See “About adding a platform” on page 50.

See “About removing a client platform” on page 51.

About adding a platform

Adding a platform that is compatible with NetBackup introduces a situation where the platform has a future, but no history. In this situation, backward compatibility cannot be guaranteed without exhaustive testing. When a platform is added for a NetBackup release, the platform is compatible with that version and subsequent versions (but not previous versions).

About removing a client platform

The customer commitment for client platform version support is **one version back** with every effort to be compatible with all versions. An exception is that the client version cannot be newer than the master and the media server version.

You can mix the individual clients that are at different version levels within a NetBackup domain. However, it is possible that during an alternate restore, the restore is sent to an older version. Alternate restores should go to the same version or newer versions.

About NetBackup EEB listings

This release incorporates fixes to several known issues that existed in previous versions of NetBackup. Many of these issues pertain to the customer-specific issues that have been documented in the form of Titan or Salesforce.com (SFDC) cases. Many of the fixes that are incorporated into this release are available as individual engineering binaries and engineering bundles (EEBs). These EEBs were created to address specific customer issues with a previous version of NetBackup. To view a listing of EEBs that are included in NetBackup 7.6, download the following document from the Symantec Support website.

NetBackup 7.6 Emergency Engineering Binary document

- http://www.symantec.com/docs/DOC6085

In addition, the SORT NetBackup Hot Fix/EEB Release Auditor has the capability to find in what release an EEB is fixed. Use the following URL to access SORT.

https://sort.symantec.com/netbackup

Chapter 3

Product dependencies

This chapter includes the following topics:

Operating system patches and updates

This topic provides information on the product dependencies of this release of NetBackup. You should verify that your operating system is up-to-date with all of the latest patches and upgrades before you install NetBackup. This section is a guide to inform you of the operating systems that require a patch or an upgrade.

Table 3-1 provides the known, minimum operating system (OS) patches and updates. A vendor may have released a more recent patch that supersedes a patch that is listed in this table. Symantec recommends that you visit the Support website of that particular vendor for their latest patch information.

Table 3-1 Operating system patches and updates for NetBackup

Operating system type and version	Patch	Notes
AIX 6.1	AIX 6.1 TL5 SP2 (6100-05-02-1034)	NetBackup 7.5 or greater requires the AIX 6.1 TL5 SP2 (6100-05-02-1034) Maintenance Pack as a minimum. (Higher patch levels should also work.) You can use the `oslevel -s` command to verify what Maintenance Pack level you have installed.
	AIX run-time libraries 9.0.0.3 or later	The run-time libraries need to be at 9.0.0.3 or later. You may need to restart after you change to version 9.0.0.3.
HP-UX	COMPLIBS.LIBM -PS32	If you install AT on an HP-UX platform, this patch is required.

Table 3-1 Operating system patches and updates for NetBackup *(continued)*

Operating system type and version	Patch	Notes
HP-UX IA64	Networking.NET-RUN: /usr/lib/libipv6.sl	
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.1	
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.sl	
	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so	
	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so.1	
	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so	
	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so.1	
	Networking.NET2-RUN: /usr/lib/libipv6.1	
HP-UX PA-RISC	Networking.NET-RUN: /usr/lib/libipv6.sl	For HP-UX PA-RISC platforms, this fileset is required.
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.1	For HP-UX PA-RISC platforms, this fileset is required.
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.sl	For HP-UX PA-RISC platforms, this fileset is required.
	Networking.NET2-RUN: /usr/lib/libipv6.1	For HP-UX PA-RISC platforms, this fileset is required.
HP-UX 11.11	PHSS_32226	This patch is a LIBCL patch.

Table 3-1 Operating system patches and updates for NetBackup *(continued)*

Operating system type and version	Patch	Notes
	PHSS_37516	Contains fixes for the following: ■ `QXCR1000593919: purifyplus` dumps core in PA32 ■ `QXCR1000589142: dld` crash in LL_new_descendent_list when the `aCC` application is exiting. ■ `QXCR1000589142: dld` crash in LL_new_descendent_list when the `aCC` application is exiting. ■ `QXCR1000746161: dlsym()` hangs ■ `QXCR1000593999: dld` emits assert messages for `chatr +mem_check` enabled 64-bit executables
	PHSS_26946	This patch is necessary to enable any C++ run-time code to work properly.
	PHSS_27740	This patch is a `libc` cumulative patch.
	PHSS_26560	This patch contains a linker tools cumulative patch.
	PHSS_32864	That is a recommended critical patch from HP that is required for successful NetBackup client backups.
	PHKL_26233	This patch enables `HP-UX 11.11 mmap()` to use large files from 2GB to 4GB.
	PHSS_35379	That is a recommended critical patch from HP that is required for successful NetBackup client backups.
	PHCO_29029	That is a recommended critical patch from HP that is required for NetBackup to use VxSS.
	PHSS_24045	Allow `POLL_INTERVAL` to be set to zero in `/var/stm/config/tools/monitor/dm_stape.cfg`. That disables the `dm_stape` monitor within the Event Monitoring System. Symantec recommends that you upgrade to IPR0109.

Table 3-1 Operating system patches and updates for NetBackup *(continued)*

Operating system type and version	Patch	Notes
	PHSS_30970	This patch can cause problems with the programs that have the `setuid` bit set. Hewlett-Packard 's IT resource center website contains information about this patch. `www1.itrc.hp.com`
	PHCO_35743	S700_800 11.11 libc cumulative patch The above patch has dependency on the following patches: ■ PHCO_31923 (critical patch): s700_800 11.11 libc cumulative header file patch ■ PHKL_34805 : 700_800 11.11 JFS3.3 patch; mmap
HP-UX 11.23	PHCO_33431	Symantec recommends that all customers running 11.23 install this patch. That applies to HP PA-RISC only because HP Itanium has moved to 11.31.
	PHSS_34858	That is a recommended critical patch from HP that is required so that `dlopen` works properly.
	PHKL_31500	That is a recommended critical patch from HP that NetBackup requires, particularly when you attempt to run NetBackup with NetBackup Access Control (NBAC).
	PHSS_37492	Contains fixes for the following: ■ `QXCR1000593919: purifyplus` dumps core in PA32 ■ `QXCR1000589142: dld` crash in LL_new_descendent_list when the `aCC` application is exiting. ■ `QXCR1000746161: dlsym()` hangs ■ `QXCR1000593999: dld` emits assert messages for `chatr +mem_check` enabled 64-bit executables
HP-UX 11.31	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.

Table 3-1 Operating system patches and updates for NetBackup *(continued)*

Operating system type and version	Patch	Notes
SUSE Linux Enterprise Server 10 x64	SUSE Linux Enterprise Server 10 update 2	The operating system version must be SUSE Linux Enterprise Server 10 update 2 or greater.
Solaris 10 SPARC 64-bit (server and client)	Update 4 (08/07) and newer	The server is supported on Update 4 (08/07) and newer.
	Recommended patch set - dated June 2011 or newer	Symantec recommends that you download the patch set dated June 2011 (or newer) from the Oracle Support website. https://support.oracle.com The patch set contains the following minimum recommended patches: The patch set contains the following minimum recommended patches: ■ 118777-17 (SunOS 5.10: Sun GigaSwift Ethernet 1.0 driver patch) ■ 139555-08 (Kernel patch with C++ library updates). ■ 142394-01 (Internet Control Message Protocol (ICMP) patch) ■ 143513-02 (Data Link Admin command for Solaris (DLADM) patch) ■ 141562-02 (Address Resolution Protocol (ARP) patch) The following patches are for Solaris 10 SPARC with NXGE cards: ■ 142909-17 (SunOS 5.10: nxge patch) ■ 143897-03 (Distributed Link Software patch) ■ 143135-03 (Aggregation patch) ■ 119963-21 (Change Request ID - 6815915) ■ 139555-08 (Change Request ID - 6723423)

Table 3-1 Operating system patches and updates for NetBackup *(continued)*

Operating system type and version	Patch	Notes
Solaris 10 x86-64	Recommended patch set - dated 12/28/2011 or newer	Symantec recommends that you download the patch set dated 12/28/2011 (or newer) from the Oracle Support website. https://support.oracle.com The patch set contains the following minimum recommended patches: ■ 118778-15 (SunOS 5.10_x86: Sun GigaSwift Ethernet 1.0 driver patch) ■ 139556-08 (Kernel patch with C++ library updates) ■ 142395-01 (SunOS 5.10_x86: ICMP patch) ■ 143514-02 (SunOS 5.10_x86: Data Link Admin command for Solaris patch) ■ 147259-02 (SunOS 5.10_x86: Aggregation patch) ■ 142910-17 (SunOS 5.10_x86 kernel patch to include NXGE fixes) ■ 142910-17 (SunOS 5.10_x86: Distributed Link Software patch) ■ 143136-03 (SunOS 5.10_x86: Aggregation patch) ■ 139556-08 (Change Request ID - 6723423) ■ 119964-21 (Change Request ID - 6815915)
Windows XP x86-32	KB936357	Microsoft microcode reliability update.
Windows XP x86-64	KB928646	Hot fix for hangs of connection attempts by PBX.
Windows Vista x86-32	KB936357	Microsoft microcode reliability update.
	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Vista x86-64	KB936357	Microsoft microcode reliability update.
	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Server 2003 x86-32 (SP1 & SP2)	KB883646	Microsoft Storport hot fix.
	KB913648	Contains the necessary updates to run Volume Shadow Copy.
	KB936357	Microsoft microcode reliability update.

Table 3-1 Operating system patches and updates for NetBackup *(continued)*

Operating system type and version	Patch	Notes
Windows Server 2003 x86-32 (SP2)	KB971383	TCP/IP protocol driver triggers a disconnect event randomly. Required for master and media servers.
Windows Server 2003 x86-64 (SP1 & SP2)	KB883646	Microsoft Storport hot fix.
	KB913648	Contains the necessary updates to run Volume Shadow Copy.
	KB928646	Hot fix for hangs of connection attempts by PBX.
	KB936357	Microsoft microcode reliability update.
Windows Server 2003 x86-64 (SP2)	KB971383	TCP/IP protocol driver triggers a disconnect event randomly. Required for master and media servers.
Windows Server 2008 x86-32	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Server 2008 x86-64	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Server 2008 (SP2)	KB979612	Hot fix to improve TCP loopback latency and UDP latency
Windows Server 2008 R2	KB2265716	Hot fix for when a computer randomly stops responding.
	KB982383	Hot fix for a decrease in I/O performance under a heavy disk I/O load.
	KB983544	Update for the "Modified time" file attribute of a registry hive file.
	KB979612	Hot fix to improve TCP loopback latency and UDP latency

Chapter 4

Operational notes

This chapter includes the following topics:

About NetBackup 7.6 operational notes

This chapter contains the topics that explain important aspects of the NetBackup 7.6 operations that may not be documented elsewhere in the NetBackup documentation set. This document is posted on the Symantec Support website and may be updated after the GA release of NetBackup 7.6. Therefore, Symantec recommends that you refer to the following document on the Symantec Support website to view the latest release information.

NetBackup 7.6 Release Notes

- http://www.symantec.com/docs/DOC6138

This release incorporates fixes to several known issues that existed in previous versions of NetBackup. Many of these issues pertain to the customer-specific issues that have been documented in the form of Titan or Salesforce.com (SFDC) cases. Many of the fixes that are incorporated into this release are available as individual engineering binaries and engineering bundles (EEBs). These EEBs were created to address specific customer issues with a previous version of NetBackup. To view a listing of EEBs that are included in NetBackup 7.6, download the following document from the Symantec Support website.

NetBackup 7.6 Emergency Engineering Binary document

- http://www.symantec.com/docs/DOC6085

The online versions of other NetBackup documents may have been updated since the GA release of NetBackup 7.6. You can access the most up-to-date version of the documentation set for this release of NetBackup at the following location on the Symantec Support website.

http://www.symantec.com/docs/DOC5332

The following is a list of Technotes that offer insight on minimum NetBackup requirements that can help you tune your NetBackup environment. These Technotes can also help you learn how to get more out of your NetBackup product.

- For minimum system requirements for the Solaris kernel when used with NetBackup.
  http://www.symantec.com/docs/TECH15131
- For information on resource allocation within NetBackup.
  http://www.symantec.com/docs/TECH137761
- For minimum OS `ulimit` settings on UNIX platforms, see the following Technote on the Symantec Support website:
  http://www.symantec.com/docs/TECH75332

Note: References to UNIX also apply to Linux, unless otherwise stated.

NetBackup installation and startup notes

This section contains the operational notes and known issues that are associated with the installation and startup of NetBackup.

- Extra steps are required to perform NetBackup 7.6 client push installations from an HP PA-RISC media server to clients that support NetBackup-Java applications.
  During the installation, `/usr/openv/java/nbj.conf` ends up empty on the receiving client. This issue applies to the `ssh`, `rsh`, `ftp`, `sftp`, and `update_clients` remote installation methods for both initial installations and upgrades.
  On the receiving client, `/usr/openv/java/nbj.conf` has zero length. From the pushing server, you encounter a message similar to the following:

  ```
  grep: can't open /usr/openv/java/nbj.conf
  ```

  If `nbj.conf` is empty, the `jpbSA` and `jnbSA` commands fail with the following error:

  ```
  Initialization of NetBackup-Java failed due to the
  following error:
  Invalid value for NB-Java configuration option
  PBX_PORT: null. Status: 520
  Configuration file: /usr/openv/java/nbj.conf
  ```

  To avoid this issue, perform NetBackup 7.6 client push installations from a server that supports NetBackup-Java applications.

To work around this issue, see the following tech note on the Symantec Support website:
http://www.symantec.com/docs/TECH210951

Note: You cannot copy `nbj.conf.bak` to `nbj.conf` because the contents of the file are different after upgrading to NetBackup 7.6.

- If the following `ssh` command is used to upgrade a pre- 7.0 NetBackup client to Version 7.6, a successful install may return an unsuccessful exit status (non-zero):
  `/usr/openv/netbackup/bin/install_client_files ssh <client>`
  If the installation encountered this particular issue, rerunning the command to the client should return a successful exit status. To work around this issue altogether, use a different remote installation method such as `rsh`, `ftp`, `sftp`, or `update_clients` to upgrade pre- 7.0 NetBackup clients.

  Note: This issue does not affect `ssh` upgrades to NetBackup 7.6 for those clients that are running Version 7.0 or newer.

  For more information, see "Installing client software with the ssh method" in the *NetBackup Installation Guide*, available from the following location:
  http://www.symantec.com/docs/DOC5332
- To install NetBackup Windows client software remotely, the system must meet certain configuration requirements. One of the requirements is that the Remote Registry service be started on the remote system. Starting with NetBackup 7.5.0.6, the NetBackup installer can enable and start the Remote Registry service on the remote system.
  If the Remote Registry service is not started, the installation receives the following error message:

```
Attempting to connect to server server_name failed
with the following error: Unable to connect to the remote system.
One possible cause for this is the absence of the Remote Registry service.
Please ensure this service is started on the remote host and try again.
```

  For more information on NetBackup remote installation, see the *NetBackup Installation Guide* and the *NetBackup Upgrade Guide*.
- Upgrades on AIX, Linux, and Solaris may fail if the `/usr/openv/db/data` directory is a link.

For Solaris, the issue affects all upgrades to NetBackup through version 7.5.0.4. For AIX and Linux, the issue only affects upgrades from NetBackup 7.5 through 7.5.0.4. The installation problem does not affect HP systems.
Additionally, this issue does not occur if the `/usr/openv/db` directory is a link. The problem is the result of how the native package installers recognize symbolic links from `/usr/openv/db/data` to an alternate location.
For more information and workaround instructions, see the *NetBackup 7.6 Upgrade Guide* or visit the following URL on the Symantec Support website:
http://www.symantec.com/docs/TECH189078

- 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.

- Beginning with NetBackup 7.0, `nbmail.cmd` is installed to the `netbackup\bin\goodies` folder. It had previously been installed to the `netbackup\bin` folder. Like the other scripts in the `netbackup\bin\goodies` folder, you now have to copy `nbmail.cmd` to the `netbackup\bin` folder. (You would then modify `nbmail.cmd` at that location for it to take effect.
- Log files for VxUL OIDs from previous releases
  Log files for VxUL OIDs that were used in a previous release may be left in the root logs directory (`/usr/openv/netbackup/logs` on UNIX and `C:\Program Files\Veritas\Netbackup\logs` on Windows) after an upgrade to NetBackup 7.0. This occurs because the OIDs do not have an OID entry in the nblog.conf file that specifies the subdirectory for their log files (<oid>.LogDirectory=name). This may occur for the following OIDs: 102, 113, 120, 142, 153, and 157. You

can display these log files with `vxlogview` in NetBackup 7.0 if you specify the following.

`-G <root log dir> -o oid`

Where *<root log dir>* is either `/usr/openv/netbackup/logs` on UNIX or `C:\Program Files\Veritas\Netbackup\logs` on Windows. And *oid* is the 102 , 113, 120, and so on.

You can remove these OIDs after the upgrade. However, you must manually delete the OIDs because the `vxlogmgr` cannot access them. If you think you may need to report a problem in a previous release, then you may want to keep them for that purpose.

- To install NetBackup on Windows 2008/Vista/2008 R2/7 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.
- The **NetBackup Tape Device Driver Installation** wizard is no longer present on the installation media. In most cases, the manufacturer's device drivers or the drivers that are included with the operating system are appropriate. In environments where the NetBackup tape device drivers are required, you can download them from the NetBackup Support Web site at the following location.
  `http://support.veritas.com/docs/287850`
- In a future release, it may be required that clients connect to the master server to complete an installation.
- Symantec recommends the following Microsoft 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`
  - Microsoft microcode reliability update. This fix applies to 32-bit and 64-bit versions of Windows Server 2003/XP/Vista: (suggested) `http://support.microsoft.com/?kbid=936357`
  - Symantec AntiVirus. Update to latest version (10.2 for Corporate Edition) and latest update (required).
  - The `Symevent` driver updates (required). Update to latest driver version.
- The default shared-memory requirements on UNIX systems are greater for NetBackup 7.0 than previous releases.
  See the *NetBackup Installation Guide for UNIX and Linux.*
  See the *NetBackup Troubleshooting Guide for UNIX, Windows and Linux*.

- The operating system may open a user interface window (for example, File Manager on a Solaris system,) when the DVD is inserted into the drive. Symantec recommends that you do not use this window to install NetBackup products because unpredictable results may occur. Follow the installation instructions that are provided in the NetBackup documentation set.

NetBackup cluster installation notes

The following list shows the items that relate to NetBackup cluster:

- UNIX ssh command
  Starting with NetBackup 7.5, UNIX clusters can run the ssh command. The root user guidelines for the ssh command are the same as those for the rsh command.
- UNIX Cluster node upgrade order
  Starting with NetBackup 7.5, you can select whether to first upgrade the inactive node or the active nodes.
- NetBackup 7.5 media server installations are not clustered with the clustering agent and the `cluster_config` procedure. Since the NetBackup 7.0 release, media servers are clustered with application clusters rather than the clustering agent. Existing NetBackup 6.x clustered media servers that use the clustering agent can be upgraded and remain clustered.
  For more information about cluster media servers on NetBackup 7.x, refer to the *NetBackup Highly Available Environments Guide*.
- For VCS Windows (SFW-HA 4.1, SFW-HA 4.2), Symantec recommends that users make sure patch 278307 is installed before you install or upgrade to NetBackup 7.1.
  See http://www.symantec.com/docs/TECH43003 for more information.
- When you launch the NetBackup Administration Console, you should log into the server using the virtual name that is associated with NetBackup.
- With the need for increased security, you must be able to configure NetBackup with access control (NBAC) in a clustered NetBackup server environment.
  See `http://www.symantec.com/docs/TECH51483`.
- After you install or upgrade NetBackup on UNIX clusters other than SunCluster, you should increase the NetBackup resource offline timeout to at least 600 seconds.
- When you install or upgrade NetBackup on Sun Clusters, make the following changes to the NetBackup resource group tuning parameters to ensure a successful failover:
  - Increase the `STOP_TIMEOUT` parameter from the default of 300 seconds to at least 600 seconds.

- Set the `pmf Retry_count` parameter to 0.

These changes can be accomplished using the following commands. Note that running these commands causes shutdown and restart of NetBackup.

```
# scrgadm -c -j scnb-hars -y Retry_count=0
# scrgadm -c -j scnb-hars -y STOP_TIMEOUT=600
# scswitch -n -j scnb-hars
# scswitch -e -j scnb-hars
```

- When you upgrade clustered NetBackup servers to NetBackup 7.0, you may encounter Windows event log messages that indicate the Sybase service (SQLANYs) failed to start. These messages are generated in a short period of time – normally a window of two to three seconds. These messages coincide with the cluster configuration portion of the upgrade. You should expect these messages and know that they do not reflect a problem with the upgrade.

NetBackup package, media, and rebranding changes

This section lists some of the changes that were made to NetBackup installation packages and branding.

- NetBackup Operations Manager (NOM)
  Starting with NetBackup 7.0, NOM has been replaced with OpsCenter. If your current 6.x NetBackup environment includes NOM 6.x, you can upgrade NOM to OpsCenter with an upgrade to NetBackup 7.x.
  See "NetBackup OpsCenter notes" on page 116.
- Starting with NetBackup 7.5, native packaging for servers on the HP-UX, RHEL, SLES, and AIX platforms has been implemented.
- The FreeBSD client has been changed to include additional binaries.
  Starting with NetBackup 7.1, the FreeBSD client has been changed to include binaries for VxUL, ACE/TAO, and so forth. That change is similar to what the other NetBackup clients already contain. VxUL and ACE/TAO make use of `$ORIGIN`. However, in FreeBSD operating system levels before 8.0, `$ORIGIN` does not work.
  Installs with the FreeBSD operating system levels that are before 8.0 install correctly and the daemon startup and shutdown scripts have been modified to set `LD_LIBRARY_PATH`.
  However, if you execute a NetBackup command directly and get a message that indicates some NetBackup libraries are not found, you must set `LD_LIBRARY_PATH` to `/usr/openv/lib` for that command to work. For 64-bit systems, set `LD_32_LIBRARY_PATH` to `/usr/openv/lib`.

Note: If the operating system level of FreeBSD is greater than 6.0, you must add `/usr/local/lib/compat` after `/usr/openv/lib` to `LD_LIBRARY_PATH` or `LD_32_LIBRARY_PATH`.

- UNIX package consolidation

  Starting with NetBackup 7.0, most of the add-on products and database agents are now installed with the NetBackup server or the client package. Separate installation for these products is no longer needed.

  The following products are now included in the NetBackup server package (if the platform supports the product):

  - BMR master server
  - NDMP
  - Vault

  The following products are now included in the NetBackup client package (if the platform supports the product):

  - BMR Boot server
  - DB2
  - Encryption
  - Informix
  - LiveUpdate agent
  - Lotus Notes
  - Oracle
  - SAP
  - Snapshot Client
  - Sybase

  The binaries for the listed products are laid down with the server or the client package. A valid license is still required to enable the product. If product configuration was required previously (such as `db2_config`), configuration is still required.

  For Solaris server upgrades, the older versions of any listed products here must be removed before an upgrade to NetBackup 7.x. For example, VRTSnbdb2, SYMCnbdb2, VRTSnbenc, SYMCnbenc, and others. The installation script displays a list of the packages it finds that must be removed.

  The Japanese, Chinese, and French language packages remain as separate add-ons. The process to install and upgrade these products remains the same.

NetBackup LiveUpdate notes

The following items describe the known limitations that relate to the NetBackup LiveUpdate feature.

- When using NetBackup LiveUpdate to upgrade an HP PA-RISC client to NetBackup 7.6, you can encounter an error if that client has the following configuration:
  - The directories `/dev/random` and `/dev/urandom` exist.
  - The default system Java JDK/JRE level is between version 1.6.0 and 1.6.0.16.
    To verify the current JDK/JRE version level, run the following command:
    `java -version`

  If you want to use LiveUpdate to upgrade an HP PA-RISC client to NetBackup 7.6, you can perform either of the following two options to avoid this issue:
  - Option 1:
    In the default system java security file (for example, `/opt/java6/jre/lib/security/java.security`), change the following:
    `securerandom.source=file:/dev/urandom`
    To:
    `securerandom.source=file:/dev/random`
  - Option 2:
    Upgrade the default system Java JDK/JRE level to version 1.6.0.16 or later.

  If you have encountered this issue, the following error text can exist in the `/opt/Symantec/LiveUpdate/liveupdt.log` file:

  ```
  <date> <time> Attempt to load guard and signature files failed
  because initialization of the security libraries failed
  <date> <time>
  <date> <time> The Java LiveUpdate session did not complete
  successfully.
  <date> <time> Return code = 233
  ```

  You should make sure that `/usr/openv/java/jre/bin/java` is a symbolic link to the default system Java binary. Then perform one of the two previous options or rerun the failed NetBackup LiveUpdate job.
- Attempts to use LiveUpdate to install or upgrade the NetBackup 7.6 patch onto an HP-UX PA-RISC client fail.
  Symantec no longer includes Java with NetBackup which results in the removal of versions of Java that NetBackup previously installed. Java is required for

LiveUpdate to work correctly. To correct this issue, make sure that you have a current version of Java installed on your client and that Java is listed in the path.

- When you use the Remote Push or Silent installation methods to install NetBackup, the LiveUpdate agent is not installed as part of the package. If you want install the LiveUpdate agent, Symantec recommends that you copy the LiveUpdate binaries from the following location to the local host and install the LiveUpdate agent manually.

  `\\<dvd_root>\Addons\<platform>\LiveUpdate`

  For more information on how to install LiveUpdate, refer to the *NetBackup LiveUpdate Guide*.

  Note: If this issue affects a large number of computers, you can use a third-party application such as Altiris to install the LiveUpdate agent.

- NetBackup LiveUpdate is not compatible with OpenVMS (UNIX) or Novell operating systems.

General NetBackup 7.6 notes

The following items describe general NetBackup 7.6 operational notes.

- Sybase SQL Anywhere performance is poor using SPARC T-series processor versions older than T4-4. Symantec recommends that you do not run your master server on this type of hardware.

  Note: NetBackup uses the Sybase SQL Anywhere database server internally to store the NetBackup configuration data and backup image headers that run on the master server.

- The `swapfile.sys` file needs to be manually excluded from Windows 8 client backups.

  On Windows 8, `swapfile.sys` is a new temporary file that resides on the Windows %SystemDrive%. If the %SystemDrive% is `C:`, then the file is located at `C:\swapfile.sys`. This file needs to be excluded from backups to save backup space and to prevent incomplete restores.

- An issue can occur where a newly-added NetBackup appliance media server also gets added to the EMM database as a master server. Subsequent attempts to delete the master server entry from the EMM database using the `nbemmcmd -deletehost` command fail with the following error:

```
$ nbemmcmd -deletehost -machinename <machine_name> -machinetype
master
NBEMMCMD, Version: <NetBackup_version>
The function returned the following failure status: "Cannot
delete machine entry '<machine_name>', it has Audit entries.
Please contact Symantec support for deleting audit entries
from the database"
```

- Support for remote-EMM and shared-EMM server configurations is withdrawn in NetBackup 7.6. In a remote- or shared-EMM server configuration, the NetBackup relational database (NBDB), the Enterprise Media Manager (EMM), and the Resource Broker (RB) are moved to a server that is not the master server. This configuration is not supported in NetBackup 7.6.

  Customers who currently use this configuration should contact Symantec Support who will engage Symantec Engineering to review the options to disengage this configuration from an environment.

- Starting with NetBackup 7.6, policy data that is copied to the Clipboard from previous versions of NetBackup cannot be copied to version 7.6 and vice versa. In such cases the paste option displays as disabled in the NetBackup Administration Console.

- In some cases, the NetBackup Job Manager (`nbjm`) on the master server may not detect the status of backup jobs on a media server. This issue generally causes `nbjm` to report a status code 40 in the job details.

  The issue occurs due to problems with the TCP stack on the media server, problems with the network between the hosts, or a catastrophic application failure on the media server. The result is a job update or exit status may not arrive and `nbjm` continues to wait for job completion. In the case of a job failure, this issue may cause a delay in job retry. In the case of a successful data transfer, `nbjm` may eventually report the job as failed and retry the job.

  This issue has the potential to occur in any environment that experiences networking, platform, or application problems. Older (pre- 6.5) versions of NetBackup with clustered media servers may also experience this issue. Pre-6.5, the issue can occur if there is a hardware or a software fault and the cluster fails over to the passive node.

  For more information on this issue, including solutions and workarounds, please see the following Technote:

  - http://www.symantec.com/docs/TECH202675

- Restore may fail for the clients that have both WAN Resiliency and client-side deduplication (Client Direct) enabled.

To work around this issue, disable WAN Resiliency for the affected clients before you attempt a restore. To disable WAN resiliency, open the NetBackup Administration Console and navigate to **Master Server Host Properties** > **Resilient Network**. Select the client and set it to **OFF**.

- Client selections for backup policies
  The client selection for Windows 8 clients and Windows Server 2012 clients is **Windows** for x86 and x64 systems. Beginning with this release of NetBackup, all Windows clients are referred to as **Windows**, instead of their release versions (such as Windows 2003/2008).
- Live browse and backup problems exist on SUSE 11 operating systems with a kernel version later than 2.6. The issues occur because the `nbfirescan` process in NetBackup 7.6 does not support kernel versions later than 2.6.
  To work around this issue, revert to the kernel 2.6 version and perform the snapshot.
- When SLP-managed backup images are processed, NetBackup needs to control the image copy expirations so they do not expire before any dependent copies are made. Before the 7.6 release, the expiration time on those copies was set to infinity and reset to the correct time once the dependent copies completed. If copies were displayed during this period of time, they would appear to have an infinite expiration time.
  Beginning with the 7.6 release, the expiration time of all SLP-managed copies is set to the correct time when the copy is created. Information that is embedded in the image controls the expiration of SLP-managed copies. Those copies do not expire even though the expiration time of the copy has passed.
- If the NetBackup Java Administration Console is used to expire NetBackup images, the image extension files remain in the catalog. However, NetBackup expires the image extension files, usually within 12 hours.
- If the backed up file system is encrypted for RHEL, then when the system is restored with the Bare Metal Restore option, the existing encryption is removed.
- In VMware vSphere, virtual machine display names, resource pool names, and vApp names are case sensitive. For example, vm1 is a different virtual machine from one that is named VM1. In NetBackup 7.5 and earlier, however, NetBackup does not recognize case when it selects virtual machines for backup automatically through a query. It considers VM1 and vm1 to be the same virtual machine.
  In 7.6, NetBackup recognizes case in VM display names, resource pool names, and vApp names. A backup policy that uses automatic selection through a query is now case-sensitive. The same is true of the new **Search Virtual Clients** function in the Backup, Archive, and Restore interface. vm1 is identified as a different virtual machine from VM1.

Note: When you upgrade to NetBackup 7.6, policies that identify virtual machines through a query may select a different set of virtual machines for backup. You may need to edit the policy query rules to reflect the case-sensitive behavior.

- You cannot use the Policy Wizard to create an Oracle snapshot policy on a Solaris x86 master server. Instead, you must use the **Policy** attributes tab.
- In a storage reuse scenario after an upgrade from NetBackup 7.x to 7.6, the storage check function is not available. Before installations of NetBackup, the user must check that more than 12% storage space remains. If the storage space is more than 12%, then the user can install NetBackup 7.6. After installation, the user should run the conversion utility to change the old data format to the new data format. If storage space is less than 12%, the user should install the current NetBackup version and expire images until more than 12% remains. The user can then upgrade to NetBackup 7.6 and run the conversion utility.
- Do not use an IP address as a host name.
  If you use an IP address for your host name and use a Storage lifecycle policy (SLP) for a backup and a duplication, your duplication jobs fail with a status 228 error. The clients with the IP address host names have to be named in a backup policy that sends data to an SLP.
- For synthetic full backups or synthetic, cumulative-incremental backups, do not enable the Encryption attribute in the backup policy. Backups fail if Encryption is enabled for synthetic backups.
- Setting the minimum number of file descriptors to 8000 is required for NetBackup to run correctly and help avoid the following issues:
  - Some jobs end with a Status 26 error in the `bpbrm` log on the media server: http://www.symantec.com/docs/TECH70191
- You can ignore any SCSI syslog messages on an HP-UX 11.31 operating system, during a backup or a restore with an HP EVA Array.
- Information at the Activity Monitor may not appear in the correct order.
  The precision that the Activity Monitor uses is measured in seconds. Starting with NetBackup 7.1, more information is printed into the Activity Monitor. Messages from the master server, media server, and clients that generate at the same second may be printed out of the order that they occurred.
- An upgrade to SQLAnywhere 11.0.1 was made in NetBackup 7.0.
  An upgrade to SQLAnywhere 11.0.1 was made in NetBackup 7.0. However, there is a restriction within that version that requires the database server name to be less or equal to 31 characters. NetBackup has been modified to change

the server name, from *VERITAS_NB_hostname.domain_name* to *NB_hostname* in `/usr/openv/db/bin/servername`. NetBackup also trims the name to 31 characters if necessary.

- Validation of the data files that reside in raw devices may fail.
  In NetBackup 7.x, validation of data files that reside in raw devices may fail even though the Clone operation was successful. You may receive an error that states the validation for specific paths failed.
- A file with Access Control Lists (ACLs) can cause the restore to complete with a **Partially successful** status.
  When backing up and restoring a Red Hat Security-enhanced Linux (Red Hat SEL) system with extended attributes (EAs) disabled and the Access Control Lists (ACLs) enabled, any file with ACLs causes the restore to complete with "partially successful" status. That is due to the RH SEL system always returning the ACLs as EAs.
  To back up and restore ACLs on a Red Hat SEL volume, you must have **user_xattr** enabled in the mount parameters. The **ACL** mount parameter setting has no effect.
- The deduplication rate is low during a multistream backup of SQL2005 to NetBackup. The issue only happens with multiple stream backups.

  You can use the following sequence to identify the known problem:

  - Create an SQL backup policy using NetBackup and set the stripes to 4.
  - Run the policy four times.
  - Check the deduplication rate of the fourth backup stream and see that it is only 25% as shown.

    ```
    1:17%  2:18%  3:20%  4:25%
    ```

  To work around this issue, run a single stream backup and expect to see good deduplication results.
  To test the workaround, repeat Create an SQL backup policy using PDDE and set the stripes to 1. The deduplication rate can reach 100%.
- Status 25 or status 54 errors can occur when legacy callback and a third-party service are allowed to listen on the same port. For more information about this issue and any possible work-arounds, see the following Technote on the Symantec Support website.
  http://www.symantec.com/docs/TECH154279
- The following list indicates the disk storage units that support Granular Recovery in NetBackup 7.6.
  - BasicDisk

- AdvancedDisk
- PureDisk
- OpenStorage

Refer to the following document for details on support for PureDisk and OpenStorage:
http://www.symantec.com/docs/TECH187917

The following list indicates the disk storage units that do **not** support Granular Recovery in NetBackup 7.6.

- SnapVault

- The upgrades and policies that use Instant Recovery
  Under certain circumstances, the environments that upgrade to NetBackup 7.5 and use Instant Recovery may experience snapshot failure.

  The problem can occur only when all of the following circumstances are true:

  - The environment was upgraded to NetBackup 7.5. New NetBackup installations are not affected.
  - Before the upgrade to NetBackup 7.5, policies had the Instant Recovery schedule attribute enabled.
  - Policies indicate a storage lifecycle policy as the Policy storage in the policy.
  - The storage lifecycle policy contains a Snapshot storage destination.

  To correct the problem, perform one of the following actions and rerun the backup:

  - Open the policy and enable the Instant Recovery schedule attribute.
  - Use Backup destinations instead of Snapshot storage destination.

- In rare cases, users may see core `bpdbm` or `nbdb_*` dumps in the ODBC layer on any server platform. That is because of a known Sybase issue, the fix for which was not available in time for the NetBackup 7.5 release cycle.
- A new installation of NetBackup 7.x may fail if the `LD_LIBRARY_PATH_64` library path has been defined and does not contain any NetBackup library paths. The ability to run or start NetBackup can be problematic if the environment variable `LD_LIBRARY_PATH_64` has been defined, and does not include the paths to NetBackup libraries.

  To resolve this issue, do the following:

  - Do not define the `LD_LIBRARY_PATH_64` path system wide, or disable the environment variable before you start NetBackup.

- Define the paths for `LD_LIBRARY_PATH_64` to ensure the following NetBackup library directories or paths are included:

  `/usr/openv/db/lib`

  `/usr/openv/lib`

  See the following Technote on the Symantec Support website:
  http://www.symantec.com/docs/TECH167024

- After the NetBackup 7.5 release, the only item under **Shadow Copy Components** that remains is **User Data**. All other items have been moved to the **System State** node. If you have any other specific directives for Shadow copy components in our policies, Symantec recommends that you remove those directives and use **System State** for backing up these components. An example is, `Shadow copy components:\System Service`.

- Snapshot creation may fail when the volume is mounted with NFS version 4. NFS version 4 is not supported without workarounds or upgrades to OnTap. Symantec recommends that you check NetApp documentation for the latest information on NFS version support.
  Until you are certain that NFS version 4 is supported, you can use NFS version 3 to create snapshots of NFS mounted volumes. Use NFS version 3 to mount the snapshots on NetBackup clients. Use the following command to determine the version currently being used for a given mountpoint.

  `nfsstat -m <mountpoint>`

- The following configuration issue exists in an environment of a UNIX master server, UNIX media server, and UNIX client, where the volume is mounted with NFS.
  If data is added to the same volume from a CIFS share (Windows host), that data may not be backed up by an incremental backup. That is due to working differences between the NFS and the CIFS technologies.

- The `nbstserv` process has connection problems with the `bpdbm` processes after an image selection does not communicate with `bpdbm` for longer than 10 minutes. To work around this issue, create the `DBMto` file with a value of 60. That keeps the connection open for a longer period of time to avoid this issue.

- Unable to create a storage lifecycle policy because the storage server name does not match the name that the Data Fabric Manager server uses. This issue causes a status code 1552 to appear.
  To work around this issue, run the `bpstsinfo -li` command and check the output for the storage server name. The name that you use to create the storage server must match this name.
  See the *NetBackup Replication Director Solutions Guide*.
  See the *NetBackup Status Codes Reference Guide*.

- The time between the master server, media server, and clients should be synchronized. It should be synchronized so the events that are displayed in the activity monitor progress log appear in the correct order.
  Make sure that the master server, media server, and clients are synchronized on time. The NetBackup 7.5 Activity Monitor provides more information for each job execution and it prints the information from media server and client processes. The timestamp information for those messages originates on the media server and client. Therefore, if the time is not correctly synchronized, it may not appear in the correct order at the Activity Monitor.
- The catalog backup disaster recovery email may contain duplicate entries.
  If you use the disaster recovery email in a recovery scenario, ensure that the duplicate entries in the file are removed.
- In the beginning of the rerouting process, active backup, restore, and duplication jobs may abort with a status code 83 (media open) and a status code 84 (media write).
  After the rerouting workflow has reached the job step **Parallel or Serial rerouting method** (which starts the actual rerouting of data), the backups, restores, and duplication jobs no longer abort with an error 83 and 84.

  Note: The job step **Parallel or Serial rerouting method** is in the PureDisk Web user interface, under **Monitor** > **Jobs** > **View jobs** by: **Policy types** > **Storage Pool Management Policies** > **Rerouting**

- In NetBackup 7.5, if the image size is less than 10GB, then image rebasing is not triggered and the image candidate is not generated.
- When the Windows NTFS Change Journal is used, it is not recommended to use the NetBackup Job Tracker.
- In the NetBackup Cloud storage, the **Used Capacity** and **Available Space** for Rackspace is inaccurate in the NetBackup Administrative Console.
  The information that is displayed for **Used Capacity** and **Available Space** for Rackspace is inaccurate in the NetBackup Administrative Console. The values are found under **Disk Pool > Devices** . Even if there is information in the disk pool, the value that is displayed for **Used Capacity** is zero. The value for **Available Space** displays the maximum amount. You must review the information on the provider website for accurate use information.

NetBackup Accelerator notes

This section contains the operational notes and known issues that are associated with NetBackup Accelerator in this release.

- Accelerator and Replication Director support for virtualized servers cannot be configured together. The Block Level incremental backup settings do not currently allow the combination.
- The creation of a NetBackup Accelerator policy can fail because it does not recognize a valid storage unit group.
  In this case, the issue is a result of uninstalling and then reinstalling the NetBackup Administration Console with a different host name (domain). To work around this issue, see the following tech note on the Symantec Support website:
  http://www.symantec.com/docs/TECH209889
- NetBackup Accelerator requires that the storage have the **OptimizedImage** Attribute enabled. To ensure that your storage is configured properly, see the documentation for your storage option:
  If you use the `bpverify` command to verify NetBackup Accelerator images that were taken using NetBackup 7.5.0.4 or earlier, then the verify operation can fail with a status code 191. The failure can occur because the total size of image in media may not match the size of the image that was recorded in the catalog metadata.
  That issue specifically pertains to an incorrect image size in the catalog metadata. It does not mean that the image is corrupt or it should not impede you from restoring the image. The following error can appear.

```
/usr/openv/netbackup/logs/bpdm/112112_00011.log ---
02:32:36.278 [28530] <2> verify_image_fragsizes:
validating abcdl2.xxxx.xxx.symantec.com:
wxyz.xxx.xxx.symantec.com_1352283783_C1_F1 imo_size=6130472960
613...
(Kbytes=5986790 remainder=512 diff=-512)

02:32:36.280 [28530] <32> verify_image_fragsizes:
The size of backup id wxyz.xxx.xxx.symantec.com_1352283783
fragment 1 for copy 1 does not match the size found on
media (6130473472 6130472960)
```

- - NetBackup **Media Server Deduplication Pool** or **PureDisk Deduplication Pool**.

The **OptimizedImage** Attribute is enabled by default beginning with the NetBackup 7.1 release. If you created the storage servers and pools in an earlier release, you must configure them for **OptimizedImage**.
See the *NetBackup Deduplication Guide*.

- Backups to a third-party disk appliance.
  The storage device must support the **OptimizedImage** Attribute.
  See the *NetBackup OpenStorage Solutions Guide for Disk*.
- Cloud storage that NetBackup supports.
  See the *NetBackup Cloud Administrator's Guide*.
- PureDisk storage pool.
  By default, PureDisk supports the **OptimizedImage** Attribute.

- Clarification of NetBackup accelerator backups to a NetBackup appliance media server.
  The NetBackup accelerator feature requires master servers, media servers, and client servers to be at the NetBackup 7.5 version level or higher. NetBackup appliance media servers require appliance version 2.5 or higher for accelerator support.
- The NetBackup Accelerator does not support the VxFS File Change Log.

Auto Image Replication notes

This section contains the operational notes and known issues that are associated with Auto Image Replication in this release of NetBackup.

- In NetBackup 7.5, if an SLP image was in progress and a manual replication was attempted that used `nbreplicate`, the command would fail with the following error message:

  ```
  INF - ReplicationJob::Replicate: Replication failed for backup
  id<backup_id>: images are in process (1519)
  INF - Replication failed for backup id <backup_id>: images are
  in process (1519)
  ```

  Starting with NetBackup 7.6, this type of manual replication request is successfully processed and does not return an error.

NetBackup AdvancedDisk option

To use encryption with AdvancedDisk, you must use the NetBackup `nbdevconfig` command to configure the storage servers and the disk pools.

See the *AdvancedDisk Storage Solutions Guide*.

NetBackup audit trail limitations

The following limitations pertain to the NetBackup audit trail feature.

- Audit records are not generated for the media server addition and deletion.
  Audit records are not generated for the media server addition and deletion for the media server deduplication pool (MSDP) and the deduplication storage server.
- Only the parent-job cancel action is audited.
  An action with parent jobs does not result in corresponding audit records for children. Child jobs actions that occur because of the actions that occur with Parent jobs are not audited.
- Need readable string values for old and new values in the **Detailed** report.
  In the **Detailed** report, old and new values shows values such as 0, 1, 2. Instead, this report should show readable, actual string values like `VmHostname`, `VmDNSName`, and so forth.
- Two restore audit records are created in a catalog restore instead of three.
  In the Activity Monitor, three restore jobs are shown for a catalog restore However, in the `nbauditreport` there are only two audit records that relate to the restore. There should be three restore audit records for each restore job.
- The multiple-attribute values that were not modified were displayed with the modified attributes in the **Audit** record when the disk pool properties were updated.
  The **Audit** record listed the values of attributes that were not modified or updated for the DiskPool when the `setattribute` and `clearattribute` options were used. Only the values of the attributes that were modified or upgraded should have been displayed.
- The **Backup selection** is stored as a UTF-8 encoded string in the Audit database. The `nbauditreport` command does not convert the UTF-8 encoded string to the current locale; therefore, the command line interface may show unrecognizable characters for the backup selection output.
- Two audit records are created for each policy operation.
  For each operation, the old and new values are first set from default values to blanks. Then these values are set from blanks to actual values. Thus, for every operation that occurred two audit records were created. Only one record should be created with the old and new values.
- Two audit records are created for each FlashBackup Windows policy operation.

The policy modification for a smart policy uses a two-step process. First, it resets the attribute value. Then it is set with a new value of the attribute. As a result, the process generates two audit records because, technically, the policy is modified twice.

Backup, Archive, and Restore operational notes

The following are the operational notes for the NetBackup Backup, Archive, and Restore interface:

- Extended attributes are lost when symbolic files are restored on UNIX clients. In particular, the security context extended attributes of symbolic files are also lost on Security-Enhanced Linux (SELinux) clients.
  After performing a single file restore operation on a UNIX client, the following error can be found under the **Task Progress** tab of the Backup, Archive, and Restore interface:

  ```
  08:19:05 (92.001) attr_set failed for <file_name> - Attribute
  security.selinux not set. Errno = 2: No such file or directory
  ```

  The error occurs when the file is a symbolic link and the target of the symbolic link no longer exists. Despite the error, the file appears to have restored successfully. However, the extended attributes of the symbolic link are lost. This issue applies to both virtual clients and physical clients.

  Note: If the target does exist, no error is reported and the extended attributes will get set on the target instead of the symbolic link.

- On Windows computers, the default **History** pane behavior is changed beginning with the NetBackup 7.6 release. When you open a restore Window, only the most recent backup or snapshot is selected by default. Previously, a range of backup images was selected.
- NetBackup Java Windows Display Console: With a remote connection from a NetBackup Java Windows Display Console that uses the English locale, the restore of files that have non-ASCII characters may fail.
  To work around this issue, see the following Symantec tech note:
  http://www.symantec.com/docs/TECH75745

NetBackup Bare Metal Restore notes

This section contains the operational notes and known issues that are associated with Bare Metal Restore (BMR) in this release of NetBackup.

- If the boot server has a base installation of Solaris 10 update 11, the creation of 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.
- During a BMR restore on Solaris 11 and newer, the following error message may be displayed:

  ```
  devfsadmd not responding. /dev may not be correct
  ```

  During a BMR restore, the service that is related to the `devfsadmd` daemon is stopped temporarily to manipulate the `/dev` and `/devices` links. As a result, when the operating system wants to do internal communication with the `devfsadmd` daemon it generates the error message.
  This message is not for BMR and it does not have any effect on a BMR restore or on the overall system. The message can be ignored. Once the system boots up after the BMR restore, the `devfsadmd` daemon restarts and the message does not display again.
- 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.

- After BMR restore completes, the Oracle Solaris Installation menu is seen for few seconds before the system is automatically restarted.

  The Oracle Solaris installation menu displays for few seconds after the BMR restore completes. This issue is harmless as the system restarts within a couple of seconds after the message displays.

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

  During first boot after a BMR restore, 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 fails if the text-installer package is not present the customized Automated Installer (AI) ISO that was created using the distribution constructor.

  For 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.

- After a client to virtual machine conversion, the OS takes time for configuration. This issue happens on Windows when the BMR client to virtual machine backup conversion occurs and the converted VM boots up for the first time. During this time, Windows automatically configures OS settings for the new hardware. This auto-configuration activity requires approximately 1-4 minutes.

  You should not restart the OS on the VM until after waiting for some time until Windows configuration is complete. This activity can be seen in a Windows dialog or status pane.

- When the `/etc/mke2fs.conf` file is restored, the restore task is shown as partially completed on the **Activity Monitor** tab in the NetBackup-Java Administration Console. The issue occurs on RHEL6 Update 2 platforms and later, and it occurs even though the bare metal recovery of the client completes successfully. The issue occurs because the security properties contain some incorrect settings for the `/etc/mke2fs.conf` file in a Bare Metal Restore environment after the file is restored.

- BMR fails to create a media shared resource tree (SRT) when a **Basic Server Installation** is performed on a Red Hat Enterprise Linux system.

  A **Basic Server Installation** of BMR on a Red Hat Enterprise Linux system fails to create media SRT. This issue occurs because the package that contains a command that is used for ISO creation is missing. This issue does not occur with a normal **Desktop** installation of Red Hat Enterprise Linux clients.

  To resolve this issue, the system administrator must manually install the missing package. The package would resemble a file similar to`genisoimage-1.1.9-11.el6.x86_64`. After this file is installed, you can use the `bmrsrtadm` command to create the media SRT.

- After a BMR restore and during the first startup, the system relabels all of the file systems and then the Linux operating system restarts the computer again.

  That is a necessary process that is related to SELinux:

  - The labels are how security contexts are associated with files and are stored as part of a file's extended attributes. If the system is started with SELinux disabled these labels can be inadvertently removed or become out of sync.
  - That usually occurs only when you label a file system for SELinux for the first time. During a BMR restore, and as file systems are newly created, it is the first time that the file systems are labeled during the first startup.

- 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.

- During 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 previous error message. However, when you log on and run `zpool status -x` you see the message, "`all pools are healthy`". That is because of the ZFS import operation that is done during the **Firstboot** sequence. BMR restores storage pools and contents in the **BMR Restoration Environment** and later imports to the **Client**

Environment during **Firstboot**. That can cause an error message or a warning message during the **Firstboot** operation.

These messages only occur during the **Firstboot** operation and you can safely ignore them.

- During a Dissimilar Disk Restore (DDR), if you opt for the creation of a ZFS storage pool on small number of disks, 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.

- The other file systems that are on a ZFS volume is not supported. If you create a file system over ZFS volumes, BMR does not support a backup and restore of those file systems over the ZFS volumes.

- Coexistence of two BMR-supported multi-path solutions (EMC PowerPath and Linux Native multi-path) with both actively configured on a client can cause issues and are currently not supported by BMR.

  A BMR issue can result if a multi-device that is configured over a SAN disk using the EMC PowerPath name, and the SAN disk is under both EMC PowerPath and the Linux Native multi-path. In addition, this configuration is unsupported. However, if the same multi-device is configured over a SAN disk using the Linux Native Multipath name then it works with BMR.

- A **BMR Legacy Restore** fails with the following error message when a restore of a Windows client is configured with `Emulex Fibre Channel` cards.

  ```
  Failed to modify txtsetup.sif
  ```

  This issue was fixed in NetBackup 7.5. However, if you see this issue with a NetBackup 7.6 client then the cause is most likely that the restore process is referring the old driver packages. In such cases, perform the following steps.

  - Delete the old driver packages that are related to the Emulex LightPulse Fibre Channel driver. If the driver package is linked to the configuration then you may also need to delete those configurations too.
  - Create a new backup of the client at NetBackup 7.6. Or create a point-in-time configuration from your earlier 7.6 backups for that client.
  - Perform a Prepare-To-Restore on the new configuration with a Legacy shared resource tree.
  - Start a restore process on the client.

- BMR restore fails during Linux DDR scenario from internal disk to SAN disk and vice versa.

BMR does not consider the disk ordering in the BIOS. In the case of a SAN disk to an internal system disk the restore may not work as expected because of the disk ordering changes in the BIOS. This may be more common in GRUB installations.

In some cases, if you remove SAN disks before restoration, then restore may work properly with the existing BIOS ordering.

- BMR can only support disk naming conventions such as `hdX`, `sdX`, `cXDn`, and so forth. BMR backups can fail on Citrix Xencentre virtualization for the following reasons.
  - BMR does not recognize disk names such as `xvdX` which are newly introduced on Citrix Xencentre virtualization. That is because the "`xen para-virtual drivers`" introduced in this type of virtual environment.
  - For modern versions of BMR that Linux systems such as SLES11SP1 support, the client computers show `hda` and `sda` disk naming conventions at the same time. And BMR does not support that.

    To work around this issue, make sure that you use the **Other media install**because it is the only template that BMR only supports in Citrix Xencentre virtual computer. And do not use the systems that BMR does not support. For example, BMR does not support SLES11SP1 and RHEL6.1 and onwards on Citrix Xencentre virtualization.
- A NetBackup System state backup would fail on certain Windows 2008 R2 systems with SFW 5.1 SP1. That was an issue that occurred on a system where the System Reserved partition did not have an assigned drive letter. With the following SFW 5.1 SP1 hot fix, this issue is resolved:

  Hotfix_5_1_10064_584_2496270

  https://sort.symantec.com/patch/detail/5438

  This issue is also resolved in the SFW 5.1 SP2 CP7.
- Users must specify the short name of the client when they install NetBackup client packages on the computer that they want to protect with Auto Image Replication and 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.
- In 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 BMR restore is successful in the disaster recovery domain and only the restore task update fails. It fails because of an invalid network configuration in the client. That is expected behavior 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 backup and restore the client in a disaster recovery domain.

On the following UNIX clients:

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

On the following Windows client:

- 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

- The PHCO_40961 patch is required to create a BMR shared resource tree (SRT) on an HP-UX IA64 11.31 platform.
  The same patch is required to create a BMR shared resource tree (SRT) on an HP-UX IA64 11.31 platform with Veritas Storage Foundation packages (VxVM, VxFS).
- IPv6 support for BMR
  This feature provides Bare Metal Restore 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.

- A failure may occur during a VxFS7-based file creation.
  During a BMR restore, a failure can occur during a VxFS7-based file creation process. To work around this issue, use a `bmrsrtadm` to patch VxFS version with 5.0 release to edit the SRT. Attempt to restore again and start a client restore.

- The BMR restore does not work on IPv6 network channels.
  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.

- Auto-boot may fail.
  Sometimes after a BMR restore and during the first boot of the client computer, the operating system auto-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 the command to enable auto-booting.
  `setboot -p <hardware_path_of_boot_harddrive>`

- 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.
  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. Make sure the IPv4 address, `client_host_name`mapping entry exists first in `/etc/hosts` before the IPv6 mapping entry.
  Run **Prepare To Restore** again.

- An issue can occur when you use `bmrsetupmaster` on the command line interface (CLI) to configure a BMR master server on an AIX 5.3 platform.
  An issue can occur when you use `bmrsetupmaster` on the command line interface (CLI) to configure a BMR master server on an AIX 5.3 platform. More specifically, this issue occurs on a 7.0 or greater BMR master server on an AIX 5.3 or greater platform. This issue occurs because the stack size, data segment

size, and max memory size `ulimit` parameters on the system are set too small. When that happens, data parsing fails while the BMR database is populated.

If you encounter this issue, use the following procedure to change the `ulimit`parameters to “unlimited” and run `bmrsetupmaster` again.

- To change the `ulimit` parameters:
  - Run the `ulimit -a` command on the BMR master server. This command prints the system resources limit.
  - Check the current limit set that is used for the `stack size`, `data seg size`, and `max memory size` parameters.
  - Set the parameters to **unlimited**. Run the following commands to change the limits:
    - `ulimit -s unlimited`
    - `ulimit -d unlimited`
    - `ulimit -m unlimited`
  - Run `bmrsetupmaster -redo` to configure the BMR master server.

    You can permanently change the resource limits by manipulating the “/etc/security/limits” file on the system.

- You can upgrade to NetBackup 7.6 only from NetBackup 7.5, 7.1, 7.0 and 6.x. You cannot directly upgrade an older standalone BMR product (BMR 4.7) to NetBackup 7.1, 7.5, or 7.6, but it can be migrated to NetBackup 7.1, 7.5, or 7.6. To migrate from BMR 4.7, refer to the, Upgrading and migrating from older BMR versions, section in the *NetBackup Bare Metal Restore Administrator’s Guide*.
- About creating a shared resource tree (SRT) for Windows

  The boot server does not support the creation of 6.5.X and 6.X Windows SRT. However a NetBackup 7.x SRT does support restores of pre-7.x NetBackup (for example, 6.5.X or 6.X) clients. The SRT that contains NetBackup 7.0 or a later version of NetBackup Client can be used to restore back-level NetBackup clients.
- About copying a pre-NetBackup 7.6 SRT

  The boot server does not support copying of 6.5.X and 6.X Windows SRT.
- About importing a pre-NetBackup 7.6 SRT

  The boot server does not support importing of 6.5.X and 6.X Windows SRT.
- BMR does not support restoring the Remote Installation Folder location of an RIS Server.

  BMR does not support restoring the Remote Installation Folder location of an RIS Server. You can restore an RIS Server using the **System Only** feature. You can also restore the RIS server by editing the client configuration, and

removing the volume that is used for the Remote Installation Folder location from the map.

- Restore of a BMR 6.5.5 Solaris 10_x64 client fails.
  The restore of aBMR6.5.5 Solaris 10_x64 client that has a NetBackup 7.6 client that is installed as part of the SRT creation process can fail intermittently. To avoid this issue, install the NetBackup 6.5.5 client into the SRT and use that SRT to restore the Solaris 10_x64 server. Do that even if the boot server version is 7.6.
- From the BMR Administration console, the source object is disabled in the user interface if mapping is successful.
  When you use the BMR Administration console to map an object, the source object is disabled in the user interface if mapping is successful. That indicates that it cannot be mapped again unless you un-map the object. For Solaris 10_x64 client configurations, when you map certain objects such as slices or volumes, even if the mapping completes successfully, the original object is not disabled. That does not mean that the mapping has failed. A BMR Restore using such a mapped configuration still completes successfully.
- The first boot after a successful restore may fail on a Linux client if the disk order in the BIOS is not correct.

  On a Linux client, if the disk order that is specified in BIOS is not: Primary Master > Primary Slave > Secondary Master > Secondary Slave, then the first boot after a successful restore may fail. For example, the order of the disks on a live client might be:

  - /dev/sdd (hd0) [Secondary Slave]
  - /dev/sda (hd1) [Primary Master]
  - /dev/sdb (hd2) [Primary Slave]
  - /dev/sdc (hd3) [Secondary Master]

  However, the disk order in the restore environment may look like the following:

  - /dev/sda (hd0)
  - /dev/sdb (hd1)
  - /dev/sdc (hd2)
  - /dev/sdd (hd3)

  Thus, during a restore, boot loader may be installed on /dev/sda, assuming it to be hd0. Then during the first boot, /dev/sdd would be mapped to hd0 because of the disk order that is specified in the BIOS and cause the first boot to fail.

To avoid this issue, set the disk order in the BIOS to reflect Primary Master > Primary Slave > Secondary Master > Secondary Slave before you attempt a restore.

- A `bmradmin` user account that is created on a Windows boot server during a boot server installation is saved and not deleted later.
  A `bmradmin` account is created on a Windows BMR boot server during the boot server registration. (It is not created on non-Windows boot servers.) This account is created unconditionally because at the boot server installation and registration time, it is not clear whether you may require a Legacy SRT or not.
  Legacy SRTs require this account to perform legacy restores that use a CD or floppy boot option. FastRestore operations do not require this account. If you determine that you do not need to perform legacy restores, then you can remove this account. However, you if remove this account, and then decide that you need it to run a legacy restore, you must recreate the account manually.
  Manually creating this account requires assistance from Symantec Support because it is originally created with a predefined password and other attributes.
- The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while the BMR SRT is created.
  The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while the BMR SRT is created. If you want to install NetBackup client versions that are older than 7.1 into the SRT, the OS architecture that you select should be 32-bit. For NetBackup 7.6, select 64-bit as the OS architecture type. While you install the NetBackup client into the SRT, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between the SRT OS architecture type and the NetBackup client version.
- You can use a shared resource tree (SRT) that contains a version of the NetBackup client of 7.x or higher restore the back-level NetBackup clients.
- After a system-only restore, the Non-Critical or Non-System ZFS storage pool of the original client may be unavailable or incorrect.
  For more information, see the following tech note on the Symantec Support website.
  http://www.symantec.com/docs/TECH179039
- After BMR restore of ZFS root pool, the spare and cache devices under ZFS root pool may be unavailable.
  For more information, see the following tech note on the Symantec Support website.
  http://www.symantec.com/docs/TECH179040
- After the first boot, you may come across issues related to mount failure of ZFS file systems.

For more information, see the following tech note on the Symantec Support website.
http://www.symantec.com/docs/TECH179042

- BMR restore of client may fail in case of Solaris client with ZFS root pool containing alternate boot environments.
  For more information about this issue, refer to the following tech note on the Symantec Support website:
  http://www.symantec.com/docs/TECH179043
- After restore, at the first boot, you may come across an error in case of SVM and ZFS file systems and the system goes into maintenance mode.
  For more information, see the following tech note on the Symantec Support website.
  http://www.symantec.com/docs/TECH179044
- After BMR restoration of RHEL6 client, during the first boot, the system may go into maintenance mode.
  For more information, see the following tech note on the Symantec Support website.
  http://www.symantec.com/docs/TECH179048
- Restore may fail on Xen virtual client of the platform SLES 10 SP3 because of the unavailability of the required drivers.
  For more information, see the following tech note on the Symantec Support website.
  http://www.symantec.com/docs/TECH179050
- On systems that run SLES 11 SP1, a restore may be successful, however the system is not able to start from the original boot disk.
  For more information, see the following tech note on the Symantec Support website.
  http://www.symantec.com/docs/TECH179053

Cloud storage notes

This section contains the operational notes and known issues that are associated with cloud storage in this release of NetBackup.

- In NetBackup 7.6, you can only create or use the storage buckets that are in the "US Standard" region. If you are using Amazon S3 cloud storage buckets in regions other than US Standard, you may encounter failures after you upgrade to NetBackup 7.6.
  Starting with Version 7.5.0.6, NetBackup supported the creation of Amazon S3 cloud storage buckets in regions other than US Standard. However, NetBackup

7.6 cannot recognize non-US Standard buckets or use them for backups. Symantec does not support an upgrade to NetBackup 7.6 if you continue to use Amazon S3 cloud storage buckets that are in a region other than the US Standard. That includes any buckets that were created outside of NetBackup, such as with the Amazon S3 web portal.

NetBackup database and application agent notes

The following topics describe operational notes and known limitations to certain NetBackup database agents:

- For the VMware backups that protect SQL Server, note the following:
  - A SQL Server database name cannot contain any of the following characters: ? * \ "
  - To use Replication Director to manage your VMware snapshots and snapshot replication with SQL Server 2012, logon account changes may be required. Logon accounts for the NetBackup Client Service must have access to the CIFS shares that are created on the NetApp disk array.
  - Change the logon account for the NetBackup Legacy Network Service to an account that has the fixed server role “sysadmin”.
  - For SQL 2012 on Windows Server 2008/2012, the account that runs the Microsoft SQL Server Service must have full permissions for the NetBackup Legacy Network Service temp directory. This directory is `C:\Users\user\AppData\Local\Temp`, where *User* is the account that runs the NetBackup Legacy Network Service.

NetBackup for Microsoft Exchange

The following list contains operational notes for the NetBackup for Microsoft Exchange database agent as they pertain to this release of NetBackup:

- SharePoint and Exchange GRT operations can fail for the VM backup images that use display names that contain parenthesis. For example, a SharePoint GRT live browse restore from the Backup, Archive, and Restore interface fails with the following error because of this issue:

  ```
  database system error
  ```

- Granular Recovery Technology (GRT) support for Microsoft Exchange Server is not supported in IPv6-enabled NetBackup 7.x environments.
- Exchange GRT functionality may fail for VMWare backup of disks that were configured as Raid 5. You may see the following line in the debug log:

```
<from Producer> VDDK-Log: Unsupported component/volume type 3
(Raid5) - volume has been skipped!
```

- The NetBackup for Exchange and NetBackup for SharePoint Agents support a restore to the same Microsoft service pack (SP) or cumulative update (CU) on which the backup was originally created. Microsoft sometimes introduces database schema changes in SPs or CUs. If you restore to a different SP or CU level, the database server may not operate correctly.
- NetBackup does not support restoring mailbox items into tenant mailboxes in a multi-tenant Exchange environment. To recover items pertaining to a tenant mailbox, redirect the recovery to a non-tenant mailbox. Backup and recovery of Exchange Server databases are fully supported in a multi-tenant environment.
- Restoring Exchange in a Cluster
  When you restore data in an Exchange cluster environment, one must set the destination client value to be the virtual server name. You can restore an Exchange database using a NetBackup client-only installation on a cluster. However, it may not be possible to change the destination client value to match the virtual server name. In that case, use a NetBackup Client user interface on a NetBackup server to change the destination client value to the virtual server name.
- The status of a DAG backup may be is empty if the restore is initiated from a node in the DAG.
  When you restore databases or granular items of a DAG backup, the restore status may be empty from the backup and restore user 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 for the virtual DAG name. Initiate the user backup from the active DAG node or manually start the backup from the NetBackup master to properly start the backup.
- Tar32 may consume more memory than normal on an Exchange restore with multiple Databases. Symantec is working on a solution to this problem in the post NetBackup 7.5 timeframe.
- The **company** field of task objects does not get properly restored.
  The **company** field of task objects does not get properly restored with Exchange 2010 granular recovery.
- The `bpfis.exe` memory usage grows when a snapshot of multiple storage groups or Exchange 2010 databases is processed.

In NetBackup testing, the `bpfis.exe` process memory usage grows by a few megabytes per storage group or Exchange 2010 database. If a single snapshot job processes a large number of storage groups or Exchange 2010 databases, the process virtual memory size can approach or exceed one gigabyte.
The workaround is to make sure that you have sufficient virtual memory to accommodate this growth, or to break up your backup into smaller snapshots.

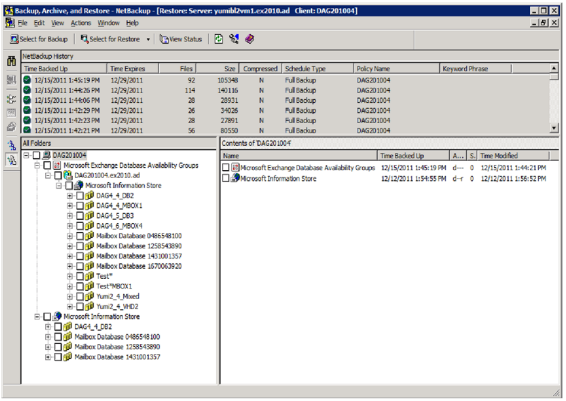
- Instant recovery backups are not supported for Exchange in a cluster environment.
  Instant recovery backups are not supported for Exchange in a cluster environment (Exchange 2007 cluster, Exchange 2007 CCR, or Exchange 2010 DAG).
- The progress log window does not display the proper messages when an Exchange backup is launched using the Snapshot Client off-host backup capability.
  When an Exchange backup is launched from the NetBackup Client user interface and uses the Snapshot Client off-host backup capability, the progress log window does not display the usual progress messages evident when a scheduled backup is executed. The lack of progress logging does not affect the backup operation. If detailed progress is desired, use the NetBackup Administrator's user interface to launch a Manual Backup operation on an Exchange policy.
  See the Testing Configurations Settings section in the *NetBackup for Exchange System Administrator's Guide* for instructions regarding a manual backup operation.
- Alternate client (off-host) backup of Exchange 2010 fails with a status 130 with NetBackup 7.1.
  An alternate client (off-host) backup of Exchange 2010 may fail with a status 130 error. That occurs if the Exchange management console (EMC) is not installed on the off-host client. This problem arises because the Exchange `eseutil` command is required on the alternate client if the EMC is not installed. For Exchange 2010, `eseutil` requires that the VC9 runtime DLLs be installed, and these DLLs are not automatically installed with NetBackup.
  From the `bpfis` log on the alternate client, the following error occurs.

  ```
  ERR - ubsStart_eseutil():CreateProcess() failed
  for "C:\Program Files\Veritas\NetBackup\temp\eseutil.exe"
  /ml "\\?\GlobalRoot\Device\HarddiskDmVolumes\
  mbdg_89d6aa17\SnapV4B3C30C0013C\db\Mailbox\Mailbox
  Database 1006745976\E00tmp.log" - 0x36b1
  ```

  You can use either of the following two solutions to address this issue:

- Install the Exchange management console on the alternate client. That prevents the use of `eseutil` for performing the Exchange consistency checks. That would be the preferred solution for this problem.
- Install the VC9 runtime DLLs. You can download these DLLs from the following Microsoft x64 VC9 download page.
  `http:www.microsoft.com/downloads/details.aspx?familyid=BD2A6171-E2D6-4230-B809-9A8D7548C1B6& displaying=en`

- A user is unable to browse for Exchange restore images from a node of a database availability group (DAG) using the Backup, Archive, and Restore interface, even if the **Distributed Application Mapping** is set in the **Master Server** properties. To work around this issue, create a `NetBackup\db\altnames` folder, with either a `No Restrictions` file. (That enables no restrictions of access from one client to another.) Or, you can create a `NetBackup\db\altnames\`*`Exchange_server_name`* file (where *`Exchange_server_name`* is the actual name of the physical Exchange server that you want to run the Backup, Archive, and Restore interface from). You should add the DAG name in this file.
  See the *NetBackup Exchange Administrator's Guide* for more information on how to create `altnames` files.
- A restore of an Exchange database that contains a bracket in the name for example, `Exch_DB[Sales]`), may fail if you select multiple images in the left pane of the Backup, Archive, and Restore interface.
  To work around this issue, select the images to be restored one at a time.
- If you perform a VMware backup with Exchange protection, you must ensure that you include the volume where the Exchange server is installed. For example, If NetBackup is installed on `F:\` and the Exchange server is installed on `C:\`, then you must choose `C:\` as part of the backup. If you choose to exclude the volume where Exchange is installed, such as the `C:\`, then the granular browse operations fail.
- Exchange 2010 databases from a DAG that are cataloged as part of an **Exchange application-aware VMware** backup are displayed differently than if these databases had been backed up with an Exchange policy (VSS backups). With an **Exchange application-aware VMware** backup, the Exchange databases are cataloged under **Microsoft Exchange Database Availability Groups\DAG_Name\Microsoft Information Store\Database_name**. For Exchange VSS backups, these databases are cataloged under **Microsoft Information Store\Database_name**.



NetBackup for Microsoft SharePoint

The following list contains operational notes for the NetBackup for Microsoft SharePoint Agent as they pertain to this release of NetBackup:

- SharePoint and Exchange GRT operations can fail for the VM backup images that use display names that contain parenthesis. For example, a SharePoint GRT live browse restore from the Backup, Archive, and Restore interface fails with the following error because of this issue:

  ```
  database system error
  ```

- The restore of some localized versions of Microsoft SharePoint Foundation Diagnostic Service results in a status code 13.
  The workaround is to rerun the SharePoint Configuration Wizard.
- Granular Recovery Technology (GRT) support for Microsoft SharePoint Server is not supported in IPv6-enabled NetBackup 7.x environments.
- SharePoint GRT functionality may fail for VMWare backup of disks that were configured as Raid 5. You may see the following line in the debug log:

  ```
  <from Producer> VDDK-Log: Unsupported component/volume type 3 (Raid5)
  - volume has been skipped!
  ```

- The NetBackup for Exchange and NetBackup for SharePoint Agents support a restore to the same Microsoft service pack (SP) or cumulative update (CU) on which the backup was originally created. Microsoft sometimes introduces database schema changes in SPs or CUs. If you restore to a different SP or CU level, the database server may not operate correctly.

- NetBackup does not support Granular Recovery Technology (GRT) with Microsoft SharePoint Server backups in a multi-tenant SharePoint environment. Backup and recovery of SharePoint Server databases are fully supported in such an environment.
- Since SharePoint metadata is stored outside of the content database, it cannot be restored using Granular Recovery Technology (GRT). You can, however, use GRT to restore SharePoint data with metadata attached to it. As long as the metadata resides in the same service application, SharePoint maintains the link between the two items.
- NetBackup 7.5 is able to back up Word Automation services and Web Analytics services , earlier limitations on these are removed.
- When you restore a list item from a localized sub-site, the job is reported as successful. However the list item fails to appear in the SharePoint user interface.
  To work around this issue, restore the item to a file system and upload the item to SharePoint.
- The SharePoint RBS backups that use the `FILESTREAM`-provider that is included in the **SQL Server Remote BLOB Store** installation package with SharePoint 2010 are supported for database-level backups and restores (full and differential).
- Restoring SharePoint GRT objects from a UNIX NetBackup master server does not cause a restore job to be initiated.
  You should initiate the restore job from the SharePoint client that the backup was cataloged under.
- The **Application State Capture** job fails for SharePoint when there is a `content-db` with no site collections present.
  To avoid this issue, remove the empty `content-db` or create a site collection in the `content-db`.
- Restoring a **SharePoint Help Search** database and index files results in a successful restore. However, the **SharePoint Help Search** is not extended to use the restored database and index files.
- SharePoint configurations with the SQL back-end servers that service multiple SQL-instances for multiple SharePoint farms, is not supported with **SharePoint Application-enabled VMware Policies**.
- The **Restore GRT Basic Meeting Workspace** shows errors when you restore even though the restore completed.
- When you perform SharePoint granular restores from the images that are produced with the VM SharePoint application-aware backups, select one image at a time to browse and restore.

- When you use a **VMWare** policy to protect SharePoint, an error is returned by the **Application State Capture** job for an SQL server that hosts multiple SharePoint farms.
- When you use a **NetBackup SharePoint** policy, SharePoint farms where there are multiple SQL instances that multiple farms use on the same SQL server is now supported.
- A SharePoint FAST search is not protected.

NetBackup for Active Directory

- If you perform a granular restore of a deleted Active Directory user account, the user account is disabled. User accounts in the **Built-in** folder are not affected.
  To work around this issue, open **Active Directory Users** > **Computers** and manually reset the password for the account and then enable the account.

NetBackup for Oracle

The following limitations pertain to the NetBackup Oracle Guided application recovery for Windows feature.

- HP-UX PA-RISC checkpoints may not be unmounted on Oracle database agents.
  For HP-UX PA-RISC checkpoints to unmount and be cleaned up, create touch file `/usr/openv/netbackup/AIO_READS_MAX` that contains the value **1**.
  See the *NetBackup for Oracle for UNIX and Linux Administrator's Guide* for more information.

Guided Application Recovery for Windows

- If you use a temporary tablespace or datafile(s), and you plan to write the datafile(s) back to the same location, do not modify the path.
  If you modify the path, make sure that it is identical to the source path. The modified path is case-sensitive and must match the source path. Otherwise, the clone fails with an error that indicates the temporary file already exists.
  This limitation does not affect UNIX and Linux systems.
- From the OpsCenter user interface, it can take a long time to display the **View Datafiles Recovery Set** window.
  Do not click the **View Datafiles Recovery Set** link if you are running on a Solaris master server. The process that is required to display the data files is time consuming.

MSDP notes

The following items pertain to the NetBackup Media Server Deduplication Option:

- NetBackup MSDP and PureDisk deduplication case sensitivity issues
  In versions before NetBackup 7.5.0.6, a problem can occur where NetBackup cannot read an image that is stored on an MSDP or PureDisk storage unit. The issue results from inconsistencies in how entries are written and read in the deduplication database on case-sensitive file systems. The types of operations that might exhibit failure due to a read error that is associated with this issue include verify, restore, duplication, and replication.
  For more information about this issue, see the following tech note on the Symantec Support website:
  http://www.symantec.com/docs/TECH207194
- NetBackup does not support client side deduplication of NDMP hosts. The backup jobs fail if the user tries to use client side deduplication for NDMP hosts.
- NetBackup does not support optimized duplication for MSDP from NetBackup 7.0 to NetBackup 7.6.
- If the `mtstrmd.log` file for the Deduplication Multi-Threaded Agent is deleted, the agent cannot write log messages because the file does not exist. To work around this issue, restart the agent, at which time it creates the log file.
- The `netbackup stop` command does not stop the deduplication daemons.

  On the HP-UX computers that function as NetBackup deduplication storage servers, the`netbackup stop` command does not stop the deduplication daemons:

  - NetBackup Deduplication Engine (`spad`)
  - NetBackup Deduplication Manager (`spoold`)

  To work around this limitation, use the following command to stop all NetBackup daemons and services:

  ```
  /usr/openv/netbackup/bin/bp.kill_all
  ```
- The `netbackup start` script may return a status 2 error on UNIX and Linux systems.
  On UNIX and Linux systems on which a deduplication storage server is not configured, the `netbackup start` script returns status 2. The status 2 indicates that the script cannot start the deduplication daemons. Because a storage server is not configured, the daemons cannot be started. The error is spurious; you can ignore it.
- No support for Snapshot Client off-host method media server Copy on NetBackup clients that deduplicate their own data.

NetBackup does not support the Snapshot Client off-host method media server Copy on NetBackup clients that deduplicate their own data.

- Information on the deduplication rates for Oracle Snapshot Client-based backups. Symantec expects Oracle database stream-based backups to achieve low deduplication rates. Stream-based backups include deduplication within a single backup and deduplication between a backup and data already backed up. However, Snapshot Client backups of Oracle databases achieve high deduplication rates across full backups within our test environments. Oracle Snapshot Client-based backups have higher deduplication because the data is aligned on consistent file or tablespace boundary.
- Antivirus software may delete the files that the NetBackup Media Server Deduplication Option requires, causing it to fail to start. Deleted files may also result in corrupt, unrestorable images.
  See http://www/symantec.com/docs/TECH128891.
- Beginning with the NetBackup 7.5 release, on Windows deduplication servers NetBackup uses shared memory for communication between the NetBackup Deduplication Manager (`spad.exe`) and the NetBackup Deduplication Engine (`spoold.exe`) .
  If you upgrade from a release earlier than 7.6 to a 7.5 or later release, verify that the following shared memory values are set in the *`storage_path`*`\etc\puredisk\agent.cfg` file:

  ```
  SharedMemoryEnabled=1
  SharedMemoryBufferSize=262144
  SharedMemoryTimeout=3600
  ```

  If they are not set, add them to the file and then restart both the NetBackup Deduplication Manager (`spad.exe`) and the NetBackup Deduplication Engine (`spoold.exe`).
- In some rare circumstances, a backup job may hang rather than fail under the following conditions:
  - The job is running on a Windows deduplication storage server.
  - The storage server uses shared memory for interprocess communication (the default beginning with NetBackup 7.5).
  - The disk pool high water mark is reached during the backup job.

  The job details may show that the `bptm` process stopped with a status 84 (for example, `Info bptm(pid=5280) EXITING with status 84`).
  You can wait one day for the job to complete. Scheduled queue processing may free up enough space for the job to complete during the one-day wait period.

Alternatively, you can cancel the job, process the transaction queue manually, then run the job again.

If the storage is not full, a different issue exists.

- If two or more storage pools have the same ID, deduplication activity may be affected. Symptoms may include the following::
  - Failed backup jobs.
  - Data loss during backup because data may be routed to the wrong storage pool.
  - Failed restore jobs.
  - Failed verify jobs.
  - Failed optimized duplication jobs.

  Check the IDs of all disk pools and storage pools in your environment, as follows:
  - For NetBackup **Media Server Deduplication Pool** and **PureDisk Deduplication Pool**, examine the `StoragePoolID` field in the following file:

    UNIX: *`storage_path`*`/etc/puredisk/spa.cfg`

    Windows: *`storage_path`*`\etc\puredisk\spa.cfg`
  - For PureDisk storage pools, log onto the SPA node and examine the `storagepoolid` field in the file in *`storage_path`*`/etc/topology.ini` file. Alternatively, see **Settings** > **Topology** in the PureDisk Web interface.
- If you cancel an optimized duplication job and then immediately start it again, the new job may fail. An optimized duplication job consumes many NetBackup components. When a job is cancelled, each component must release its resources. If one of the components has not yet released its resources when you restart a job, the job may fail.

  If a job fails, restart it.

NetBackup documentation notes

This section provides supplemental documentation and identifies some of the known inconsistencies in the NetBackup documentation set for this release.

NetBackup 7.6 documentation supplemental content

This section includes the supplemental documentation that does not appear in the rest of the NetBackup documentation set.

Resolving failed backup indexing jobs due to a corrupt index

If client backup indexing jobs consistently fail with status codes 5025 or 5027, it may be a symptom of a corrupt index. In some cases, the issue is a result of a disk error.

To resolve the issue, you must first resolve any disk errors that might have caused the index corruption. After you resolve any disk errors, you need to complete the following steps:

To resolve a failed backup indexing job due to a corrupt index

1. Suspend any indexing job activity. From a command prompt on the master server, enter the following command:

   ```
   nbindexutil -suspend -indexserver <indexing_server_name>
   ```

   For example:

   ```
   nbindexutil -suspend -indexserver lidabl11
   ```

2. Identify the name of the corrupt index. From a command prompt on the master server, enter the following command:

   ```
   nbindexutil -listindices -indexserver <indexing_server_name> |
   grep "<client_name>"
   ```

   For example:

   ```
   nbindexutil -listindices -indexserver lidabl11 | grep
   "lidaclvm134"
   ```

   The output from this command is the name of the corrupt index. For example:
   `NBUC_lidaclvm134_1376494972_1_0`

3. Invalidate the corrupt index. From a command prompt on the master server, enter the following command:

   ```
   nbindexutil -invalidateindices -indexserver <indexing_server_name>
   -index <corrupt_index_name>
   ```

   For example:

   ```
   nbindexutil -invalidateindices -indexserver lidabl11 -index
   NBUC_lidaclvm134_1376494972_1_0
   ```

4 Re-index the old images. From a command prompt on the master server, enter the following command:

```
nbindexutil -reindex -invalid –indexserver <index_server_name>
```

For example:

```
nbindexutil -reindex -invalid -indexserver lidabl11
```

5 Resume indexing job activity. From a command prompt on the master server, enter the following command:

```
nbindexutil -resume -indexserver <indexing_server_name>
```

For example:

```
nbindexutil -resume -indexserver lidabl11
```

Removing a trusted master server

The new trusted master server feature lets you specify trusted master servers. A trust relationship between domains helps with replication operations.

If a remote trusted master server is offline, you can remove the trust relationship with it. To do so, use the following NetBackup command on the source master server:

- UNIX:
  `/usr/openv/netbackup/bin/admincmd/nbseccmd -setuptrustedmaster -remove -masterserver master_server_name -remotemasterserver remote_master -localonly`
- Windows:
  `install_path\NetBackup\bin\admincmd\nbseccmd -setuptrustedmaster -remove -masterserver master_server_name -remotemasterserver remote_master -localonly`

For more information about trusted master servers, see the*NetBackup Administrator's Guide, Volume I* available from the following location:

http://www.symantec.com/docs/DOC5332

Windows deduplicated file system backup requirement

To back up a Microsoft Windows deduplicated file system correctly, ensure that the Windows deduplication store files are included in the backup policy. The Windows deduplication store files are located in the following directory of the disk drive:

`driveletter:\System Volume Information\dedup`

If you select an entire drive, the deduplication store files are included in the backup.

If you select files and folders but not the entire drive, the deduplication store files are not included. You must also select the deduplication store files.

If you do not include the deduplication store files in the backup, NetBackup cannot determine if the file system is deduplicated. Backups become larger than the actual amount of deduplicated data and the backup may be incomplete.

In NetBackup, a backup of a deduplicated file system is known as an optimized backup. For more information, see the “Enable optimized backup of Windows deduplicated volumes” in the *NetBackup Administrator’s Guide, Volume I*, available from the following location:

http://www.symantec.com/docs/DOC5332

About restoring from a Windows deduplicated file system backup

Only full backups of a Windows deduplicated file system are optimized backups. To restore from a Microsoft Windows deduplicated file system backup, select **from Optimized Backup**. (In NetBackup, a backup of a deduplicated file system is known as an optimized backup.) Also, ensure that you adhere to the following guidelines:

- If the target volume for restore does not contain the Windows deduplication store files, ensure that those files are included in the restore. The Windows deduplication store files are located in the following directory of the disk drive:

  driveletter:\System Volume Information\dedup

  The Windows deduplication store files may not exist for several reasons. The drive may have been erased and reformatted, or the drive may be a new drive. Regardless, include the deduplication store files in the restore. Also ensure that the file system is configured correctly in Windows as a deduplicated file system.

- If the target volume for restore contains the Windows deduplication store files, you do not have to include those files in the restore. The Windows deduplication store files are located in the following directory of the disk drive:

  driveletter:\System Volume Information\dedup

- Ensure that a backup of the drive or folders and files in not running. A restore and a backup of a deduplicated file system cannot run at the same time.

Incremental and user backups of a Windows deduplicated file system are backed up as normal files. Therefore, you must restore those files from normal backups. In the NetBackup Backup, Archive, and Restore Interface, select **from Normal Backup** as the restore type. Those files do not appear as optimized backup files.

For more information, see the “Enable optimized backup of Windows deduplicated volumes” in the *NetBackup Administrator’s Guide, Volume I*, available from the following location:

http://www.symantec.com/docs/DOC5332

NetBackup Administrator's Guide, Volume I corrections

The following corrections apply to the *NetBackup Administrator's Guide, Volume I*:

- The topic "System requirements for Active Directory granular NetBackup backups and recovery" contains an incomplete list of the operating systems that support Active Directory backups and restores. The list should also contain Windows Server 2012.

  For the most up-to-date and complete information about supported platforms, see the NetBackup 7.x Operating System Compatibility List at the following location:

  http://www.symantec.com/docs/TECH59978

NetBackup LiveUpdate Guide corrections

The following corrections apply to the *NetBackup LiveUpdate Guide*:

The topic "Copying NetBackup LiveUpdate formatted packages to your LiveUpdate server" contains an inaccurate procedure. The following is the corrected version of the procedure:

To download NetBackup release updates or hot fixes to your NetBackup LiveUpdate server

1. On your NetBackup LiveUpdate server, log on as the administrator.
2. Open your Internet browser and enter the following address:

   http://www.symantec.com/business/support/index?page=home
3. Enter the following in the **Knowledge Base Search** box:
   - In the **Enter keywords or phrase** box enter **download links**.
   - In the **Add a product for best results** box, enter **NetBackup Enterprise Server**.
4. Click the magnifying glass to run the search.
5. In the search results, click the hyperlink that corresponds to the correct version of NetBackup for your environment.
6. On the page of download links, scroll down until you reach the **LiveUpdate** section of the tech note.

7 Follow the appropriate links to download the LiveUpdate packages for the required platform.

To update any UNIX hosts, you must download all UNIX release update files.

To update Windows hosts, download the appropriate release update files for your hardware versions.

8 Decompress the files into a directory on your LiveUpdate server.

NetBackup for Oracle Administrator's Guide corrections

The following corrections apply to the *NetBackup for Oracle Administrator's Guide*:

- The topic "NetBackup for Oracle features" contains the following incorrect statement: "An Oracle instance discovery service automatically polls the clients throughout the NetBackup environment every four hours."
  The correct statement is: "An Oracle instance discovery service automatically polls the clients throughout the NetBackup environment every five minutes."
- The topic "About the NetBackup Discovery Service" contains the following incorrect statement: "The service polls the clients upon NetBackup installation and periodically after installation (every four hours)."
  The correct statement is: "The service polls the clients upon NetBackup installation and periodically after installation (every 5 minutes)."

NetBackup Plug-in for VMware vCenter Guide corrections

The following corrections apply to the *NetBackup Plug-in for VMware vCenter Guide*:

- The *NetBackup Plug-in for VMware vCenter Guide* includes the topic “Grant the Log On As Service right.” The topic is included as a step in a larger procedure for enabling NetBackup Web Services on the Windows master server.

  Note: The “Grant the Log On As Service right” step is not required.

NetBackup for Microsoft Exchange Server Administrator’s Guide corrections

The following corrections apply to the *NetBackup for Microsoft Exchange Server Administrator’s Guide*:

- For Exchange GRT operations, the granular proxy host must be installed on a version of Windows that is supported for that version of Exchange. (For example,

for Exchange 2010, the granular proxy host must be installed on Windows 2008 SP2 or R2 or on Windows 2012.

For more information, see the *NetBackup Database and Application Agent Compatibility List* at the following location:

http://www.symantec.com/docs/TECH59978

Graphical interface notes

The following subsections contain the operational notes and known issues of various NetBackup graphical interfaces and consoles.

NetBackup Administration Console for Windows

This section contains the general operational notes and known issues for the NetBackup Administration Console for Windows that can be found in this release of NetBackup.

- A rendering issue that affects radio button controls in the NetBackup Administration Console may occur when you use Remote Desktop Connection on Mac OS X.

  The issue can occur in, but may not be limited to, the **Instance** tab when you create an Oracle Intelligent Policy, and under **Applications Node** in the **Oracle Instance Credentials** dialog.

  To work around this issue, disconnect and then re-connect again through RDC.

- The errors that are logged from a NetBackup 6.0 media server are only logged on the Media log and not in separate logs.

  When you log errors from a 6.5 media server, NetBackup stores the errors in the Media log. NetBackup also saves the errors into separate logs. That enables you to view specific error types such as tape errors in Tape log report or disk errors in the Disk log report.

  However, if you attempt to log errors from a 6.0 media server, you can only view the errors in the Media log. NetBackup does not log the errors into separate error logs. If you select, **NetBackup Management > Reports > Tape reports > Tape logs**, no result is produced. The **Tape log** report appears empty.

- Availability of storage unit creation pages.

  The storage unit creation pages are not available in the **Disk Pool Configuration** wizard if the logged on host is a media server. These pages are applicable only for a master server.

NetBackup Java Administration Console for UNIX/Linux

This section contains the general operational notes and known issues for Java interfaces that can be found in this release of NetBackup.

- Intermittent issues may occur with X forwarding of the NetBackup Java 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.
  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-Java Administration Console.
  Reduced functionality (only the Backup, Archive, and Restore component available) or **Cannot Connect** errors during initialization of the NetBackup-Java Administration Console occurs if one or more of the NetBackup services or daemons on the host that is specified in the logon dialog is not running.
- The NetBackup-Java administration console on Windows (WDC) cannot connect to a UNIX master sever with a Japanese package.
  The NetBackup-Java administration console on Windows (WDC) cannot connect to a UNIX master sever with a Japanese package. When you attempt to log on to the master server, the NetBackup-Java administration console hangs at a point when the following status statement appears.

  ```
  Checking if NBAC is configured.
  ```

  For more information about this issue and a workaround solution, refer to the following Technote on the Symantec Support website.

  `http://entsupport.symantec.com/docs/335933`
- Memory requirements to run the NetBackup-Java Administration Console
  Memory requirements to run the NetBackup-Java Administration Console
  Symantec recommends that you run the console (`jnbSA`, `jbpSA`, or Java Windows Display Console) on a computer with at least 1 gigabyte of physical memory and 256 megabytes of memory available to the application.
- No remote display of the NetBackup-Java console in multi-byte locale environments.
  Remote display of the NetBackup-Java console in multi-byte locale environments is not supported.
- Defining which Symantec products are not susceptible to Java vulnerabilities.

The following Symantec products use the Java Runtime Environment (JRE):

- NetBackup
- NetBackup OpsCenter
- Veritas Backup Reporter (VBR)
- NetBackup PureDisk remote office Edition

The JRE implementation that these products use does not allow external input, Applets, or Web Start to run. As a result, a Sun JRE untrusted Applet and Web Start security issue does not affect them. For more information, refer to the following Technote on the Symantec Support website.
http://www.symantec.com/docs/TECH50711

NetBackup Java Windows Administration Console

- The **OK** button does not appear during LiveUpdate policy creation in the Backup Policy and Configuration Wizard. In addition, the **OK** button is not present under the **Clients** tab of LiveUpdate policies.
  To work around the issue in the wizard, clicking the **Cancel** button saves the policy and no further action is necessary. For any edits that are made in the **Clients** tab of LiveUpdate policies, navigating back to the **Attributes** tab saves the changes to the policy.
- Beginning with Windows Vista/Server 2008 and up, you might encounter status code 521 (NB-Java Configuration file *file_name* does not exist) when you run the Java Windows Administration Console. This error occurs in User Access Control (UAC)-enabled environments because of inadequate permissions. If you run the Java Windows Administration Console or its installer (`Setup.exe`) while UAC is enabled, a warning and a prompt to disable UAC is displayed.
  To work around this issue, Symantec recommends that you disable UAC before you run the Java Windows Administration Console. If UAC is not disabled adequately, non-built-in administrators are required to launch the Java Windows Administration Console by choosing the **Run as administrator** option.
  Although a warning is displayed, you can still run the Java Windows Administration Console installer in a UAC-enabled environment. The error only occurs when you run the console itself.

Note: Starting with Windows 7/Server 2008 R2, UAC cannot be adequately disabled through the use of the slider bar. To disable UAC on these newer Windows platforms, you have to modify a registry key.

- A rendering issue that affects radio button controls in the NetBackup Administration Console may occur when you use Remote Desktop Connection on Mac OS X.

  The issue can occur in, but may not be limited to, the **Instance** tab when you create an Oracle Intelligent Policy, and under **Applications Node** in the **Oracle Instance Credentials** dialog.

  To work around this issue, disconnect and then re-connect again through RDC.

Storage unit configuration

The following list shows operational notes for the storage unit configuration.

- Starting with NetBackup 7.0, the maximum fragment size of a disk storage unit was increased from 2 gigabytes to .5 terabytes.

  If a media server of a previous release has Disk storage units (DSUs) configured with a different maximum fragment size, the storage units are not automatically increased to the new default of 524,288 megabytes after an upgrade. To make the best use of the storage unit, consider increasing the fragment size on upgraded storage units.

- `bpstuadd` is not supported.

  Beginning with NetBackup 7.0, the `bpstuadd` command line option `-dspath` is no longer valid or supported.

NetBackup internationalization and localization notes

This section contains the operational notes and known issues that are associated with internationalization and localization in this release of NetBackup.

- VMware does not support non-US ASCII characters in virtual machine display names or in other objects that are associated with the virtual machine. Examples are annotations, floppy image name, parallel port or serial port file name, and CD-ROM ISO name. For the complete list of objects that VMware does not support with non-US ASCII characters, see the following article on the VMware Knowledge Base website:

  http://kb.vmware.com/kb/1003866

  In keeping with VMware's position, NetBackup does not support non-US ASCII characters in display names or in other vSphere objects. Symantec recommends that you follow VMware's guidelines in naming vSphere objects.

- NetBackup for Hyper-V does not support virtual machine display names that contain non-ASCII characters. To configure a policy to back up the virtual machine, select VMhostname or VMGUID as the ClientNameSelection type.

- A core dump issue may occur if the NetBackup Java administration console is used on Solaris 10 SPARC 64-bit Update 2 and newer with the Simplified Chinese UTF-8 locale. If you encounter this issue, you must install specific Solaris patches to fix the problem.
  For more details and patch information, see the following Bug ID on the Oracle Technology Network website:
  http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6901233
- On traditional Chinese and Korean Windows platforms, client backups and resotre operations fail if you install the NetBackup client software to a path that contains spaces (such as `C:\Program Files`). If you use these platforms, Symantec recommends that you do not install the NetBackup client software to a path that contains spaces.
- Unless your master server and media servers are NetBackup appliances, you should not mix non-English versions of Windows and UNIX platforms within your NetBackup server environment.
  If you mix non-English versions of Windows and UNIX platforms, differences in operating system architecture and encodings may cause non-ASCII file names and folder names to be displayed incorrectly within the user interface. That may cause functional failures.
- NetBackup can be installed to environments running different versions of UNIX-based operating systems as long as the system locales are identical. The use of different locales across UNIX platforms may cause non-ASCII file names and folder names to be displayed incorrectly within the user interface, which can lead to functional failures.
- The NetBackup menu user interfaces (MUI) do not accept non-US ASCII characters, such as high ASCII or multi-byte characters. The following list identifies the various menu user interfaces:
  - `bp`
  - `bpadm`
  - `tpconfig` menu
  - `vmadm`
  - `vltadm`
- The NetBackup-Java Administration console core dumps if you use Simplified Chinese UTF-8 locale on a Solaris SPARC 64-bit system with Solaris 10 Update 2 and above installed.
  This problem is the Oracle issue 6901233. For more information about this issue, see the following link:
  http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6901233

If you encounter this issue, apply the Solaris patch that Oracle provides to fix this issue.

- Spaces in the pathname can cause a backup to fail.
  When you run on a non-English locale, a problem can occur if you use spaces in the pathname. Spaces in the pathname can cause a backup to fail.
- You should install NetBackup client software to a path that does not contain spaces.
  The installation of NetBackup client to traditional Chinese paths that contain spaces such as `C:\Program Files` may cause backup failures. You should install NetBackup client software to a path that does not contain spaces.
- Paths that contain non-ASCII characters may cause failures.
  Installation to paths that contain non-ASCII characters may cause backup or restore failures.
- Notes on installing an English version of NetBackup on top of an existing localized version of NetBackup.
  If you plan to install an English version of NetBackup on top of an existing localized version of NetBackup without installing the localized contents in the language package CD first, you must remove the localized contents that are installed on your system.
- Symantec does not recommend running any language packs that are not at the same level as the English version. For example, do not run the NetBackup 7.5 language pack with the English version of NetBackup 7.6. Please remove any previously installed language packs before updating the English version.
- The install path must not contain multi-byte characters.
  For Windows and UNIX installations, the install path must not contain multi-byte characters.
- The NetBackup Java administration console does not support user-defined characters (UDC) and vendor-defined characters (VDC) because of the implementation of Java's encoding converters.
- On non-English versions of Windows and UNIX systems, the NetBackup Java administration console may display non-US ASCII characters incorrectly, which can lead to functional failures.
  The issue is a result of a character encoding mismatch between the NetBackup server and the remote Java administration console. For a detailed description of the configuration, see the following tech note on the Symantec Support website:
  http://www.symantec.com/docs/TECH75745
- Certain database and application agents have restricted support of localized environments. That applies to all supported platforms.

At the time of this release, the following database agents have restricted support of localized environments:

- NetBackup for DB2
- NetBackup for Informix
- NetBackup for Oracle
- NetBackup for SAP
- NetBackup for SharePoint
- NetBackup for SQL Server with Snapshot Client
- NetBackup for Sybase ASE

When you use any of these agents, the use of non-US ASCII characters is not supported in:

- Any database object names, like instance, database, table space, file group, data files, portals, and so forth
- Any path names of database files, directory, transaction log, or other database storage location
- Any path names that are specified in the policy backup selection, like notification script, template or batch file
  That applies to all supported platforms, including the use of previous versions of those NetBackup database agents with NetBackup 6.0 servers.

- The following NetBackup user-defined strings must not contain non-US ASCII characters:
  - Host name (master server, media server, EMM server, Volume Database Host, Media Host, Client)
  - Policy Name
  - Policy `KEYWORD` (Windows only)
  - Backup, Archive, and Restore `KEYWORD` (Windows only)
  - Storage unit name
  - Storage unit disk pathname (Windows only)
  - Robot Name
  - Device name
  - Schedule Name
  - Media ID
  - Volume group Name

- Volume Pool Name
- Media Description
- Vault Policy Names
- Vault Report Names
- BMR SRT Name

NetBackup IPv6 notes

The following list contains known IPv6 limitations for various NetBackup features.

- In IPV6-enabled NetBackup 7.x environments, granular (GRT) backup and recovery is not supported for Microsoft Exchange Server or Microsoft Sharepoint Server.
- VMware backup and restore are not currently supported using IPv6 addresses as server host names.
  See "NetBackup for VMware notes" on page 140.
- 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.
- Symantec has not qualified the Dynamic Host Configuration Protocol (DHCP) version 6.
- IPv6 is not supported for Symantec's Storage Foundation for Oracle RAC (SFRAC).
- The use of IPv6 link-local addresses is not supported in NetBackup. IPv6 link-local addresses are the addresses that start with fe80::.
- NetBackup BMR cannot restore on an IPv6-only network. BMR can back up IPv6 information, however, BMR requires an IPv4 network connection to do restores.

- If you have a clustered environment, the clustered environment defines a highly available resource with a virtual name that is only a single address. You can make that address an IPv4 address that is highly available or an IPv6 address is highly available. You cannot have a virtual name that resolves to both.
- For this release of NetBackup, Symantec does not fully qualify the SAN Client to support IPv6.
- For this release of NetBackup, OpsCenter cannot monitor an IPv6-only server. Each server must have an available IPv4 address for it to be monitored. However, this release does support a dual-stack server. For a dual stacked server, the available IPv4 address is used.
- Upon upgrading to NetBackup 7.x, a configuration that lists an IP address for the REQUIRED_INTERFACE entry may experience a change on the choice of interfaces after the upgrade. (For example, REQUIRED_INTERFACE = IP_address.)
  If the host name that is associated with the IP address resolves to more than one IP address, each of those addresses is used, rather than the first address.
  Symantec recommends the use of a host name that resolves to one address with REQUIRED_INTERFACE or replacing it with the PREFERRED_NETWORK equivalent in NetBackup 7.x.
- In an IPv4 environment, if you attempt an NDMP three-way backup using NAS Filers that are configured to use IPv6, the backup fails with the error, `to many datablocks`. The error occurs when you run the backup to a tape drive that is attached to a NAS FILER that is configured for IPv6.
  To avoid this issue, add the entry: `NDMP_IPV6_DISABLE` in the `/db/config/ndmp.cfg` file to tell NetBackup that IPv6 is not to be used.
  See the *NetBackup for NDMP Administrator's Guide* for more information.

NetBackup for NDMP notes

This section contains the operational notes and known issues that are associated with NetBackup for NDMP in this release of NetBackup.

- NetBackup NDMP multiplexed (MPX) restores may generate excessive numbers of messages to the `bptm` log and cause the `bptm` program and the Activity Monitor to hang. This issue can occur when a `NON_MPX_RESTORE` touch file exists on the NetBackup master server. This issue applies only to NDMP MPX restores on both UNIX and Windows platforms.
  For information on a workaround for this issue, please see the following tech note on the Symantec Support website:
  http://www.symantec.com/docs/TECH207556

NetBackup OpsCenter notes

This section contains the operational notes and known issues that are associated with NetBackup OpsCenter in this release.

- The following NetBackup OpsCenter branding and name changes take effect in NetBackup 7.6:
  - Symantec OpsCenter has been changed to Symantec NetBackup OpsCenter.
  - Java View Builder has been changed to Symantec NetBackup OpsCenter Analytics View Builder.
- The following list contains some of the NetBackup OpsCenter support changes take effect in NetBackup 7.6:
  - NetBackup OpsCenter Server is no longer supported on HP-UX 11.31 IA64.
  - NetBackup OpsCenter Server is no longer supported on AIX 6.1 and 7.1 64-bit POWER.
- On 64-bit Windows systems, if OpsCenter language packs or maintenance (triple-dot) releases are installed on top of an installation of version 7.5, an upgrade to OpsCenter 7.6 may fail. For example, if you upgrade OpsCenter 7.5 to 7.5.0.6, an upgrade to OpsCenter 7.6 may fail.
  For upgrade and workaround instructions, please see the following tech note on the Symantec Support website:
  http://www.symantec.com/docs/TECH211070
- OpsCenter user names that contain an ampersand (&) cannot be edited after an upgrade to version 7.6. After upgrade, user edits such as reset password, enable and disable, and change user role can fail. For fresh installations of version 7.6, the issue only prohibits resetting the user's password. In both cases, the edits fail with the following message:

  ```
  Error performing User action.
  ```

  During a password reset operation, the user name only displays with the characters before the ampersand.
- In OpsCenter 7.6, you can add and monitor NetBackup 2.6 appliances. You can also collect certain hardware information from the appliances.
- Extra steps are required to access the OpsCenter console using Internet Explorer version 6, 7, or 8 on a 32-bit Windows computer. For more information, see "About web browser considerations" in the *NetBackup OpsCenter Administrator's Guide*, available from the following location:
  http://www.symantec.com/docs/DOC5332

- If you perform a search search for a NetBackup master server with the status **Retired** and put its data on hold, the hold process fails with the following error:

  ```
  Cannot put images on hold; getting the 'Master Server Not
  Connected' error.
  ```

- During OpsCenter 7.6 installation or upgrade on a UNIX system, ensure that the Korn shell (`ksh`) is installed on the host where you want to install or upgrade OpsCenter 7.6 Server.

  Warning: If you fail to install `ksh` before installation or upgrade, you may not be able to log in to the OpsCenter web interface.

- A cloud metering data collection failure can occur if one or more media servers with credentials to access a cloud storage server (data movers) is unreachable for some reason.
  Workaround: From the unreachable media server, use `tpconfig` to remove the credentials of that media from all cloud storage servers on the master. Cloud metering data collection should then succeed. All the cloud metering data from the media servers that were missed earlier can now be collected.
- In the OpsCenter Analytics View Builder, if you move a node that has any objects that are assigned to it within a view, the object may seem to appear missing after the move operation. In this case, the object is temporarily invisible and becomes visible over time.
  To work around the issue, Symantec recommends that you wait for some time and then log back in to the view builder to see the updated view.

  Note: Objects may take several hours or a couple of days to reappear in the view builder.

- In NetBackup OpsCenter 7.6 and earlier releases, data collection by OpsCenter fails if the specified basic-disk storage unit (STU) path is more than 256 characters. To work around the issue, you must create a storage unit path that has 256 characters or less.
- Certain reports do not show any data when the **Include Accelerator Job Only** filter is applied for a NetBackup master server at Version 7.5 or 7.5.0.x. These reports include any Tabular Backup reports or any Custom reports that include accelerator data-related columns. The reports do not show any data because NetBackup Accelerator support is enabled in NetBackup OpsCenter 7.6.

To work around the issue, do not apply **Include Accelerator Job Only** on NetBackup OpsCenter 7.6 reports for a master server that runs NetBackup 7.5 or NetBackup 7.5.0.x.

- The Browse functionality in Operational Restore is not usable with some variants of the Internet Explorer 8 browser. To use the Browse functionality in Operational Restore, Symantec recommends Internet Explorer 9 or newer, or Firefox.
- For OpsCenter restore, the **Browse and Select client** functionality result displays the NetApp volume as the client name for Replication Director VM backups. This selection does not display any files. For browsing the files and directories and for performing an operational restore, it is necessary to select the actual VM client name.
- Starting from NetBackup OpsCenter 7.6, the following products are not supported:
  - Enterprise Vault (EV)
  - IBM Tivoli Storage Manager (TSM)
  - EMC NetWorker (EMC)

  In OpsCenter 7.6, you cannot collect data from EV, TSM, or EMC servers. Therefore, you cannot generate reports for these products. You also cannot view the data specific to EV, TSM, or EMC NetWorker using the OpsCenter web interface or the OpsCenter View Builder interface. If you have upgraded to OpsCenter 7.6 (or manually upgraded the database), the data specific to EV, TSM, or EMC is still retained. You can retrieve this data using the custom SQL option on the OpsCenter web interface. Navigate to **Reports** > **Create New Report** > **Run SQL Query** to use the custom SQL option.

  For more detailed information on product support in OpsCenter 7.6, see the *NetBackup OpsCenter Administrator's Guide*.
- During an OpsCenter database upgrade, if you have customized the `database.conf` file, make sure that it contains only the database location string. If the file contains characters or strings other than the database location, a database upgrade does not succeed. Please note, if you want to change the database path, you should replace the original path with the new one instead of commenting out the original path. If you need a reference, you can create a backup copy of the original `databases.conf` file with a different file name.

  For more information on this issue, please see the following tech note on the Symantec Support website:
  - http://www.symantec.com/docs/TECH205138
- The reports email may not be received when the reports are scheduled in bulk.

If the size of the attachment in the report email exceeds the SMTP server limit, then you cannot receive the report email.

- In OpsCenter 7.6, you cannot assign any alerts to a newly added OpsCenter user. The new users are not listed on the **Monitor** > **Alerts** page in the **Assigned To** column. New users must log in to OpsCenter first before they appear in the **Assigned To** column. Once a user appears in the column, you can then assign the alerts to that specific user.
- A newly created user is not listed in the combo box (drop-down list) for **Copy User Profile**.

  As a new user, to work around this issue you have to log into OpsCenter with the newly-created user name and then log out. The new user name gets registered with **Copy User Profile** after it has logged in at least once. The user name should then appear in the **Copy User Profile** drop-down list.
- If the Backup Exec server password contains HTML characters such as &, <, >, or /, and you make edits to the Backup Exec data collector on OpsCenter, it causes the data collection to fail.

  To resolve the issue, you can use one of the following workarounds:

  - Change the password of the Backup Exec server to a non-HTML character password.
  - Delete the existing entry of the Backup Exec data collector and add a new entry.
- When jobs are viewed from OpsCenter Monitor, the **File List** tab shows up empty for active jobs.

  In OpsCenter 7.5 and forward, the **File List** tab appears to be empty when the job is in progress. The **File List** tab gets populated only when the job is successfully completed.
- Users that are part of a subgroup with special characters do not get authorized.

  If a subgroup name has special characters, then the authorization fails to return the parent or chain-of group names. The parent or chain-of group names are required to determine if any of the parents is an OpsCenter user. Therefore, users who are part of subgroup that contains special characters like "PD_#QE%" do not get authorized.
- After you install OpsCenter, if you run a third-party utility, such as `version.sh` in Tomcat, you get the following error message:

  'Neither the JAVA_HOME nor the JRE_HOME environment variable is defined'

  If you encounter this issue, use the following workarounds:

  - For Windows: After you install OpsCenter, you have to first execute the command `setEnv.bat` and then run any third-party utility.

The path for `setEnv.bat` is *INSTALL_PATH*`\OpsCenter\server\bin`.

- For UNIX: After you install OpsCenter you have to first execute the command `setEnv.sh` and then run any third-party utility.

  The path for `setEnv.sh` is `<`*INSTALL_PATH*`>/SYMCOpsCenterServer/bin`.

Note: The `version.sh/bat` file is a Tomcat script and it is advised that you not modify it. You have to run the `setEnv.sh/bat` file and run the `version.sh/bat` file to find the Tomcat and JRE versions.

- As of OpsCenter 7.5, Symantec OpsCenter Agent supports 64-bit software on Windows systems. 32-bit Agent software is not supported on 64-bit Windows systems in versions 7.5 and later. The installer automatically installs 64-bit Agent software on a 64-bit Windows system.
- In the SFR Timeline View, for the images that are collected in OpsCenter, the data format is shown as `unknown` because of the lack of data.
- OpsCenter does not support creating or editing multiple reports simultaneously for the same user session from different tabs or windows. You cannot open the same OpsCenter console in two or more browser tabs or windows and create or edit standard and custom reports simultaneously. That causes an exception to occur.
- The Deduplication reports do not show any data when you select the **Report On** parameter as **Storage Unit Name**.
- For VMware or Hyper-V clients, the search and restore operations work only if the client name is the same as host name. If the client name is the same as display name, UUID, or DNS name then only the Search functionality is available. You cannot perform restore operations in this case. The following table provides details on whether Search and Restore functionality is available when the client name is the host name, display name, etc.:

Client Name Type	Search	Restore
Host Name	Yes	Yes
Display Name	Yes	No
UUID	Yes	No
DNS Name	Yes	No

- OpsCenter installation and deployment information and best practices.

  The following list contains information about installing OpsCenter and some best practices information:

- Symantec recommends that you do not cancel or interrupt the installation process once it is started.
- You may be unable to log on to the OpsCenter interface if it is installed on a server that has an underscore (_) in the host name. To avoid this issue, ensure that the OpsCenter Server host name does not contain any underscores like `opshost`.
- Installing OpsCenter components in a location that is mounted from a remote host is not supported.

- A file selection list that contains more than 50 items does not appear in OpsCenter.

  For a specific job ID in an OpsCenter Analytics custom report, breakup job data is available only for 50 job directories. That is because when a NetBackup policy or job is associated with more than 50 backup selections, data is available for only 50 backup selections. The NetBackup user interface truncates data for the subsequent backup selections (greater than 50).

  With VBR, you can view the breakup job information for all of the job directories that are associated with a job or policy. That is because data collection in VBR happened through CLI's (and not through `nbsl`).

- OpsCenter does not provide the option to purge breakup jobs.

  Unlike VBR, OpsCenter does not provide the option to purge breakup jobs. In the VBR console, you can purge specific breakup jobs from the **Settings** > **Global Settings** > **Data Retention** section.

- An uninstall script is removed if an uninstall process for an OpsCenter Server or Agent is canceled or interrupted.

  If an uninstallation process for OpsCenter Server or Agent is canceled or interrupted on UNIX, then the uninstall script (`uninstallOpsCenterServer` and `uninstallOpsCenterAgent`) is removed from `/opt/VRTS/install`. If you want to uninstall the OpsCenter Server again, you can use the uninstall scripts from the OpsCenter DVD.

- Some result sets for a stored procedure that has multiple result sets may not appear.

  When you run a stored procedure that has multiple result sets, the output of only the first result set is displayed on the interface. The output of other result sets is not shown on the interface.

- The number of characters for a virtual name by the clustering technology on Windows is limited.

  The virtual host name must be the short name (not FQDN) and less than 15 characters.

- Some reports may only consider Full and Incremental schedule type jobs.

On applying Schedule/Level Type filter with value **All**, the following reports consider only Full and Incremental schedule type jobs:

- Advanced Success Rate
- All Failed Backups
- Consecutive Failures Report
- Success Rate Line

- The `NetBackupOpsCenter` resource is offline after you have installed an OpsCenter cluster.
  After installing an OpsCenter cluster on a Windows 2008 R2 x64 system, you must manually bring the `NetBackupOpsCenter` resource online. You can bring the `NetBackupOpsCenter` resource online from the command line interface or by using the cluster user interface.
  You can use the following command:
  `hares -online <resource name> -sys <Name of the active node>`
  `Example: hares -online newonelatest-OpsCenter -sys OPS-CLUSTER-1`

- On Windows systems, the `log.conf` file is not created properly. That causes the `vxlogview` to return a `No logs to be displayed` message.

  Use the following commands to view logs for OpsCenter GUI (OID-147) and Infrastructure components (OID-761):

  - OpsCenter GUI:
    - `<INSTALL_PATH>\OpsCenter\server\bin\vxlogview -p 58330 -o 147 -G`
    - `<INSTALL_PATH>\OpsCenter\gui\logs`
  - Infrastructure components:
    - `<INSTALL_PATH>\OpsCenter\server\bin\vxlogview -p 58330 -o 761 -G`
    - `<INSTALL_PATH>\OpsCenter\gui\logs`

- The object merger utility in OpsCenter fails on the master server.
  The object merger utility in OpsCenter (**Settings > Configuration > Object merger**) does not work (fails) for a master server. The object merger utility works for clients and media servers.

- The **Custom Tabular Backup and Custom-Client count** report does not return data after an upgrade from VBR.
  The **Custom Tabular Backup and Custom-Client count** report does not return any data after you have upgraded from VBR to OpsCenter.

To work around this issue, you must manually change the filter settings to get the correct report data after the upgrade is complete. The following steps guide you to change the filter settings:

- Open the report, then select **Edit Report**.
- From the **Filters** section, select **Job**.
- From the **Column** drop-down list, select **Product Type**. The default operator is the equals sign character, **=**.
- From the **Value** drop-down list, select the same product type that you selected for VBR and click **Add**.
- Click **Next** to view the report. Once the changes are made, the reports display the correct data.
- Save the report.

- The OpsCenter server can stop receiving events from the master server after a NetBackup upgrade.

  If all following conditions are applicable, add the **OPS_CENTER_SERVER_NAME** entry to the `bp.conf` file on UNIX or the registry on Windows to set OpsCenter's server name. Symantec recommends that you do add the entry before you attempt to upgrade.

  - The **REQUIRED_INTERFACE** is configured on the master server.
  - The OpsCenter server monitors the master server.
  - The **OPS_CENTER_SERVER_NAME** entry is not configured on the master server

  If you do not add this entry, the OpsCenter server stops receiving events from the master server after the upgrade.

- An enhancement has been made in OpsCenter to maintain VBR parity.
  You can now search for clients from the **Monitor** > **Hosts** > **Clients** page. You can use host names or substrings to accomplish that.
  However, you can only search for clients and not other attributes such as, **CPU Count**, **CPU Speed**, **Discovered Agent Server**, and others.

- An issue occurs in the **Job Count Workload Analyzer**: For each cell, the sum of occurrences differs from the total in the first column when the time basis that is selected is Active. That is expected because a job can be active and span across a multiple-hours time frame. Hence, the same job is counted for all the hours. But the count in the first column shows the exact count of jobs that were active for these seven days. That is different from the implementation of Time basis=**Start** or **End**. In these cases, the sum of the occurrences in the cell match with the number displayed in first column.

- The **Master server job throughput** report appears without a report output in **My dashboard** after an upgrade from NOM to OpsCenter. The reason is that it is an SQL query-based report and is a part of composite report that is not migrated in the dashboard.
- Daylight savings time (DST) support for Historical reports in OpsCenter
  If data for the historical reports is synchronized during the hour when daylight savings time begins, it can cause problems in a distributed database system. The user can also lose data.
  A workaround is to use Universal Time (UTC) as the time zone, or use a time zone that does not have daylight savings time.
  To set the time zone, refer to the *Symantec OpsCenter Administrator's Guide*.
- When you upgrade from OpsCenter 7.0.x to OpsCenter 7.x, the Installation Choice screen displays the available space on the system drive. This issue occurs even if your previous installation is on a different drive (a drive other than the system drive).

Known issue in upgrading OpsCenter cluster setup to 7.6

While upgrading from Opscenter 7.1.x or 7.x cluster to 7.6 cluster, there may be a problem in getting shared drive access during installation or upgradation. Due to a configuration issue, installer may not get access of shared drive which in turn causes an issue in creating the domain.

To create domain again in cluster,

1. Freeze the cluster setup.
2. Stop the OpsCenter services.
3. Open **security.conf** file on the path **Shared_Drive\OpsCenter\Server\config**.
4. Change the value of parameter **vxss.initialized** from **False** to **True** (vxss.initialized = True).
5. Restart the OpsCenter services again.
6. Unfreeze the cluster setup.
7. Access OpsCenter.

Replication Director notes

With OpenStorage integrations like Replication Director, the partner releases their plug-in separately from the NetBackup media. For NetApp, the name of this plug-in is “NetApp Plug-in for NetBackup” (NetApp plug-in). For this release, the NetApp plug-in was made available for Beta in early January 2013 on the NTAP website.

The following list contains the known operational notes that apply to the NetBackup Replication Director feature and its associated plug-ins:

- SnapVault replications can fail when the NetApp Plug-in for NetBackup version 1.1 is used with DataFabric Manager 5.2P1 on Windows and the default login protocol is `rsh`.

  Workaround: Set the default login protocol to `ssh` on the NetApp DataFabric Manager server.

- Replication Director replications may fail after a Point-in-time restore is performed.

  This issue relates to replication job failures for the policies that are configured for Replication Director. This issue occurs when version 1.1 of the NetApp Plug-in for NetBackup is used under the following circumstances:

  - First, the Replication Director policy runs successfully. The policy uses an SLP that contains a Snapshot operation of the primary data, as well as a Replication (SnapVault) operation in the topology.
  - Next, one or more Point-in-time (PIT) restores are performed successfully from the volumes in the policy with the following option enabled: **Force rollback even if it destroys later snapshots**.

  The replication jobs fail the next time that the policy runs. The DataFabric Manager server produces the following error message:

  ```
  DFM Job (On-demand Protection) is failing with Error base
  snapshot for transfer no longer exists on the source.
  ```

  The replication jobs fail because the PIT restore deletes the base snapshot (given that the specified option was enabled for the restore). The Replication operation did not have the base snapshot to replicate.
  To return to successful replication jobs, resynchronize the relationship between the primary volumes and the target volumes using the NetApp CLI.

- If using NetApp SAN devices, an unsupported Windows version may cause a Backup From Snapshot job or a snapshot import to fail with status code 4213 (Snapshot import failed) when using LUNs. The state of the snapshot device cannot be detected properly if the version is not Windows 2003/2008 R2. Windows 2012 is supported for NetApp NAS devices only.
- NetBackup 7.6 supports both Version 1.0.1 and Version 1.1 of the NetApp Plug-in for Symantec NetBackup. However, Version 1.0.1 is only compatible with the features that are present in NetBackup 7.5. To take advantage of the latest features and functionality, you must update the plug-in to Version 1.1.
- For Version 1.1 of the NetApp Plug-in, replication can fail with error code 84 (media write error) if both of the following conditions are true:

- The NetBackup policy has backup selections that are volumes coming from multiple DFMs (configured in NetBackup as a storage unit group).
- The SLP has a fan-out topology (multiple replications coming from the same source). The following is an example of fan-out topology:

```
Snapshot
 |
 -------------- Replication (SnapVault)
 |
 -------------- Replication (SnapMirror)
```

Workaround: If you have a fan-out topology, configure policies so that they have volumes from a single DFM (split the policy into multiple policies).

- Changes were made to `bpfis` to pass different XML to provide different backup selection results.
- NetBackup has to send a **delete call** if a user deletes a policy and it has no catalog entries.
- Currently, the state of the storage server that is specified in a disk pool is not verified. If the state of the disk pool is **DOWN**, then the policy validation should fail.
- A policy may get validated if the volume is in an offline state and the snapshot fails with a status 20 error.
- If there are READ_ONLY volumes or volumes that are full with no space remaining on the filer, then the backup job can fail with the following error.

  ```
  invalid command parameter(20)
  ```

  To work around this issue, use `VOLUME_EXCLUDE_LIST` to exclude the read-only volumes.
- When you add credentials, if a short name is used when you add the ESX server in the VMware server credentials, it fails to prompt to the expected server name. Subsequent attempts also fail with the following message:

  ```
  Server not found.
  ```

  The first attempt to add credentials makes an entry in EMM database. To work around this issue, use the `nbemmcmd` from the command line interface to remove the ESX server entries.
- VxFS is supported with VxVM only. VxFS is not supported directly on disks in this release of NetBackup.
- Linux logical volume manager (LVM) is not supported.
- Native file system on partition fails with an EXIT 130 status on RHEL.

- Use of an LSU from multiple storage servers under one policy is not supported.
- Multiple failures can display the same error code as the end result.
- Replication index can fail with an exit status 226 when an SLP is configured as **snapshot > backup** from **snapshot > snapshot replication > index from replica snapshot**.
- Policy validation fails for `vxdmp` configured devices.
- You should explicitly exclude `/vol/vol0` from the backup if the **All_FileSystems** directive is used.
  The `VOLUME_EXCLUDE_LIST` parameter = `/vol/vol0`
- If you have **Backup from Snapshot** or **Index from Snapshot** configured using Storage Lifecycle Policy, and VMware snapshot deletion takes a long time (over 10 minutes), it is possible that these two operations can overlap. When that happens, the **Backup from Snapshot** or the **Index from Snapshot** job, for that particular VM whose snapshot takes a long time to be deleted, can fail.
- Replication Director for VMware virtual machines does not support NDMP, Instant Recovery, and Accelerator.
- When you browse the files in the **Backup, Archive, and Restore** user interface, the following error may be reported:
  `ERROR: database system error`
  This message can indicate a variety of issues, such as an unsupported file system, a snapshot mount failure, or other hardware or networking problems.
- The size of the `ncflbc` and `ncfnbhfr` logs that are generated as a result of an indexing job can be very large. The size of the log files can grow rapidly when the log level is set to 4 or higher.
  To work around this issue, you can lower the NCF logging level (to 3 or less). In addition, you can adjust the log file rollover mode, maximum log file size, or number of log files if you want to continue to accommodate a higher NCF logging level.
- Discovery can fail on virtual machines running vCenter 2.5 or ESX 3.5 and older. Note that vCenter versions before version 4 are not officially supported.
- A hardware snapshot occurs on a boot disk even when **Virtual disk selection** is set to **Exclude boot disk** on the **Advanced** options of the **VMware** policy tab.
  This option only applies when a Backup From Snapshot operation is performed and a tar image is created of the VM in the snapshot.
- A NetBackup Accelerator-enabled backup operation in an SLP can fail with status code 13 (file read failed) if it encounters very slow storage read speeds.

In particular, the issue occurs when NetBackup cannot read at least 500 MB of data in five minutes.

Workaround: Adjust the global client timeout value from the default five minutes (300 seconds) to a larger value, such as 10 minutes (600 seconds). You can make the adjustments in the NetBackup Administration Console (**Host Properties > Timeouts > Client read timeout**) or in the `bp.conf` file (`CLIENT_READ_TIMEOUT = 600`).

- For Oracle Intelligent Policy, instance group names cannot be localized.
- For VSS, the Volume GUID is not supported.
- For policies with alternate client configuration, the Activity Monitor may show the wrong value in the **Kilobytes** column for snapshot jobs.
- A snapshot job of an NFS mount can fail with status code 20 on Linux due to an NFS remount failure. However, subsequent runs of the snapshot job may succeed.
- Certain actions can fail with error 4213 in a VxVM environment. The actions include live browse of backup images, index from snapshot, and backup from snapshot.

  For more information about this issue, see the following tech note on the Symantec Support website:

  http://www.symantec.com/docs/TECH209057
- Replication Director for VMware uses automatic selection of VMs based on a query (the **Select automatically through query** option in the policy). In the policy's Query Builder, you can use the **Test Query** option as a pre-test of the selection criteria to see which VMs Replication Director plans to back up.

  In some cases, the VMs listed in the test query results may not be identical to the VMs that get selected when the backup runs. If a VM resides on a VMFS datastore rather than an NFS datastore, Replication Director does not select the VMFS VM for backup. The Test Query option may incorrectly indicate that the VMFS VM will be included in the backup. (When the backup runs, the job details show that the VM does not meet hardware requirements.)

  Review the Test Query results carefully. Note that only VMs on an NFS datastore get backed up by Replication Director.
- The NetApp Plug-in for Symantec NetBackup version 1.0.1 can crash under the following circumstance:
  - Running an NDMP storage lifecycle policy
  - Export workflow (indexing, backup, restore or browse)
  - Export for copy 2 or 3 (not for copy 1)

To work around this issue, upgrade to the latest version of the NetApp Plug-in for Symantec NetBackup that contains a fix to this issue.

- You may experience replication failures if you use the NetApp Plug-in for Symantec NetBackup version 1.0.1. Replication can fail if all the following conditions are met:
  - Multiple volumes are present in the backup selections
  - The destination is SnapMirror
  - At least 60% of the volume is full
  - NAS storage is used

  The following are some of the symptoms that may indicate failures:
  - In the NetBackup Activity Monitor:

    ```
    Replicate failed for backup id <backup id>
    with status 174 failed waiting for child process  (34)
    ```

  - In the `bpdm` logs:

    ```
    Error bpdm (pid=19319) <async> wait failed:
     error 2060001: one or more invalid arguments
    ```

  - In the NetApp Management Console:

    ```
    destination volume too small; it must be equal to
    or larger than the source volume
    ```

- For NetApp, there is an issue when you clean up **ALL** images for a policy that has a Primary > Mirror topology. You may experience snapshot leaks where the snapshots are deleted from the NetBackup catalog but not deleted from storage.

  To delete the snapshots and reclaim storage, execute the following command on the DataFabric Manager (DFM) server:

  ```
  snapmirror release <src_vol> <dst_filer>:<dst_vol>
  ```

- You may receive the following warning when you restore from an incremental backup that was created with Replication Director:

  ```
  Warning: unable to obtain list of files using specified search
  criteria.
  ```

  NetBackup performs the differential or the cumulative incremental backups that are indicated in a backup policy, even if there are no file changes to back up.

Since there have been no file changes since the last backup, the image for the incremental backup contains no files. However, the Backup, Archive, and Restore interface presents the user with an icon for that empty incremental backup. When the user selects the icon, the message appears. To access images, select the icon for the previous backup.

- If using Data ONTAP 8.1.1 or 8.1.2, the length of the path to any file that is backed up should not exceed 529 characters. If the path exceeds 529 characters, point-in-time rollback restores and SnapVault copy exports fail. Copy-back restores continue to work. To recover or import the data from a SnapVault copy, upgrade to ONTAP 8.1.3.
- Replication Director for virtual machines:
  If the virtual machine and its datastore have identical names, the BAR restore interface displays two separate images when you browse to restore the virtual machine or its files. The image with an `OST_FIM` image format should not be displayed. If the virtual machine has more than one datastore, this `OST_FIM` image may not present all the data that the virtual machine contains. Do not use the `OST_FIM` image: Select the other image for restore.
  This issue will be fixed in a future NetBackup release.
- If the storage lifecycle policy (SLP) was not configured to index the virtual machine (or indexing is not complete), the BAR interface accesses the files directly from the snapshot. When you browse the files, the message `ERROR: database system error` may appear. This message can indicate a variety of issues, such as an unsupported file system, a snapshot mount failure, or other hardware or networking problems.
- Problems with backups and restores exist on RHEL 5.3 operating systems with kernel version 2.6.18-128.el5. Backups and restores from snapshots do not work properly because of an issue with the `kobject_add` process. The issue occurs because NetBackup 7.6 does not support this kernel version. This kernel version is supported with the release of RHEL 5.9.
  For more information, refer to the *NetBackup Replication Director Solutions Guide*.
- NetBackup Windows Client backups fail when NetApp and CIFS shares are configured with certain security and access privileges.
  If a NetApp volume is configured with a “Mixed” security style and is used with a NetApp CIFS share that does not give read access to the client user, then client backups fail. This issue only occurs when the NetApp volume is configured with the “Mixed” security style. This issue does not affect the volumes that are configured with NTFS or UNIX styles.
  A workaround for this issue is to add explicit read access on the CIFS share to the user under which the NetBackup client service is running.

- The NetApp Qtree fan-in configuration is not supported with Replication Director.
- Replication Director does not support backup and restore of snapshots on a NetApp volume that contains a mix of Qtree and non-Qtree data. Backups and restores are supported if the volume contains one or the other.
- The time on the NetBackup servers, the DFM server, and the filer must be synchronized or have a difference of less than 5 minutes.
  The time on the Windows domain controller and the filer must be synchronized or have a difference of less than 5 minutes. If the difference is greater than 5 minutes, the filer does not give the Windows client CIFS share access. This issue results in an error on the filer console.

NetBackup SAN Client and Fibre Transport notes

The following list contains the operational note information that pertains to SAN Client and Fiber Transport:

- NetBackup Client Encryption Option is not supported.
  The NetBackup Client Encryption Option is not supported on UNIX and Linux SAN clients.
- A QLA-2344 four-port FC adapter's usable aggregate performance is not significantly greater than a two-port QLA-2342 adapter.
  The QLA-2344 four-port FC adapter's usable aggregate performance is not significantly greater than a two-port QLA-2342. That is true when the QLA-2344 four-port FC adapter is used in the same PCI-x slot for SAN Client target mode. The advantage that a QLA-2344 HBA offers is the ability to spread its aggregate performance over four ports instead of two.

  The QLA-2344 HBA performs similarly to two QLA-2342 HBAs but uses one less PCI slot if the following is true:

  - If you use a direct-connection (rather than FC switches or bridges) between SAN clients and a Fibre Transport (FT) media server.
  - And only two ports are fully loaded with Fibre Transport traffic at the same time.
- IBM 6228 HBAs require an AIX FC driver.
  IBM 6228 HBAs require the following version of the AIX FC driver to ensure that the appropriate data is returned when a task is aborted. Not installing the following driver can result in a hung Fiber Transport (FT).

  ```
  AIX FC driver version level 5.2.0.75 for IBM 6228 card _ AIX
  Oslevel 5200-07
  ```

- For 64-bit NetBackup media servers, PCI-express, and PCI-X slots are supported for the QLogic Fibre Channel HBAs.
  For 64-bit NetBackup media servers, PCI-express, and PCI-X slots are supported for the QLogic Fibre Channel host bus adapters (HBAs) that are used to connect to the NetBackup SAN clients. `Legacy PCI 33 and 66 Mhz` slots are not supported.
- On the NetBackup media servers, Symantec recommends that you do not use legacy PCI cards on the same bus as a QLogic FC HBA that is used to connect to SAN clients.
  On the NetBackup media servers, Symantec recommends that you do not use legacy PCI cards on the same bus as a QLogic FC HBA that is used to connect to SAN clients. A slower PCI card reduces the speed of the controlling bus and therefore all other cards in that bus. Consequently, data transfer rates are reduced and performance is degraded.
- Data compression or encryption can cause the Fibre Transport pipe performance to degrade significantly for backups and restores.
  If you use data compression or encryption for backups, backup, and restore Fibre Transport pipe performance may degrade significantly. In some configurations, compression may reduce performance by up to 95% of uncompressed performance.

NetBackup Search notes

This section contains the operational notes and known issues that are associated with Search in this release of NetBackup.

- If client backup indexing jobs consistently fail with status codes 5025 or 5027, it may be a symptom of a corrupt index. In some cases, the issue is a result of a disk error.
  See "Resolving failed backup indexing jobs due to a corrupt index" on page 102.
  For more information, see "Suspending and resuming indexing jobs," "Marking an index as invalid," and "Re-indexing backup images" in the *NetBackup Search Administrator's Guide*, available from the following location:
  http://www.symantec.com/docs/DOC5332
- A Search & Hold operation in NetBackup OpsCenter can fail with the error "Master Server Not Connected" after a master server has been reinstalled.
  The issue occurs because two master server entires now exist in the OpsCenter database. If you encounter this issue, please contact Symantec Support.
- An Index for Search job or an Index Cleanup for Search job can hang for a very long time on a loaded system and may not recover.

This issue is a result of socket connection issues between the indexing server and the master server. The following symptoms may indicate that the job has encountered this particular issue:

- Several hours have passed and there is no change in the **Files** count for an Index for Search job in the Activity Monitor.
- Any similar indexing jobs (that were started after the hung job was started) complete successfully.
- Certain running indexing processes (`nbci` and `nbcidelete`) do not log anything in the `ncfnbci` logs for hours.

If the job exhibits these symptoms and remains hung for more than 24 hours, use the following steps to work around the issue:

1. In the Activity Monitor, go to **Job Details > Detailed Status > Status** of the hung job and record the `pid` number. For example, `RUNCMD (pid=12345)`.
2. On the indexing server host of the hung job, go to the task manager and find the process using the `pid` number. The process is `nbci` for Index for Search jobs and `nbcidelete` for Index Cleanup for Search jobs. End that particular process.
3. After the process ends, the job fails with either status code 50 (client process aborted) or status code 150 (termination requested by administrator). For status code 50, the job automatically re-initiates. For status code 150, the job needs to be manually re-initiated.

   For more information, see “Re-initiating indexing jobs that have failed” in the *NetBackup Search Administrator's Guide*, available from the following location:

   http://www.symantec.com/docs/DOC5332

- Indexing jobs may fail with status code 25 (cannot connect on socket). This issue can occur on stressed or loaded systems due to a timeout occurring during socket connection operations in indexing processes (`nbci` and `nbcidelete`).
  Workaround: Reduce the maximum indexing jobs that can run in parallel on the indexing server from the host properties of the master server. From the NetBackup Administration Console, select **Host Properties > Global Attributes > Maximum indexing jobs per index server** and change the value.
  You must re-submit failed indexing jobs using the `nbindexutil -add` command. Refer to the "Re-initiating indexing jobs that have failed" section in the *NetBackup Search Administrator's Guide* for more details.

NetBackup SharedDisk support notes

- The SharedDisk option was no longer supported beginning with the NetBackup 7.0 release.
- You can use a NetBackup 7.x master server to configure, manage, and operate SharedDisk on NetBackup 6.5 media servers.
- For information about using SharedDisk, see the documentation for your NetBackup 6.5 release.

NetBackup Snapshot Client notes

This section contains the operational notes and known issues that are associated with NetBackup Snapshot Client in this release.

- A **Standard** policy that is configured with the following selections causes the NetBackup Policy Execution Manager (`nbpem`) to crash and to core dump with an assertion failure:

  ```
  Policy storage = lifecycle policy with only a Snapshot target
  Perform snapshot backups
  Retain snapshot for Instant Recovery or SLP management
  Perform off-host backup
  Use: Data Mover
  Machine: Network Attached Storage
  Options: Snapshot method for this policy = NAS_Snapshot
  ```

  Although this configuration is normally supported, it is not recommended. SLPs offer no benefit in this configuration because they do not perform any further operations on the snapshot. An NDMP-generated NAS snapshot cannot be converted to a TAR image by an SLP.

  To work around this issue, Symantec recomends that you set the policy storage to an actual storage unit.

- A point-in-time (PIT) restore from a VxVM-based plex snapshot can fail with status code 5 (the restore failed to recover the requested files).

  This issue occurs if the restore is attempted while another plex snapshot of the primary volume exists in the `SNAPDONE` state. However, the resync operation completes in the background even though the failure is reported. Further attempts to restore the snapshot from the catalog also fail. The snapshot remains intact only if no writes are performed on the primary volume.

Warning: If you encounter this issue, ensure that no writes are made on the primary volume.

An EEB has been issued that addresses this issue. If you believe that you could encounter this issue in your NetBackup environment, contact Symantec Support to obtain the EEB. If you have already encountered this issue, use the following workaround to manually retain the snapshot that was used for the PIT restore.

Workaround: Confirm that the background resync operation is finished by running the following command:

`/usr/sbin/vxprint -g <DG_NAME_ON_WHICH_PRIMARY_VOLUME_RESIDES> -q -t -e 'assoc="<PRIMARY_VOLUME_NAME>"'`

If the resync operation is finished, all of the plexes should be in the `SNAPDONE` state except the first, such as in the following example:

```
pl vol1-01      vol1         ENABLED  ACTIVE   4194304  CONCAT    -        RW
pl vol1-02      vol1         ENABLED  SNAPDONE 4194304  CONCAT    -        WO
pl vol1-03      vol1         ENABLED  SNAPDONE 4194304  CONCAT    -        WO
```

Once the resync operation is finished, manually perform a backup job of the snapshot from the NetBackup Administration Console. That ensures the snapshot that was used for the PIT restore gets retained.

- NetBackup does not support creating a disk array snapshot if a VxVM disk group on the array contains a software-based snapshot of the VxVM volume.

  If a software-based snapshot (such as from the VxVM method) already exists of a VxVM volume on the disk array, NetBackup cannot create a disk array snapshot of a file system that is configured on the VxVM volume. Snapshot creation fails (with final status 156), and the `bpfis` log contains a message that reports a `vxmake` command failure.

  You must delete the existing VxVM snapshot from the VxVM disk group before you run a backup with a disk array snapshot method. This issue will be fixed in a future release of NetBackup.

  Examples of disk array snapshot methods are EMC_CLARiiON_SnapView_Snapshot, HP_EVA_Snapshot, Hitachi_CopyOnWrite, and IBM_StorageManager_FlashCopy. All disk array methods are described in the *NetBackup Snapshot Client Administrator's Guide*, in the chapter titled "Configuration of snapshot methods for disk arrays."

- Instant Recovery restores can fail from a backup that a FlashSnap off-host backup policy made.

  From a policy that was configured with the FlashSnap off-host backup method and with Retain snapshots for Instant Recovery enabled, the backups that were made at different times may create snapshot disk groups with the same name. As a result, only one snapshot can be retained at a time. In addition, NetBackup

may not be able to remove the catalog images for the snapshots that have expired and been deleted. It appears that you can browse the expired snapshots and restore files from them. But the snapshots no longer exist, and the restore fails with status 5.

- The following items pertain to restoring individual files from an Instant Recovery snapshot:
  - When you restore files from a snapshot that is made for an Instant Recovery off-host alternate client backup: NetBackup consults the exclude list on the alternate client even when it restores files to the primary client. If the exclude list on the alternate client is different from the exclude list on the primary client, any files that are listed in the exclude list on the alternate client are not restored to the primary client.

    For example, if the alternate client's exclude list has the entry *.jpg, and some .jpg files were included in the primary client backup, the .jpg files can be selected for the restore but are not in fact restored. To restore the files, you must change the exclude list on the alternate client.
  - When you restore files from a snapshot that is made for an Instant Recovery backup (local or off-host alternate client): If the exclude list is changed after the backup occurred, NetBackup honors the latest version of the exclude list during the restore. Any of the files that are listed in the current exclude list are not restored. Also, as noted in the previous item, the exclude list on the alternate client takes precedence over the exclude list on the primary client.

    For example: If the current version of the exclude list has the entry *.jpg, and some .jpg files were included in the backup, the .jpg files can be selected for the restore but are not in fact restored. To restore the files, you must change the exclude list on the primary (or alternate) client.

    Note: For ordinary backups (not based on snapshots), any files that were included in the exclude list are not backed up. For snapshot-based backups, however, all files are included in the snapshot. The exclude list is consulted only when a storage unit backup is created from the snapshot. If the snapshot is retained after the backup (for the Instant Recovery feature) and the snapshot is available at the time of the restore, NetBackup restores files from the snapshot. Since all files are available in the snapshot (including those that would be excluded from a storage unit backup), NetBackup incorrectly consults the current exclude list on the client or alternate client. Any files in the exclude list are skipped during the restore.

    This issue will be addressed in a future release of NetBackup.

- Problem with "Restore from Point in Time Rollback"
  When you start a "Restore from Point in Time Rollback" from an Instant Recovery backup, the primary file system is verified against the snapshot to make sure that no new files were created on the primary file system after the snapshot was taken. Note that a rollback deletes all files that were created after the creation-date of the snapshot that you restore. Rollback returns a file system or volume to a given point in time. Any data changes or snapshots that were made in the primary file system after that time are lost as a result of the rollback.
  However, during the verify operation for the rollback, the snapshot is mounted and in some cases, the snapshot cannot be unmounted. In that case, the Point in Time Rollback operation is aborted.

  Note: For a rollback of a database backup such as Oracle, the file system verification is mandatory and this issue prevents a successful rollback.

  For a rollback of a file system, you can skip file verification by selecting "Skip verification and force rollback" on the restore dialog. The problem that is described here is avoided and the rollback succeeds.

  Caution: Use **Skip verification and force rollback** only if you are sure that you want to replace all the files in the original location with the snapshot. Rollback deletes all files that were created after the creation-date of the snapshot that you restore.

  See "Instant Recovery: point in time rollback" in the *NetBackup Snapshot Client Administrator's Guide* for more information on rollback.

- HP-UX 11.31 has a limitation that it cannot allow a new device to be present on the same SCSI path where a different device was visible to the host. During the snapshot process, when the old snapshot is deleted and a new snapshot is created, the new snapshot appears on the same SCSI path as the older snapshot. That causes a conflict within the HP-UX system and it logs an error message.
  During a snapshot with NetBackup 7.5 installed on a computer that has HP-UX 11iv3 installed, the Syslog error messages are similar to the following:

  ```
  class : lunpath, instance 15
  Evpd inquiry page 83h/80h failed or the current page 83h/80h
  data do not match the previous known page 83h/80h data on
  LUN id 0x0 probed beneath the target path (class = tgtpath,
  instance = 4) The lun path is (class = lunpath, instance 15).
  Run 'scsimgr replace_wwid' command to validate the change
  ```

```
class : lunpath, instance 15
Evpd inquiry page 83h/80h failed or the current page 83h/80h
data do not match the previous known page 83h/80h data on
LUN id 0x0 probed beneath the target path (class = tgtpath,
instance = 4) The lun path is (class = lunpath, instance 15).
Run 'scsimgr replace_wwid' command to validate the change
class : lunpath, instance 15
An attempt to probe existing LUN id 0x4007000000000000 failed
with errno of 14.
0/3/1/0.0x50001fe150070028.0x4007000000000000 eslpt
0/3/1/0.1.27.0.0.0.7 sdisk
64000/0xfa00/0x69 esdisk
```

The administrators of the HP-UX 11iv3 host machines are requested to ignore the log messages if they encounter them during backups with NetBackup.

- Backup of an AIX 64-bit client with the NetBackup media server (data mover) method and the VxVM or VxFS_Checkpoint snapshot method may fail with NetBackup status code 11. This failure may occur if the client volumes are configured with Storage Foundation 5.0 MP3. A NetBackup message similar to the following appears in the job's Detailed Status tab:

  ```
  12/09/2010 23:23:23 - Error bpbrm (pid=458874) from
  client p5201: ERR - bp_map_open, err 2059
  ```

  This error occurs because the required VxVM libraries for 64-bit AIX are not installed in the correct location. The libraries should be installed in `/opt/VRTSvxms/lib/map/aix64/`.

  ```
  cp /usr/lpp/VRTSvxvm/VRTSvxvm/5.0.3.0/inst_root/
  opt/VRTSvxms/lib/map/aix64/* /opt/VRTSvxms/lib/map/aix64/
  ```

  Note: This issue has been fixed in later versions of Storage Foundation, starting with 5.0MP3RP3, 5.1RP1, and 5.1SP1.

- Regarding snapshot jobs that end with status code 156 or 1541 or other error
  These errors may occur in the following situation: An administrator manually (or by using a script) starts multiple snapshot jobs at a high frequency. (For example, one snapshot job every 5 seconds.)
  At the same time, multiple rotation processes begin. The processes operate on the same catalog information, which includes information about existing snapshots. Because the processes work on the same information at the same time, a problem of inconsistency can occur. Some of the processes delete the snapshots and update the catalog while other processes continue to refer to the obsolete information. The result is that the snapshot jobs can end with status

codes 156 (snapshot error encountered), 1541 (snapshot creation failed), or other unpredictable errors.

This behavior does not occur for scheduled snapshot jobs, as NetBackup controls the job execution.

- A snapshot can fail if the volume name exceeds 15 characters.

  When you create and name a volume, a prefix\ suffix is added to the volume name. If the volume name contains more than 15 characters and the prefix\suffix is added, the snapshot volume name can exceed the limit of 27 characters. When you run the command 'vxassist snapshot', the command does not recognise the lengthy snapshot volume name and so the snapshot fails.

  For example, if the primary volume name is PFItest123456789vol and the suffix 00043c8aaa is added to it, the volume name exceeds the limit. The command 'vxassist snapshot' does not recognise the name 'PFItest123456789vol_00043c8aaa' and the snapshot fails.

  To avoid this it is recommended that you limit the primary volume names to up to 15 characters to create the Vxvm mirror snapshots.

- Snapshot creation fails when the same volume is mounted on multiple mount points of the same host

  For example, when the volume `f3170-7-15:/vol/sample1` is mounted on the mount points `/sample1 on f3170-7-15:/vol/sample1 rsize=32768,wsize=32768,NFSv3,dev=4000033` and `/test1 on f3170-7-15:/vol/sample1 rsize=32768,wsize=32768,NFSv3,dev=4000034` snapshot creation fails with the following error.

  ```
  mount: f3170-7-15:/vol/sample1 is not mounted on /test1
  ```

  The snapshot fails as this type of configuration is not supported.

  The backup of NFS share mounted by two different mount points for OST_FIM is not supported in this release.

Resilient network operational notes

The following are resilient network connection operational notes of which you should be aware:

- Resilient connections apply between clients and NetBackup media servers, which includes master servers when they function as media servers. Resilient connections do not apply to master servers or media servers if they function as clients and back up data to a media server.
- NetBackup protects only the network socket connections that the NetBackup Remote Network Transport Service (`nbrntd`) creates. Examples of the connections that are not supported are Granular Recovery for Exchange,

SharePoint Granular Recovery Technology, and the NetBackup `nbfsd` process are not supported.

- NetBackup protects connections only after they are established. If network problems prevent a connection to be established, there is nothing to protect.

Virtualization notes

This section contains the operational notes and known issues that are associated with virtualization technologies in this release of NetBackup.

- When you execute the `nbrestorevm` command, the usage statement incorrectly mentions a `-vmvxd` option. This option is not valid. Instead, the option should be listed as `-vmvmxd`. This option allows the selection of the VMware VM to be restored to the same datastore where the vmx file exists.

NetBackup for VMware notes

This section contains the operational notes and known issues that are associated with NetBackup for VMware in this release.

- For backup hosts with limited memory, simultaneous backups of VMware VMs may fail due to lack of memory. The `bpbkar` log contains a message that includes the phrase “failed to allocate.”
  Reschedule the backups so they do not occur at the same time, or add more memory to the backup host.
- In either of the following cases during a vCloud Director backup, NetBackup may be unable to correctly record the name of the vCloud catalog and the expiration status of a vApp template:
  - Two vApp templates of the same name are present in the same vCloud Director organization.
  - A large number of vApp templates exist in the same vCloud Director organization.

  During VM discovery for backup, a policy query rule using `vCDCatalog` or `vCDIsExpired` may return incorrect results.
  When you restore the VM, it may have incorrect values for its expiration status and the name of the vCloud Director catalog.
- In rare instances, the NetBackup `bpbkar` process may core dump (although backups complete successfully). If the VMware backup host is configured for core dump generation, the dump files may occupy too much space and affect performance.
  As a workaround, delete the core files or disable core-dump generation.

For more information on this VMware issue, see “Threads still running after VixDiskLib_Exit call” in the VMware VDDK 5.1.1 release notes:
http://www.vmware.com/support/developer/vddk/vddk-511-releasenotes.html
http://www.symantec.com/docs/TECH211060

- For a policy that uses the Query Builder to automatically select VMs in vCloud Director, the `vCDIsExpired` keyword does not operate as expected. The `vCDIsExpired` keyword correctly selects VMs that have expired. However, it also selects VMs in a vApp that has a run-time lease setting of Never Expire. This issue will be fixed in a future release.
- The following features are not supported for dual boot virtual machine configurations:
  - Enable file recovery from VM backup
  - Optimizations:
    Exclude deleted blocks
    Exclude swapping and paging files
    Exclude boot disk
    Exclude data disks
- A restore of a VM with the hotadd transport mode or the SAN transport mode may not succeed if the VM’s disk geometry in the backup image differs from the VM’s default values. VM disk geometry refers to the layout of the virtual disk (cylinders, heads, sectors) as specified in the vmdk file.
  The NetBackup restore job reports partial success with status code 1 (the requested operation was partially successful). For more information about this issue and available workarounds, see the following tech note on the Symantec Support website:
  http://www.symantec.com/docs/TECH210611

  Note: The restored VM may not be able to start. VMware has documented the cause of this issue in their VDDK 5.1 release notes, under Known Issues and Workarounds: "Metadata write is not supported for HotAdd and SAN transport."

  http://www.vmware.com/support/developer/vddk/VDDK-510-ReleaseNotes.html

- With VMware VDDK 5.1, backups that use the hotadd or SAN transport modes do not include the VM's metadata changes in the backup. The status log of the NetBackup job contains messages similar to the following:

```
07/25/2013 12:37:29 - Info tar (pid=16257) INF - Transport Type
= hotadd
07/25/2013 12:42:41 - Warning bpbrm (pid=20895) from client
```

```
<client_address>: WRN - Cannot set metadata (key:geometry.
biosSectors, value:62) when using san or hotadd transport.
```

As a workaround, retry the backup with a different transport mode (`nbd` or `nbdssl`).

This problem is a known VMware issue. For more details, refer to the VMware VDDK 5.1 release notes at the following URL:
http://www.vmware.com/support/developer/vddk/VDDK-510-ReleaseNotes.html#knownissues

- VMware has identified an issue in ESXi server 5.1 that affects application-level quiesced snapshots for incremental backups. This issue affects VMware VMs that run Windows Server 2003, 2008, 2008 R2, and 2012. The changed block tracking system overstates the amount of the changed data, creating a larger backup than necessary. As a result, incremental backups may take longer than expected and may not complete within the backup window. This issue affects NetBackup for VMware incremental backups.
  To fix this problem, update your ESXi 5.1 servers with the ESXi 5.1 Patch 02 that is described in the following VMware Knowledge Base article:
  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2052143
  The following VMware “VDDK 5.1 Release Notes” article contains more information on this issue. See under “With application level quiescing, Changed Block Tracking overstates changes”:
  http://www.vmware.com/support/developer/vddk/VDDK-510-ReleaseNotes.html#knownissues
- A restore of the virtual machine can fail with status code 220 (database system error) if all of the following are true of the backup:
  - The backup was run from an incremental schedule and **Enable block-level incremental backup** was enabled on the policy VMware tab.
  - **Enable file recovery from VM backup** was disabled on the policy VMware tab.
  - At the time of the incremental backup, the data in the VM had not changed since the previous backup.

  To work around this issue, restore from the full image rather than the incremental image. Because there is no change of data since the full backup, a restore from the full image is exactly the same as a restore from the incremental backup.
- NetBackup for VMware does not support the policy’s **Enable file recovery from VM backup** option for Linux and Windows dual-boot VMs. If **Enable file recovery from VM backup** is selected, the backup fails with status code 13 (file read failed).

- For the VMware policies that select VMs automatically, the backup data may be inconsistent in either of the following cases:
  - Two VMware policies are run at the same time and both policies back up the same VM.
  - A snapshot was created, reverted, consolidated, or deleted by a non-NetBackup component during the backup.

  In this case, the second backup job may remove the snapshot before the first backup is complete. As a result, the data that was captured in the first backup may be inconsistent. When you use Replication Director for VMware, the data inconsistency is not detected until one of the following occurs: The VM is duplicated from the hardware snapshot, the VM is indexed, or the VM is restored. The duplication, index, or restore operation may fail.
- By default, NetBackup waits one hour before the policy Query Builder detects changes in the virtual environment. Until one hour has passed, the Query Builder does not detect the changes when you click the "Load values" icon next to the Value(s) field. To make the changes immediately available to the Value(s) field, use the following procedure to refresh the display.

  Note: The Query Builder's "Reuse VM selection query results for" option does not affect the display of virtual environment changes in the Query Builder. The reuse option determines how long NetBackup reuses the current backup list for future executions of the policy.

  To refresh the Query Builder's view of the virtual environment:

  1. On the Windows desktop of the local host, click **Start** > **Run** and enter **regedit**.
  2. To be on the safe side, make a backup of the current registry (**File** > **Export**).
  3. Go to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Veritas** > **NetBackup** > **CurrentVersion** > **Config** and create a key that is called **BACKUP**.
  4. Create a new DWORD under BACKUP, called **xmlCacheLimit**.
  5. Set this DWORD to the number of seconds you want. A value of 15 allows the Query Builder to be refreshed after 15 seconds.
  6. If the policy editor is open in the NetBackup Administration Console, close it and reopen it.

- The following VMware configuration for High Availability (HA) is not supported for virtual machine backup: vSphere 5.1 with Single Sign On Server in an HA configuration that is behind an F5 load balancer (or any other load balancing software).

- A granular recovery of files, folders, and applications is not supported on Windows 8 server volumes that have data deduplication enabled. Volumes are also not supported that are formatted by a ReFS file system.
- NetBackup supports native multipathing for SAN storage devices on Linux systems.
  If you use Device Mapper on a Linux system, use the device names that appear under `/dev/mapper` and avoid using the `/dev/dm-*` device path.
- If you restore a virtual machine to an ESX 5.0 server and the virtual machine display name contains a `$`, the virtual machine does not start.

  Note: VMware fixed this issue in vSphere 5.0 Update 1.

- The following applies to the NetBackup plug-in for vCenter:
  With vCenter systems that run on Windows 2003, it may be necessary to install a Windows hotfix. Without the hotfix, you may not be able to access the NetBackup vCenter plug-in: the message "Action Canceled" appears.
  You can download the hotfix from the following Microsoft support article:
  http://support.microsoft.com/kb/968730
- Several VMware issues may occur if the virtual machine has a large number of snapshots. To avoid backup problems, NetBackup places a limit of up to 30 snapshots per virtual machine. If the virtual machine has more than 30 snapshots, the backup results in messages similar to the following:

  ```
  10/18/2012 4:56:59 PM - Critical bpbrm(pid=4604)
  from client
  Umesh_w2k3_hypervm33: FTL - vSphere_freeze: Unable to
  remove existing snapshot, too many existing snapshots (91).

  10/18/2012 4:56:59 PM - Critical bpbrm(pid=4604) from
  client
  Umesh_w2k3_hypervm33: FTL - VMware_freeze: VIXAPI freeze

  (VMware snapshot) failed with 26:
  SYM_VMC_REMOVE_SNAPSHOT_FAILED
  ```

  To back up a virtual machine that has more than 30 snapshots, consolidate or delete the existing snapshots. Then rerun the backup.

  Note: The limitation of 30 snapshots per virtual machine does not apply to backups that were made by the Replication Director.

- If the VMware virtual machine has a large number of snapshots, the backup may fail with NetBackup status code 13 (file read failed). This issue can also occur if there are a large number of delta files present because of a VM snapshot consolidation failure.
  The following is an example of the job details of a snapshot job that encounters the consolidation failure:

  ```
  8/12/2013 6:44:39 PM - Info bpbrm(pid=9332) INF - vmwareLogger:
  ConsolidateVMDisks: SYM_VMC_ERROR:  TASK_REACHED_ERROR_STATE
  8/12/2013 6:44:39 PM - Info bpbrm(pid=9332) INF - vmwareLogger:
  ConsolidateVMDisksAPI: SYM_VMC_ERROR:  TASK_REACHED_ERROR_STATE
  ```

  To work around the issue in both cases, consolidate or delete the existing snapshots and then rerun the backup.
  VMware has acknowledged this issue in the release notes for VDDK 5.1 and VDDK 5.0. See the item *Problem in GetMetdataKeys with large number of snapshots* at the following URLs:
  http://www.vmware.com/support/developer/vddk/VDDK-510-ReleaseNotes.html
  https://www.vmware.com/support/developer/vddk/VDDK-500-ReleaseNotes.html
- Restart VIP jobs individually in the Activity Monitor
  For the jobs that a Virtual Machine Intelligent Policy (VIP) starts, you can restart any of the virtual machine jobs individually. In the Activity Monitor, right-click on the job and select "Restart Job." This feature is handy if the policy backs up a large number of virtual machines and you do not want to re-run the entire policy.
- During restore of individual files to a Windows NetBackup client earlier than 7.6, the restore seems to fail if it includes multiple directories with named streams. The progress log incorrectly indicates that more files have been restored than were requested. In fact all files have been restored. The restore job status can be ignored.
- You may receive a status 191 error in the following case: if you attempt to duplicate the images that were backed up from VMware policies from a 7.6 storage unit to 7.1 tape storage.
  BPTM must know the client type. If the VMware type is an unknown type to a NetBackup 7.1 media server, then the 7.1 media server does not duplicate the images.
- If the virtual machine's display name was changed after the virtual machine was backed up, a restore of the virtual machine to its original location fails.
  As a workaround, restore the virtual machine to a different location.
- VMware has identified a problem that prevents the restore of a thin-provisioned virtual machine. The problem occurs in the following case:

- The virtual machine that you want to restore had a thin-provisioned virtual disk when it was backed up.
- The block size of the target datastore for the restore is larger than the block size of the original datastore.
- The size of the thin-provisioned virtual disk when it was backed up is not a multiple of the block size of the target datastore. For example: The original datastore used a block size of 1 MB. The restore datastore uses a block size of 2 MB. The virtual disk to be restored is 101 MB in size.

If all the above are true, the restore fails. As a workaround, try the restore as follows:

- On the **Recovery Options** screen, select a different transfer type (such as **NBD**).
- Or, on the **Storage Destination** screen, do the following: select a datastore with a block size that is compatible with the size of the thin provisioned disk to be restored. The size of the virtual disk to be restored must be a multiple of the target datastore's block size.

- VMware APIs do not currently support IPv6 addresses as server host names. As a result, you cannot add NetBackup credentials for VMware servers using IPv6 addresses as host names. When adding NetBackup credentials, only fully qualified domain names are supported. This restriction applies to vCenter servers and to ESX servers.
- During a virtual machine restore with the SAN transport mode, if any of the virtual machine's vmdk files are not a multiple of the VMFS block size, the last partial-block write may fail. As a result, the restore job fails with status 2820. VMware has acknowledged this issue (see http://kb.vmware.com/kb/1035096). The NetBackup job details log may contain messages similar to the following:

```
12/12/2011 3:12:28 AM - Critical bpbrm(pid=3560) from client
io.acme.com: FTL - Virtual machine restore: file write failed
...
12/12/2011 3:23:00 AM - end Restore; elapsed time: 00:23:32
VMware policy restore error(2820)
```

  As a workaround, use the NBD or the NBDSSL transport mode when you restore the virtual machine.

- Hotadd restore job reports error status 1 with Windows 2008 or 2003 restore host and vSphere 5.0

  A virtual machine restore with the hotadd transfer type may finish with a status 1 (partially successful) if the restore host is Windows 2008 or 2003. (Hotadd

transfer can be used when the VMware backup host or restore host is installed in a virtual machine.)

When this problem occurs, messages similar to the following appear in the job's detailed status log:

```
17:23:09 FTL - Virtual machine restore: file write failed
```

This issue has been reported to VMware (VMware SR# 11117129311) . As a work-around, use any of the following:

- The `nbd` transport mode.
- The SAN or `nbd` transport mode if the restore host is a physical computer.

- With a Linux restore host, a hotadd restore from an incremental backup may fail.

  Because of an issue in the VMware Linux VDDK, a virtual machine restore from an incremental backup my fail even though restore from the full backup succeeds. This failure may occur when the restore host is Linux and the selected transport mode is hotadd.

  Try the restore with the hotadd and nbd transport modes instead of hotadd only.

- The Linux ext4 file system includes a persistent pre-allocation feature, to guarantee disk space for files without padding the allocated space with zeros. When NetBackup restores a pre-allocated file (to any supported `ext` file system), the file loses its preallocation and is restored as a sparse file. The restored file is only as large as the last byte that was written to the original file. Subsequent writes to the restored file may be non-contiguous.

  Note: The restored file contains all of its original data.

vCloud Director notes

This section contains the operational notes and known issues that are associated with NetBackup for VMware vCloud Director in this release.

- Restoring a vCloud virtual machine to an existing vApp template is not supported.
- Restores of vCloud backup images are not supported from the vCenter plug-in. This type of restore is only supported using the Backup, Archive, and Restore interface.
- vCloud organization networks are not displayed on the **Network Connections** screen for restore; only vSphere networks are displayed.

- Instant Recovery cannot restore a vCloud virtual machine into vCloud. The virtual machine is restored into vSphere. You can copy the restored virtual machine into vCloud by means of the **Copy** option in vCloud. Note that the **Import** option does not work with a virtual machine that runs from a NetBackup datastore.
- An issue exists where `multiple organizations per policy` is disabled and the VIP query result contains a virtual machine from multiple organizations. The policy validation is successful, but the backup job fail.
- NetBackup for VMware does not support Single Sign-On (SSO) for vCloud Director. You must add NetBackup credentials for the vCloud server, not for the SSO server.

Known issues with restoring virtual machines into vCloud Director

The NetBackup 7.6 for VMware Guide describes how to restore virtual machines into a vCloud Director vApp or vApp template. (The topic is titled "Restoring virtual machines into vCloud Director.") The vApp, and any metadata changes that were made to the vApp before the backup, should restore correctly. Examples of vApp metadata are settings for the vApp's network connection, boot order, run-time lease, and storage lease.

For a vApp that has only one VM, the metadata changes are not restored if the vApp is restored as a template. This issue will be fixed in a future NetBackup release. Until then, the vApp restore procedure in the NetBackup for VMware Guide is incorrect for the vApp templates that contain only one VM.

How to restore a vApp template that has one VM

1. In the NetBackup Backup, Archive, and Restore interface (BAR), select the VM in the vCloud Director vApp that you want to restore. Click **File > Specify NetBackup Machines and Policy Type > Search VM Clients**. For more details on this part of the procedure, see “Restoring the full VMware virtual machine” in the NetBackup for VMware Guide.
2. Start the restore (click **Restore** or **Actions > Restore**).
3. On the **Recovery Destination** dialog, select **Alternate location in vCloud Director**.
4. On the **Recovery Options** dialog, select the NetBackup recovery host and transport mode for the restore.
5. On the **Recovery vApp Options for vCloud Director** dialog, do the following:
   - Select **Create a new vApp**.

- Select the vCloud server and the organization.
- Enter a name for the vApp.

Note: Do not select **Create vApp as a template in catalog**.

6 On the **Recovery Destination Options for vCloud Director** dialog, you can specify a new name for the VM that you want to restore.

7 On the **Virtual Machine Options** dialog, select the appropriate options for the virtual machine and its disk provisioning.

8 On the **Network Connections** dialog, select the network for the restored virtual machine (or **Retain original network configuration**).

9 On the **Perform Recovery** dialog, run a pre-recovery check. To begin the restore, click **Start Recovery**.

10 After the recovery has finished, log in to vCloud Director and find the restored vApp.

11 Right-click on the vApp and select **Add to Catalog…**.

12 Complete the **Add to catalog** dialog. Click **OK** to add the vApp to the desired catalog. The vApp template is now restored and available.

NetBackup for Hyper-V notes

The following describes operational information for the NetBackup Hyper-V agent:

- A full restore of a Hyper-V VM to an alternate location fails if any of its virtual disks has an ampersand (&) in its path.

  As a workaround, do one of the following:

  - Restore the VM to its original location.
  - Restore the VM to a staging location and register the VM manually.

- NetBackup cannot perform a redirected restore of a virtual machine to a Hyper-V 2008 R2 server if the virtual machine contains a compressed .vhd file. The NetBackup job Detailed Status tab contains a message similar to the following:

```
12/11/2009 17:35:58 - started process bpdm (pid=2912)
...
the restore failed to recover the requested files  (5)
12/11/2009 17:47:06 - Error bpbrm (pid=1348) client restore
EXIT STATUS 185: tar did not find all the files to be restored
```

A message similar to the following appears in the `eventvwr.msc` file:

```
Failed to update the configuration with the new location of
virtual hard disk 'F:\REDIR_VM\f\ADD_VHD\IDE_1_DISK.vhd' for
virtual machine '<virtual_machine_name>': The requested
operation could not be completed due to a virtual disk system
limitation.  Virtual disks are only supported on NTFS volumes
and must be both uncompressed and unencrypted. (0xC03A001A).
Remove the disk from the virtual machine and then attach the
disk from the new location.
(Virtual machine ID <virtual_machine_ID.)
```

This issue is due to a Microsoft limitation. See the following Microsoft link for more information:
http://technet.microsoft.com/en-us/library/dd440865.aspx

- On a restore, NetBackup recreates the linking between a Linux hard link and its original file only if the link file and its target file are restored in the same job. If each file is restored individually in separate restore jobs, they are restored as separate files and the link is not re-established.

Chapter 5

End-of-life notifications

This chapter includes the following topics:

About future NetBackup end-of-life notifications

Symantec is committed to providing the best possible data protection experience for the widest variety of platforms, operating systems, databases, applications, and hardware. Symantec continuously reviews NetBackup's support of these items. 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 Symantec continually adds support for new features, platforms, and applications, 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.

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

Much of this support information is available through the NetBackup SORT home page widget *NetBackup Future Platform and Feature Plans*. Also, included in the widget are the list of platforms, databases, and applications that are not supported in a given release. You can access SORT at the following webpage:

https://sort.symantec.com/netbackup

Another SORT resource is to provide users with End of Life (EOL) and End-of-Support Life (EOSL) information for NetBackup licensed software.

- NetBackup EOL information can be found at the following URL: https://sort.symantec.com/nbufutureplans
- To view NetBackup EOSL information, go to https://sort.symantec.com/netbackup and navigate to **Support** > **Related Links**. Click on the link to *End of Assisted Support information*. Alternatively, you can follow the direct link to https://sort.symantec.com/eosl.

Platform compatibility

This release of NetBackup contains changes in support for various versions of software and hardware platforms.

See "New and discontinued server and client operating system support for NetBackup 7.6" on page 39.

Other information about NetBackup can be found in the various compatibility lists that are listed in the NetBackup Master Compatibility List.

See "About NetBackup compatibility lists" on page 43.

http://www.symantec.com/docs/TECH59978

Appendix A

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.

The following topics in this section describe the various guides and technical manuals that relate to this release NetBackup.

Unless otherwise specified, the NetBackup documents that are described in the following topics can be downloaded in PDF format from the following location:

http://www.symantec.com/docs/DOC5332

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

About release notes

The following release notes documents were released with this version of NetBackup.

- *NetBackup Release Notes*
  This document contains a great deal of assorted information about this release 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 a table of information that describes the known issues that were identified, fixed, and available to NetBackup customers in the form of an Emergency Engineering Binary (EEB).

About administration documents

The following administrator guides were released with this version of NetBackup.

- *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 were released with this version of NetBackup.

- *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 Symantec OpenStorage.
- *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 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 vCenter Guide*
  This guide explains how to install and use the NetBackup vCenter plug-in to monitor virtual machine backups and restore virtual machines.
- *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 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 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 Search Administrator's Guide*
  This guide explains how to install, configure, and use NetBackup Search to index backups, edit and save queries, search across multiple domains, and perform search actions in NetBackup OpsCenter.
- *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 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 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 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.

About administration of database agents

The following administrator guides for NetBackup database agents were released with this version of NetBackup.

- *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 Symantec 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 installation documents

The following guides were released with this version of NetBackup.

- *NetBackup Upgrade Guide*
  This guide is provided to help assist you plan and accomplish your upgrade to this release of NetBackup. This guide is updated periodically to provide you with the most up-to-date information.
- *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.

About configuration documents

The following configuration guides for NetBackup options were released with this version of NetBackup.

- *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 troubleshooting documents

The following troubleshooting guides were released with this version of NetBackup.

- *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 guides were released with this version of NetBackup.

- *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 Symantec NetBackup and OpsCenter products.