

# Symantec NetBackup™ 7.5 Release Notes

UNIX, Linux, and Windows

NetBackup 7.5

# NetBackup 7.5 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: 7.5

PN: 21220060

## Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec, NetBackup, and the Symantec Logo 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.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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.

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

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# 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 Web site at the following URL:

[www.symantec.com/business/support/](http://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 Web page:

<http://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.

## Contacting Technical Support

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

[www.symantec.com/business/support/](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>

# Contents

Technical Support .....	4
Chapter 1	About NetBackup 7.5 new features ..... 11
	About NetBackup 7.5 new features ..... 12
	About new NetBackup commands and status codes ..... 13
	About Accelerator ..... 16
	About AdvancedDisk new features and enhancements ..... 16
	About NetBackup Cloud improvements ..... 17
	About NetBackup Deduplication Option new features and enhancements ..... 18
	About NetBackup OpsCenter enhancements ..... 19
	About NetBackup Replication Director ..... 31
	About NetBackup Search ..... 32
	About Telemetry ..... 33
	About Virtualization ..... 34
	About resilient network connections ..... 34
	About General NetBackup enhancements ..... 35
	General NetBackup performance improvements ..... 35
	About adding clients to LiveUpdate policies ..... 36
	About NetBackup license deployment reporting ..... 36
	Disambiguating status codes 2, 5, and 6 ..... 36
	About BMR AIX client support ..... 39
	Auto Image Replication support for BMR ..... 39
	About alert notification ..... 40
	About NetBackup support utility enhancements ..... 40
Chapter 2	Platform compatibility ..... 43
	About server and client platform compatibility ..... 43
	About NetBackup server and client platform compatibility ..... 44
	NetBackup compatibility lists ..... 45
	About platform life cycles ..... 47
	About adding a platform ..... 48
	About Removing a client platform ..... 48
	About software release types ..... 48
	About compatibility with NetBackup 7.5 ..... 49

	NetBackup compatibility .....	50
	Platform compatibility with the NetBackup Administration Consoles for UNIX .....	52
	Platform compatibility for NetBackup Cloud .....	53
	About Operating systems no longer compatible as of NetBackup 7.0 and beyond .....	54
	NetBackup binary sizes .....	54
	About NetBackup EEB listings .....	57
Chapter 3	Product dependencies .....	59
	Operating system patches and updates .....	59
Chapter 4	Operational notes .....	67
	About operational notes in NetBackup .....	68
	NetBackup Accelerator operational notes .....	69
	NetBackup AdvancedDisk option .....	69
	NetBackup audit trail limitations .....	70
	NetBackup Bare Metal Restore .....	71
	NetBackup database agent operational notes .....	80
	About NetBackup for Microsoft Exchange .....	81
	About NetBackup for Microsoft SharePoint .....	84
	About NetBackup Oracle Guided application recovery for Windows .....	85
	NetBackup Deduplication Option operational notes .....	86
	NetBackup Documentation Notes .....	89
	NetBackup Hyper-V .....	90
	NetBackup installation and start-up notes .....	91
	NetBackup media and rebranding changes .....	91
	About NetBackup installation and upgrade notes .....	95
	Installing NetBackup in Solaris 10 zones .....	100
	NetBackup cluster .....	101
	NetBackup interfaces .....	102
	NetBackup Administration Console for Windows .....	102
	NetBackup Java interfaces .....	102
	Storage unit configuration .....	104
	NetBackup Internationalization and localization .....	104
	NetBackup IPv6 notes .....	107
	NetBackup OpsCenter notes .....	109
	About Replicaton Director notes .....	117
	NetBackup SAN Client and Fibre Transport notes .....	117
	NetBackup SharedDisk support notes .....	118
	NetBackup Snapshot Client notes .....	119



	NetBackup for VMware notes .....	123
	General NetBackup 7.x notes .....	127
	Resilient network operational notes .....	133
Chapter 5	End-of-life notifications .....	135
	NetBackup 7.x end-of-life notifications .....	135
	About general NetBackup notifications .....	135
	About the operating systems that may not be supported in the next major release .....	136
Chapter 6	Related Documents .....	139
	About related NetBackup documents .....	139
	About NetBackup release notes .....	140
	About getting started guides .....	140
	About installation guides .....	140
	About administrator's guides .....	141
	About other documents .....	141
	About administration of options .....	142
	About administration of database agents .....	144
	About the Troubleshooting guide .....	145
Appendix A	About the NetBackup Rehydration improvements for deduplicated files .....	147
	About the NetBackup rehydration improvements for deduplicated files .....	147
	Environmental factors that affect rehydration performance .....	148
	About changes and updates to the deduplication tuning parameters that affect restore performance and rehydration performance .....	149
	About the PREFETCH_SIZE parameter .....	149
	About the RESTORE_DECRYPT_LOCAL parameter .....	150
	About the META_SEGKSIZE parameter .....	150
	About the PrefetchThreadNum parameter .....	150
	Editing the ReadBuffer Size parameter .....	150
	NetBackup tuning parameters that affect restore performance and rehydration performance .....	151



# About NetBackup 7.5 new features

This chapter includes the following topics:

- [About NetBackup 7.5 new features](#)
- [About new NetBackup commands and status codes](#)
- [About Accelerator](#)
- [About AdvancedDisk new features and enhancements](#)
- [About NetBackup Cloud improvements](#)
- [About NetBackup Deduplication Option new features and enhancements](#)
- [About NetBackup OpsCenter enhancements](#)
- [About NetBackup Replication Director](#)
- [About NetBackup Search](#)
- [About Telemetry](#)
- [About Virtualization](#)
- [About resilient network connections](#)
- [About General NetBackup enhancements](#)
- [About NetBackup support utility enhancements](#)

## About NetBackup 7.5 new features

The NetBackup 7.5 release emphasizes availability and performance in protecting mission-critical data and applications in physical and virtualized environments. This release contains the following new features:

- **Symantec Replication Director**  
This feature offers a unified, policy-based management of backups, snapshots and replication.
  - User interface for backup and snapshot and replication.
  - Near-instant data protection leveraging NetApp array-based snapshots and replication by NetApp SnapMirror and SnapVault as well as support for Symantec FileStore.
  - Manage data through its lifecycle across tiers of storage & tape (snapshots to backup disk and tape under NetBackup policy control).
  - Utilization reporting and alerting.
  - Client support for Windows, Linux, Solaris, HP, AIX.
- **Deduplication**  
This release offers improved deduplication integration, scalability, performance, and stability.
  - Integration of Auto Image Replication for media server deduplication
- **Virtualization**  
NetBackup for VMware has these major improvements:
  - Support for vSphere 5
  - Granular recovery for Exchange and SharePoint virtual machines
  - Back up event logging in vCenter
  - Leverages the media server load balancingNetBackup for VMware & Hyper-V have these improvements:
  - File-level recovery for ext4 file system on Red Hat/SUSE virtual machines
  - New policy-type for VMware & Hyper-V
- **Accelerator**  
This feature offers intelligent, streamlined backups to disk. It addresses the increase in the amount of data to backup and the need to reduce the backup windows.
- **Search**

This feature provides an Information Management solution that couples backup, recovery, archive, and discovery.

- Search across multiple domains, save, edit, and export and search queries for legal traceability.
- Robust solution for legal hold management. Hold reports in OpsCenter provide insight into size of legal hold and length of time of the associated holds.
- Cloud-based data protection.  
 This release contains a new Cloud-based storage that features Encryption.
  - Media server encryption with Key Management System.
  - Bandwidth throttling to control the read and write speeds across the network pipe.
  - Metering the amount of read and writes going over the network pipe.
  - Enablement of additional public cloud storage provider.
- Telemetry  
 This feature provides data collection and upload capabilities for NetBackup and OpsCenter installations.
- New platform support has been added to provide automated Bare Metal Restore of more platforms and configurations; expand embedded deduplication, and expand support to address market needs for database agents.
  - BMR Client and boot server support for the following platforms:
    - Red Hat 6
    - AIX 7.1
    - Solaris 10 ZFS (Sparc/x64)
    - Linux native multi-path
  - Auto Image Replication for BMR images
  - Added support for the following agents
    - Enterprise Vault 10
    - Sybase Agent (Solaris 10 x64)
    - Informix Agent (Solaris 10 x64)

## 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 7.5:

■ `nbplupgrade`

The `nbplupgrade` utility upgrades policies from the MS-Windows type to the new VMware or Hyper-V policy type. This upgrade is necessary if you want the policy to use the newer VMware or Hyper-V features. This utility is especially useful when doing bulk policy upgrades.

■ `nbfindfile`

The `nbfindfile` command lets you search files or folders based on simple search criteria like file name and path.

■ `W2Koption`

This Windows-only command runs the utility program that modifies normal backup and restore behavior.

■ `nbdiscover`

This command tests the query rules for automatic selection of VMware virtual machines for backup.

■ `nbperfchk`

This command measures the read and write speed of a disk array such as the disks that host deduplicated data.

■ `nbevingest`

A utility for ingesting file system data restored from NetBackup into Enterprise Vault for e-discovery of NetBackup data.

■ `vnetd`

This is the NetBackup communication daemon. This command allows all socket communication to take place while connecting to a single port.

■ The following is a new command line option for the `nbstl` command:

`-conflict`

This is the command line equivalent of the **Validate Across Backup Policies** in the SLP user interface dialog. When `-conflicts` is specified, the changes to the SLP described by the other options on the command are submitted for policy/SLP validation. The proposed content of the SLP is compared with all the policies that use the SLP and any errors found are displayed on `stdout`. The changes are not committed when `-conflicts` is used. If no errors are found, you can submit the changes without the `-conflicts` option to commit the changes.

The same conflict detection will be performed when the changes are committed (where the `-conflicts` option was previously used or not) and errors found must be corrected before the commit can proceed.

- The following are new `nbstlutil` command line options:

- `-version <num>`

The `-version` option can be used with the `list` operation. When used, the `-lifecycle` option must also be used. The `-version` option restricts the `list` output to only those images that the specified version of lifecycle controls.

- `-jobid <value>`

You can use the `-jobid` option with the `list` operation. When used, it restricts the output to those images where the selected job creates one or more of the image copies.

- `-policy <name>`

You can use the `-policy` option with the “list” operation. When used, it restricts the output those images that have been created via the specified backup policy.

- The following new `nbstlutil` command line operation has been added:

`redo -backupid <value> -slpindex <value>`

The `-backupid` option specifies with image should be affected. The `-slpindex` option determines which operation within the SLP should be redone. The **slp index** values can be obtained from the `nbstl -L` output. When `redo` is used, it takes the actions necessary to repeat that particular SLP operation. The intent is cases where a copy of an image has been lost/damaged/destroyed due to action outside of NetBackup. That provides a way for the user to recreate the copy. If the original source copy is no longer available, the `redo` fails.

- The following commands are new search commands:

- `nbholdutil`

The `nbholdutil` command runs the utility that places legal holds on backup images. Legal holds provide a mechanism to override existing retention levels.

- `nbindexutil`

The `nbindexutil` command runs the utility that adds, lists, or removes indexing requests for existing backup images.

The following is a list of the new status codes released in NetBackup 7.5:

- 1002
- 1401 - 1426

- 1450 - 1468
- 2820
- 5000 - 5034

## About Accelerator

This feature provides fast, streamlined backups to disk. To accomplish that, it leverages change tracking, deduplication, and optimized synthetics functionality.

Integrating these capabilities allows full backups of files and folders to be performed almost as quickly as incremental backups.

A **Use Accelerator** check box appears in the **Attributes** tab of the Policy creation user interface if NetBackup deduplication is in use. By checking this box, Accelerator is used for full backups. The initial Accelerator full backup is a traditional full backup.

After the initial Accelerator full backup, only changed files are read, deduplicated, and transferred to disk. An optimized, synthetic-full backup is created. That generates a block map of the new full backup, so no additional data movement is required. The NTFS change journal can be enabled and used to remove the need for NetBackup to enumerate the file system. Deduplication can be performed on either the NetBackup client, media server, or appliance. NetBackup Cloud storage is also supported with Accelerator.

OpenStorage (OST) devices which support Optimized Synthetics functionality are supported with the NetBackup 7.5 GA release and once an OST vendor's software has been qualified with NetBackup.

---

**Note:** The NetBackup Accelerator is not supported on OpenVMS clients.

---

## About AdvancedDisk new features and enhancements

The following are new features and enhancements for AdvancedDisk in the NetBackup 7.5 release:

- Support for the Common Internet File System is now included in the **Disk Pool Configuration Wizard**.
- Data encryption. The following are the operating systems on which encryption is supported:
  - AIX
  - HP-UX



- RedHat
- Solaris 10
- SUSE
- Windows 2008 R2

See the *NetBackup AdvancedDisk Storage Solutions Guide*.

## About NetBackup Cloud improvements

In addition to being able to write and read data to and from the cloud, additional functionality was added to improve the management and usability of this feature. Additional layered plug-ins were added to improve security, increase control, and measure throughput to and from Cloud storage.

The following features comprise the Cloud enhancements:

- Media server encryption with Key Management System
- Bandwidth throttling to control the read and write speeds across the network pipe.
- Metering the amount of read and writes going over the network pipe
- Enablement of additional public Cloud storage providers.
- Configuring host credentials for Cloud

After initial configuration, you can add additional media servers to your Cloud environment. The procedure to add media servers differs from the procedure for adding non-Cloud media servers. More information is available about adding additional media servers to a Cloud environment. See the Additional media servers section in the *Symantec NetBackup Cloud Administrator's Guide*.

These features offer the following benefits to you:

- Provides an alternative to client side encryption, which reduces the load on the client. Also provides a centralized key management system versus maintaining that on the individual clients.
- Lets you control the amount of bandwidth that is allocated to backups. That eliminates the potential of the backup application saturating the network bandwidth.
- Lets you measure the reads and writes to the cloud, and use this data to bill back the individual business units for that usage.
- Give the end user more choice in cloud storage providers.

## About NetBackup Deduplication Option new features and enhancements

This release contains improved deduplication integration, performance, and stability.

---

**Note:** Some of these new features and enhancements affect a deduplication upgrade to the NetBackup 7.5 release. Before you upgrade, see “New features and enhancements for NetBackup 7.5” in the *NetBackup Deduplication Guide*.

---

The following deduplication features and improvements are included in the NetBackup 7.5 release:

- Support for the AIX 5.3, 6.1, and 7.1 operating systems for deduplication servers and for client-side deduplication.
- 64-TB support for media server deduplication pools.
- Resilient network connections provide improved support for remote office client deduplication.
- iSCSI support.  
PureDisk 6.6.3 supports iSCSI disks in PureDisk storage pools only if the storage pool is deployed exclusively for PureDisk Deduplication Option (PDDO) use. iSCSI storage pools for PDDO use must be configured with the XFS file system and cannot be clustered.  
The PureDisk 6.6.3 documentation does not describe how to configure or manage a PureDisk storage pool that includes iSCSI disks. Information about how to use iSCSI disks in a PureDisk environment is in the PureDisk 6.6.1 documentation.  
<http://www.symantec.com/docs/DOC3878>  
For known issues about iSCSI storage pools, a Symantec tech note is available.  
<http://www.symantec.com/docs/TECH137146>
- Enhancements that improve restore performance.
- Deduplication integrity enhancements.
- Windows storage server performance enhancements.  
The Interprocess communication changes on Windows hosts improve performance to be similar to UNIX and Linux hosts.
- FlashBackup performance improvements.
- Backup image delete and import performance improvements.
- The performance of the first backup of a remote client can be improved.

- **A new stream handler for EMC NDMP.**  
 NetBackup 7.5 includes a new stream handler for the EMC NDMP data format. Stream handlers improve backup deduplication rates by processing the underlying data stream. The EMC NDMP stream handler extracts files from EMC NDMP streams so that identical files and segments on EMC filers deduplicate appropriately.  
 After you upgrade to NetBackup 7.5, deduplication rates for backups of EMC NDMP data that has already been deduplicated decrease. The EMC NDMP stream handler processes the stream differently than in previous NetBackup releases. The low rate applies only to the first backup after you upgrade. The stream handler supports all of the versions of EMC filers that EMC supports.
- **NetBackup now reserves 4 percent of the storage space for the deduplication database and transaction logs rather than 10 percent.**
- **Fibre Channel connections to NetBackup 5020 appliances.** Fibre Channel is supported on x86-64 hosts that run the Red Hat Enterprise Linux 5 or SUSE Enterprise Linux Server 10 SP1 operating systems.

## About NetBackup OpsCenter enhancements

OpsCenter continues to provide a robust user interface for monitoring, alerting, and reporting for operators and backup administrators. This release includes special focus on parity with reporting the features that were available in Veritas Backup Reporter. In addition, it provides improvements with the custom reporting and enhancements that ensure that reports are easier to understand & interpret. In addition to reporting enhancements, this release adds two major functions that simplify the management of NetBackup restore, and provide better access controls.

Restore requests can take significant time to service as you are required to know how the data was originally backed up. In many cases restore operators have to fill in the blanks. Was the G: drive a NAS filer? Which of the following 10 files are required for the restore request. Where is the data now? The following items describe how these challenges are addressed in this release:

- **Restore with Search**  
 OpsCenter offers a restore user interface that is available to operators in a Web browser. Not only can you browse the NetBackup catalog as you have in the past, you can now search across multiple client and multiple NetBackup domains. That enables you to search and find the files or directories, even with limited information and service the restore request as quickly as possible. All of that is accomplished without any additional NetBackup infrastructure.

Search results appear within seconds and you can refine or cancel them as needed to find the files fast.

- OpsCenter 7.5 enables you to monitor, manage, report, and alert on a NetBackup appliance master server.

OpsCenter 7.5 also enables you to monitor hardware of multiple NetBackup appliances from the OpsCenter console. You can monitor appliance master and media servers and quickly identify any hardware failures in the appliances from the OpsCenter console. To monitor appliance hardware and view hardware summary of the appliance master or media servers, go to **Monitor > Appliance Hardware** in the OpsCenter console.

OpsCenter can monitor NetBackup appliance 2.0 master servers. OpsCenter 7.5 can also monitor appliance 1.2 and 2.0 media servers that are attached to an appliance 2.0 master server or to a regular NetBackup 7.5 master server. A new data type that is called **Appliance Hardware** has been added to collect appliance-specific data.

- View-based Access Control

You now search across many clients because the access control model has been updated in OpsCenter. You can now have a particular user associated to a particular grouping of hosts. That enables you to create a new user, "Jimmy" for example. You then give Jimmy the role "Restore Operator". That means the user, "Jimmy" can search, browse, and restore files as well as start and stop jobs. Furthermore, if Jimmy's role in the organization is limited in scope, you can then limit the privileges. You can limit "Jimmy" so that that user can only manage, monitor, report, and restore on a View in OpsCenter. And the View is composed only of the hosts in that geographic locale.

The reverse is also true. If an administrator named Barbara has privileges to all NetBackup servers and clients world-wide in your enterprise, you can give that user full privileges to every host that is attached to OpsCenter.

You can expect to see three major benefits from this feature:

- Less sophisticated IT staffers can service restores. In addition, those staff members can search for the files, directories, and ultimately restore the files faster with higher accuracy.
- The OpsCenter Access Control model now more closely resembles IT operations where roles can be assigned but only for certain groups of IT assets.
- Continued focus on high-quality reporting capabilities ensures that you can publish reports to stakeholders that are inside and outside of IT. You also ensure that everyone is confident that their data is fully protected.

The following list identifies the additional view-based Access Control enhancements that have been added for this release:

- **Ability to view data in permitted views**  
 The logged-in user in OpsCenter can view the data for the permitted views only. Only the permitted views appear in the **View** drop-down list in the **View** pane.
- **You can view the data that is relevant to the selected view.** For example for a client view, media details are not valid. Hence if you select a client-type view and click **Monitor** > **Media**, you see the following error message:  

```
Data is not applicable for the view that you selected.
Click UI access for specific view types for details about the
applicable view types.
```
- **Only a Security Administrator or Administrator can create or modify the views.**
- **An OpsCenter user can specify the default view to be shown in OpsCenter from **Settings** > **User Preferences** > **General**.** This default view would be used when you log on to OpsCenter. If you modify the view selection after logging on to OpsCenter from the View Pane, then that view selection is used for that session throughout OpsCenter except reporting.  
 You can also specify the default view to be used for report templates. This default view is used only for the standard reports.
- **A Security Administrator can view information about permitted view for the user from **Settings** > **Users**.** As this view is restricted to Security Administrator, only the user with Security Administrator is able to see the views that are assigned to a specific user.
- **All the non-admin users get the access to the **ALL MASTER SERVERS** view only if permitted.** A Security Administrator can only grant read access to this view but cannot modify or delete this view. During upgrade, all the existing users are given read access to the **ALL MASTER SERVERS** view.
- **The Analyst user role is no longer available.** When you upgrade from an earlier version to OpsCenter 7.5, all the existing Analyst users are upgraded to Reporter in OpsCenter 7.5. Because an Analyst has default read permission on all the views, after an upgrade, all upgraded-Analyst users get read permission on all of the views in OpsCenter.
- **The Java View Builder is now available for free as part of Symantec OpsCenter.** The Java View Builder was earlier available only with the licensed version (Symantec OpsCenter Analytics).
- **If an OpsCenter user does not have access to any view, the user gets the following message immediately after login:**

OpsCenter login was successful. You may not be able to proceed further as you do not have access to any View. For more details, contact the administrator.

- Consider a scenario where an OpsCenter user has saved a view-based report, and now the user no longer has access to the specific view. If the user tries to run this report, the following message is displayed:

You might not have access to the View selected for this report. You can, however, edit the report and then change the View.

- Ability to generate traditional licensing reports for master servers  
OpsCenter 7.5 helps you to generate traditional licensing reports for master servers of version 6.5.6 and higher (supported by `nbdeployutil`). You can find information about traditional licenses by going to **Manage > Deployment Analysis > Traditional Licensing** in the OpsCenter console.
- OpsCenter 7.5 can monitor and report on cloud configurations on multiple NetBackup 7.5 master or media servers. To monitor your cloud configuration, go to **Monitor > Cloud** in the OpsCenter console. A new report category that is called **Cloud reports** has been added to **Reports > Report Templates**.
  - Job Success Rate
  - Data Expiring in Future
  - Cloud Metering
  - Average data transfer Rate
  - Cloud Metering Chargeback
- In OpsCenter 7.5, the top 50 standard reports and also custom reports have been enhanced for report definition and data correctness. The following enhancements have been made:
  - The top 50 standard OpsCenter reports have been enhanced for report definition correctness to be at par with the earlier NOM or VBR reports.
  - The top 50 standard OpsCenter reports have been enhanced for report data correctness to be at par with the earlier NOM or VBR reports.
  - The custom reports have been enhanced for report definition and data correctness.
  - Reports in earlier versions of OpsCenter, showed incorrect data if you selected a time frame that contains a Daylight Saving Time (or DST) change. However, it does affect performance if you run a standard or a custom report that meets both of the following conditions:

- The report is Historical (has a Time Frame Grouping filter) or is tabular with a **Date** or a **Date Time** column.
- The time frame that was selected to run the report contains the DST change. For example, if you select **CST (GMT -6:00)** as the **Data Display Time Zone** on OpsCenter Server. And while the report runs, you specify the timeframe from Oct 22, 2010 to November 22, 2010. The DST setting for the CST timezone that ended on Nov 7, 2010 at 2:00 AM Since the DST ends in the middle of the selected timeframe on November 7, the selected timeframe contains the DST change.

To overcome such performance issues, Symantec recommends that you configure the timezone for the OpsCenter Server as either GMT or a timezone that does not have any DST. To configure the **Data Display Time Zone** from the OpsCenter console, click **Settings > User Preferences > General** and browse to the **Basic Preferences** section.

Folder Name	Report Name
Backup > Job Activity	File Count
	Job Count
	Job Size
	Client Count
	Job Duration
Backup > Planning Activity > Forecast	Backup window > Job Count
	Job Size - Forecast
Backup > Status & Success Rate	Advanced SuccessRate
	Success Rate - All Attempts
	Success Rate - First Attempt
	Success Rate - All Jobs

Folder Name	Report Name
Backup > Status & Success Rate > Status	Consecutive Failures Report
	Week at a Glance
	Job Status
	Failed Job Count
	Partially Successful Job Count
	Successful Job Count
	Success Rate Line
	Job Attempt Status Detail
Backup > Planning Activity > Scheduled Job	Job Details Scheduled vs. Actual
	Backup > Planning Activity > Scheduled
	Job Count Scheduled Vs. Actual
	Job Count within Backup Window
Backup > Deduplication	Deduplication Size Savings
	Backup > Deduplication
	Deduplication Size Factor
	Pre Vs. Post Deduplication
Job Activity > Variance	Throughput Variance
	Backup Job Size Variance
Backup > Job Browser	Tabular BackupReport
Backup > Planning Activity > Stored Backup Images	Stored backup Images on Media
Chargeback	Backup Chargeback
	Deduplication Chargeback
Client Reports > Risk Analysis	Recovery point Objective
	Client Risk Analysis
	Client Coverage
Client Report	Client Restore
	Client Not Backed up
	Job Success By Client
	Virtual Client Summary



Folder Name	Report Name
Disk & Tape Device Activity	Current Disk Usage
	Drive Throughput
	Media ReportsDrive Utilization
Media Reports	Media Utilization
	Media Expiration Schedule
	Media State
Performance Reports	Master Server Job Throughput
	Disk Usage
Policy Reports	Policy Summary Dashbaord
	Top 10 Policies Using most Server Space
Restore	Restore Job Details
	Restore Job Summary by Job Count
	Restore Job Summary by Volume Restored

If you have saved one or more reports that are based on any of the report templates mentioned or any custom reports, and you upgrade from an earlier OpsCenter version to OpsCenter 7.5, you see the link named **View modified saved reports** under **Reports > MyReports**. Since the saved reports are based on the templates that have been modified in OpsCenter 7.5, these saved reports may appear modified. Click the link to view the modified saved reports.

- The following report-definition changes are included in this release that are valid for some or all of the above mentioned standard (or canned) reports:
  - A unit called **Years** has been added for Relative Timeframe selection for all of the reports. You can now view report data for the last x years with Symantec OpsCenter Analytics for the reports. You can also see the **Years** tab on the top-right corner of the reports.
  - Trend line display option is now available for some of the canned historical reports. You can use trendlines to specify whether the report includes a trendline, and the length of the interval between points on the trend line. The following check box is available under **Timeline Chart Properties** on the **Modify Display Options** pane:**Show trend line with moving average period of <select value>**. The trendline option is available for the following reports:

- Backup > Deduplication > Deduplication Size Saving
  - Backup > Deduplication > Deduplication Size Factor
  - Backup > Job Activity > File Count
  - Backup > Job Activity > Job Count
  - Backup > Job Activity > Job Size
  - Backup > Status & Success Rate > Status > Failed Job Count
  - Backup > Status & Success Rate > Status > Job Status
  - Backup > Status & Success Rate > Status > Partially Successful Job Count
  - Backup > Status & Success Rate > Status > Successful Job Count
  - Backup > Planning Activity > Stored Backup Images > Stored Backup Images on Media
  - Chargeback > Backup Chargeback
  - Chargeback > Deduplication Chargeback
- The **Week at a Glance** report can now show the files and directories that are backed up for each client. The following checkbox has been added on the **Modify Display Options pane when you edit the report**: Show the files and directories that are backed up for each client. If you check this option and click **RunReport**, you can view the client name and the backed up directory in the **ClientName** column of **Week at a Glance** report.
- Drilldown reports are now available for the following reports:

Report	Drill down report
Backup > Job Browser > Tabular Backup Report (click any link in the JobPrimary ID column)	Skip File Details
Client Reports > Job Success By Client (click the bar chart)	Job Details by Client
Media Reports > Media Expiration Schedule (click the bar chart)	Media Expiration Details
Restore > Restore Job Attempt Summary by Job Count (click the bar chart)	Restore Job Attempt Details

## Report

**Restore > Restore Job Attempt Summary by Volume restored** (click the bar chart)

## Drill down report

**Restore Job Attempt Details**

- A new value that is called **unknown** has been added for filters like Policy type, Job Type. The **Charts** section now shows **unknown** as legend instead of blank.
- The following are some of the report definition changes that have been implemented for custom reports:
  - The unit Years and Quarters has been added for Relative Timeframe selection. You can now view report data for the last x years or the last x quarters with Symantec OpsCenter Analytics.
  - A new subcategory that is called **Disk Pool** has been added under the **Backup/Recovery** category for custom reports.
  - A new checkbox named **TargetPerformance** has been added to the **Modify Display Options** page. This checkbox is visible when you create a custom historical report. You can use the **TargetPerformance** option to specify where a report draws the target line, with which you can compare the actual performance shown. The **TargetPerformance** option lets you specify the target for Y1 or Y2 axis (in case of dual axis). In case you set a value of say 100 for Y1 axis and run the report, you see a straight-line parallel to X-axis and the value as 100 on Y1 axis. Using this option, you can easily compare the actual performance with the target performance.
  - A new checkbox option that is called **Display unique rows in the report** has been added for custom tabular reports. This option appears on the **Modify Display Options** page when you create custom tabular reports. When you select this option, a single row replaces all duplicate rows in the report and only distinct records are shown. Duplicate rows generally appear if the rows do not have a unique ID.
  - When you create custom reports (Distribution, Historical, Tabular, or Ranking) in the **Modify Display Options** page, if you select report data for chart-based reports then the function or Operation drop-down list is populated dynamically with the supported values. For example if you create a **Distribution, Historical, or Ranking** custom report, and select **ReportData** as the Job Primary ID, only valid functions like Count, Distinct Count, Maximum, and Minimum are shown in the other drop-down list. In earlier releases all the functions were displayed.

Similarly if you create a tabular custom report, and add **Job Retention Level** as a selected column, the **Operation** drop-down list shows only the applicable functions such as Count and Distinct Count.

- You can now choose to start from the beginning of a Relative time frame for custom reports. The following checkbox has been added in Relative Timeframe:

**Start from the beginning of <selected unit>.** <selected unit> may stand for Hours, Days, Weeks, Months, Quarters, or Years depending on what you select.

If you specify a relative timeframe and check **Start from the beginning of <selected unit>**, the Relative timeframe is calculated starting from the first day for week, month, quarter, or year selection, from 12:00 A.M. for day selection, and from the earliest whole number (no minutes or seconds) for hour selection. Do not select the **Start from the beginning of <unit>** check box if you want to view data for the entire period that is specified in Relative Timeframe.

Examples:

- The current date is June 13, 2010. If you select the Relative Timeframe as **Previous 1 Month** and do not select the **Start from the beginning of Month** check box, the report shows data from May 14, 2010 to June 13, 2010. However if you select the **Start from the beginning of Month** check box, the report shows data from June 1, 2010 to June 13, 2010.
- The current date and time are September 13, 2010 at 10:30 P.M. If you select the Relative Timeframe as **Previous 2 Days** and do not select the **Start from the beginning of Days** check box, the report shows data from September 11, 2010 at 10:30 P.M. to September 13, 2010 at 10:30 P.M. However if you select the **Start from the beginning of Days** check box, the report shows data from September 12, 12 A.M. to September 13, 2010 at 10:30 P.M.
- The current time is 4:25 P.M. If you select the **Relative Timeframe** as **Previous 2 Hours** and do not select the **Start from the beginning of Hour** check box, the report shows data from 2:25 P.M. to 4:25 P.M. However if you select the **Start from the beginning of Hours** check box, the report shows data from 3:00 P.M. to 4:25 P.M.

---

**Note:** If you specify a relative time frame and check **Start from the beginning of <selected unit>**, the report displays that data collected over the interval ending at the current date. That is effectively equivalent to specifying a time frame; the report's contents remain static whenever you display it.

---

- The following checkboxes have been added for Absolute Time frame in custom reports:

Ignore From Date	<p>Check this option to view all the data on and before the <b>To</b> date.</p> <p>Example: Suppose you specify a timeframe: From March 1, 2004 at 12:00 A.M. to April 30, 2004, at 12:00 A.M. The report displays data from the time period between the start and the end dates. Now if you check Ignore From Date, the report ignores the From Date and displays all data before April 30, 2004 at 12:00 A.M.</p>
Ignore To Date	<p>Check this option to view all data on and after the From date.</p> <p>Example: Suppose you specify a timeframe: From March 1, 2004, 12:00 A.M. to April 30, 2004, 12:00 A.M. The report displays data from the time period between the start and the end dates. Now if you check <b>IgnoreToDate</b>, the report ignores the To Date and displays all data on and after March 1, 2004, 12:00 A.M.</p>

Use **Ignore From Date** or **Ignore To Date** to indicate an open-ended time interval for an Absolute Timeframe.

- A new value that is called **unknown** has been added for filters like Policy type, Job Type, Schedule/Level Type etc. The charts section now shows **unknown** as legend instead of blank.
- Symantec OpsCenter Analytics 7.5 lets you perform a NetBackup Search operation. A license for NetBackup Search is required. After you have added the license, the Search tab is visible in the OpsCenter console.
- OpsCenter 7.5 now supports the feature of asset tags. This feature deploys ISO 19770-2 standard software asset tags with OpsCenter 7.5 components like Server, Agent, and View Builder. An Asset tag helps to identify if a particular software product or component is deployed on a host.

This feature specifies the format and location of the tag that can help any software asset management (SAM) tool to detect and report on Symantec OpsCenter.

- In OpsCenter 7.5, the following infrastructure components have been upgraded to higher versions:
  - The Apache Tomcat Web server has been upgraded to version 6.0.32.0 (from version 6.0.29.0) for all platforms. The Web server has been upgraded to address the security vulnerabilities in the earlier version.
  - Starting from OpsCenter 7.5, Java Runtime Environment (JRE) is embedded in the OpsCenter Server package. The JRE component has been upgraded to higher versions based on the respective platforms.

The following table shows the new upgraded version of JRE in OpsCenter 7.5 for each platform:

Platform	Old version	New version
Windows x86, Windows x64, Linux SUSE, Linux RHEL, Solaris SPARC, Solaris x86	1.6.0_17	1.6.0_23
HP-UX	1.6.0.05.00	1.6.0.09.00
AIX	6.0.0.150	6.0.0.250

- OpsCenter 7.5 installers for Windows and UNIX are now shipped with a telemetry data collection and uploading utility. Using this utility, the installer can collect OpsCenter installation information from your system like system environment, installation data, and configuration log files. The telemetry utility can bundle this data into a .tar.gz format and optionally (with your permission) attempt to upload details of the installation to Symantec. This data would help Symantec to guide future product development and also analyze issues.

A new option named **AllowOpsCentertosendinformationbacktoSymantec** has been added to the **License Agreement** page when you install OpsCenter components on Windows. This option is checked by default. You may opt to check or uncheck this option. If you check this option, the installer collects OpsCenter installation information from your system and uploads details of the installation to Symantec.

Similarly you are now prompted for the following when you install OpsCenter components on UNIX:

**May we collect and upload OpsCenter installation and usage data from this system? [y,n] (y)**

- Additional OpsCenter enhancements:
  - OpsCenter 7.5 can monitor and manage all NetBackup master server versions between 6.5.x and 7.5.
  - OpsCenter 7.5 can now be installed on Solaris 11 SPARC platform.
  - OpsCenter 7.5 can now collect data from Symantec Enterprise Vault 9.
  - You can access OpsCenter 7.5 using Internet Explorer 7.x, 8.x, and 9.0. You can also access OpsCenter 7.5 using Firefox 3.0, 3.5.x, and 4.0.

## About NetBackup Replication Director

More enterprise customers deploy advanced data protection solutions such as snapshots and replication for data protection and disaster recovery. In addition to traditional backup applications, when you deploy these technologies you enable a tiered menu of protection and recovery offerings with appropriate costs and RPO and RTO characteristics. However, such dual deployments also introduce complexity. Many people and products to manage, non-integrated, disjointed, and dissimilar backup and recovery processes, separate scripts, or products for backup and replication management.

For more information about the NetBackup Replication Director, see the *NetBackup Replication Director Solutions Guide*.

NetBackup currently has limited capabilities to leverage snapshots and replication for data protection. However, this release provides many enhancements that improve NetBackup's capabilities to leverage all forms of replication. Starting with NetBackup 7.5, the following is enabled:

- One application (NetBackup) to centrally manage policies, schedules, catalog, and the user interface to perform backup and snapshot replication.
- Near-instant data protection leveraging NetApp array-based snapshots and replication by NetApp SnapMirror and SnapVault as well as support for Symantec FileStore.
- Manage data through its lifecycle across tiers of storage & tape (snapshots to backup disk and tape under NetBackup policy control).
- Meet SLAs with centralized rapid recovery, independent of location. Browse, point, click.
- Simplified file restore (SFR) for an OpsCenter, user interface restore.

More specifically, NetBackup 7.5 provides the following integration between NetBackup and NetApp arrays as a licensable feature:

- OST plug-in architecture for NetApp and FileStore integration.
- End-to-end, disk-to-disk-to-tape policy management with snapshots, SnapVault and SnapMirror, and NDMP.
- NAS support for file services.
- File-level browse and restore functionality from snapshots and backups.
- Import the SnapVault and SnapMirror replication relationships that already exist.
- Auto-discovery of unprotected data.
- Job activity monitoring that encompasses job success, failure, status, and progress.
- Utilization reporting and alerting.
- Client support for Windows, Linux, Solaris, HP, and AIX.
- SLP-managed snapshots.
- Roll back from a copy for Replication Director.
- NDMP support for Replication Director.
- Configuring NetBackup to use storage replication.
- Simplified file restore (SFR) from snapshots.

## About NetBackup Search

NetBackup Search provides a mechanism to index the file system metadata that is associated with backup images. That makes searching for relevant information simple, powerful, and fast. Once information is found, the user can take actions based on that information. NetBackup Search provides a robust legal hold mechanism which ensures that images relevant to a legal case are not inadvertently deleted or allowed to expire based on retention levels.

---

**Note:** NetBackup Search is a licensable feature.

---

The following capabilities are a part of this feature:

- Advanced search capabilities enable you to find relevant information faster with the following advanced search capabilities:
  - Search across multiple domains.



- Save and edit search queries for legal traceability.
- Robust solution for legal hold management.
  - Legal holds provide a mechanism to override existing retention levels to ensure that the backup images (and associated media) are retained until the legal proceeding is complete.
- Hold reports in OpsCenter provide insight into size of legal hold and length of time of the associated holds.

## About Telemetry

This release of NetBackup has a new feature that is called Telemetry. The technology of Telemetry provides automatic recording and transmission of data from a remote source to a receiving station for analysis. The focus of this feature is to provide data collection and upload capabilities for NetBackup and OpsCenter installations.

When you install NetBackup and OpsCenter you see an additional prompt that asks you to allow the upload of installation data to Symantec. If you agree to allow this data collection to occur, your answer is saved and any future installation (such as, release updates) does not prompt you again. You also have the option to opt out of enabling this feature.

If you choose to enable this feature, the collection runs during the installation only. You can view the information that is collected, and that data is saved in a local file so that you can review it at any time. Data collection is supported on Windows, Linux, and UNIX environments.

When you enable this feature the following types of information are collected:

- Name and type of the Host. (Is it a virtual or a physical host?)
- Operating system name and version
- Hardware platform
- The CPU type and the memory
- Any previously installed versions of NetBackup or OpsCenter
- What components are installed, for example, NetBackup master, media, client, OpsCenter server, and agents.
- Installation problems
- License keys

## About Virtualization

NetBackup 7.5 for VMware offers the best virtual machine (VM) protection, whether protecting a few VMs or an entire virtual datacenter.

This release contains the following improvements:

- Enhanced Windows application protection
  - One-click Windows application protection now available in VMware policy:
    - Backup of application-consistent snapshot.
    - Cataloging of entire application.
    - Database transaction log truncation processing.
  - Any-level recovery for SQL Server VMs  
Single pass VM backup provides any-level of recovery for SQL Server 2005 and later: VM, file, or database recovery.
- New VMware policy  
Convert from the FlashBackup-Windows policy for improved management, monitoring, and reporting of VMware backups.
- New file-level recovery for RedHat/SUSE EXT4 file systems – extends previous support of EXT2 and EXT3 file systems.
- Ability to perform Exchange and SharePoint backups of virtual machines.  
Ability to perform database recovery and granular recovery (GRT) for Exchange and SharePoint from a VMware backup. All Exchange and SharePoint Agent recovery options are supported from a VMware backup. A single application-aware VMware backup provides the following: VM recovery, file recovery, database recovery, and granular recovery.  
This feature supports Exchange 2007 or later and SharePoint 2007 or later on Windows 2008 and 2008R2
- Support for VMware vSphere 5 features, including Storage DRS.
- vCenter Event Logging  
NetBackup now logs backup success and failure statuses, and snapshot delete failures directly into the vCenter event list.
- VMware policy now supports media server load balancing.

## About resilient network connections

This release of NetBackup provides the ability to configure resilient network connections. A resilient connection allows backup and restore traffic between a client and NetBackup media servers to function effectively in high-latency,

low-bandwidth networks such as WANs. Symantec believes that the most common use case is for clients in a remote office that back up their own data (client-side deduplication). The data travels across a wide area network (WAN) to media servers in a central datacenter.

Resilient connections support the following storage destinations:

- **AdvancedDisk**
- **BasicDisk**
- **Media Server Deduplication Pool**

Resilient network is documented in the following guides:

- *NetBackup Administrator's Guide for UNIX and Linux, Volume I.*
- *NetBackup Administrator's Guide for Windows, Volume I.*
- *NetBackup Deduplication Guide.*

See [“Resilient network operational notes”](#) on page 133.

## About General NetBackup enhancements

The following topics describe the general NetBackup enhancements that are contained in this release.

- Performance Improvements.
- Disambiguate status codes 2, 5, and 6.
- NetBackup license deployment reporting.
- NetBackup OpsCenter enhancements.

### General NetBackup performance improvements

This topic describes the enhancements that were made to NetBackup that improve the core product, make it more user-friendly, and improve the performance. The following list shows the areas in which these improvements were made:

- Usability Enhancements in the areas of installation, status codes, and logging.
- Security enhancements.
- Improved licensing management.
- For performance improvement, changes were made to help users who use multiple user interfaces at the same time.

- NetBackup can now support 40,000 jobs and as many as 10 concurrent user interfaces.
- The user interface refresh rate has been improved. That leads to greater efficiency as you manage NetBackup.

## About adding clients to LiveUpdate policies

This feature provides a quick and intuitive one-step method for adding a large number of clients to a LiveUpdate policy. You can use this feature to do the following:

- Add the ability to import a list of clients from a text file.
- Add the ability to import all or a subset of clients from an existing backup policy into a LiveUpdate policy.

## About NetBackup license deployment reporting

To improve your experience with using NetBackup, this release contains improvements to ensure that you have a clear understanding of how NetBackup is deployed. You can now compare the number of licenses that you have purchased versus the number of licenses you currently use. That enables you to have a confident understanding of compliance and to also plan for future purchases.

The following two features comprise this feature:

- **New Traditional License Reports:**  
We introduced license reporting for the Capacity license model. In NetBackup 7.5 a report for the Traditional model was added so that you can count server, clients, tiers, and other components of the NetBackup solution. This report includes an automated report that is available from OpsCenter and a command-line tool for a single master server.
- **Capacity License Report Enhancements:**  
This release contains a number of enhancements to the Capacity report that was available in NetBackup 7.1. These enhancements mean that less manual review is required for you to interpret the report.

## Disambiguating status codes 2, 5, and 6

In past versions, the NetBackup restore jobs failed for a large number of reasons. However, you would only see one of three different error codes that did not accurately describe the error that occurred. Symantec took time to improve this area by providing a unique error code for all of the possible error scenarios. The following table shows these errors, and the appropriate error status code.

---

**Note:** This feature is scheduled to be ready for the Beta 2 release.

---

<b>Data Type</b>	<b>Restore Selection</b>	<b>Steps to Reproduce</b>	<b>Expected Status Code</b>
Oracle	Restore of data where the primary copy is on an offline media server.	Shut down NetBackup processes on the media server containing the backup data. Initiate a restore.	2760
SAP	Restore of data where the primary copy is on an offline media server.	Shut down NetBackup processes on the media server containing the backup data. Initiate a restore.	2760
MS-SQL	Restore of data where the primary copy is on an offline media server.	Shut down NetBackup processes on the media server containing the backup data. Initiate a restore.	2760
Oracle	Restore of data to a client that does not have the media server defined in the server list	Remove the media server entry from the server list on the destination restore client.	2761
SAP	Restore of data to a client that does not have the media server defined in the server list	Remove the media server entry from the server list on the destination restore client.	2761
MS-SQL	Restore of data to a client that does not have the media server defined in the server list	Remove the media server entry from the server list on the destination restore client.	2761
Oracle	Restore data from corrupt image.	Manual edit the image file with an incorrect fragment number.	2762
SAP	Restore data from corrupt image.	Manual edit the image file with an incorrect fragment number.	2762
MS-SQL	Restore data from corrupt image.	Manual edit the image file with an incorrect fragment number.	2762
Oracle	Restore of data with client network failure during transfer	Manual reset the client NIC while restore is in progress	2763
SAP	Restore of data with client network failure during transfer	Manual reset the client NIC while restore is in progress	2763
MS-SQL	Restore of data with client network failure during transfer	Manual reset the client NIC while restore is in progress	2763

Data Type	Restore Selection	Steps to Reproduce	Expected Status Code
Oracle	Restore of data with media server network failure during transfer	Manual reset the media server NIC while restore is in progress	2764
SAP	Restore of data with media server network failure during transfer	Manual reset the media server NIC while restore is in progress	2764
MS-SQL	Restore of data with media server network failure during transfer	Manual reset the media server NIC while restore is in progress	2764
Oracle	Restore of data with error reading tape or disk	Reset device while reading from tape or disk	2765
SAP	Restore of data with error reading tape/disk	Reset device while reading from tape or disk	2765
MS-SQL	Restore of data with error reading tape or disk	Reset device while reading from tape or disk	2765
Oracle	Restore of data with error reading OST Device	Reset OST device while reading data	2766
SAP	Restore of data with error reading OST Device	Reset OST device while reading data	2766
MS-SQL	Restore of data with error reading OST Device	Reset OST device while reading data	2766
Oracle	Restore of data where Oracle is down	On Oracle client, shut down Oracle services	2820
Oracle	Restore of data with incorrect permissions	Initiate restore with incorrect permissions to restore	2821
Oracle	Restore of data with data file mounted	Initiate restore of database in mounted state (ORA-19573)	2822
MS-SQL	Restore of data where SQL is down	Begin restore, shut down SQL Services	2840
MS-SQL	Restore of data with incorrect permissions	Initiate restore with incorrect permissions to restore	2841
MS-SQL	Restore of data with database in use	Connect to database by SQL Enterprise manager, begin restore	2842
MS-SQL	Move database by restore with incorrect paths	Select SQL Move script, fail to correctly modify the file paths	2843
MS-SQL	Restore of Striped SQL data with multiplexing	Restore a SQL striped data that has been multiplexed to tape	2844

Data Type	Restore Selection	Steps to Reproduce	Expected Status Code
SAP	Restore of data where SAP is down	Begin restore, shut down SAP Services	2870
SAP	Restore of data with incorrect permissions	Initiate restore with incorrect permissions to restore	2871

## About BMR AIX client support

- The BMR AIX 7.1 client support includes AIX virtualization support for BMR and SAN boot support in AIX for BMR.
- AIX Virtualization support for BMR
 

The virtual I/O server is a part of the IBM system p5 power virtualization hardware feature. The virtual I/O allows sharing of physical resources between the logical partitions that include SCSI and virtual networking. That allows more efficient utilization of physical resources through sharing between the logical partitions and the facilitates-server consolidation. The BMR client is supported as a boot server that can be run in the AIX 7.1 TL0/AIX 6.1 TL6guest operating systems. The following are the types of restores that are supported:

  - Virtual-to-virtual self restore
  - Virtual-to-virtual DSR restore
  - Virtual-to-physical DSR restore
  - Physical-to-virtual DSR restore
- SAN boot support in AIX for BMR
 

This feature enables BMR to do a SAN-based restore where the SAN storage can act as a root disk .

## Auto Image Replication support for BMR

Auto Image Replication enables you to automatically replicate copies of mission-critical backups between different NetBackup domains. It simplifies and speeds up recovery in the event of a site loss. It enables you to send copies of backups to a “bunker” location for long-term storage. In addition, you can use Auto Image Replication to replicate Bare Metal Restore information along with backups while still providing a simplified and faster server recovery at the disaster recovery site.

## About alert notification

When an administrator performs an action through the NetBackup Administration Console and the action is successful, but auditing failed, you see a desktop alert. The alert is shown if the **Alert notification** setting is turned on. The administrator does that by right-clicking on the console status bar on the **Alert notification** button.

The three settings for Alert notification are **On**, **Off**, and **Blink**.

- If **ON** is set, the desktop alert with a warning message is always shown.
- If **Off** is set, the desktop alert is never shown.
- If **Blink** is set, then the icon for the alert notification on the status bar blinks, indicating there was an alert. You can see the details of the warning as a desktop alert if you double-click the **Alert notification** button on the status bar.

The setting is preserved as a preference for the Administrator on the NetBackup Administration Console that is launched from the present system.

## About NetBackup support utility enhancements

NetBackup 7.0 includes three support utilities: NBSU, NBCC, and NBCCR. The following list summarizes the enhancements that have been made to each utility in this release:

- NetBackup Support Utility (NBSU)  
The NBSU utility assists you in gathering NetBackup and operating system diagnostic information. This tool queries the host on which it runs and gathers diagnostic information about NetBackup and the operating system. In addition, it provides a wide range of control over the types of diagnostic information gathered.  
In this release, a new version of the NBSU utility is available with improved cluster support and updates to numerous diagnostics.
- NBCC and NBCCR utilities  
The NBCC utility uses the output from various OS and NetBackup commands to analyze the consistency state of the NetBackup configuration. It also analyzes the consistency state of NetBackup databases and catalogs as they relate to tape media. If inconsistencies are detected, NBCC consolidates, and packages the resulting data into a bundle that can be sent to Symantec Tech Support for analysis.  
The NBCCR utility processes database and catalog repair actions as defined in a special file that you can generate under the guidance of Symantec Technical



Support. This file is created as part of the analysis of the data that the NBCC utility collects and any site-specific situations.

This release of NetBackup includes enhanced consistency checks and repairs to each of these utilities.



# Platform compatibility

This chapter includes the following topics:

- [About server and client platform compatibility](#)
- [NetBackup compatibility lists](#)
- [About platform life cycles](#)
- [About software release types](#)
- [About compatibility with NetBackup 7.5](#)
- [Platform compatibility with the NetBackup Administration Consoles for UNIX](#)
- [Platform compatibility for NetBackup Cloud](#)
- [About Operating systems no longer compatible as of NetBackup 7.0 and beyond](#)
- [NetBackup binary sizes](#)
- [About NetBackup EEB listings](#)

## About server and client platform compatibility

You can find the NetBackup platform compatibility information and other various compatibility lists on the Symantec Support Web site. These compatibility lists offer a variety of up-to-date information about the operating systems that are compatible with NetBackup and NetBackup features. This section also contains the following types of information:

- Descriptions of the compatibility lists that are on the Symantec Support Web site
- Instructions on how to locate the NetBackup compatibility lists
- NetBackup compatibility information

- NetBackup binary sizes that include NetBackup media server software and NetBackup client software

---

**Note:** This document is posted on the Symantec Support Web site and may be updated after the GA release of NetBackup 7.5. Therefore, Symantec recommends that you refer to the following Technote on the Symantec Support Web site to view the latest NetBackup 7.5 release information.

<http://www.symantec.com/docs/DOC5041>

---

## About NetBackup server and client platform compatibility

This release of NetBackup contains many changes and enhancements to the compatible platforms and operating systems on which NetBackup is supported. The following list describes some of the major changes that apply the NetBackup 7.5:

- NetBackup 7.5 does not support the following operating systems on the defined CPU Architecture:
  - Mac OS X 10.5 (32-bit, 64-bit, and POWER)
  - AsianUX 2.0 (64-bit)
  - Ubuntu 8.04 (64-bit)
  - Debian 4.0 (64-bit)
  - SUSE Linux Enterprise Server 9, IA64 & zArchitecture
- The NetBackup client is not supported on the following operating systems on the defined CPU Architecture from NetBackup 7.5 forward.
  - Windows Server 2003 R2 IA64
  - Windows Server 2003 SP1 IA64
  - Windows Server 2008 IA64
- The NetBackup Accelerator is not supported on OpenVMS clients.
- All UNIX 32-bit system support has been discontinued. To upgrade these systems to NetBackup 7.5, you must first migrate your current NetBackup 6.x catalogs and databases to a system with a compatible platform. However, you can use NetBackup 6.x media servers and clients that run on 32-bit platforms with a NetBackup 7.5 master server that is on a supported 64-bit platform.

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 7.5, you also must update the vendor plug-in to a 64-bit version.

- NetBackup 7.5 supports client operations on all 64-bit platforms except FreeBSD and MAC.
- NetBackup 7.1 and 7.5 are not supported on IRIX and Tru64. Servers and clients with operating the systems that use NetBackup 6.x are compatible with NetBackup 7.5 servers.
- You cannot use HP-UX PA-RISC as a master server. This platform is compatible only as a media server without the EMM server or a client. In addition, HP-UX PA-RISC is not supported with the media server deduplication Pool.
- Novell NetWare is only compatible as a client.
- For this release, the following platforms have been added.
  - Canonical Ubuntu 11.04 X64 for 64-clients
  - CentOS 6.0 X64 for 64-bit clients and and 64-bit servers
  - Debian GNU/Linux 6.0 X64 for 64-bit clients
  - Mac OS X 10.7 X64 for 64-bit clients
  - OpenVMS 8.4 IA64 for 64-bit clients
  - Red Hat Enterprise Linux 6.0 (base) z/Architecture for 64-bit clients and 64-bit servers
  - Solaris 11 SPARC and X64 for 64-bit clients and 64-bit servers

The most up-to-date compatibility information on platforms, peripherals, drives, and libraries is located in various compatibility lists on the Symantec Support Web site.

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

## 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 Web site. You can use the following methods to locate these lists:

- The following URL guides you to a set of tools that can help you locate the latest platforms, peripherals, drives, and libraries.

<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 Web site:  
<http://www.symantec.com/docs/TECH59978>

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

- The *NetBackup Enterprise Server and Server 7.x OS Software Compatibility 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.

That list contains information about each of the following NetBackup Enterprise features:

- NetBackup Enterprise servers and client
- Bare Metal Restore (BMR)
- NetBackup Access Control (NBAC)
- Network Data Management Protocol (NDMP)
- NetBackup SAN Client and Fiber Transport
- NetBackup Virtual System compatibility
- MSEO (media server encryption option)
- NetBackup Media Server Deduplication Option
- NetBackup OpsCenter
- File System Capability

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.

- The *NetBackup server 7.x hardware compatibility list* includes information for compatible drives, libraries, virtual tape devices, robot-types, fibre-channel HBAs, switches, routers, bridges, iSCSI configurations, and encryption devices

That list includes information about the compatible drives, robot types, switches, routers, and bridges, and iSCSI configurations that coincide with the following hardware:

- OpenStorage
- Virtual tape libraries (VTLs)
- Network Data Management Protocol (NDMP)
- Host bus adapters (HBAs)
- Encryption
- *NetBackup Database Agent 7.x Software Compatibility List*  
This compatibility list contains the most current platform compatibility information for NetBackup database agents.
- *NetBackup 7.x Snapshot Client compatibility lists*
- *NetBackup 7.x BMR File System and Volume Manager compatibility lists*  
See also the *NetBackup Bare Metal Restore Administrator's Guide* for the following additional compatibility lists:
  - BMR compatible shared resource tree (SRT) versions
  - BMR compatible file systems and volume managers
  - BMR compatible cluster solutions
  - BMR disk space requirements
- *NetBackup 7.x Cluster Compatibility List*
- *NetBackup Desktop/Laptop Option compatibility list*
- *Backup Exec Tape Reader compatibility list*

## 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 48.

See [“About Removing a client platform”](#) on page 48.

## 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 go to the same version or newer versions.

## About software release types

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

NetBackup products and the NetBackup Appliance products use this same process.

- A major release is the first in a series of single-dot releases such as 2.0 or 7.0. 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, 2.1, 7.1, 7.5, and so forth. 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 release update is a double-dot release, for example, 2.0.1, 7.0.1, 7.0.2, and so forth. This release type may contain a few new features and enhancements as well as a many product fixes. Only those documents that are applicable to the new features or enhancements are updated and republished.
- A maintenance update is a triple-dot release, for example, 2.0.0.1, 7.1.0.1, 7.1.0.2, and so forth. This release type is comprised of a small number of fixes that are developed to address issues in either a major, minor, or release update. This release type only contains fixes to known issues and does not contain new features or enhancements to NetBackup. The only documentation that is



provided is an online Readme and a NetBackup Release Notes document that is available on the Symantec Support Web site.

## About compatibility with NetBackup 7.5

Symantec NetBackup has always maintained that the master server within your environment must be at a version level that is equal to or greater than the version levels of your media servers and client servers within the same environment. With NetBackup and the NetBackup Appliances, you can apply a maintenance update (for example 7.5.0.1) to a media server or client server within an environment where your master server is at a version level of 7.5. This same scenario can apply to the maintenance updates that are released under a minor release or release update.

See [“About software release types”](#) on page 48.

For information about NetBackup compatibility with the NetBackup appliances, see the [NetBackup 5xxx Appliance Compatibility](#) Technote on the Symantec Support Web site.

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

- If a master server is at 7.1, then the media servers and client servers cannot be at a single-dot version level that is higher than 7.1, such as 7.2 or 7.5.
- If a master server is at 7.1, then the media servers and client servers cannot be at a double-dot version level that is higher than 7.1, such as 7.1.x.
- If a master server is at 7.1.1, then the media servers and client servers cannot be at a double-dot version level that is higher than 7.1.1, such as 7.1.2.

The following table uses the NetBackup 7.1 product line to demonstrate the various compatibility schemes that a mature product line can support. In this example, maintenance updates have been released. The same schemes apply with the new NetBackup 7.5 line.

**Table 2-1** NetBackup release compatibility matrix where maintenance updates have been released

NetBackup master server	NetBackup media server	NetBackup client
7.1	7.1	7.1
7.1	7.1	7.1.0.1
7.1	7.1	7.1.0.2

**Table 2-1** NetBackup release compatibility matrix where maintenance updates have been released (*continued*)

NetBackup master server	NetBackup media server	NetBackup client
7.1	7.1.0.1	7.1.0.1
7.1	7.1.0.1	7.1.0.2
7.1	7.1.0.2	7.1.0.1
7.1	7.1.0.2	7.1.0.2
7.5	7.5	7.5

The following table shows the various compatibility schemes that are supported with the current NetBackup 7.5 product line.

**Table 2-2** NetBackup release compatibility for the 7.5 product line

NetBackup master server	NetBackup media server	NetBackup client
7.5	7.0	6.0, 6.5, 7.0
7.5	7.0.1	6.0, 6.5, 7.0, 7.0.1
7.5	7.0.2	6.0, 6.5, 7.0, 7.0.1, 7.0.2
7.5	7.1	6.0, 6.5, 7.0, 7.0.x, 7.1, 7.1.0.x
7.5	7.1.0.1	6.0, 6.5, 7.0, 7.0.x, 7.1, 7.1.0.x
7.5	7.1.0.2	6.0, 6.5, 7.0, 7.0.x, 7.1, 7.1.0.x
7.5	7.1.0.3	6.0, 6.5, 7.0, 7.0.x, 7.1, 7.1.0.x
7.5	7.5	6.0, 6.5, 7.0, 7.0.x, 7.1, 7.1.0.x, 7.5

**Note:** Support for the NetBackup 6.x product line is scheduled to end October, 2012.

## 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 7.5](#)” on page 49.

---

**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 Web site 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 7.5, 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/opensv/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 7.5](#)” on page 49.
- 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 Web site.  
<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 Web site.

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

## 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 Guides*. And for information on how to use the NetBackup Administration Console, see the *NetBackup Administrator's Guide, Volume 1*.

---

**Note:** The window managers in the following table are compatible with NetBackup when you use NetBackup Java. You may encounter some user-interface anomalies when you use the various window managers that are available on UNIX platforms. Many of these problems are documented and can occur because of unusual or non-standard window manager configurations. In the most common cases of misplaced or shifted components within a dialog, resize the dialog. This action refreshes the display and causes the interface to display the information correctly.

---

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 7.x Operating System Compatibility List](http://www.symantec.com/docs/TECH59978) on the Symantec Support Web site.

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

---

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

---

## 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 7.5 media server. More information is available about supported media servers.

See, <http://www.symantec.com/docs/TECH76648>

# About Operating systems no longer compatible as of NetBackup 7.0 and beyond

For an up-to-date listing of the operating systems that NetBackup 7.x no longer supports, see the "Operating sytems no longer supported by NetBackup" section in the *Symantec NetBackup Enterprise Server and Server 7.x OS Software Compatibility List*. Use the following URL to locate this document on the Symantec Support Web site.

<http://www.symantec.com/docs/TECH76648>

A list of operating systems that may no longer be compatible with the next major release of NetBackup, refer to the "End-of-life notifications" Chapter.

See "About the operating systems that may not be supported in the next major release" on page 136.

## NetBackup 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.

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 5.3, 6.1, 7.1	POWER		1865MB		5290MB	
Asianux 3.0	x64		1013MB		4368MB	
Canonical Ubuntu 9.04, 9.10, 10.04, 11.10	x64		1013MB			
CentOS 5.2, 5.3	x64		1013MB			
CentOS 6.0	x64		1013MB		4368MB	Media server or client compatibility only.
Debian GNU/Linux 5.0, 6.0	x64		1013MB			
FreeBSD 6.1, 6.2, 6.3, 7.x, 8.x	x86	176MB				

**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	x64	176MB				
HP-UX 11.11, 11.23, 11.31	PA-RISC		1172MB		2628MB	Media server or client compatibility only.
HP-UX 11.31	IA64		1964MB		5812MB	
Mac OS X 10.6	x86	155MB				
Mac OS X 10.6, 10.7	x64	155MB				
Novell Open Enterprise Server 2	x64		1005MB		4348MB	
Novell Open Enterprise Server 11	x64		1005MB		4348MB	
OpenVMS 5.5, 6.2, 7.3	HP VAX	128MB				
OpenVMS 6.1, 6.2, 7.3, 8.2, 8.3, 8.4	HP Alpha		128MB			
OpenVMS 8.2, 8.3, 8.3-1H1, 8.4	HP IA64		128MB			
Oracle Enterprise Linux 5.0	x64		1013MB		4368MB	
Oracle Enterprise Linux 6.0	x64		1013MB		4368MB	
Red Flag Linux 5.0	x64		1013MB		4368MB	
Red Hat Enterprise Linux 5.0 (base)	x64		1013MB		4368MB	
Red Hat Enterprise Linux 5.0 (AS)	x64		1013MB		4368MB	
Red Hat Enterprise Linux 6.0 (base)	x64		1013MB		4368MB	
Red Hat Enterprise Linux 6.0 (AS)	x64		1013MB		4368MB	
Red Hat Enterprise Linux Desktop 5.0	x64		1013MB			

**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 5.0 (base)	IA64		802MB			
Red Hat Enterprise Linux 4.0 (AS)	POWER		312MB			
Red Hat Enterprise Linux 5.0 (base)	POWER		312MB			
Red Hat Enterprise Linux 5.0 (base)	z/Architecture		798MB		3487MB	Media server or client compatibility only.
Red Hat Enterprise Linux 6.0 (base)	z/Architecture		798MB		3487MB	Media server or client compatibility only.
Solaris 9	SPARC		991MB			
Solaris 10	SPARC		1136MB		3398MB	
Solaris 10	x64		883MB		3280MB	
Solaris 11	SPARC		1136MB		3398MB	
Solaris 11	x64		883MB		3280MB	
Solaris 11 Express	SPARC		1136MB			
Solaris 11 Express	x64		897MB			
SUSE Linux Enterprise Server 10 (SP1)	IA64		772MB			Compatible with client only.
SUSE Linux Enterprise Server 11	IA64		772MB			Compatible with client only.
SUSE Linux Enterprise Server 10 (SP1)	x64		1005MB		4348MB	
SUSE Linux Enterprise Server 11	x64		1005MB		4348MB	
SUSE Linux Enterprise Server 9	POWER		317MB			Compatible with client only.
SUSE Linux Enterprise Server 10 (SP1)	POWER		317MB			Compatible with client only.



**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
SUSE Linux Enterprise Server 10 (SP1)	z/Architecture		772MB		3480MB	Media server or client compatibility only.
SUSE Linux Enterprise Server 11	z/Architecture		772MB		3480MB	Media server or client compatibility only.
Windows	x86	620MB		1540MB		Covers all compatible Windows x86 platforms
Windows	x64		820MB		1850MB	Covers all compatible Windows x64 platforms

## About NetBackup EEB listings

Since the release of NetBackup 7.1 a number of Engineering Emergency Binaries have been released. These EEBs are now contained within NetBackup 7.5. If you want to see this list, you can use the following URL to download it from the Symantec Support Web site.

<http://www.symantec.com/docs/DOC5130>



# Product dependencies

This chapter includes the following topics:

- [Operating system patches and updates](#)

## 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 Web site 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 5.3	AIX runtime libraries 8.0.0.10 or 9.0.0.3 or later	You may need to restart after changing to version 9.0.0.3.
	x1C.rte 8.0.0.10 fileset	For the x1C.rte 8.0.0.10 fileset, you may need to install the IY91284 fix to avoid a potential issue when creating or updating the NetBackup database. The IY91284 fix is part of Maintenance Level 6.

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

Operating system type and version	Patch	Notes
	AIX 5.3 TL12 SP2 (5300-12-02-1036)	NetBackup 7.5 requires the AIX 5.3 TL12 SP2 (5300-12-02-1036) Maintenance Pack as a minimum. (Higher patch levels should also work.)  You can use the <code>oslevel -s</code> command to verify what Maintenance Pack level you have installed.
AIX 6.1	AIX 6.1 TL5 SP5 (6100-05-02-1034)	NetBackup 7.5 requires the AIX 6.1 TL5 SP5 (6100-05-02-1034) Maintenance Pack as a minimum. (Higher patch levels should also work.)  You can use the <code>oslevel -s</code> command to verify what Maintenance Pack level you have installed.
	AIX runtime libraries 9.0.0.3 or later	The runtime libraries need to be at 9.0.0.3 or later. You may need to restart after you change to version 9.0.0.3.
HP-UX	COMPLIBS.LIBM-PS32	If you install AT on an HP-UX platform, this patch is required.
HP-UX IA64	Networking.NET-RUN: /usr/lib/libip6.sl	
	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.1	
	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.sl	
	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so	
	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so.1	
	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so	
	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so.1	
	Networking.NET2-RUN: /usr/lib/libip6.1	

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

Operating system type and version	Patch	Notes
HP-UX PA-RISC	Networking.NET-RUN: /usr/lib/libip6.sl	For HP-UX PA-RISC platforms, this filesset is required:
	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.1	For HP-UX PA-RISC platforms, this filesset is required:
	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.sl	For HP-UX PA-RISC platforms, this filesset is required:
	Networking.NET2-RUN: /usr/lib/libip6.1	For HP-UX PA-RISC platforms, this filesset is required:
HP-UX 11.11	PHSS_35385	This patch is required for JAVA 6.0.
	PHSS_32226	This patch is a LIBCL patch.
	PHSS_37516	<p>Contains fixes for the following:</p> <ul style="list-style-type: none"> <li>■ QXCR1000593919: purifyplus dumps core in PA32</li> <li>■ QXCR1000589142: dld crash in LL_new_descendent_list when the aCC application is exiting.</li> <li>■ QXCR1000589142: dld crash in LL_new_descendent_list when the aCC application is exiting.</li> <li>■ QXCR1000746161: dlsym() hangs</li> <li>■ QXCR1000593999: dld emits assert messages for chatr +mem_check enabled 64-bit executables</li> </ul>
	PHSS_26946	This patch is necessary to enable any C++ runtime 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.

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

Operating system type and version	Patch	Notes
	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 <code>POLL_INTERVAL</code> to be set to zero in <code>/var/stm/config/tools/monitor/dm_stape.cfg</code> . That disables the <code>dm_stape</code> monitor within the Event Monitoring System. Symantec recommends that you upgrade to IPR0109.
	PHSS_30970	This patch can cause problems with the programs that have the <code>setuid</code> bit set. Hewlett-Packard's IT resource center Web site contains information about this patch.  <a href="http://www1.itrc.hp.com">www1.itrc.hp.com</a>
	PHCO_35743	S700_800 11.11 libc cumulative patch The above patch has dependency on the following patches: <ul style="list-style-type: none"> <li>■ PHCO_31923 (critical patch): s700_800 11.11 libc cumulative header file patch</li> <li>■ PHKL_34805 : 700_800 11.11 JFS3.3 patch; mmap</li> </ul>
HP-UX 11.23	PHSS_37201	This patch is required for JAVA 6.0.
	PHCO_33431	Symantec recommends that all customers running 11.23 install this patch. This applies to HP PARISC only because HP itanium has moved to 11.31.
	PHSS_34858	That is a recommended critical patch from HP that is required so that <code>dlopen</code> 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).

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

Operating system type and version	Patch	Notes
	PHSS_37492	<p>Contains fixes for the following:</p> <ul style="list-style-type: none"> <li>■ QXCR1000593919: <code>purifyplus</code> dumps core in PA32</li> <li>■ QXCR1000589142: <code>dld</code> crash in <code>LL_new_descendent_list</code> when the <code>aCC</code> application is exiting.</li> <li>■ QXCR1000746161: <code>dlsym()</code> hangs</li> <li>■ QXCR1000593999: <code>dld</code> emits assert messages for <code>chatr +mem_check</code> enabled 64-bit executables</li> </ul>
HP-UX 11.31	PHSS_37202	This patch is required for JAVA 6.0.
	QPK1131 (B.11.31.0809.326) patch bundle	This patch bundle is required for NetBackup media server support. This is an HP-UX September 2008 patch bundle.
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 to run NetBackup 7.0.
Solaris 9 SPARC 64-bit client	111712-11 (or greater)	Change Request ID - 6815915
	111722-04 (or greater)	
	Patch: 112908-29 (or greater)	
	Patch: 112874-31 (or greater)	
	122300-53	Change Request ID - 6723423
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.

Table 3-1

Operating system patches and updates for NetBackup *(continued)*

Operating system type and version	Patch	Notes
	Recommended OS Patchset - dated June 2011 or later	<p>Symantec recommends that you download the recommended patch set dated June 2011 from the <a href="#">Oracle Support Web</a> site. This patch set contains the following patches:</p> <ul style="list-style-type: none"><li>■ 118777-17 (SunOS 5.10: Sun GigaSwift Ethernet 1.0 driver patch)</li><li>■ 139555-08 (Kernel patch with C++ library updates).</li><li>■ 142394-01 (Internet Control Message Protocol (ICMP) patch)</li><li>■ 143513-02 (Data Link Admin command for Solaris (DLADM) patch)</li><li>■ 141562-02 (Address Resolution Protocol (ARP) patch)</li></ul> <p>The following patches are for Solaris 10 SPARC with NXGE cards:</p> <ul style="list-style-type: none"><li>■ 142909-17 (SunOS 5.10: nxge patch)</li><li>■ 143897-03 (Distributed Link Software patch)</li><li>■ 143135-03 (Aggregation patch)</li><li>■ 119963-21 (Change Request ID - 6815915)</li><li>■ 139555-08 (Change Request ID - 6723423)</li></ul>



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

Operating system type and version	Patch	Notes
Solaris 10 x86-64	Recommended OS Patchset - dated June 2011 or later	<p>Symantec recommends that you download the recommended patch set dated 12/28/2011 from the <a href="#">Oracle Support Web</a> site.</p> <p>Contains the following patches:</p> <ul style="list-style-type: none"> <li>■ 118778-15 (SunOS 5.10_x86: Sun GigaSwift Ethernet 1.0 driver patch)</li> <li>■ 139556-08 (Kernel patch with C++ library updates)</li> <li>■ 142395-01 (SunOS 5.10_x86: ICMP patch)</li> <li>■ 143514-02 (SunOS 5.10_x86: Data Link Admin command for Solaris patch)</li> <li>■ 147259-02 (SunOS 5.10_x86: Aggregation patch)</li> <li>■ 142910-17 (SunOS 5.10_x86 kernel patch to include NXGE fixes)</li> <li>■ 142910-17 (SunOS 5.10_x86: Distributed Link Software patch)</li> <li>■ 143136-03 (SunOS 5.10_x86: Aggregation patch)</li> <li>■ 139556-08 (Change Request ID - 6723423)</li> <li>■ 119964-21 (Change Request ID - 6815915)</li> </ul>
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 IA64 (SP1 & SP2)	KB913648	Contains the necessary updates to run Volume Shadow Copy.
	KB928646	Hot fix for hangs of connection attempts by PBX.
Windows Server 2003 x86-32 (SP1 & SP2)	KB883646	Microsoft Storport hot fix.

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

Operating system type and version	Patch	Notes
	KB913648	Contains the necessary updates to run Volume Shadow Copy.
	KB936357	Microsoft microcode reliability update.
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 IA64	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.

# Operational notes

This chapter includes the following topics:

- [About operational notes in NetBackup](#)
- [NetBackup Accelerator operational notes](#)
- [NetBackup AdvancedDisk option](#)
- [NetBackup audit trail limitations](#)
- [NetBackup Bare Metal Restore](#)
- [NetBackup database agent operational notes](#)
- [NetBackup Deduplication Option operational notes](#)
- [NetBackup Documentation Notes](#)
- [NetBackup Hyper-V](#)
- [NetBackup installation and start-up notes](#)
- [NetBackup interfaces](#)
- [NetBackup Internationalization and localization](#)
- [NetBackup IPv6 notes](#)
- [NetBackup OpsCenter notes](#)
- [About Replicaton Director notes](#)
- [NetBackup SAN Client and Fibre Transport notes](#)
- [NetBackup SharedDisk support notes](#)
- [NetBackup Snapshot Client notes](#)

- [NetBackup for VMware notes](#)
- [General NetBackup 7.x notes](#)
- [Resilient network operational notes](#)

## About operational notes in NetBackup

The chapter contains the topics that explain important aspects of NetBackup 7.5 operations that may not be documented elsewhere in the NetBackup documentation set. This document is posted on the Symantec Support Web site and may be updated after the GA release of NetBackup 7.5. Therefore, Symantec recommends that you refer to the following Technote on the Symantec Support Web site to view the latest NetBackup 7.5 release information.

<http://www.symantec.com/docs/DOC5041>

To view a listing of Emergency Engineering Binary's (EEBs) that are included in NetBackup 7.5, download the following document from the Symantec Support Web site.

<http://www.symantec.com/docs/DOC5130>

The online versions of other NetBackup documents have been updated since the GA release of NetBackup 7.5. You can view the latest versions of the NetBackup documentation set, at the following location on the Symantec Support Web site.

<http://www.symantec.com/docs/DOC5138>

The following list of links offer insight on minimum NetBackup requirements that can help you tune your NetBackup environment as well as help you understand how to get more out of your NetBackup product.

- For minimum system requirements for the Solaris kernel when used with NetBackup, refer to the following Technote:  
<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 Web site:  
<http://www.symantec.com/docs/TECH75332>

---

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

---

# NetBackup Accelerator operational notes

The following items describe operational notes for the NetBackup Accelerator feature:

- The 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:
  - 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.
- NetBackup accelerator backups to a NetBackup appliance media server are not supported.  
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 are not support on NetBackup appliance media servers.
- The NetBackup Accelerator does not support Windows network drives.
- Storage unit groups are supported only if the storage unit selection in the group is Failover.

## 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 *NetBackup 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.
- An incorrect user name may appear in the Audit Report.  
An incorrect user name is displayed in the Audit Report when the EMM server is on the remote host.
- 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 **Backupselection** 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.

## NetBackup Bare Metal Restore

The following list contains the items that relate to the NetBackup Bare Metal Restore feature.

- 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 `bmrprtadm` 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: bmrsl101.vxindia.verita
```

```
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 **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 multipath solutions (EMC PowerPath and Linux Native multipath) with both actively configured on a client can cause issues and are currently not supported by BMR.

A BMR issue results 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 multipath. 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 7.5 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 7.5. Or create a point-in-time configuration from your earlier 7.5 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 Hotfix, 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 is restored 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 `bmrstadm` 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 BRM 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 **HP BIOS > 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` 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 7.5 only from NetBackup 7.1, 7.0 and 6.x. You cannot directly upgrade an older standalone BMR product (BMR 4.7) to NetBackup 7.1 or 7.5, but it can be migrated to NetBackup 7.1 or 7.5. 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 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 7.5 or a higher version NetBackup Client can be used to restore back-level NetBackup clients.
- About copying a pre-NetBackup 7.5 SRT  
The boot server does not support copying of 6.5.X and 6.X SRT.
- About importing a pre-NetBackup 7.5 SRT  
The boot server does not support importing of 6.5.X and 6.X SRT.
- Restoring a client backup to the original hardware when EMCPowerPath software is running.  
When EMC PowerPath software is running on the original client, BMR can only support the restoration of a client backup onto the original hardware.
- 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.
- No support for GPT disks.  
BMR does not support Windows x64 client systems that have one or more GPT disks. No work-around exists to completely support GPT disks; but BMR backup may succeed in case of such systems.  
If the backup was successful, BMR may be able to restore the system; although the GPT disks are implicitly restored as MBR-based disks. Also, as Windows 2003 and XP do not support system or boot volumes on GPT disks, a "System-only" restore should work correctly.  
For self-restores to the same physical GPT disks, the behavior is undefined and unknown.
- Restore of a BMR 6.5.5 Solaris 10\_x64 client fails.  
The restore of a BMR 6.5.5 Solaris 10\_x64 client that has a NetBackup 7.5 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 7.5.
- 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 `bmrstadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while the BMR SRT is created.  
The `bmrstadm` 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 7.5, select 64-bit as the OS architecture type. While you install the NetBackup client into the SRT, `bmrstadm` 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 Technote on the Symantec Support Web site.  
<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 Technote on the Symantec Support Web site.  
<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 Technote on the Symantec Support Web site.  
<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 Technote on the Symantec Support Web site:  
<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 Technote on the Symantec Support Web site.

<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 Technote on the Symantec Support Web site.

<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 Technote on the Symantec Support Web site.

<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 Technote on the Symantec Support Web site.

<http://www.symantec.com/docs/TECH179053>

## NetBackup database agent operational notes

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

- No granular recovery support for certain database agents in IPv6-enabled NetBackup 7.x environments.

In IPV6-enabled NetBackup 7.x environments, granular recovery is not supported for Microsoft Exchange Server or Microsoft Sharepoint Server.

- For Exchange or SharePoint protection in VMware backups, it is advisable to only perform GRT browse and restore from one backup image at a time.
- Exchange and 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!
```

- You cannot perform a GRT restore of multiple mailboxes from multiple databases (Exchange 2010) or multiple storage groups (Exchange 2007) from a VMware, application-protected backup.



- 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/opensv/netbackup/AIO_READS_MAX` that contains the value 1. See the *NetBackup for Oracle for UNIX and Linux Administrator's Guide* for more information.
- Sybase ASA performance is poor when the UltraSparc-T series processor is used. For example, the Sybase ASA database does not perform well when Solaris is used with the UltraSparc-T series processor. Thus, Symantec recommends that you do not use this type of hardware on your master/EMM server.

---

**Note:** NetBackup uses the Sybase ASA database server internally to store the NetBackup configuration data and backup image headers, that run on master/EMM Server.

---

For more information on how to improve the performance of an UltraSparc-T series processor, see the following Technote on the Symantec Support Web site.

<http://www.symantec.com/docs/TECH137761>

## About 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:

- 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 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`

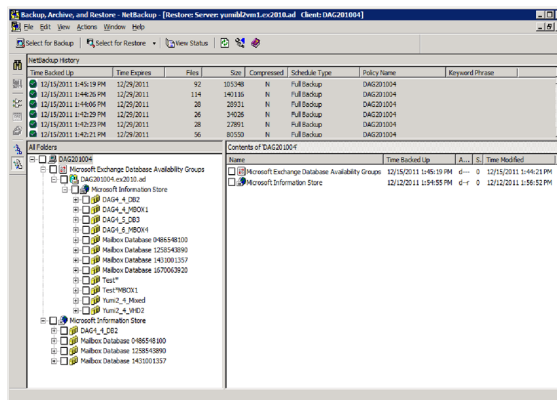
- Exchange 2003 off-host backups that use Storage Foundation for Windows (SFW) 5.1 are not supported with NetBackup 7.5. .
- A user is unable to browse for Exchange restore images from a node of a database availability group (DAG) using the Backup, Archive, and Restore interface, even if the **Distributed 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**.



## About 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:

- A Status 71 error can occur if multiple SharePoint farms use the same SQL instance.
- NetBackup 7.5 is able to backup Word Automation services and Web Analytics services, earlier limitations on these are removed.
- A SharePoint large document GRT restore may finish with status 0. A SharePoint large document GRT restores finish with status 0 but the document is not restored. This issue occurs because a network packet limit is reached. The problem can be avoided by increasing the 'network packet size (B)' value.
- SharePoint configured with Claims Based Authentication is not supported with this release of NetBackup. Refer to Technote TECH164938 on the Symantec Support Web site for more information about this issue.

### Restoring SharePoint 2010 Web Applications configured with "Claims-based Authentication"

- 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**.
- **Restore GRT Basic Meeting Workspace** shows errors when restoring even though the restore completed.
- When you perform SharePoint granular restores from images that are produced with the VM SharePoint application-aware backups, select one image at a time to browse and restore.

## About NetBackup Oracle Guided application recovery for Windows

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

- NetBackup Oracle Guided application recovery limitation  
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.

## NetBackup Deduplication Option operational notes

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

- 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/opensv/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.

- Cluster support on deduplication storage servers.  
 NetBackup does not support clustering of deduplication storage servers or load balancing servers.
- The NetBackup Media Server Deduplication Option does not support NFS mounted file systems.  
 The NetBackup Media Server Deduplication Option does not support NFS mounted file systems. Therefore, do not enter an NFS file system when you configure the data storage path.

- 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.
- Deduplication backup jobs may fail with status code 2106 or status code 2074. Deduplication backup jobs may fail with status code 2106 or 2074 even though a suitable storage unit exists. The deduplication servers usually must be under heavy load for that to occur.  
To work around this issue, add the following touch file to the deduplication storage server and to any load balancing servers:  
UNIX: `/usr/openv/netbackup/db/config/DPS_PROXYDEFAULTRECVTMO`  
Windows:  
`install_path\Veritas\NetBackup\db\config\DPS_PROXYDEFAULTRECVTMO`  
The file content must be the integer 800. No other file content is required.
- 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>.
- On Windows deduplication servers, NetBackup now uses shared memory for communication between the NetBackup Deduplication Manager (`spad.exe`) and the NetBackup Deduplication Engine (`spoold.exe`).  
After you upgrade to NetBackup 7.5, verify that the following shared memory values are set in the `storage_path\etc\puredisk\agent.cfg` file:  

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

  
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 in 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.

- The PureDisk Deduplication Option does not support IPV6. You should use only IPV4 addressing on NetBackup media servers that host a PureDisk Deduplication Option agent.  
 The PureDisk Deduplication Option is an agent that is part of the PureDisk software. It is packaged, delivered, licensed, and purchased separately from NetBackup.
- For optimized duplication between two PureDisk storage pool authorities, NetBackup reports that the deduplication rate is 100%. However, deduplication does not occur during optimized duplication. Therefore, ignore the deduplication rate statistics.

NetBackup can manage duplication between two PureDisk storage pool authorities by using the PureDisk Deduplication Option agent. The agent that is part of the PureDisk software. It is packaged, delivered, licensed, and purchased separately from NetBackup.

- If you replace a deduplication storage server host, process the transaction queue manually before you begin the replacement procedure. (See “Replacing the deduplication storage server host computer” in the *NetBackup Deduplication Guide*.)

When you configure the new environment, the NetBackup Deduplication Engine processes the transaction log. If many transactions have to be processed, timeouts may occur and interrupt the configuration process. If this issue occurs, do the following:

- Wait until the NetBackup Deduplication Engine process (`spoold`) starts, at which time the queue processing is complete.
- Delete the storage server configuration.



See “Deleting the deduplication storage server configuration” in the *NetBackup Deduplication Guide*.

Begin the deduplication configuration again.

- If you restart the NetBackup Deduplication Engine, it processes the transaction queue and loads database metadata immediately. While this process occurs, other deduplication activity does not occur. The length of time during which activity does not occur depends on several factors. The factors include the following:

- The amount of the data that is stored
- The number of transactions in the queue
- The capabilities of your CPU
- The speed of your disk

Because of the factors, predicting the completion time is difficult. It may take as little as several seconds or as long as several hours. When the startup processing completes, normal deduplication activity resumes.

- If you stop the `postgres` process when it cannot write to disk, the process may panic and generate a core dump. The process tries to flush data to disk, causing the core dump. Reasons for which the process cannot write to disk include the following:

- Failure of the disk on which the Postgres database resides.
- The file system on which the Postgres database resides is mounted as read-only. This mount may occur because the system kernel detects file system corruption or disk I/O errors. The kernel then may remount the file system as read-only to prevent further corruption.

If this Postgres problem occurs, resolve the underlying issue before restarting the `postgres` process.

Postgres is the application for the deduplication database. Postgres is not a Symantec product.

## NetBackup Documentation Notes

The following list identifies some known inconsistencies in the NetBackup documentation that has been released with NetBackup 7.5.

- The *NetBackup Shared Storage Guide* is retired.
- The new *NetBackup AdvancedDisk Storage Solutions Guide* documents the AdvancedDisk storage option.

- The new *NetBackup OpenStorage Solutions Guide for Disk* documents how to use intelligent disk appliance storage with NetBackup.
- The Shared Storage Option documentation is now included in the *NetBackup Administrator's Guide for UNIX and Linux, Volume II* and the *NetBackup Administrator's Guide for Windows, Volume II*.
- The *NetBackup Search Administrator's Guide* is a new document that contains the following information:
  - Installing NetBackup Search in clustered environment
  - Decommissioning an indexing server
  - Restoring the data on hold and ingesting into Enterprise Vault
  - Troubleshooting information
- The *NetBackup Cloud Administrator's Guide* is a new document in this release. It explains how to back up and restore data from cloud Storage as a Service (STaaS) vendors.
- The *NetBackup Replication Director Solutions Guide* is a new document in this release. It describes the implementation of NetBackup OpenStorage-managed snapshots and snapshot replication, where the snapshots are stored on the storage systems of partnering companies.
- The `bpcd -restrict_if` option is no longer displayed in the command usage. The `bpcd -restrict_if` option is no longer displayed in the usage. It is possible it may be specified at run time, but it is ignored.  
See, <http://www.symantec.com/docs/TECH171318>.

## NetBackup Hyper-V

The following describes operational information for the NetBackup Hyper-V agent:

- 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  
 '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 on  
 supported on NTFS volumes and must be both uncompressed and unencrypted.  
 (0xC03A001A). Remove the disk from the virtual machine and then attach t  
 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.

## NetBackup installation and start-up notes

The following subsections offer additional the information that can help you install NetBackup or use NetBackup.

### NetBackup media and rebranding changes

The following list describes the NetBackup DVD and NetBackup rebranding enhancements:

- 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/obj/ld/lib` for that command to work. For 64-bit systems, set `LD_32_LIBRARY_PATH` to `/usr/obj/ld/lib`.

---

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

---

- Veritas Storage Migrator (VSM)

This product has reached its end of life and is no longer supported.

- 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.

- The following list describes general NetBackup changes within 7.5:

- Enhanced NetBackup image metadata management

Starting with NetBackup 7.5, all backup image metadata is stored in the relational database (NBDB). Previous versions stored this data in both the NBDB and flat ASCII files (image header files).

The following describes the advantages of this change:

- Eliminates the consistency issues for any data that previously existed in multiple databases
    - Improves the product search performance, especially in large catalogs.
    - Improves the performance of restores, policy scheduling, and image cleanups.

After an upgrade from a previous version of NetBackup, post-upgrade migration of pre-existing image metadata from the file system to the NetBackup database occurs.

---

**Note:** This enhancement affects upgrades. To help ensure a successful upgrade to NetBackup 7.5, please visit the NetBackup 7.5 Upgrade Portal for complete upgrade details.

<http://www.symantec.com/docs/TECH74584>

---

- UNIX platforms

The following describes the UNIX platform changes:

- Linux zSeries SUSE 64-bit This platform now uses SLES 10, patch 2. NetBackup 7.5 cannot be installed on these systems if the OS kernel is older than 2.6.16.

- Linux RedHat x86\_64 and Linux zSeries RedHat 64-bit These platforms now use RH 5, update 4. NetBackup 7.5 cannot be installed on these systems if the OS kernel is older than 2.6.18.
- Solaris x64 Starting with NetBackup 7.5, this platform supports Informix 11.
- Macintosh OS X This platform now uses version 10.6. NetBackup 7.5 cannot be installed on these client systems if the OS version is older than 10.6.
- UNIX server packages  
 NetBackup 7.5 completes the native packaging implementation for servers on the HP-UX, RHEL, SLES, and AIX platforms as follows:
  - The installation script installs the package by using the appropriate OS installation command for that server platform.
  - The installation script installs the package by using the appropriate OS installation command for that server platform.
  - The installation script installs the package by using the appropriate OS installation command for that server platform.
- Novell NetWare  
 This platform is no longer supported for use as a client.
- Windows IA64  
 Server and client support are discontinued for this platform in NetBackup 7.5.  
 NetBackup 7.5 provides back-level support only for Windows IA64 clients.
- NetBackup Product Improvement Program  
 Starting with NetBackup 7.5, the NetBackup Product Improvement Program captures installation deployment and product usage information. During the installation, you can choose to participate in the NetBackup Product Improvement Program and send this information automatically and in a secured manner to Symantec. The information received becomes part of a continuous quality improvement program that helps Symantec understand how customers configure, deploy, and use the NetBackup product. This information is then used to help Symantec identify improvements in product features, testing, technical support, and future requirements.  
 To learn more about the NetBackup Product Improvement Program, refer to the NetBackup license agreement section **17.19 Privacy; Data Protection**. The following describes where to find the license agreement:
  - UNIX

See the file LICENSE in the base directory of the UNIX images on theDVDmedia or from the downloaded media images from FileConnect

- Windows

From the DVD media or the downloaded media images from FileConnect, start the installation wizard (Browser.exe). On the Home page, click **Installation**. On the **Installation** page, select either **Server Software Installation** or **Client Software Installation**. On the **Welcome** page, click **Next** to advance to the **License Agmt** page.

- UNIX clusters

- 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.

- Cluster node upgrade order

Starting with NetBackup 7.5, you can select whether to first upgrade the inactive node or the active nodes.

- 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`, `VRTSnbcnc`, `SYMCnbcnc`, 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.

- Clustered media server support changes

New NetBackup 7.x media server installations cannot be clustered. However, existing 6.x clustered media servers can be upgraded to version 7.x and remain clustered.

- All compressed files are compressed using gzip.

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.

## About NetBackup installation and upgrade notes

This topic contains the information that applies to the installation of NetBackup 7.5. It also contains information about upgrades to this version of NetBackup.

- Warning: If you currently use NetBackup versions 7.0.x and want to upgrade a Solaris SPARC media server that hosts a media server deduplication pool, an updated version of the `pduninstall.sh` script is required. You must install the new script before you upgrade to NetBackup 7.5.

Please see the following Technote on the Symantec Support Web site to download the updated script.

<http://symantec.com/docs/TECH146243>

If you upgrade before this file is updated, the Technote also describes the necessary steps that you must follow to fix any related problems.

- During automated test installations on Windows x86 systems, the following error occurred intermittently during new NetBackup 7.5 installations:

```
ERROR: NetBackup Database Creation Failed
```

Failures did not occur when new NetBackup 7.5 installations were performed manually. Manual installations are those typically performed by a network administrator.

In the unlikely event that this error occurs, do the following:

- Exit from the NetBackup 7.5 Installation Wizard.
- Check the Windows Registry for the following entries and remove them:  
 HKEY\_LOCAL\_MACHINE\SOFTWARE\Veritas\NetBackup\*\\*  
 HKEY\_LOCAL\_MACHINE\SOFTWARE\VERITAS\VxDBMS
- Reinstall NetBackup 7.5.
- Starting with NetBackup 7.5 executing the `pkgrm SYMCnetbp` command on a Solaris system no longer displays the following question:

```
Are you doing this pkgrm as a step in an upgrade process?
```

The `pkgrm` is part of an upgrade and therefore a full removal of all NetBackup files does not occur. To completely remove NetBackup from your Solaris system, see Chapter 6, "Removing NetBackup server software" in the *NetBackup Installation Guide for UNIX and Linux*.

- Use of IPv6 addresses as server names.  
 Symantec recommends that you do not use IPV6 addresses as server names in the install.
- NetBackup 7.5 client installations can fail on FreeBSD 7.x or 8.x systems.  
 NetBackup 7.5 client installations can fail on FreeBSD 7.x or 8.x systems. That can happen if the `pbx_exchange` daemon is not able to start.

If you encounter a failure, you can find references to missing libraries in the PBX installation log. For example:

```
/libexec/ld-elf.so.1: Shared object "libm.so.4" not found, required  
by "vxlogcfg.bin"
```

Perform the following steps to install a 7.x client if you encounter this installation failure.

- Install the following compatibility package:  
 On FreeBSD 7.x systems, you can install the compatibility package `compat6x-i386-6.3.603000.200801` that comes with the operating system.



On FreeBSD 8.x systems, you can download and install the following compatibility package:

```
ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/  
packages-8-stable/Latest/compat6x-i386.tbz
```

- Use the following command to remove the partially installed PBX:

```
pkg_delete VRTSpbx
```

- Install the NetBackup 7.x client.

- PBX may not start after a restart on an AIX platform.

If you upgrade from NetBackup 6.5.x to NetBackup 7.x on an AIX system and then perform a restart. You should verify that the PBX and NetBackup services have started after you started NetBackup again. If the services did not restart, the cause may be that the entry, `install_assist` already exists in the `/etc/inittab` file. This entry exists if the issue occurred when you installed AIX on an IBM computer.

If you encounter this issue, determine if the `install_assist` entry already exists in the `/etc/inittab` file. If it does, you can comment the entry or remove it from the file and attempt to restart again. After the restart completes, make sure that the PBX and NetBackup services start.

- You may receive some `Text file busy` error messages if you use the `update_clients` command.

When you use the `update_clients` command to push to HP PARISC or Itanium clients, you may see some messages similar to the following:

```
rm: /usr/opensv/lib/libvxexticuST.sl.1 not removed.  
Text file busy  
rm: /usr/opensv/lib/libvxlisST.sl.1 not removed.  
Text file busy  
rm: /usr/opensv/lib/libvxulST.sl.1 not removed.  
Text file busy  
rm: /usr/opensv/lib/libvxACEST.sl.3 not removed.  
Text file busy
```

If you use the `install trace` and see that the client package installed successfully before any of these error messages appear, you can safely ignore the messages. For example, you may verify the following:

- Installing SYMCnbclt package.
- Installation of SYMCnbclt was successful.

These error messages occur when the install attempts to clean some old files and those files are temporarily held open. The files are cleaned during the next attempt.

- Check for available disk space before you upgrade to NetBackup 7.5  
During an upgrade, 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/opensv/db/data` for UNIX-based operating systems and `\Veritas\NetBackupDB\data` for Windows-based operating systems when you use default installation methods.
- 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/opensv/netbackup/logs` on UNIX and `C:\Program Files\Veritas\Netbackup\logs` on Windows) after an upgrade to NetBackup 7.x. 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.x if you specify the following.  

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

  
Where `<root log dir>` is either `/usr/opensv/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.
- If you install NetBackup server on top of an existing NetBackup client to upgrade the client to a server, PDDE is non-functional. That issue applies to

SLES, Red Hat, and Solaris platforms. You must completely remove the NetBackup client and then install the NetBackup server software. Follow the instructions in the *NetBackup Installation Guide for UNIX and Linux*.

- 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://www.symantec.com/docs/TECH51096>
- 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.
- Symantec recommends the following third-party updates when you run NetBackup on Windows operating systems:
  - QLA2340 Q\*Logic HBA driver 9.1.4.15 (required)  
[http://support.qlogic.com/support/oem\\_product\\_detail.asp?p\\_id=253&oemid=65&oemname=QLA2340](http://support.qlogic.com/support/oem_product_detail.asp?p_id=253&oemid=65&oemname=QLA2340)
  - QLA2340 Q\*Logic HBA BIOS 1.47 (required)  
[http://support.qlogic.com/support/oem\\_product\\_detail.asp?p\\_id=253&oemid=65&oemname=QLA2340](http://support.qlogic.com/support/oem_product_detail.asp?p_id=253&oemid=65&oemname=QLA2340)
  - All other Q\*Logic HBAs use latest driver and BIOS (suggested) [http://support.qlogic.com/support/oem\\_product\\_list.asp?oemid=65](http://support.qlogic.com/support/oem_product_list.asp?oemid=65)
- The default shared-memory requirements on UNIX systems are greater for NetBackup 7.x than previous releases.  
See the *NetBackup Installation Guide for UNIX and Linux*.  
See the *NetBackup Troubleshooting Guide for UNIX, Windows and Linux*.

- UNIX 32-bit system support has been discontinued for all platforms except FreeBSD and Macintosh (universal - i386/ppc). If you currently use NetBackup 6.x on any 32-bit systems other than FreeBSD and Macintosh, you cannot upgrade those systems to 7.x. However, you can migrate the NetBackup 6.x catalogs and databases on those systems to a supported 64-bit platform system and then upgrade to 7.x.

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.

- Symantec recommends that you have the master server services up and available during a media server upgrade.
- Symantec recommends that all customers running HP-UX 11.23 on PARISC install the patch (PHCO\_33431). If you do not install the patch before you install NetBackup on a system with an updated version of 11.23, the installation may fail. That does not apply to HP Itanium because the HP Itanium OS has moved to version 11.31.
- 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 7.0 documentation set.
- In case of NetBackup in a remote configuration, install the remote EMM server before you install the master server.
- In some cases, when you perform a push installation on Windows, the default installation folder is incorrectly presented as `C:\Program Files (x86)\Veritas`. However, there are no known issues with product functionality if you install to `C:\Program Files (x86)`. Symantec recommends that you use an installation folder of `C:\Program Files\Veritas`.  
 If you encounter this issue, please modify the default folder specification to `C:\Program Files\Veritas`.
- When using the NetBackup client deduplication (or client direct) feature with NetBackup 7.5 media server, the client server must have, at a minimum, NetBackup 7.0.1 already installed.

## Installing NetBackup in Solaris 10 zones

Zones are the isolated application execution environments that an administrator can create on a single, Solaris 10 instance. For the information that describes

NetBackup's support for Oracle Solaris Virtualization, refer to the following Technote on the Symantec Support Web site.

<http://www.symantec.com/docs/TECH162994>

The Technote contains the following information:

- How to install NetBackup standard client software in local zones
- Solaris 10 logical domains support
- BMR client support in Solaris zones

## NetBackup cluster

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

- NetBackup 7.5 media server installations cannot be clustered. However, you can upgrade existing NetBackup 6.x clustered media servers to version 7.5 and they remain clustered.
- 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 interfaces

The following subsections contain the release and operational information about the NetBackup interface, such as the NetBackup Administration Console, and the Activity Monitor.

### NetBackup Administration Console for Windows

The following items pertain to the NetBackup Administration Console for Windows:

- 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 interfaces

The following is the general operational information that pertains to the NetBackup-Java Administration 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 Web site.

<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 Web site.

<http://www.symantec.com/docs/TECH50711>

## 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

The following identifies the issues that relate to Internationalization and localization.

- Do not mix non-English version of Windows and UNIX platforms.  
If you mix non-English versions of Windows and UNIX platforms, differences in operating system architecture and encodings may cause non-English file names and folder names to be displayed incorrectly within the user interface. That may cause functional failures.
- The NetBackup command-line menu user interfaces (MUIs) cannot input and modify multi-byte characters.  
The NetBackup command-line menu user interfaces (MUIs) cannot input and modify multi-byte characters and they are not localized to any language. The following list identifies the various menu user interfaces:
  - `bp`
  - `bpadm`
  - `tpconfig` **menu**
  - `vmadm`
  - `vltadm`
- May need to apply the Sun Solaris patch 6901233 to fix an.  
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 Sun Microsystems™ issue, 6901233.

See, [http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=6901233](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6901233) for more information about this issue.

If you encounter this issue, apply the Solaris patch that Sun provides to fix this issue 6901233.

- 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 NetBackup, without installing the localized contents in the Language package CD first, you must remove the localized contents that are installed on your system.
- 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).  
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.
- NetBackup can be installed to environments running different versions of UNIX based operating systems as long as the system locales are identical. Use of different locales across UNIX platforms can cause issues with the user interface.
- Mixing non-English versions of Windows and UNIX platforms may cause functional failures.  
If you mix non-English versions of Windows and UNIX platforms, differences in operating system architecture and encodings may cause non-English file

names and folder names to be displayed incorrectly within the user interface. That may cause functional failures.

- On non-English versions of Windows and UNIX systems, the NetBackup-Java Administration Console may display non-English characters incorrectly leading to functional failures.
- Certain database agents have restricted support of localized environments.

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 localized characters (for example, non-ASCII, multi-byte characters) is not supported in:

- Any database object names, like instances, databases, tablespaces, filegroups, data files, portals, and so forth
- The path names of database files, directories, transaction logs, or other database storage locations
- The path names that are specified in the policy **Backup Selections**, like script, template, or batch file locations  
That applies to all supported platforms, including the use of previous versions of those NetBackup database agents with NetBackup 6.0 servers.
- Specific NetBackup user-defined strings must not contain Multi-byte characters.

The following NetBackup user-defined strings must not contain Multi-byte 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
- BMR Configuration 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 123.
- 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 OpsCenter notes

The following operational notes pertain to NetBackup's OpsCenter.

- 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 logon to the OpsCenter GUI 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`.
- If you edit certain standard reports and select **Backup from Snapshot Job type from the Filters** section, incorrect data is shown if data for Backup from Snapshot jobs exists. That also happens when you create image-related reports using custom reporting and apply Backup from Snapshot job type filter. The following standard reports display incorrect data when you select Backup from Snapshot job type from the Filters section:
  - **Hold Reports > Image Retention Summary**
  - **Backup > Planning Activity > Stored Backup Images > Duplicate copies**
  - **Backup > Planning Activity > Stored Backup Images > Stored Backup Images on Media**
  - **Backup > Planning Activity > Stored Backup Images > Valid Backup Images**
  - **Backup > Planning Activity > Capacity Planning > Forecasted Size**
  - **Backup > Planning Activity > Capacity Planning > Historical Size**
- In a Solaris cluster, the Search broker is not a clustered component and the NetBackupOpsCenterAgent does not monitor it.
- The Drive Throughput and Drive Utilization reports display data only till 1:00 A.M. and not till the time when you run the report. That is because OpsCenter collects data for Drive Throughput and Drive Utilization report once per day at 1:00 A.M. everyday after midnight.

Therefore the Drive Throughput or Drive Utilization reports are only able to report on data up until 1:00 A.M. on that day, even when run with a relative timeframe of Previous 24 hours. Similarly if you run **Drive Throughput** and **Drive Utilization** reports at 2:00 P.M. in the afternoon, the reports display the data that is collected until 1:00 A.M. only.

- When you click the Symantec OpsCenter Administrator's Guide link from the login page of the OpsCenter GUI, the Administrator Guide opens in English language. That happens even when you install a language pack or change your preferred language to a language other than English.
- The **Job Attempt Status Detail** report may provide inaccurate information. This report provides information about the completion status for a NetBackup job.

This report provides inaccurate output when a Job ID is reset in NetBackup such as catalog recovery or by manually resetting of the Job ID. In case the Job ID is reset, you must delete the NetBackup master server from the OpsCenter console and add it again.
- Beginning with this release, Symantec OpsCenter no longer supports Backup Exec 10.x.
- Beginning with this release, Symantec OpsCenter supports 64 bit on Windows.
- A known issue in Firefox 8.x causes the downloaded attachments to be named as `ExportReportAction.do` or some other file name and type which cannot be opened.

That issue affects you if you use Firefox 8.x to access the OpsCenter console and generally occurs when you export a report or an export job and audit logs. Because of the Firefox 8.x issue, when you export an OpsCenter report, the report is saved with the name `ExportReportAction.do` and does not open.

To resolve this issue, Symantec recommends that you upgrade to Firefox 9.0. If you want to continue using Firefox 8.x, when you export a report or job logs using Firefox 8.x and are prompted to open or save the exported file, click **Save File**. In the **Enter name of file to save to** dialog box, select Save as type as **All Files** and then rename the file with the proper extension (like replace the default name `ExportReportAction.do` with `filecount.pdf`) and click **Save**. You can then open this report.

---

**Note:** If you do not see **Enter name of file to save to** dialog box, click `Firefox > Options > General` and check the **Always ask me where to save files** option.

---

- If you use OpsCenter to the appropriate license keys for the licensed version (OpsCenter Analytics), the breakup jobs may still not be displayed. To display the breakup jobs, disable and then enable the data collection for the master server from **Settings > Configuration** in the OpsCenter console.
- An alert policy that you had created in OpsCenter 7.0.x or 7.1.x may not be visible when you upgrade to OpsCenter 7.5. That happens if some other user in OpsCenter 7.0.x or 7.1.x modified this policy.

- An alert policy based on the Agent Server Communication Break condition is always based on the **ALL MASTER SERVERS** view. If you created an alert policy based on the Agent Server Communication Break condition, and you do not have access to the **ALL MASTER SERVERS** view, alerts are not generated for the alert policy.
- OpsCenter supports normal restores only. Other restore types like Archived, Raw Partition, True Image, Virtual Machine, and so forth are 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 (like Backup Sub Job File Count, Backup Sub Job Size) is available only for 50 job directories. That is because when a NetBackup policy or job has more than 50 backup selections that are associated with it, the breakup jobs data for only 50 backup selections is available with NetBackup. 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 as data collection in VBR happened through CLI's (and not by NBSL).
- OpsCenter Analytics custom reports may show inaccurate data.

OpsCenter Analytics custom reports may show inaccurate data for the following columns:

  - **Backup Media HSize**

That is applicable only if data is collected from NetBackup master servers 7.0 and 7.0.1. That generally happens when you generate a custom report using the **Media** filter and select the **Backup Media HSize** column.
  - **Backup Image Copy Multiplexed State**

That is applicable only if data is collected from NetBackup master servers 7.0 and 7.0.1. That generally happens when you generate a custom report using the **Image** filter and select the **Backup Image Copy Multiplexed State** column.
- 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.
- Consider the following best-practice suggestions about report names in OpsCenter 7.x

Review the following points about report names in OpsCenter 7.x:

- The report name must be unique across the report tree.
- The report name must not contain any special characters like (/ \ \* ? | ")
- The report name must not be more than 220 characters.

If there are special characters in a report name like (/ \ \* ? | "), these special characters are replaced with an underscore "\_" when you upgrade from NOM, VBR, OpsCenter 7.0 or 7.0.1 to OpsCenter 7.x. For example, a **media\*summary** report in OpsCenter 7.0 is renamed as **media\_summary** report in OpsCenter 7.x.

- 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 OpsCenter server can stop receiving events from the master server after a NetBackup 7.x upgrade.

If all following conditions are applicable, you should add the **OPS\_CENTER\_SERVER\_NAME** entry to the `bp.conf` file on a UNIX system or the registry on a Windows system to set the OpsCenter server name. Symantec recommends that you do add the entry before you attempt to upgrade to 7.x.

- 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 7.x upgrade.

- If you attempt to restore snapshot backups from OpsCenter, expanding the snapshot backup folders from the search results or browsing the snapshot backup clients using the Browse tab may fail with the following exception on the GUI: "Tree table fetch failed".

This issue generally occurs when you browse snapshot backups in the following scenarios:

- If there are a large number of snapshot backup images (more than 1000) for the specified time range.
- If there are a large number (at least 32) of the SLP-managed snapshot jobs that are running on NetBackup simultaneously in the background.

A possible workaround is the following:



- Try browsing the clients when NetBackup is not running a large number of snapshot jobs. The actual number and type of jobs depends on the NetBackup master server computer configuration.
- Select a smaller time range for search e.g. a week.
- 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 the absolute 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.
- When you add or edit a NetBackup master server, if you try to add different values in the **OpsCenter's Preferred Network Address** Symantec recommends that you disable the **connection pooling** option in OpsCenter. If the option is not disabled, you may not be able to locate the NetBackup server or and get the required results.

The same is true when you create or edit an OpsCenter Agent and add values in the **OpsCenter Server Network Address** field.

To disable connection pooling, add the following property **nbu.orb.common.jacorb.connection.server\_timeout=5000** to the `config/scl.conf` file and restart the OpsCenter services.

When you finish the testing, remove the property from the `config/scl.conf` file and restart the OpsCenter services.
- When a rollback is run, some snapshots are deleted. To see which snapshots are deleted, uncheck the **Force rollback even if it destroys later snapshots** option and run the rollback operation again. A list of snapshots to be deleted or invalidated is provided in the *Detailed Status* of the failed restore job. Check the list and if you determine that it's okay to lose that data, then select the **Force rollback even if it destroys later snapshots** option and run the rollback again.
- If you create a custom report as a dual axis and select the **Y1 and Y2 axis** chart type as either a Stack Bar chart or a Bar Chart, the chart that is plotted for the Y1 axis gets hidden behind the Y2 chart.
- When you click on a status code on the OpsCenter Status Code Help, the contents on the right side of the Help pane are different from the contents on the left side. For example, if you click on **status code 2074** on the left-side, the description of some other status code is displayed on the right side of the Help pane. This type of error is generally encountered when the OpsCenter Server is installed on a Windows system.

- Page 175 of the Symantec OpsCenter Administrator's Guide mentions the following under Adjusting the default heap size for the OpsCenter server section.  
 "If the OpsCenter server processes are consuming a lot of memory (which may happen with large OpsCenter configurations), it may be helpful to increase the OpsCenter Server heap size. The OpsCenter Server default heap size can be increased from 1024MB up to 1400 MB for 32-bit platforms."  
 Additionally note that if you configure the heap size for OpsCenter Server to be more than 1400 MB on 32-bit systems, the OpsCenter Server service starts and then stops within a few seconds. You must configure the heap size to a value lesser or equal to 1400 MB and start the OpsCenter Server service again. See Adjusting the default heap size for the OpsCenter server section in the Symantec OpsCenter Administrator's Guide for details.
- The Offline Until column under Monitor > Hosts > Client in the OpsCenter console displays inaccurate information.
- You cannot browse or restore from backups for policy type **MS-Windows** and snapshot type **OST FIM** using **Manage > Restore** tab in OpsCenter.
- Consider a scenario where a client (like ABC) is backed up by two master servers. And you then create a CSV file with the following contents:
  - Client, V1, ABC:NetBackup1
  - Client, V1, ABC:NetBackup2

In this example, the client ABC is backed-up by two master servers NetBackup1 and NetBackup2. If you import this CSV file using View Builder, then the view that is created contains only one node (and not two). OpsCenter treats these two as different clients having the same name. However, if you import two clients with same name using CSV or TSV under the same parent then only one client gets imported. The other client needs to be added manually.

- If you create a VMWare policy on the master server and add the virtual client names that have spaces like `vmware _sr`, OpsCenter interprets the client name as `asvmware%20_sr`. Because OpsCenter interprets a space in the client name as `%20`, values in the **Exist in the policy** column in the **Virtual Client Summary** report are inaccurate and show the values as **No**.
- If you create an alert policy based on the **Mount Request** alert condition and select master servers with version 7.0 and above, the alert that is generated does not provide all the details like RVSN, Mode, Request ID etc. These fields may appear blank.
- If you try to restore a Windows client using OpsCenter, selecting the parent node to select all components of the client like drives does not work from **Select Files or directories > Browse**. You must select each component (or

drive) and add it to the Restore Cart separately. Similarly, you must select all the individual components separately (and not the parent node) to perform restores. Click **Restore now** to begin the restore.

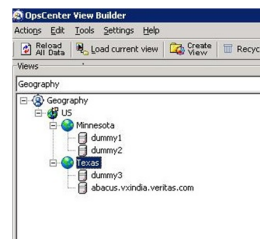
If you attempt to restore a UNIX client with OpsCenter, adding the “/” folder by selecting the corresponding checkbox does not work from **Select Files or directories > Browse**. You must select all the individual contents of the folder and add them to restore cart separately. Similarly you must select all individual contents of the folder to perform restores. Click **Restore now** to begin the restore..

- The view selection for the **Monitor > Alerts and Manage > Alert Policies** pages is separate from the view selection for the other pages. The default view that is selected on **Monitor > Alerts and Manage > Alert Policies** is **Ignore View** filter. On all other OpsCenter pages, the default view is **ALL MASTER SERVERS**. Any time when you move back and forth between these pages, the appropriate view selections for **Monitor > Alerts and Manage > Alert Policies** pages and view selections for all other OpsCenter pages are preserved separately.

However, when you click the **Alert Summary by Severity** section on the **Monitor > Overview** page, then during navigation to **Monitor > Alerts** page, the view selection for **Monitor > Alerts** is replaced by the view that is selected for all other OpsCenter pages. For example, suppose the **Monitor > Jobs** page has view **V1** selected and the **Monitor > Alerts** page has view **V2** selected. After you click on the **Alert summary by Severity** section and navigate to the **Monitor > Alerts** page, then the **Monitor > Alerts** page shows view **V1** to be selected.

The process of deleting a view needs better documentation.

Consider a view that is called **Geography** that has several nodes under it such as **US, Minnesota, and Texas**.



The view Geography contains four levels and the last level contains clients. You may delete this view or its components in the following manner:

Deleting the entire View – for example, delete **Geography**:

- If you select a view, i.e. select Geography and delete it, all the components that are under Geography are also deleted.

- The entire view (including all components like nodes) is deleted from the OpsCenter database. You cannot restore this view using the recycle bin .

Deleting a non-leaf node – for example, delete **US**:

- When you delete a node, say US, then node 'US' and all its components are deleted.
- Node US and all its components are moved to the recycle bin and are available for restore. All objects (like dummy1, dummy2, dummy3, and abacus.vxindia.veritas.com) are also available in "Object not in selected view" tab for reassignment.
- You can restore the deleted node "US" from the Recycle bin. To restore any node, ensure that the parent is also restored. You can select the node US and all its components from the recycle bin and click Restore.
- In the OpsCenter database, US and its children are marked as deleted but are not deleted from the database. However you can delete US from the database by purging US and its components from the recycle bin .

Deleting a leaf node– or example, delete **Minnesota**:

- If you delete a node, the contents of the node are also deleted. For example, deleting Minnesota also deletes dummy1 and dummy2.
- In the OpsCenter database, the node Minnesota and its components are marked as deleted but they are not deleted from the database. However you can delete Minnesota and its components from the database by purging them from the recycle bin .
- You can restore a node and its components that you have deleted (like Minnesota) from the recycle bin . Note that the recycle bin displays a flat list and does not display any hierarchy. To restore any component, ensure that the parent is restored. For example to restore dummy1, you must restore the parent Minnesota. You can also select the node and all its components and click **Restore**.

Deleting an object:

- When you delete an object, say dummy1, then only that object gets deleted and is available in **Object not in selected view** tab.
- In the OpsCenter database, dummy1 is marked as deleted but is not deleted from the database. However, you can delete dummy1 from the database by purging this object from the recycle bin .
- You can restore any deleted object from the recycle bin .

## About Replicaton Director notes

This section contains known operational notes that apply to the NetBackup Replication Director feature.

- The NetApp q-tree fan-in configuration is not supported with Replication Director.
- Replication Director does not support backup and restore of snapshots on NetApp volumes that contain a mix of qtree and non-qtrees data. Backup and restore is supported if the volume contains one or the other.
- Do not configure a NetBackup domain to include more than one DataFabric Manager server. If you configure more than one Network\_NTAP Storage Server per NetBackup domain, snapshots will only be deleted from one of the storage servers at image expiration time.
- For Replication Director, NetApp's `NBUAdapter` doesn't have IPv6 support. In NetBackup 7.5, the `NBUAdapter` does not support IPv6. IPv4 is automatically used instead.
- 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, resulting in 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 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

The following operational notes and limitations pertain to the NetBackup Snapshot Client.

- 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`

`rsi=32768, wsi=32768, NFSv3, dev=4000033` and `/test1` on `f3170-7-15:/vol/sample1` `rsi=32768, wsi=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.

## NetBackup for VMware notes

The following operational notes pertain to NetBackup's VMware feature:

- VMware has identified a problem that prevents the restore of a thin-provisioned virtual machine.

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, and 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, 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.

See, VMware SR#-1615494851 for more information.

- VMware backup and restore are not currently supported on IPv6 networks.

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. This restriction applies to vCenter servers and to ESX servers.

If you specify an IPv6 address as a Virtual machine server name, the "Validate Credentials" option on the **Add Virtual Machine Server** dialog fails. If you attempt to back up the virtual machines that reside on that VMware server by means of these credentials, the backup fails with NetBackup status 156.

- Thin provisioned disks may be stored as thick provisioned disks when a VMware virtual machine is restored.

When a VMware virtual machine is restored, its thin provisioned disks are restored as thick provisioned in the following case:

- Hard disk 1 on the source virtual machine is thick provisioned.
- One or more of the other disks that are on the source virtual machine are thin provisioned.

- 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 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 workaround, use any of the following:

- The **nbd** transport mode.
- The **SAN** or **nbd** transport mode if the restore host is a physical computer.
- 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
iolite.min.vrts.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.

- Restoring a virtual machine with the `nbdssl` transport mode fails if the destination is an ESX 3.5u 5.0 server that vCenter 5.0 manages. The **Job Detailed Status** log contains messages similar to the following:

```
6/14/2011 7:09:13 PM - Critical bpbrm(pid=4068) from client vnet8:
FTL - Virtual machine restore: VxMS initialization failed". Job id = [17
```

This error results from a VMware issue and is reported as VMware Support Request 11107948110.

As a workaround, do one of the following:

- Enter NetBackup credentials for the 3.5 ESX server as a **VMware Restore ESX Server**. That ESX server performs the restore.
- Use the `nbd` transport mode to restore the virtual machine (not `nbdssl`).
- 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.
- An issue with VMware VDDK 5.0 prevents the full reporting of write failures to an offline SAN disk during a virtual machine restore. If a write failure to an offline SAN disk occurs during a restore over the SAN, NetBackup may be unable to detect the error. The restore operation appears successful but the restored vmdk files may not contain any data.

Make sure that the status of the SAN disk on the restore host is online (not offline). Disk status can be checked or changed using the Windows `diskpart.exe`

utility or the Disk Management utility (diskmgmt.msc). When the disk status reads online, retry the restore.

See the following VMware articles for more information:

<https://www.vmware.com/support/developer/vddk/VDDK-500-ReleaseNotes.html>

<http://kb.vmware.com/kb/2010428>

- An issue with VMware VDDK 5.0 prevents the full reporting of write failures to an offline SAN disk during a virtual machine restore. If a write failure to an offline SAN disk occurs during a restore over the SAN, NetBackup may be unable to detect the error. The restore operation appears successful but the restored vmdk files may not contain any data.

Make sure that the status of the SAN disk on the restore host is online (not offline). Disk status can be checked or changed using the Windows diskpart.exe utility or the Disk Management utility (diskmgmt.msc). When the disk status reads online, retry the restore.

See the following VMware articles for more information:

<https://www.vmware.com/support/developer/vddk/VDDK-500-ReleaseNotes.html>

<http://kb.vmware.com/kb/2010428>

- VMware does not support the restore of virtual machines directly to an ESX 5.x server that vCenter manages. To restore the virtual machine, select the vCenter server as the destination.

You can give NetBackup access to a dedicated restore ESX server. SAN-based restores that go directly to a restore ESX server are faster than restores through the vCenter server. For more information, see "Adding NetBackup credentials for VMware in the NetBackup for *VMware Administrator's Guide*.

- 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. As a result of writing 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.

---

- On an ESX 3.5 server that is managed by a vCenter 4.0 or later server, virtual machine backup or restore by means of the hotadd transport mode fails. This error results from a known issue in VMware licensing (VMware support request 11081899907).

Note the following workarounds:

- Use the **nbd transport** mode instead of hotadd.
- Use the **hotadd transport** mode with an ESX 3.5 server that vCenter 2.5 manages.
- Use the hotadd transport mode with an ESX 4.x or 5.x server.
- To restore a virtual machine in a datastore cluster and retain its DRS configuration, the target server must have the VMware "Storage DRS" and "Profile-Driven Storage" licenses. If the target server does not have those licenses, the restore fails with NetBackup status 2820.  
To restore to a VMware server that is not licensed for storage DRS, do not select "Restore storage DRS configuration" on the NetBackup "Virtual Machine Options" dialog.
- 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.

## General NetBackup 7.x notes

The following items describe general NetBackup 7.5 operational notes.

- 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.
- In this release, the NetBackup Cloud feature does not support a remote EMM server configuration.
- In this release, NetBackup performs additional validations before it allows the creation of storage lifecycle policies. In previous versions, NetBackup allowed the creation of all SLPs with undetected errors. After a NetBackup environment is upgraded to 7.5, when an administrator opens a previously permitted, but invalid SLP, the SLP must be corrected in order for it to be saved and run in 7.5.
- 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 can have a positive impact on NetBackup and help avoid the following issues:

- Insufficient system file descriptors can cause the `EMM_DATA.db` file to grow very large.  
<http://www.symantec.com/docs/TECH168846>
- Some jobs end with a Status 26 error in the `bpbrm` log on the media server:  
<http://www.symantec.com/docs/TECH70191>
- The NetBackup 7.x line contains several new error status codes.  
With the release of the NetBackup 7.x product line came several new error status codes. They are intended to be more informative replacements for some status 5 (restore failed) cases. Some confusion might occur when a command-line operation is executed from a back-level client and causes a new error code to appear. In this situation, the new code appears on the older client along with a message that indicates that it is an unknown error code. However, the correct message appears on the master server as well as on any new clients.
- 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 are generated at the same second may be printed out of the actual order in which 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/opensv/db/bin/servername`. NetBackup also trims the name to 31 characters if necessary.
- NetBackup supports software system management standards.  
To support software system management standards, NetBackup installs two XML files on each NetBackup host. These files do not affect NetBackup functionality. In addition, you can identify these files by the suffix `.swidtag`.
- 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 Web site.

<http://www.symantec.com/docs/TECH154279>

- The following list indicates the disk storage units that support Granular Recovery in NetBackup 7.5.

- BasicDisk
- AdvancedDisk
- PureDisk

The following list indicates the disk storage units that do **not** support Granular Recovery in NetBackup 7.5.

- OpenStorage
- SnapVault

- If you attempt to restore a large number of files such as 2,000,000, the restore job may remain in the queue state in the NetBackup Administration Console. If that happens, you cannot restore those files.

This issue is the result of the `bprd` process, which uses almost 100% of the CPU utilization and a significant amount of memory. These two things together, causes the restore job to remain in the queued state.

- About NetBackup mixed version support

The NetBackup catalog resides on the master server. Therefore, 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.

- 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.
- This release introduces a change in syntax for the parameters in the `LIFECYCLE_PARAMETERS` file, that affects storage lifecycle policies. The administrator can create a `LIFECYCLE_PARAMETERS` file to customize how the NetBackup storage lifecycle manager (`nbstserv`) runs duplication and import jobs. The parameters are described in the *NetBackup Administrator's Guide, Volume I*.

---

**Note:** With NetBackup 7.5, the syntax of the parameters has changed. An equals (=) sign is now used between the parameter name and the value. For example,

```
IMPORT_SESSION_TIMER = 1.
```

---

- This release contains new and corrected LIFECYCLE\_PARAMETER values. The spelling of **TRESHOLD\_JOB\_COUNT** has been corrected to **THRESHOLD\_JOB\_COUNT**. And the new **MAX\_IMAGES\_PER\_SNAPSHOT\_REPLICATION\_JOB** parameter has been added. That parameter sets the maximum number of images that can be included in a snapshot replication job. The value is used to tune the size of replication jobs to avoid overloading the hardware vendor replication infrastructure.
- 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/opensv/db/lib

/usr/opensv/lib

See the following Technote on the Symantec Support Web site:

<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.

- Cannot use **Any\_Available** in a storage lifecycle policy.  
Beginning with NetBackup 7.5, you cannot specify **Any\_Available** in the **Storage Unit** field of an SLP operation. It does not appear in the pick list in the user interfaces. Existing SLPs continue to execute as before if **Any\_Available** is already used in the SLP as long as the SLP is not changed. If the SLP is edited, the **Any\_Available** selections must be replaced with real storage units or storage unit groups before the changes can be successfully committed.
- If you try to expire the image or the image copies manually that are not SLP-complete, the request fails with a 1573 error. To expire the image or images, you can do one of the following:
  - Wait for the image or copy to become SLP-complete.
  - Use the `nbslutil cancel` command to terminate the SLP processing.
  - Add the `-force_not_complete` option to the `bpexpdate` command to force the expiration even if the image or copy is not SLP-complete.
- The `nbserv` 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 for UNIX, Windows, and Linux.*  
*See the NetBackup Status Codes Reference Guide for UNIX, Windows, and Linux.*
- 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 using the Windows NTFS Change Journal 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 Web site for accurate use information.

## 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 `nbfssd` 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.

See [“About resilient network connections”](#) on page 34.

# End-of-life notifications

This chapter includes the following topics:

- [NetBackup 7.x end-of-life notifications](#)

## NetBackup 7.x end-of-life notifications

This section contains information about the features, platforms, and devices that may no longer be compatible with NetBackup in the next major release.

---

**Note:** This document is posted on the Symantec Support Web site and may be updated after the GA release. Therefore, Symantec recommends that you refer to the following Technote on the Symantec Support Web site to view the latest NetBackup release information.

<http://www.symantec.com/docs/DOC5041>

---

Another resource that you can use to view end-of-life information is the Symantec Operations Readiness Tools (SORT). That is a Web-based tool that supports Symantec enterprise products. Part of this support is to provide users with "End of Life (EOL)" and "End of Support Life (EOSL)" information for NetBackup licensed software. To view this information, Go to the [SORT > Support > Related Links](#) page on the [SORT for NetBackup Users Web](#) site.

See, <https://sort.symantec.com/eosl>.

## About general NetBackup notifications

The following is a list of general NetBackup end-of-life notifications that go into effect as of the next major release of NetBackup:

- Beginning with this release, Symantec OpsCenter no longer supports Backup Exec 10.x.

- In the next major release, support for all of the active and the passive media server clusters that use the NetBackup clustering agents is withdrawn.
- In the next major release after 7.5, support for Remote-EMM and Shared-EMM server configurations will be withdrawn. Remote-EMM and Shared-EMM server configurations are defined by the components that include the NetBackup relational database (NBDB), Enterprise Media Manager (EMM), and Resource Broker (RB) being defined on a server that is not the master server.  
See the section, “About the Enterprise Media Manager” in the *NetBackup Administrator's Guide - Volume 1* for more information.
- Starting with the next major release of NetBackup, the NetBackup-Java Administration Console is no longer supported.
- Backup Exec Tape Reader (BETR) refers to the ability within NetBackup to import and restore from Backup Exec (BE) backup sets (images). As of the next major release, NetBackup, BETR is no longer compatible.
- NetBackup 7.5 no longer supports the Windows Itanium (IA64) platform for NetBackup clients and servers. However, NetBackup 7.5 offers back-level support for NetBackup 7.1 Windows IA64 clients.

The following is a list of features or functionality that are no longer compatible with NetBackup.

- NetBackup 7.x does not support OpenAFS.
- OpsCenter 7.x does not support Internet Explorer 6.x.
- The `ovpass` driver on AIX is no longer supported as of this release of NetBackup. However, support for robotic control devices with an IBM inquiry string that use the IBM Atape driver is still supported.
- The NearStore disk type storage unit is no longer supported with NetBackup starting with this release.
- The NetWare client is no longer compatible.

## About the operating systems that may not be supported in the next major release

Changes to the operating systems that Symantec supports may directly affect you. Symantec is committed to notifying you of these changes before the major release where the support is discontinued.

The following lists show the operating systems that may not be supported in the next major release of NetBackup and a change in the client support. For the most recent list of supported platform information, download the NetBackup operating



system compatibility list from the Symantec Support Web site with the following URL.

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

- The following operating systems may not be supported at the next major release of NetBackup.
  - AIX 5.3
  - FreeBSD 6.1, 6.2, 6.3, 7.0, 7.1, and 7.2
  - HP-UX PA-RISC 11.11, 11.23, and 11.31
  - Red Hat Enterprise Linux 4.0

---

**Note:** The status of any operating system that is identified in the following table can change if the market or the vendor's support positions change.

---

- Exchange 2003 will no longer be supported in the next major release of NetBackup.
- In the next major release of NetBackup this Client will be supported with 64-bit binaries only.
  - FreeBSD 8.0 and 8.1 (32-bit)
  - Mac OS X 10.6 (32-bit)

---

**Note:** Back-level support of NetBackup 7.x Clients are available until NetBackup 7.x reaches the end of support.

---



# Related Documents

This chapter includes the following topics:

- [About related NetBackup documents](#)
- [About NetBackup release notes](#)
- [About getting started guides](#)
- [About installation guides](#)
- [About administrator's guides](#)
- [About other documents](#)
- [About administration of options](#)
- [About administration of database agents](#)
- [About the Troubleshooting guide](#)

## About related NetBackup documents

This topic lists and describes the technical manuals that relate to NetBackup.

The DVD-ROM for each NetBackup product has a copy of the related manuals in Adobe Portable Document Format (PDF). The PDF files are either in the root directory or the Doc directory on the disk.

To view the PDF copies of the manuals, you need an Adobe Acrobat reader. You can download a copy of this product from the Adobe Web site at the following URL:

<http://www.adobe.com>

Symantec assumes no responsibility for the correct installation or use of the reader.

## About NetBackup release notes

The following release notes documents were released with this version of NetBackup.

- *Symantec NetBackup Release Notes*  
NetBackup\_Release\_Notes.pdf

This document contains information about NetBackup on UNIX-, Linux-, and Windows-based servers, such as the platforms and operating systems that are supported. It also contains any operating notes that may not be in the NetBackup manuals or the online help .

## About getting started guides

The following getting started guides were released with this version of NetBackup.

- *Symantec NetBackup Getting Started Guide*  
NetBackup\_GettingStarted\_Guide.pdf

Provides a high-level description of the latest NetBackup release. This document also contains the information that explains the content of the NetBackup media kit.

- *Symantec NetBackup Backup, Archive, and Restore Getting Started Guide*  
NetBackup\_BAR\_GS\_Guide.pdf

Explains how to use the NetBackup Backup, Archive, and Restore interface to perform backup and restore operations for UNIX, Windows, and Linux systems.

## About installation guides

The following Installation documents were released with this version of NetBackup.

- *Symantec NetBackup Installation Guide for UNIX*  
NetBackup\_Install\_UNIX.pdf

Explains how to install NetBackup software on UNIX- and Linux-based platforms.

- *Symantec NetBackup Installation Guide for Windows*  
NetBackup\_Install\_Win.pdf

Explains how to install NetBackup software on Windows-based platforms.

- *Symantec NetBackup LiveUpdate Guide*  
NetBackup\_LiveUpdate\_Guide.pdf

This guide explains a feature that provides a cross-platform, policy-driven method to distribute NetBackup Release Updates to NetBackup hosts.

## About administrator's guides

The following administrator guides were released with this version of NetBackup.

- *Symantec NetBackup Administrator's Guide for UNIX and Linux, Volume I*  
NetBackup\_AdminGuideI\_UNIXServer.pdf  
Explains how to configure and manage NetBackup on a UNIX or Linux server. This document also includes information on how to configure storage devices and media, and how to manage storage units, backup policies, catalogs, and host properties.
- *Symantec NetBackup Administrator's Guide for UNIX, Volume II*  
NetBackup\_AdminGuideII\_UNIXServer.pdf  
Explains additional NetBackup features and provides overview and reference information. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).
- *Symantec NetBackup Administrator's Guide for Windows, Volume I*  
NetBackup\_AdminGuideI\_WinServer.pdf  
Explains how to configure and manage NetBackup on a Windows server. This document also includes information on how to configure storage devices and media, and how to manage storage units, backup policies, catalogs, and host properties.
- *Symantec NetBackup Administrator's Guide for Windows, Volume II*  
NetBackup\_AdminGuideII\_WinServer.pdf  
Explains additional NetBackup features and provides overview and reference information. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).

## About other documents

The following device configuration guide was released with this version of NetBackup.

- *Symantec NetBackup Clustered Master Server Administrator's Guide*  
This guide provides information on how to install and configure NetBackup to work with different clustering solutions.
- *Symantec NetBackup Commands for UNIX, Windows, and Linux*  
NetBackup\_Commands.pdf  
Describes the NetBackup and Media Manager commands and the processes that you can run from a UNIX or Linux command line or a Windows command prompt.

- *NetBackup in Highly Available Environments Administrator's Guide*  
NetBackup\_AdminGuide\_HighAvailability.pdf  
This guide discusses various methods for making NetBackup highly available and provides guidelines for protecting NetBackup against single point of failures.
- *Symantec NetBackup Security and Encryption Guide*  
NetBackup\_SecEncryp\_Guide.pdf  
This guide provides information about on how to secure NetBackup. It also includes information on how to use access control, enhanced authorization and authentication, and encryption.  
Explains additional NetBackup features such as access control and enhanced authorization and authentication. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).

## About administration of options

The following administrator guides for NetBackup database agents and options were released with this version of NetBackup.

- *Symantec NetBackup AdvancedDisk Storage Solutions Guide*  
NetBackup\_AdvDisk\_Guide.pdf  
Explains how to configure and use the disk storage that is exposed to NetBackup as a file system for backups.
- *Symantec NetBackup Bare Metal Restore Administrator's Guide*  
NetBackup\_AdminGuide\_BMR.pdf  
Describes how to install, configure, and use Bare Metal Restore to protect and restore client systems. For UNIX, Windows, and Linux.
- *Symantec NetBackup Cloud Administrator's Guide*  
NetBackup\_AdminGuide\_Cloud.pdf  
Explains how to back up and restore data from cloud Storage as a Service (STaaS) vendors.
- *Symantec NetBackup Deduplication Guide*  
NetBackup\_Dedupe\_Guide.pdf  
Explains how to configure and use NetBackup media server deduplication and NetBackup client deduplication.
- *Symantec NetBackup OpenStorage Solutions Guide for Disk*  
NetBackup\_OST\_Disk\_Guide.pdf  
Describes how to configure and use an intelligent disk appliance in NetBackup for backups.

- *Symantec NetBackup for VMware Administrator's Guide for UNIX, Windows, and Linux*  
 NetBackup\_AdminGuide\_VMware.pdf  
 Provides backup and restore of the VMware virtual machines that run on VMware ESX servers.
- *Symantec NetBackup for Hyper-V Guide*  
 NetBackup\_AdminGuide\_Hyper-V.pdf  
 NetBackup for Hyper-V provides snapshot-based backup of the virtual machines that run on Windows 2008 Hyper-V servers.
- *Symantec NetBackup for NDMP Administrator's Guide*  
 NetBackup\_AdminGuide\_NDMP.pdf  
 Explains how to install, configure, and use NetBackup for NDMP to control backups on an NDMP host.
- *Symantec NetBackup SAN Client and Fibre Transport Guide*  
 NetBackup\_SANClient\_Guide.pdf  
 Explains how to configure and use NetBackup SAN Client and Fibre Transport for high-speed backups of important clients.
- *Symantec NetBackup Search Administrator's Guide*  
 NetBackup\_AdminGuide\_Search.pdf  
 Provides a mechanism to index the file system metadata that is associated with backup images.
- *Symantec NetBackup Snapshot Client Administrator's Guide*  
 NetBackup\_AdminGuide\_SnapshotClient.pdf  
 This guide explains how to install, configure, and use Symantec NetBackup Snapshot Client. It combines the features of snapshot backup, FlashBackup, BLI Agent, off-host backup , and Instant Recovery.
- *Symantec NetBackup Replication Director Solutions Guide*  
 NetBackup\_RepDirector\_Guide.pdf  
 Describes the implementation of NetBackup OpenStorage-managed snapshots and snapshot replication, where the snapshots are stored on the storage systems of partnering companies.
- *Symantec NetBackup Vault Operator's Guide*  
 NetBackup\_OperGuide\_Vault.pdf  
 Describes the procedures for sending tapes off site, receiving tapes on site, and running reports on off-site media and vault jobs. For UNIX, Windows, and Linux.
- *Symantec NetBackup Vault Administrator's Guide*  
 NetBackup\_AdminGuide\_Vault.pdf

Describes how to install, configure, and use the NetBackup Vault feature, which allows customers to select and duplicate backup images to media that will be transferred to offsite storage for disaster recovery or archival purposes, and to generate reports that enable customers to manage the location and contents of this media. For UNIX, Linux, and Windows.

- *Symantec OpsCenter Administrator's Guide*  
NetBackup\_AdminGuide\_OpsCenter.pdf  
Explains Symantec's Web-based software application that provides visibility to an organizations data protection environment. OpsCenter is a combination of the two Symantec products namely NetBackup Operations Manager (NOM) 6.5.4 and Veritas Backup Reporter (VBR) 6.6.

## About administration of database agents

The following user guides were released with this version of NetBackup.

- *Symantec NetBackup for DB2 Administrator's Guide*  
NetBackup\_AdminGuide\_DB2.pdf  
Explains how to install, configure, and use NetBackup for DB2.
- *Symantec NetBackup Enterprise Vault Agent Administrator's Guide for Windows*  
NetBackup\_AdminGuide\_EntVault.pdf  
Explains how to install, configure, and use the Enterprise Vault Agent so you can protect Enterprise Vault configuration information and data that Enterprise Vault has archived.
- *Symantec NetBackup for Informix Administrator's Guide*  
NetBackup\_AdminGuide\_Informix.pdf  
Explains how to install, configure, and use NetBackup for Informix to back up and restore the Informix databases that are on a UNIX NetBackup client.
- *Symantec NetBackup for Lotus Notes Administrator's Guide for Windows*  
NetBackup\_AdminGuide\_LotusNotes.pdf  
Explains how to install, configure, and use NetBackup for Lotus Notes to back up and restore Lotus Notes databases and transaction logs on a client.
- *Symantec NetBackup for Microsoft Exchange Server Administrator's Guide*  
NetBackup\_AdminGuide\_MSExchg\_Win.pdf  
Explains how to configure and use NetBackup for Microsoft Exchange Server to perform online backups and restores of Microsoft Exchange Server.
- *Symantec NetBackup for Microsoft SQL Server Administrator's Guide for Windows*  
NetBackup\_AdminGuide\_MSSQL\_Win.pdf



Explains how to install, configure, and use NetBackup for Microsoft SQL Server to back up and restore Microsoft SQL Server databases and transaction logs.

- *Symantec NetBackup™ for Microsoft SharePoint Server Administrator's Guide for Windows*

NetBackup\_AdminGuide\_SharePoint.pdf

Explains how to install, configure, and use NetBackup for SharePoint Portal Server 2003 to back up and restore the SharePoint databases that are on a Windows NetBackup client.

- *NetBackup for Oracle Administrator's Guide*

NetBackup\_AdminGuide\_Oracle.pdf

Explains how to install, configure, and use NetBackup for Oracle and Microsoft Oracle to back up and restore the Oracle databases that are on a UNIX or Windows NetBackup client.

- *Symantec NetBackup for SAP Administrator's Guide*

NetBackup\_AdminGuide\_SAP.pdf

Explains how to install, configure, and use NetBackup for SAP on UNIX- and Windows-based servers.

- *Symantec NetBackup for Sybase Administrator's Guide*

NetBackup\_AdminGuide\_Sybase.pdf

Explains how to install, configure, and use NetBackup for Sybase to back up and restore Sybase databases that are on UNIX and Windows NetBackup clients.

## About the Troubleshooting guide

The following troubleshooting guide was released with this version of NetBackup.

- *Symantec NetBackup Troubleshooting Guide for UNIX and Windows*

NetBackup\_Troubleshoot\_Guide.pdf

Provides troubleshooting information for UNIX-, Linux-, and Windows-based NetBackup products, including Media Manager.

- *Symantec NetBackup Status Codes Reference Guide*

NetBackup\_RefGuide\_StatusCodes.pdf

Provides descriptions of all of the supported status codes for NetBackup, media manager, device configuration, device management, and robotic status codes.



# About the NetBackup Rehydration improvements for deduplicated files

This appendix includes the following topics:

- [About the NetBackup rehydration improvements for deduplicated files](#)
- [Environmental factors that affect rehydration performance](#)
- [About changes and updates to the deduplication tuning parameters that affect restore performance and rehydration performance](#)
- [Editing the ReadBuffer Size parameter](#)
- [NetBackup tuning parameters that affect restore performance and rehydration performance](#)

## About the NetBackup rehydration improvements for deduplicated files

This release of NetBackup contains several changes that can improve restore performance and rehydration performance.

When a client is backed up to deduplicated storage, its files are divided into segments and written to disk. When the file changes, the backup software analyzes the changes in the file and writes the changed segments to disk. If you need to restore the file, the backup software *rehydrates* the file by reassembling the file from its segments and writing the restored file back out to disk or tape.

Under certain circumstances, a file's segments might become increasingly scattered across the disk storage units as the file continues to change and continues to be backed up. When you request a restore of one of these files, the backup software spends time finding and reassembling the file, which can take a long time for longer and older files. Slow disk speeds and slow tape mounting speeds can further degrade restore performance.

Duplicating to tape is particularly sensitive to low transfer rates. Data transfer to physical tape is optimal when the source data streaming rate matches or exceeds the minimum streaming rate of the physical tape drive. If the transfer rate from the source storage is less than this minimum streaming rate, the tape drive can write even more slowly than the source data streaming rate.

If you applied the NetBackup rehydration update, you can safely apply NetBackup 7.5. Parameters you set are untouched by the NetBackup 7.5 installation process.

The following topics describe the rehydration features in NetBackup 7.5:

- See [“Environmental factors that affect rehydration performance”](#) on page 148.
- See [“About changes and updates to the deduplication tuning parameters that affect restore performance and rehydration performance”](#) on page 149.
- See [“Editing the ReadBuffer Size parameter”](#) on page 150.
- See [“NetBackup tuning parameters that affect restore performance and rehydration performance”](#) on page 151.

## Environmental factors that affect rehydration performance

Generally, restore jobs and tape rehydration jobs complete more quickly in a backup environment that includes fast disks and a fast network. The NetBackup 7.1.0.3 release update includes several new tuning parameters that can improve performance.

If restore performance or rehydration performance does not improve after you upgrade to NetBackup 7.1.0.3, one or more of the following other factors might need to be examined:

- On-disk placement of a file's backup segments and on-disk distance between the backup segments
- Disk speed
- Data transfer connection
- CPU performance

- System state
- Backup image size
- Backup file size
- System memory (RAM)
- Tape mounting and tape repositioning

## About changes and updates to the deduplication tuning parameters that affect restore performance and rehydration performance

NetBackup 7.5 includes the following changes and additions to deduplication tuning parameters:

- New parameters in the `pd.conf` file. The new parameters and their settings are as follows:
  - `PREFETCH_SIZE=33554432`
  - `RESTORE_DECRYPT_LOCAL=0`
  - `META_SEGKSIZE=16384`
- New `PrefetchThreadNum` parameter in the `[CRDataStore]` section of the `contentrouter.cfg` file. By default, this parameter is `PrefetchThreadNum=1`.

The following topics contain more information about these parameters:

- See [“About the PREFETCH\\_SIZE parameter”](#) on page 149.
- See [“About the RESTORE\\_DECRYPT\\_LOCAL parameter”](#) on page 150.
- See [“About the META\\_SEGKSIZE parameter”](#) on page 150.
- See [“About the PrefetchThreadNum parameter”](#) on page 150.

### About the PREFETCH\_SIZE parameter

This parameter resides in the `pd.conf` file. It specifies the buffer size, in bytes, that NetBackup uses when it prefetches data segments for restore operation. The default is `33554432`. Symantec recommends that you do not change this value unless instructed to do so by a technical support staff member.

## About the RESTORE\_DECRYPT\_LOCAL parameter

This parameter resides in the `pd.conf` file. It specifies where decryption and decompression occurs during restores. The default is 0, which enables decryption and decompression on the media server. When you set `RESTORE_DECRYPT_LOCAL=1`, NetBackup performs decryption and decompression on the client.

Depending on your environment, you might want to change this setting to obtain better performance.

## About the META\_SEGKSIZE parameter

This parameter resides in the `pd.conf` file. It specifies the segment size for metadata streams. This setting determines the segment size used for writing the `.hdr` and `.map` images.

The default is 16384 and is specified in terms of KB. The size you specify must be a multiple of 32 and fall in the range 32-16384. Symantec recommends that you do not change this value unless instructed to do so by a technical support staff member.

## About the PrefetchThreadNum parameter

This parameter specifies the number of threads used to preload segments when data is being restored. By default, this parameter is `PrefetchThreadNum=1`.

Symantec recommends that you keep this parameter's default setting, which is 1. Depending on your disks, you might obtain better performance with a value as high as 4, but significant testing on your part is needed to ensure that a value greater than 1 yields better performance. Poorer performance can result from increasing this parameter above the default.

## Editing the ReadBuffer Size parameter

The `ReadBufferSize` parameter resides in the `[CRDataStore]` section of the `contentrouter.cfg` file. By default, the NetBackup 7.1.0.3 update sets `ReadBufferSize=65536`.

On most Linux and UNIX systems, Symantec testing has shown that `ReadBufferSize=65536`, the default, generally offers good performance.

On most Windows systems, Symantec testing has shown that `ReadBufferSize=1048576`, which is 1M (or 1024 X 1024), generally offers good performance.

Depending on the read speeds you obtain from the content router disks in your backup environment, you might need to reset this parameter to obtain optimal restore speeds and rehydration speeds. Make sure to do your own testing and reset the `ReadBufferSize` parameter if needed. The following procedure explains how to edit the `contentrouter.cfg` file.

#### To edit the `contentrouter.cfg` file on a PureDisk storage server

- 1 Use a text editor to open the content router configuration file on the storage server.

On Windows storage servers, the content router configuration file is at the following location:

```
storage_path\etc\puredisk\contentrouter.cfg
```

---

**Note:** On Windows systems, use `notepad.exe` to edit the `contentrouter.cfg` file. If you use a different editor, existing data in the file might become corrupted.

---

On Linux and UNIX storage servers, the content router configuration file is at the following location:

```
storage_path/etc/puredisk/contentrouter.cfg
```

- 2 Locate the `CRDataStore` section.
- 3 Edit the `ReadBufferSize` parameter in the `CRDataStore` section.
- 4 Save and close the file.

## NetBackup tuning parameters that affect restore performance and rehydration performance

To obtain optimal restore and rehydration performance, Symantec recommends that you examine the following parameters that reside in tuning files:

- `NET_BUFFER_SZ`
- `NUMBER_DATA_BUFFERS`
- `SIZE_DATA_BUFFERS`

Depending on your environment, these parameters might be set to values that are tuned to your backup environment. NetBackup 7.1.0.2 does not reset these parameters.

If your restore and rehydration performance does not improve after you apply NetBackup 7.1.0.2, consider setting or resetting these tuning parameters to the values in the following procedure.

#### To set the NetBackup tuning parameters

- 1 Determine whether the `NET_BUFFER_SZ`, the `NUMBER_DATA_BUFFERS`, and the `SIZE_DATA_BUFFERS` files are set on the media server.

These parameters are set in tuning files that reside in the following directories:

- On Windows systems:

```
install_path\NetBackup\NET_BUFFER_SZ  
install_path\NetBackup\db\config\NUMBER_DATA_BUFFERS  
install_path\NetBackup\db\config\SIZE_DATA_BUFFERS
```

- On Linux or UNIX systems:

```
/usr/opensv/netbackup/NET_BUFFER_SZ  
/usr/opensv/netbackup/db/config/NUMBER_DATA_BUFFERS  
/usr/opensv/netbackup/db/config/SIZE_DATA_BUFFERS
```

- 2 (Conditional) Back up the parameter files that currently exist.

Perform this step only if these files currently exist and are set to values that differ from the ones needed for rehydration.

- 3 Set the parameters to the following values:

- Set `NET_BUFFER_SZ` to 262144.
- Set `NUMBER_DATA_BUFFERS` to 64.
- Set `SIZE_DATA_BUFFERS` to 262144.

---

**Note:** If you have already changed these, or other tuning parameters, as a result of your own performance tests, do not change these parameters again. Please keep the values that currently exist in your backup environment. The preceding list shows the parameter values that Symantec used in its rehydration testing, and these values generally improve rehydration performance.

---

For information about how to set these parameters on a Windows media server, see the following tech note:

<http://www.symantec.com/business/support/index?page=content&id=TECH18422>



For information about how to set these parameters on a Linux or UNIX media server, see the following tech note:

<http://www.symantec.com/business/support/index?page=content&id=TECH1724>

- 4 Perform this procedure on all media servers in your NetBackup environment that are involved in the rehydration program.

You can reset these parameters again, if necessary.

- 5 Adjust other aspects of the backup environment if performance does not improve after you change the NetBackup tuning parameter settings.

If performance does not increase after you change the `NET_BUFFER_SZ`, the `NUMBER_DATA_BUFFERS`, and the `SIZE_DATA_BUFFERS` files, consider taking the following other actions:

- Examine the tape configuration to see if changes can be made.
- Change the `ReadBufferSize` parameter in the `contentrouter.cfg` file.  
For information about how to change this parameter, see the following:  
See [“Editing the ReadBuffer Size parameter”](#) on page 150.

