Symantec NetBackup™ Release Notes

UNIX, Windows, and Linux

NetBackup 7.1

21159725

Symantec

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: 7.1

PN: 21159725

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

New NetBackup features

This chapter includes the following topics:

- About SQL server backup enhancements

About NetBackup proliferation

The following platform proliferations were added with this release of NetBackup:

- Added BMR support for Storage Foundation for Windows 5.x.
  BMR now provides bare metal recovery on Windows 2003/2008/2008 R2 servers where SFW 5.0 or 5.1 are deployed.

  Note: BMR support for Windows 2008/2008 R2 was introduced with NetBackup 7.0.1.

- Added BMR client support for HP-UX 11i v3 (11.31) IA64.
  The initial support for HP-UX 11iv3 IA-64 was introduced with NetBackup 7.0.1. This feature provides the final support, and removes previous volume management and dissimilar hardware limitations.
- Added Snapshot Client hardware-based Frozen Image Method support for SFRAC.
- Added support of CDP Frozen Image Method for Linux.
- Added support for NetBackup Media Server Deduplication Option and NetBackup Client Deduplication to HP-UX 11.31 IA64 and Red Hat 6.0 x64 systems.
- The NetBackup Cloud Storage for Nirvanix OpenStorage plug-in enables NetBackup to back up data to and restore data from the Nirvanix Storage Delivery Network.

  The following list shows the supported platforms:

  - Linux - Red Hat 4 and 5
  - Solaris - SPARC 10
  - Windows - 2008 R2 64 bit

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 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.

You can use this data to assess whether your systems are ready to install or upgrade to NetBackup 7.1.

To access SORT, go to the following Web page:

http://sort.symantec.com

About new NetBackup commands

This release of NetBackup contains new commands and utilities. For a description of each of the following commands, refer to the NetBackup Commands guide:

- `nbrbutil`

  The `nbrbutil` command runs the utility that configures the Resource Broker (`nbrb`) functionality. The utility can list and release resource allocations, display the jobs that use a resource (drive, media, storage unit), and set Resource Broker tuning parameters.

- `nbreplicate`

  The `nbreplicate` command initiates the creation of a backup copy (replicate) on a storage server. You can use this command to create up to 10 copies of unexpired backups.

- `nbcertupdater`

  The certificate update utility (`nbcertupdater`) provides an automated mechanism to contact a set of NetBackup hosts that can run a `setuptrust` operation with a specified authentication broker. The utility can also query the `NBU_Machines`private domain of the local authentication broker to generate the set of NetBackup hosts that can then be contacted for the `setuptrust` operation.

About NetBackup audit trail

With NetBackup audit trail you can keep a record of user activities in a NetBackup environment. With this release, you can audit many more categories than were covered with policies and restore jobs in NetBackup 7.0.1. In addition, you can configure and view audit trails with OpsCenter. This feature enables customers to track who made changes, when the changes were made, and the types operations were changed in a backup environment.

To complete this feature, OpsCenter now offers the ability to manage auditing, monitor audit trails, and view audit trail reports.

About BMR support for Storage Foundation for Windows 5.x

With this feature in NetBackup 7.1 you can recover Windows 2003/2008/2008R2 servers where SFW 5.0 or 5.1 are deployed using BMR. The restore process involves the new improvised **Legacy OS based SRT and not the Fast Restore or Win PE based SRT**. That is due to the inherent limitations of SFW running under Windows PE.

The SRT creation involves the following two additional steps:

- Apply the SFW Maintenance Pack to the SRT.
- Apply the relevant hotfixes to the SRT. This step is optional for certain versions.

Note: Changes to the following table may occur after the release of NetBackup 7.1. You can use the following link to download or view an electronic version of this document from the Symantec Support Web site. That document contains the most up-to-date information about NetBackup 7.1 and the contents of the following table.

http://www.symantec.com/docs/DOC3412

Table 1-1 SRT contents to restore SFW clients

Operating system	SFW version on the client	Minimum base SFW version in the SRT	Maintenance Pack Required in the SRT	Hotfix required in the SRT	MSXML 6.0 required
Windows 2003 (32 or 64-bit)	SFW 5.0, SFW 5.0 RP1, SFW 5.0 RP2	SFW 5.0	RP2	None	None
Windows 2003 (32 or 64-bit)	SFW 5.1, SFW 5.1AP1, SFW SP1, SFW SP2	SFW 5.1	AP1	Hotfix_5_1_01004_407_1974940b https://sort.symantec.com/patch/detail/ 3354/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	Yes http://www.microsoft.com/downloads/en/details.aspx?FamilyId=993c0bcf-3bcf-4009-be21-27e85e1857b1&displaylang=en

Table 1-1 SRT contents to restore SFW clients *(continued)*

Operating system	SFW version on the client	Minimum base SFW version in the SRT	Maintenance Pack Required in the SRT	Hotfix required in the SRT	MSXML 6.0 required
Windows 2008 (32 or 64-bit)	SFW 5.1, SFW 5.1AP1	SFW 5.1	AP1	Hotfix_5_1_01004_407_1974940b https://sort.symantec.com/patch/detail/ 3354/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None
Windows 2008 (32 or 64-bit)	SFW 5.1 SP1	SFW 5.1	SP1	Hotfix_5_1_10012_584_1946291 https://sort.symantec.com/patch/detail/ 3491/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None
Windows 2008 (32 or 64-bit)	SFW 5.1 SP2	SFW 5.1	SP2	None	None
Windows 2008 R2 (32 or 64-bit)	SFW 5.1 SP1	SFW 5.1	SP1	Hotfix_5_1_10012_584_1946291 https://sort.symantec.com/patch/detail/ 3491/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None
Windows 2008 R2 (32 or 64-bit)	SFW 5.1 SP1 AP1	SFW 5.1	SP1	Hotfix_5_1_10012_584_1946291 https://sort.symantec.com/patch/detail/ 3491/0/cGF0Y2gvc2VhcmNobWF0cml4LzIxLzIvMQ	None
Windows 2008 R2 (32 or 64-bit)	SFW 5.1 SP2	SFW 5.1	SP2	None	None

About embedded security services

This feature embeds the security services (VxAT and VxAZ) into NetBackup. Users no longer need to depend on the shared VxAT and VxAZ infrastructure.

The following list describes the benefits of this feature:

- Security services (AT and AZ) are installed as part of the NetBackup install, and do not require a separate ICS installer. In addition, you can remove these services as part of the NetBackup uninstall.
- NetBackup owns its security data, for example all the credentials and private keys are private to the NetBackup product. That provides the following benefits:
  - NetBackup does not need to shut down because of installs of other products that need to upgrade a shared AT and AZ.
  - Other products' users do not affect NetBackup. That eliminates the potential of another user inadvertently changing the credentials in the shared directories
  - It eliminates the possibility of NetBackup security data being deleted with other NetBackup data during an uninstall.
- Clustering of security services is now integrated with NetBackup clustering. The security services are now monitored services along with other critical NetBackup daemons. In addition, the `bpnbaz -SetupMaster` command is now cluster aware. This one command configures security on all nodes.
- This feature contains seamless integration of the Logging of Authentication service with NetBackup's UL logging.
- Upgrades from older releases with NBAC automatically migrate the security information to the embedded services. (If Security services are not co-resident with the NetBackup master install, custom steps are involved.)
- The Authorization Service's Database is now integrated with the NetBackup databases. And with this feature comes the addition of the `NBAZDB` database.
- Other changes in this feature include the following:
  - You can use the `bpnbaz -SetupMedia` and `bpnbaz -SetupClient` commands to configure security on the older media servers and the older clients that are newer than NetBackup 6.5.
  - You can use the `bpnbaz -SetupAuthBroker` command to configure a remote authentication broker for cross-domain and cross-OS Authentication requirements.

About installation and upgrade features

The following sections describe the new features and enhancements that relate to the installation and upgrade of the NetBackup 7.1 release.

NetBackup LiveUpdate now supports major release upgrades for NetBackup clients

NetBackup 7.1 lets you upgrade NetBackup 6.5.x and 7.0.x UNIX and Windows clients (but not servers) by using NetBackup LiveUpdate. A separate DVD is provided for you to copy the client packages to your NetBackup LiveUpdate server.

Windows integrated cluster installation and upgrade process is improved

The process to install and upgrade cluster installations has been improved to provide feedback to customers, and to validate cluster environments before configuration takes place.

New preinstallation checker added to NetBackup for Windows

This tool lets you check those computers that you want NetBackup to be installed on or upgraded. A report or log is generated that describes the complete results. The log specifically identifies whether anything needs to be addressed before an installation or an upgrade to NetBackup 7.1.

About back-level administration capabilities by the NetBackup-Java console

NetBackup 7.1 provides additional ways to perform back-level administration of the back-level versions that are compatible. That includes the packaging and the installation of the NetBackup 6.0 MP7 and 6.5.6 versions of the NetBackup-Java console on compatible UNIX and Linux platforms.

About IPv6 support in NetBackup 7.1

The following topics describe how NetBackup 7.1 supports IPv6 128-bit addressing.

NetBackup core now supports IPv6

The IPv6 for NetBackup feature implements changes to NetBackup to provide support for operation in IPv6 networks with the servers and the clients that have IPv6 addresses. That means NetBackup is fully functional on the hosts that are connected to IPv6 networks as well as those on today's IPv4 networks. And that includes hosts with multiple interfaces that are configured for IPv4 and IPv6 in any combination, or both simultaneously.

Offering IPv6 support in NetBackup means that the following features are available to the user:

- 128-bit address support.
- Sybase upgrade to version 10
- Clients/devices can be directly connected to the network with an auto configure function.
- You can control the use of IPv4 and IPv6 networking in NetBackup, and be able to prohibit one or the other protocol through a bp.conf configuration option.

IPv6 support for NDMP

This feature covers the changes that are required in the NDMP protocol and NDMP messages to support IPv6 128-bit addressing for NDMP data connections. NDMP "data" connections are the connections made between filers or between a NetBackup media server and a filer to transfer the backup image. Currently the NDMP V4 specification supports only IPv4 32-bit addressing for data connections. This feature contains an NDMP extension to support IPv6.

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 supported only over an IPv4 network because there are many network boot protocols that are not supported over an IPv6 channel.

IPv6 support for MSDP

This feature enhances all PDDE modules to support the use of IPv6, both by the server and its clients.

Note: This feature does not include adding IPv6 support for PureDisk remote office Edition.

About duplication to a remote master server domain

With storage lifecycle policies (SLP) in NetBackup 7.1, you can copy backup images from one NetBackup master server domain to a matching device in a remote NetBackup master server domain. This process is called Automatic Image

Replication. When the image arrives at the target domain, an SLP automatically executes an optimized import process to make that backup image immediately available for restore as well as for further SLP duplications. That eliminates the complicated processes that involved catalog recovery into remote master servers.

Automatic Image Replication is supported between NetBackup domains that use deduplication. Replication must be from one **Media Server Deduplication Pool** in the source domain to a **Media Server Deduplication Pool** in the target domain.

Support for other environments depends on when those vendors provide it, as follows:

- OpenStorage disk appliance vendors must implement the support for this functionality in their OpenStorage plug-ins.
- NetBackup PureDisk Deduplication Option support is scheduled for a future release of PureDisk.

This feature builds on the earlier Hierarchical Duplication feature of SLPs that does the following:

- Enables you to eliminate the transportation of physical tape for off-site vaulting.
- You can quickly and efficiently make the backup images that are ready for recovery at a remote domain site.
- You can centralize duplication to tape in hub-and-spoke duplication configurations.

In addition to this feature, OpsCenter offers additional reporting for SLP and duplication to a remote master server domain.

Upgrade note for OpenStorage optimized duplication

The duplication to a remote master server domain and the optimized duplication features that use OpenStorage may conflict if you use both of them and do not configure them correctly. If the features are configured incorrectly, unpredictable duplication results may occur.

Table 1-2 describes the two features.

Table 1-2 OpenStorage duplication features

Feature	Description
Duplication to a remote master server domain	Duplication to a remote master server is a new feature in NetBackup 7.1. With this feature, you can duplicate backup images to a different master server domain. For information about duplication to a remote master server domain, see the *NetBackup Administrator's Guide , Volume I*.
Optimized duplication	OpenStorage optimized duplication copies backup images to different storage within the same NetBackup master server domain. For information about OpenStorage optimized duplication, s ee the *NetBackup Shared Storage Guide*. For information about optimized duplication of deduplicated data, see the *NetBackup Deduplication Guide*. NetBackup deduplication uses the OpenStorage framework.

If you use both features, the critical configuration detail is when you select the target storage server or servers. For duplication to a remote master server, a target storage server must not also be a storage server for the source domain. Therefore, choose the target storage server or servers carefully.

These duplication features are supported in the following environments:

- From a disk appliance to a disk appliance.
  The disk appliances must support the Symantec OpenStorage API.
- From a NetBackup **Media Server Deduplication Pool** to another **Media Server Deduplication Pool**.

About duplication performance improvements

Changes have been made to the write-algorithms that NetBackup uses to improve the performance of backups and duplications when the images are small (less than one gigabyte). Many of these changes are most noticeable when multiplexed write operations to physical tape devices are performed. Backups or the write-side of a duplication job are examples of multiplexed write operations to physical tape devices.

The duplication of small images from a disk has been enhanced to avoid a disk resource allocation cycle on each image. That is most noticeable when the master server process `NBRB` is heavily loaded.

Duplication of small images to a physical tape device has been enhanced to avoid synchronizing delays between each image. A technique called “deferred validation”

is used to synchronize between groups of small images. The definition of what a small image (in KB's) and the size of the group of images is configurable on each media server. The file, `/usr/openv/netbackup/db/config/DEFERRED_IMAGE_KBSIZE`, can contain the size of what is considered a small image (the default is 1GB). The file, `/usr/openv/netbackup/db/config/DEFERRED_IMAGE_LIMIT`, can contain the size of the group. The default size is eight, and can be 1 to 128.

About NetBackup support utility enhancements

This release of NetBackup contains updated versions of the `nbcplogs`, `nbdna`, and `nbsu` utilities. This release contains the following version levels for these utilities; `nbcplogs` 1.3, `nbdna` 2.1.1 and `nbsu` 1.5 . In addition, the FTP capability has been added to the NetBackup support utility `nbsu`. In addition, this release contains a new diagnostic utility that is called, `nbdiag`.

The following list describes the enhancements that each utility contains:

- `nbcplogs` 1.3

  By default, `nbcplogs` (NetBackup log uploader) now runs the `nbsu` utility and uploads `nbsu` information for the host system. This capability improves our user 's support experience. It saves the customer time and keystrokes to gather and upload information to Symantec Support. Enhancements were also made to gather additional log information for clusters and pack history information.

- `nbdna` 2.1.1

  This update of `nbdna` (Network diagnostic utility) adds the ability for `nbdna` to function in IPv6 network environments. It also adds the ability to test PBX connections between SAN Clients and the master server. With the exception of Windows IA64, `nbdna` was ported to all other server and client platforms.

- `nbsu` 1.5

  This update of `nbsu` (NetBackup Support Utility) adds FTP capability to `nbsu`. This capability also improves our user 's support experience. It saves the customer time and keystrokes to gather and upload information to Symantec Support. Enhancements were made to a number of diagnostics and some new diagnostics were added.

- `nbdiag` - NetBackup 7.1 contains a new diagnostic utility that is called `nbdiag`. This utility enables NetBackup support personnel to more quickly identify the source of certain NetBackup-related problems.

About OpsCenter updates

The following sections describe the new OpsCenter features and enhancements that were released with NetBackup 7.1

OpsCenter reporting for storage lifecycle policies and duplication to a remote master server domain

New in NetBackup 7.1 is OpsCenter reporting for storage lifecycle policies (SLP) and duplication to a remote master server domain. Until now users have had no GUI-driven method to gain end-to-end visibility of SLP activities and to answer the following important questions:

- Is the SLP performing well enough to complete on time?
- Have the second, third, etc. copies been made?
- How much data remains to be copied to each hierarchical storage destination?
- Which clients' backups are not yet off-site?
- What is the average lag time for getting my “Gold” backups to the remote master?
- Has the SLP backlog grown larger over the past six months?
- Where are problems originating; which copy is the bottleneck?

These reports let you obtain the answers to such questions in a logical fashion with drill-down functionality to enable viewing of data at the desired level of granularity.

About Capacity License reporting

A **Capacity Licensing** report gives a summary of the amount of data that is protected. The options **Enterprise Disk**, **PureDisk**, and **RealTime** classify this report. The report gives capacity totals for each client, and makes it easier to verify the capacity totals for each client.

Note: You must install the agent to use the Capacity Licensing feature for all versions of OpsCenter.

Management and Reporting for audit trails

An audit trail keeps a record of user activities in a NetBackup environment. For regulatory compliance purposes, the ability to track changes in a backup

environment is important. With this feature, you have the ability to do the following from OpsCenter:

- Manage the auditing. You can enable, disable, and set the retention period for the audit trails.
- Monitor the audit trails over a specified timeframe.
- View the audit trail reports. These reports display the count of actions that were performed on the entities.

Breakup Jobs In OpsCenter

This feature enhances OpsCenter so that it provides more granular level reporting of the jobs that NetBackup backs up. You can use this feature to do the following:

- Collect and report on file system-level data of jobs.
- Use data from the NetBackup's catalog to break up a job so that the size and the backup file count are of a finer granularity.
- You can explicitly list multiple paths in your policy to include lists in NetBackup.
- This feature is an optional addition for an existing data collection. That means you can enable or disable this feature based on specific requirements.

Other OpsCenter enhancements

With this feature, the following new tables were added to the OpsCenter database:

- `nb_JobDbInstanceArchive`
- `domain_VaultStoreGroup`
- `lookup_EnterpriseVaultVersions`

In addition, multiple database views were changed. The following list shows the views that were changed:

- `nom_NBJob`
- `nom_NBVolume`
- `nom_NBJobPassRate`
- `nom_NBPolicy`
- `nom_NBMediaSummary`
- `nom_NBMediaFullTapeCap`
- `nom_NBMedia`

- nom_Drive
- nom_Robot

Other OpsCenter enhancements include changes to improve performance that includes report performance.

About Tomcat and Sybase upgrades for OpsCenter

Some of the important infrastructure components that OpsCenter server relies on are, Tomcat, Sybase ASA, and Struts. In previous releases of NetBackup you had to install these components externally from separate native packages. This release of the NetBackup OpsCenter server has Tomcat 6.0.29, the latest EBF of Sybase SQL Anywhere, and Struts 1.3.10 embedded in it.

About the workload analyzer report in OpsCenter

The workload analyzer reports feature provides detailed insight into activity on an hourly basis, each day, for a duration of seven days. This report provides 168 data points (the number of hours over seven days) of analysis in terms of activity. The following list describes the basis of the analysis and reporting:

- Timing is measured from the standpoint of when the jobs start, the periods in which they are active, and when the jobs end.
- Queuing is measured from the standpoint of how much time a task or job spends in a queued state before the actual CPU cycles are applied.
- Size is measured from the standpoint of how much data is moved from target to destination and how the volume of data is broken down in terms of what is moved in any given hour.
- Throughput is measured from the standpoint of data transmission rates in Kbytes/Sec.

About RealTime integration for RedHat Linux

New in RealTime 7.1 is the ability to protect RedHat 5 Linux hosts. With that capability comes NetBackup 7.1 integration so that Snapshot Client can perform Instant Recovery bookmarks of known good points in time on the Linux hosts. RealTime provides crash-consistent, any-point-in-time, recovery. In addition, NetBackup integration with RealTime marks periodic application-consistent points in time over the continuous RealTime timeline, based on NetBackup schedules and policies.

About the disambiguation of the NetBackup Status 5 error code

This feature is part of a set of features that are intended to improve the supportability and overall customer experience of NetBackup. This feature provides more granularity of return codes for failed NetBackup restores. In the past, a **Status 5** error code would be the status that was returned for all failed restore jobs.

In this feature, jobs that fail because of media server errors return the error code for the specific media server error that was encountered as the job status. Other restore failures now return an error code that is specific to each policy type to help distinguish the failure.

About the per job process flow log

This feature provides additional messages in the **Detailed Status** of NetBackup jobs. These messages may help enable customer support to diagnose and identify the cause of a job-related failure.

About file-level recovery for Linux virtual machines

For VMware and Hyper-V virtual machines, NetBackup now supports the restore of individual files from a RedHat or SUSE virtual machine backup.

A number of restrictions apply. Please refer to the NetBackup for VMware or NetBackup for Hyper-V administrator's guides.

About VM Intelligent Policy

Instead of manually selecting VMware virtual machines for backup, NetBackup now includes a feature to automatically select virtual machines based on a range of criteria. You specify the criteria in the new Query Builder on the **NetBackup Policy Clients** tab. When a backup is about to occur, NetBackup selects the VMs that match the criteria and launches backup jobs.

Automatic selection of VMware virtual machines has the following advantages:

- It saves time for sites with large virtual environments. You do not need to manually select from a long list of virtual machines. NetBackup selects all the virtual machines that meet the selection criteria that is recorded in the policy.
- Eliminates the need to manually update the policy Client-list, each time a VM is added or removed.

About SQL server backup enhancements

This feature enables OpsCenter to provide a hierarchical view of Client-initiated SQL database backups. Before NetBackup7.1, the hierarchical view of SQL jobs in OpsCenter was available only for server-initiated backups.

Chapter 2

Platform compatibility

This chapter includes the following topics:

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 topic 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 backward 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 7.1. Therefore, Symantec recommends that you refer to the following Technote on the Symantec Support Web site to view the latest NetBackup 7.1 release information.

http://www.symantec.com/docs/DOC3412

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 7.1:

- All UNIX 32-bit system support has been discontinued. To upgrade these systems to NetBackup 7.1, 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 7.1 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 7.1, you also must update the vendor plug-in to a 64-bit version.
- NetBackup 7.1 supports client operations on all 64-bit platforms except FreeBSD and MAC.
- NetBackup 7.1 is no longer supported on IRIX and Tru64.
  Servers and clients with operating the systems that use NetBackup 6.x are compatible with NetBackup 7.1 servers.
- Windows IA64 is supported only as a NetBackup 7.1 client.
- You can no longer use Linux SUSE and Linux RedHat Itanium server platforms as a NetBackup 7.1 master or a media server. These platforms are only supported as NetBackup 7.1 clients.
- You can no longer 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.
- Linux Red Hat IBM zSeries platforms compatibility has switched to 64-bit clients.
- Novell NetWare is no longer compatible for use as a media server. This platform is only compatible as a client.

- For this release, the following platforms have been added.
  - AIX 7.1 POWER for 64-client and 64-bit server
  - Canonical Ubuntu 9.04 X64 for 64-clients
  - Canonical Ubuntu 10.04 X64 for 64-clients
  - FreeBSD 8.x X86 for 32-bit clients
  - FreeBSD 8.x X64 for 32-bit clients
  - Red Hat Enterprise Linux 6.0 (base) X64 for 64-bit clients and 64-bit servers
  - Red Hat Enterprise Linux 6.0 (advanced) 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. The following compatibility lists are available on the Symantec Support Web site:

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

- 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 7.0 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

- *NetBackup7.x Cluster Compatibility List*
- *NetBackup Desktop/Laptop Option compatibility list*

- *Backup Exec Tape Reader compatibility list*

To locate platform compatibility information on the Symantec Support Web site

1. Go to the following URL:

   www.symantec.com/business/support

2. Select the **NetBackup Enterprise Server** link under the **Top Products** title on the Web page .

3. Select **NetBackup Master Compatibility List** link under the **Compatibility List** title on the Web page .

   The Web page refreshes and contains a list of compatibility documents. From this Web page, you can refine your search to find a link to the appropriate document. (The compatibility list documents are in PDF format. You must have Adobe Acrobat Reader to view these documents.)

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 31.

See "About Removing a client platform" on page 31.

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 Operating systems no longer compatible as of NetBackup 7.0 and beyond

Table 2-1 displays the operating systems that are no longer compatible with NetBackup starting with the release of NetBackup 7.0 and beyond. The operating systems that are identified in this table also apply to NetBackup 7.1.

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

See "About the operating systems that may not be supported in the next major release" on page 116.

Table 2-1 Operating systems no longer compatible with NetBackup as of NetBackup 7.0 and beyond

OS/Version	Hardware	Comments
AIX 5.1	Power	
AIX 5.2	Power	
Asianux 3.0	x86	
FreeBSD 5.3	i386 (x86)	
FreeBSD 5.4	i386 (x86)	
FreeBSD 6.0	i386 (x86)	
HP-UX 11.00	PA-RISC	
HP-UX 11.11	PA-RISC	Media server and client compatible only
HP-UX 11.23	PA-RISC	Media server and client compatible only
HP-UX 11.31	PA-RISC	Media server and client compatible only
HP-UX IA64 11.23	IA64	
IRIX 6.5.26 and greater		
Mac OS X 10.3	Apple Macintosh	
Mac OS X 10.4	POWERPC, i386	
NetWare 5.1	x86	
NetWare 6.0	x86	

Table 2-1 Operating systems no longer compatible with NetBackup as of NetBackup 7.0 and beyond *(continued)*

OS/Version	Hardware	Comments
NetWare 6.5	x86	Client compatible only
Novell OES (Linux) 1 SP2		
Red Flag Linux 4.1	x86	
Red Hat 2.1	x86	
Red Hat 3.0	x86	
Red Hat 3.0	x64	
Red Hat 3.0	IA64	
Red Hat 3.0	z/Architecture	
Red Hat 4.0	IA64	Client compatible only
Red Hat 5.0	IA64	Client compatible only
Solaris 8.0	SPARC	
Solaris 8.0	x86	
Solaris 9.0	x86	
Solaris 9.0	x64	
Solaris 10.0 x86	x86	
Solaris 10.0 x86	x64	
SUSE Desktop 9.0	x86	
SUSE Desktop 9.2	x86	
SUSE Desktop 9.3	x86	
SUSE Linux Enterprise Server 8	x86	
SUSE Linux Enterprise Server 8	x64	
SUSE Linux Enterprise Server 8	IA64	
SUSE Linux Enterprise Server 9	x86	
SUSE Linux Enterprise Server 9	x64	

Table 2-1 Operating systems no longer compatible with NetBackup as of NetBackup 7.0 and beyond *(continued)*

OS/Version	Hardware	Comments
SUSE Linux Enterprise Server 9	IA64	Client compatible only
SUSE Linux Enterprise Server 10 SP1	IA64	Client compatible only
Tru64 5.1a	Alpha	
Tru64 5.1b and greater	Alpha	
Windows Server 2000	x86 and x64	
Windows Server 2003 SP1 and R2	IA64	Client compatible only

About 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.

Table 2-2 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 2-2 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	POWER		1073MB		3599MB	64-bit binary compatible.
AIX 6.1	POWER		1073MB		3599MB	64-bit binary compatible.
AIX 7.1	POWER		1073MB		3599MB	New platform in this release.
Asianux 2.0, 3.0	x64		624MB		2564MB	
Canonical Ubuntu 8.0	x64		624MB			
Canonical Ubuntu 9.04	x64		624MB			New platform in this release.
Canonical Ubuntu 10.04	x64		624MB			New platform in this release.
CentOS 5.2, 5.3	x64		624MB			
Debian GNU/Linux 4.0, 5.0	x64		624MB			

Table 2-2 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 6.1, 6.2, 6.3, 7.x, 8.x	x86	120MB				Added the 8.x platform in this release.
FreeBSD 8.x	x64	120MB				New platform in this release.
HP-UX 11.11	PA-RISC		738MB		1797MB	64-bit binary compatible. Media server or client compatibility only.
HP-UX 11.23	PA-RISC		738MB		1797MB	64-bit binary compatible. Media server or client compatibility only.
HP-UX 11.31	PA-RISC		738MB		1797MB	64-bit binary compatible. Media server or client compatibility only.
HP-UX 11.31	IA64		1235MB		3648MB	
Mac OS X 10.5	POWER	194MB				
Mac OS X 10.5, 10.6	x86	194MB				
Novell Open Enterprise Server 2	x64		611MB		2492MB	
OpenVMS 5.5	HP VAX	16MB				
OpenVMS 6.2	HP VAX	16MB				
OpenVMS 7.3	HP VAX	16MB				
OpenVMS 6.1	HP Alpha		16MB			
OpenVMS 6.2	HP Alpha		16MB			
OpenVMS 7.3	HP Alpha		16MB			
OpenVMS 8.2	HP Alpha		16MB			
OpenVMS 8.3	HP Alpha		16MB			
OpenVMS 8.2	HP IA64		16MB			
OpenVMS 8.3	HP IA64		16MB			
OpenVMS 8.3-1H1	HP IA64/Alpha		16MB			

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

OS/Version	CPU Architecture	32-bit client	64-bit client	32-bit server	64-bit server	Notes
Oracle Enterprise Linux 4.0	x64		624MB		2564MB	64-bit binary compatible.
Oracle Enterprise Linux 5.0	x64		624MB		2564MB	64-bit binary compatible.
Red Flag Linux 5.0	x64		624MB		2564MB	
Red Hat Enterprise Linux 4.0 (AS)	x64		624MB		2564MB	64-bit binary compatible.
Red Hat Enterprise Linux 5.0 (base)	x64		624MB		2564MB	64-bit binary compatible.
Red Hat Enterprise Linux 5.0 (AS)	x64		625MB		2564MB	
Red Hat Enterprise Linux 6.0 (base)	x64		624MB		2564MB	64-bit binary compatible. New platform for this release.
Red Hat Enterprise Linux 6.0 (AS)	x64		624MB		2564MB	64-bit binary compatible. New platform for this release.
Red Hat Enterprise Linux Desktop 4.0	x64		624MB			
Red Hat Enterprise Linux Desktop 5.0	x64		624MB			64-bit binary compatible.
Red Hat Enterprise Linux 4.0 (AS)	IA64		490MB			Compatible with client only.
Red Hat Enterprise Linux 5.0 (base)	IA64		490MB			Compatible with client only.
Red Hat Enterprise Linux 4.0 (AS)	POWER		228MB			
Red Hat Enterprise Linux 5.0 (base)	POWER		228MB			
Red Hat Enterprise Linux 4.0 (AS)	z/Architecture		447MB		1906MB	Media server or client compatibility only.
Red Hat Enterprise Linux 5.0 (base)	z/Architecture		447MB		1906MB	Media server or client compatibility only.
Solaris 9.0	SPARC		621MB			64-bit binary compatible.

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

OS/Version	CPU Architecture	32-bit client	64-bit client	32-bit server	64-bit server	Notes
Solaris 10.0	SPARC		738MB		2260MB	64-bit binary compatible.
Solaris 10.0	x64		535MB		2133MB	64-bit binary compatible.
SUSE Linux Enterprise Server 10 (SP1)	IA64		477MB			Compatible with client only.
SUSE Linux Enterprise Server 11	IA64		477MB			Compatible with client only.
SUSE Linux Enterprise Server 10 (SP1)	x64		611MB		2492MB	
SUSE Linux Enterprise Server 11	x64		611MB		2492MB	
SUSE Linux Enterprise Server 10 (SP1)	POWER		240MB			Compatible with client only.
SUSE Linux Enterprise Server 10 (SP1)	z/Architecture		429MB		1868MB	Media server or client compatibility only.
SUSE Linux Enterprise Server 11	z/Architecture		429MB		1868MB	Media server or client compatibility only.
Windows	x86	600MB		1700MB		Covers all compatible Windows x86 platforms
Windows	x64		700MB		1900MB	Covers all compatible Windows x64 platforms
Windows	IA64		600MB			Compatible with client only.

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.

Table 2-3 is a list of platforms that are compatible with the NetBackup-Java Administration Console and the Backup, Archive, and Restore user interface in this release.

Table 2-3 Platforms that are compatible with the NetBackup-Java Administration Console and Backup, Archive, and Restore user interface

OS/Version	CPU Architecture	NetBackup-Java administration console	Backup, Archive, and Restore interface	JRE upgrade version
AIX 5.3	POWER	Yes	Yes	Java 6 SR6
AIX 6.1	POWER	Yes	Yes	Java 6 SR6
HP-UX 11.31	IA64	Yes	Yes	6.0.05
Red Hat Enterprise Linux 4.0 (AS)	x64	Yes	Yes	1.6-17
Red Hat Enterprise Linux 5.0 (base)	x64	Yes	Yes	1.6-17
Red Hat Enterprise Linux 4.0 (AS)	IA64		Yes	1.6-17
Red Hat Enterprise Linux 5.0 (base)	IA64		Yes	1.6-17
Red Hat Enterprise Linux 4.0 (AS)	POWER		Yes	
Red Hat Enterprise Linux 5.0 (base)	POWER		Yes	
Red Hat Enterprise Linux 4.0 (AS)	z/Architecture		Yes	
Red Hat Enterprise Linux 5.0 (base)	z/Architecture		Yes	
Red Hat Enterprise Linux Desktop 4.0	x64	Yes	Yes	1.6-17
Red Hat Enterprise Linux Desktop 5.0	x64		Yes	1.6-17
Solaris 9.0	SPARC		Yes	1.6-17

Table 2-3 Platforms that are compatible with the NetBackup-Java Administration Console and Backup, Archive, and Restore user interface *(continued)*

OS/Version	CPU Architecture	NetBackup-Java administration console	Backup, Archive, and Restore interface	JRE upgrade version
Solaris 10.0	SPARC	Yes	Yes	1.6-17
Solaris 10.0	x64	Yes	Yes	1.6-17
SUSE Linux Enterprise Server 9	IA64		Yes	1.6-17
SUSE Linux Enterprise Server 10 (SP1)	x64	Yes	Yes	1.6-17
SUSE Linux Enterprise Server 10 (SP1)	POWER		Yes	
SUSE Linux Enterprise Server 10 (SP1)	z/Architecture		Yes	
SUSE Linux Enterprise Server 11	IA64		Yes	1.6-17
SUSE Linux Enterprise Server 11	x64	Yes	Yes	1.6-17
SUSE Linux Enterprise Server 11	z/Architecture		Yes	
Windows 7	x86	Yes	Yes	1.6-17
Windows 7	x64	Yes	Yes	1.6-17
Windows Server 2003 Enterprise Edition (SP1)	x86	Yes	Yes	1.6-17
Windows Server 2003 Enterprise Edition (R2)	x86	Yes	Yes	1.6-17
Windows Server 2003 Enterprise Edition	x64	Yes	Yes	1.6-17
Windows Server 2003 Enterprise Edition (R2)	x64	Yes	Yes	1.6-17
Windows Server 2003 Enterprise Edition	IA64	Yes	Yes	1.6-17
Windows Server 2003 Enterprise Edition (R2)	IA64	Yes	Yes	1.6-17
Windows Server 2008 Enterprise Edition	x86	Yes	Yes	1.6-17
Windows Server 2008 Enterprise Edition	x64	Yes	Yes	1.6-17

Table 2-3 Platforms that are compatible with the NetBackup-Java Administration Console and Backup, Archive, and Restore user interface *(continued)*

OS/Version	CPU Architecture	NetBackup-Java administration console	Backup, Archive, and Restore interface	JRE upgrade version
Windows Server 2008 Enterprise Edition (R2)	x64	Yes	Yes	1.6-17
Windows XP Professional SP2	x86 or x64	Yes	Yes	1.6-17
Windows XP Professional SP2	IA64	Yes	Yes	1.6-17
Windows Vista	x86 or x64	Yes	Yes	1.6-17

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

NetBackup backward 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.

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`

Table 2-4 shows the different server version levels that are compatible with NetBackup in this release.

Table 2-4 Mixed-server compatibility for NetBackup 7.1

Master server version	Media server version	Client version
NetBackup 7.1	7.1	7.1
NetBackup 7.1	7.1	6.5 (and later), 6.0 (and later)
NetBackup 7.1	6.5 (and later), 6.0 (and later)	6.5 (and later), 6.0 (and later)

For more information about upgrading NetBackup, refer to the *NetBackup Installation Guide* for either UNIX or Windows.

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 7.1, it is necessary to have enough free disk space to accommodate three complete copies of the NetBackup database. That includes all transaction logs and database files in the data directory including BMR if it is configured and in use. This directory is typically `/usr/openv/db/data` for UNIX-based operating systems and `\Veritas\NetBackupDB\data` for Windows-based operating systems when you use default installation methods.
- In a mixed-server environment, the master server must run the highest version of NetBackup in use in that configuration.
- 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.
- 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.

About NetBackup EEB listings

Since the release of NetBackup 7.0 a number of Engineering Emergency Binaries have been released. These EEBs are now contained within NetBackup 7.1. 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/DOC3566

Chapter 3

Product dependencies

This chapter includes the following topics:

Operating system patches and updates

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

Table 3-1 provides the known, minimum operating system (OS) patches and updates. A vendor may have released a more recent patch that supersedes a patch that is listed in this table. Symantec recommends that you visit the Support 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.
	`xlC.rte 8.0.0.10` fileset	For the `xlC.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 TL7 SP5 (5300-07-05-0831)	NetBackup 7.0 requires the AIX 5.3 TL7 SP5 (5300-07-05-0831 Maintenance Pack as a minimum. (Higher patch levels should also work.) You can use the `oslevel -s` command to verify what Maintenance Pack level you have installed.
AIX 6.1	IZ16878	When you start Java user interface applications on AIX 6.1 platforms an exception can occur. To prevent the exception, Symantec recommends that you install patch IZ16878 from IBM® Support.
	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/libipv6.sl	
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.1	
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.sl	
	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so	
	Networking.NET2-RUN: /usr/lib/hpux32/libipv6.so.1	
	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so	
	Networking.NET2-RUN: /usr/lib/hpux64/libipv6.so.1	

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

Operating system type and version	Patch	Notes
	Networking.NET2-RUN: /usr/lib/libipv6.1	
HP-UX PA-RISC	Networking.NET-RUN: /usr/lib/libipv6.sl	For HP-UX PA-RISC platforms, this fileset is required:
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.1	For HP-UX PA-RISC platforms, this fileset is required:
	Networking.NET-RUN-64: /usr/lib/pa20_64/libipv6.sl	For HP-UX PA-RISC platforms, this fileset is required:
	Networking.NET2-RUN: /usr/lib/libipv6.1	For HP-UX PA-RISC platforms, this fileset is required:
HP-UX 11.11	PHSS_35385	This patch is required for JAVA 6.0.
	PHSS_32226	This patch is a LIBCL patch.
	PHSS_37516	Contains fixes for the following: ■ `QXCR1000593919: purifyplus` dumps core in PA32 ■ `QXCR1000589142: dld` crash in LL_new_descendent_list when the `aCC` application is exiting. ■ `QXCR1000589142: dld` crash in LL_new_descendent_list when the `aCC` application is exiting. ■ `QXCR1000746161: dlsym()` hangs ■ `QXCR1000593999: dld` emits assert messages for `chatr +mem_check` enabled 64-bit executables
	PHSS_26946	This patch is necessary to enable any C++ runtime code to work properly.
	PHSS_27740	This patch is a `libc` cumulative patch.
	PHSS_26560	This patch contains a linker tools cumulative patch.

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

Operating system type and version	Patch	Notes
	PHSS_32864	That is a recommended critical patch from HP that is required for successful NetBackup client backups.
	PHKL_26233	This patch enables `HP-UX 11.11 mmap()` to use large files from 2GB to 4GB.
	PHSS_35379	That is a recommended critical patch from HP that is required for successful NetBackup client backups.
	PHCO_29029	That is a recommended critical patch from HP that is required for NetBackup to use VxSS.
	PHSS_24045	Allow `POLL_INTERVAL` to be set to zero in `/var/stm/config/tools/monitor/dm_stape.cfg`. That disables the `dm_stape` monitor within the Event Monitoring System. Symantec recommends that you upgrade to IPR0109.
	PHSS_30970	This patch can cause problems with the programs that have the `setuid` bit set. Hewlett-Packard 's IT resource center Web site contains information about this patch. `www1.itrc.hp.com`
	PHCO_35743	S700_800 11.11 libc cumulative patch The above patch has dependency on the following patches: ■ PHCO_31923 (critical patch): s700_800 11.11 libc cumulative header file patch ■ PHKL_34805 : 700_800 11.11 JFS3.3 patch; mmap
HP-UX 11.23	PHSS_37201	This patch is required for JAVA 6.0.

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

Operating system type and version	Patch	Notes
	PHCO_33431	Symantec recommends that all customers running 11.23 install this patch.
	PHSS_34858	That is a recommended critical patch from HP that is required so that `dlopen` works properly.
	PHKL_31500	That is a recommended critical patch from HP that NetBackup requires, particularly when you attempt to run NetBackup with NetBackup Access Control (NBAC).
	PHSS_37492	Contains fixes for the following: ■ `QXCR1000593919: purifyplus` dumps core in PA32 ■ `QXCR1000589142: dld` crash in LL_new_descendent_list when the `aCC` application is exiting. ■ `QXCR1000746161: dlsym()` hangs ■ `QXCR1000593999: dld` emits assert messages for `chatr +mem_check` enabled 64-bit executables
HP-UX 11.31	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)	

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

Operating system type and version	Patch	Notes
	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.
	139555-08	Change Request ID - 6723423
	119963-21	Change Request ID - 6815915
Solaris 10 x64	119964-21	Change Request ID - 6815915
	139556-08	Change Request ID - 6723423
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 x86-64 (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 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.

The following additional product dependency information applies to this release of NetBackup:

- Product dependency notification for customers running Microsoft Windows Vista or Windows 2008 server.
  If you want to protect client (or server) systems that are running either Microsoft Windows Vista or Windows 2008 server, you may need to install Microsoft hot fix number KB952696. If you attempt to back up any protected files that have been encrypted by the operating system, NetBackup cannot back up these files. NetBackup reports that it is unable to access the encrypted files and the backup continues with all of the remaining files.

Note: That does not apply to NetBackup encryption. NetBackup encryption is separate from the file system encryption, meaning that NetBackup-encrypted files are backed up. In addition, this hot fix is not needed for any Windows version before Microsoft Windows Vista or Windows 2008 server. If you are running Vista or Server 2008, please refer to KB952696 to see if this hot fix is required for your operating system version

VxFS and VxVM compatible versions

Table 3-2 shows the versions of VxFS and VxVM that are compatible with Symantec NetBackup, and the corresponding operating systems for each.

Table 3-2 Versions of VxFS and VxVM that are compatible with Symantec NetBackup

Operating system	OS Version	Version of VxFS	Version of VxVM	Notes
AIX 5L	5.3 (64 bit)	5.1 SP1 and higher	5.1 SP1 and higher	
	6.1 (64 bit)	5.0 MP3 and higher	5.0 MP3 and higher	
HP-UX PA-RISC	11.11	3.3 and 3.5	3.5 only	
	11.23	3.5, 4.1, and 5.0	3.5, 4.1, and 5.0	
	11.31	4.1 and higher	4.1 and higher	
HP-UX IA64	11.23	3.5, 4.1, and 5.0	3.5, 4.1, and 5.0	
	11.31	4.1 and higher	4.1 and higher	
Red Hat Enterprise Linux 4.0 (AS)	x86-64	4.1 to 5.0MP3RP3	4.1 to 5.0MP3RP3	
	IA64	4.1 to 4.1MP4RP4	4.1 to 4.1MP4RP4	
	POWER	5.0 LoP phase1, phase2, and phase 3 only	5.0 LoP phase1, phase2	
Red Hat Enterprise Linux 5.0 (AS)	x86-64	LxRT4.1MP4 and higher on the 4.1 line, 5.0MP3 and higher on the 5.0 line	LxRT4.1MP4RP1 and higher on the 4.1 line, 5.0MP3 and higher on the 5.0 line	

Table 3-2 Versions of VxFS and VxVM that are compatible with Symantec NetBackup *(continued)*

Operating system	OS Version	Version of VxFS	Version of VxVM	Notes
	IA64	LxRT4.1MP4 and higher on the 4.1 code line only	4.1MP4RP1 and higher in the 4.1 code line only	
	POWER	5.0RU3 and 5.0RU4 only	5.0RU3 and higher	
Solaris (SPARC)	9	5.1SP1 and higher	5.1SP1 and higher	
	10	4.1 MP2 and higher	4.1 MP2 and higher	
SUSE Linux Enterprise Server 10	x86-64	4.1MP3 and higher in 4.1 codeline. 5.0MP3 and higher on 5.0 codeline.	4.1MP3 and higher in 4.1 codeline. 5.0MP3 and higher on 5.0 codeline.	
	IA64	4.1MP3 and higher in 4.1 codeline only.	4.1MP3 and higher in 4.1 codeline only.	
	POWER	5.0RU3 and 5.0RU4 only	5.0RU3 and higher	
SUSE Linux Enterprise Server 11	x86-64	5.0RU1 and higher	5.0RU1 and higher	
	IA64	NA	NA	
	POWER	5.0RU4 and higher	5.0RU4 and higher	
Windows 2003	x86-64	NA	4.3 and higher	
Windows 2008	x86-64	NA	5.0 and higher	
Windows 2008 R2	x86-64	NA	5.1 SP1 and higher	

NetBackup has improved its integration with the Veritas File System (VxFS) product to ensure interoperability on all compatible VxFS versions. If you run a VxFS version that is older than VxFS 4.0 then y9ou need to install new VxFS libraries on the client to back up the systems that run VxFS. You can search and download the appropriate VxFS libraries to your system from Patch Central on the Symantec Support Web site.

See, `https://sort.symantec.com/labs/patch`.

See, `http://entsupport.symantec.com/docs/320193`.

Table 3-3 Shows the integration improvements that were made between the various operating systems and the Veritas File System (VxFS).

Table 3-3 Improved Integration with Veritas File System (VxFS)

Operating system	OS Version	VxFS 5.0	VxFS 4.1	VxFS 3.5
AIX	5.3	X	NA	NA
HP-UX PA-RISC	11.11	NA	NA	X
	11.23	X	NA	NA
	11.31	X	NA	NA
HP-UX IA64	11.23	X	X	NA
	11.31	X	NA	NA
Red Hat Enterprise Linux 4.0 (AS)	x86-64	X	NA	NA
Red Hat Enterprise Linux 5.0 (AS)	x86-64	X	NA	NA
SUSE Linux Enterprise Server SLES 10	x86-64	X	NA	NA
	IA64			
SUSE Linux Enterprise Server SLES 11	x86-64	X	NA	NA
	IA64			
Solaris (SPARC)	9	X	NA	NA
	10	X	X	NA

Chapter 4

Operational notes

This chapter includes the following topics:

Operational Notes in NetBackup

The chapter contains the topics that explain important aspects of NetBackup 7.1 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 7.1. Therefore, Symantec recommends that you refer to the following Technote on the Symantec Support Web site to view the latest NetBackup 7.1 release information.

http://www.symantec.com/docs/DOC3412

To view a listing of Emergency Engineering Binary's (EEBs) that are included in NetBackup 7.1, download the following document from the Symantec Support Web site.

http://www.symantec.com/docs/DOC3566

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

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/openv/lib` for that command to work.

- 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 7.0.
- UNIX package consolidation
  In 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
  - NetBackup Vault

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

  - BMR Boot server
  - DB2
  - NetBackup 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 7.0. For example, VRTSnbdb2, SYMCnbdb2, VRTSnbenc, SYMCnbenc, and others. The installation script displays a list of the packages it finds that must be removed.
The Japanese, Chinese, and French language packages remain as separate add-ons. The process to install and upgrade these products remains the same.

- Clustered media server support changes
  New NetBackup 7.0 media server installations cannot be clustered. However, existing 6.x clustered media servers can be upgraded to version 7.0 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 7.1 installations and upgrades

This topic contains the information that applies to the installation of NetBackup 7.1. It also contains information about upgrades to this version of NetBackup.

- You need to update a script if you want to upgrade a Solaris media server that has a media server deduplication pool installed.
  If you want to upgrade a Solaris SPARC media server that hosts a media server deduplication pool, you must install an updated version of `pduninstall.sh` script. You must install this new script before you begin upgrading from NetBackup 7.0 or 7.0.1 to NetBackup 7.1.
  Please see the following Technote on the Symantec Support Web site to download the updated script.
  http://symantec.com/docs/TECH146243
- Use of IPv6 addresses as server names.
  Symantec recommends that you do not use IPV6 addresses as server names in the install.
- NetBackup 7.1 client installations can fail on FreeBSD 7.x or 8.x systems.
  NetBackup 7.1 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 7.1 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 7.1 client.

- Upgrading from NetBackup 6.x or 7.x NetBackup 7.1 fails to add `nbatd` and `nbazd` to the Monitored Services registry.
  When you upgrade from NetBackup 6.x or 7.x to NetBackup 7.1 on a NetBackup master server with NBAC enabled in a Windows clustered environment (VCS Windows or MSCS), the upgrade fails to add `nbatd` and `nbazd` to the monitored service list. That caused the NetBackup cluster group to not fail over if the `nbatd` and `nbazd` service fails.
  To work around this issue, use the following command lines to add `nbatd` and `nbazd` to the monitored service list:

  ```
  <InstallPath>\Veritas\NetBackup\bin\bpclusterutil.exe -enableSvc
  'nbatd'
  <InstallPath>\Veritas\NetBackup\bin\bpclusterutil.exe -enableSvc
  'nbazd'
  ```

- `bpclusterutil` command limitation in a Linux environment.
  The `bpclusterutil` command with the *`-online`* and *`-offline`* options does not work in a Linux environment.

- PBX may not start after a restart on an AIX platform.
  If you upgrade from NetBackup 6.5.x to NetBackup 7.1 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/openv/lib/libvxexticuST.sl.1 not removed.
Text file busy
rm: /usr/openv/lib/libvxlisST.sl.1 not removed.
Text file busy
rm: /usr/openv/lib/libvxulST.sl.1 not removed.
Text file busy
rm: /usr/openv/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 7.1
  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/openv/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/openv/netbackup/logs` on UNIX and `C:\Program Files\Veritas\Netbackup\logs` on Windows) after an upgrade to NetBackup 7.0. This occurs because the OIDs do not have an OID entry in the nblog.conf file that specifies the subdirectory for their log files (<oid>.LogDirectory=name). This may occur for the following OIDs: 102, 113, 120, 142, 153, and 157. You can display these log files with `vxlogview` in NetBackup 7.0 if you specify the following.
  `-G <root log dir> -o oid`
  Where *<root log dir>* is either `/usr/openv/netbackup/logs` on UNIX or `C:\Program Files\Veritas\Netbackup\logs` on Windows. And *oid* is the 102 , 113, 120, and so on.
  You can remove these OIDs after the upgrade. However, you must manually delete the OIDs because the `vxlogmgr` cannot access them. If you think you may need to report a problem in a previous release, then you may want to keep them for that purpose.
- To install NetBackup on Windows 2008/Vista/2008 R2/7 UAC-enabled environments, you must log on as the official administrator. Users that are assigned to the Administrators Group and are not the official administrator cannot install NetBackup in UAC-enabled environments.
  To allow users in the Administrators Group to install NetBackup, disable UAC.
- 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://support.veritas.com/docs/287850`
- In a future release, it may be required that clients connect to the master server to complete an installation.
- Symantec recommends the following Microsoft updates when you run NetBackup on Windows operating systems:

- Microsoft `storport` hot fix. This fix applies to Windows x86 and x64, on both SP1 and SP2: (required) `http://support.microsoft.com/?id=932755`
- Microsoft microcode reliability update. This fix applies to 32-bit and 64-bit versions of Windows Server 2003/XP/Vista: (suggested) `http://support.microsoft.com/?kbid=936357`
- Symantec AntiVirus. Update to latest version (10.2 for Corporate Edition) and latest update (required).
- The `Symevent` driver updates (required). Update to latest driver version.

- 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
  - QLA2340 Q*Logic HBA BIOS 1.47 (required) http://support.qlogic.com/support/oem_product_detail.asp?p_id=253&oemid=65&oemname=QLA2340
  - All other Q*Logic HBAs use latest driver & BIOS (suggested)http://support.qlogic.com/support/oem_product_list.asp?oemid=65
- The default shared-memory requirements on UNIX systems are greater for NetBackup 7.0 than previous releases.
  See the *NetBackup Installation Guide for UNIX and Linux*.
  See the *NetBackup Troubleshooting Guide for UNIX, Windows and Linux*.
- 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 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.

- 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.
- When executing /usr/openv/netbackup/bin/bp.start_all on HP-UX PA-RISC, IBMzSeries RedHat, and IBMzSeries SUSE media servers, you may see the following messages:
  - `/usr/openv/netbackup/bin/nbpem is either missing or not executable.`
  - `/usr/openv/netbackup/bin/nbstserv is either missing or not executable.`

  You can safely ignore these messages. In a future release, this script will be fixed to not display these messages.
- While using NetBackup in a remote EMM configuration, the following can occur.
  If you install the master server before the EMM server in a remote configuration, during the installation a core dump can occur with `nbdb_admin`. The installation succeeds however, later a catalog backup can fail with an error code status 2.
  To avoid this issue when you install NetBackup in a remote configuration, install the remote EMM server before you install the master server. Installing in this order means the master server gets the `vxdbms.conf` file from the EMM server during the installation. As a result, the master`vxdbms.conf` file contains the appropriate `VXDBMS_NB_DATABASE` entry.
  If you happen to install the master before you install the EMM server the catalog backup does not work. Symantec recommends that you execute the following command to resolve the issue.
  `/usr/openv/db/bin/nbdb_admin -quiet -dba nbusql`

Installing NetBackup client software in Solaris 10 zones

The following instructions clarify how to install NetBackup client software in Solaris 10 non-global zones. Technote 65627 on the Symantec Support Web site contains more information.

- NetBackup server is supported only in a global zone.

- On a server whose non-global zone does not use a read-only loopback device for the `/usr` directory, the client push-install or local install is done normally. Please see the appropriate installation guide.

If the server does not have a master or a media server on the global zone, and has a sparse non-global zone using a read-only loopback device for the `/usr` directory, use the following procedure.

To provide clarification for installing NetBackup client software in Solaris 10 non-global zones

1. In the global zone, create `/usr/openv` as a symbolic link to the location in which you install the software to in the non-global. That needs to be done even if the global zone does **not** have that directory.

   For example:

   ```
   # ln -s /nonglobdir/openv /usr/openv
   # ls /nonglobdir/openv
   /nonglobdir/openv: No such file or directory
   # ls -al /usr/openv
   rwxrwxrwx 1 root root 10 Aug 23 15:13
   /usr/openv -> /nonglobdir/openv
   ```

2. In the non-global zone, make sure that `/usr/openv` exists as a link.

   For example:

   ```
   # ls -al /usr/openv
   rwxrwxrwx 1 root root 10 Aug 23 15:13
   /usr/openv -> /nonglobdir/openv
   ```

   If the `/usr/openv` link does not already exist, you must use the `zlogin` process to become "Zone root" on the non-global zone. Then you can create a link from /usr/openv/ to a writeable location on the non-global zone.

3 In the non-global zone, make sure that the directory link exists and is writable.

For example:

```
# ls -al /nonglobdir/openv
total 32
drwxr-xr-x 9 root bin 512 Aug 18 15:23 ./
drwxr-xr-x 18 root bin 512 Aug 18 15:30 ../
```

4 Client push-install or local install can now be done normally according to guides.

Starting with NetBackup 7.0, you may see one or more messages that are similar to the following:

```
cp: cannot create /usr/kernel/drv/snapctl.conf: Read-only file system

mkdir: Failed to make directory "/usr/share/regid.1992-11.com.symantec"
Read-only file system

The asset tag file /usr/openv/swidtag.xml could not be copied to
directory /usr/share/regid.1992-11.com.symantec.
```

If the server does have a master or a media server on the global zone, and has a sparse non-global zone using a read-only loopback device for the `/usr` directory, use the following procedure:

To provide clarification for installing NetBackup client software in Solaris 10 global zones

1. In the global zone, the `/usr/openv` in a default installation is a link to `/opt/openv`. Alternatively, the master or the media server can be installed in a base directory (`BASEDIR`) other than the default `/opt`. And you can link `/usr/openv` to `/BASEDIR/openv`. Verify the directory that `/usr/openv` is linked to.

   For example:

   ```
   # ls -al /usr/openv
   rwxrwxrwx 1 root other 10 Aug 18 11:39
   /usr/openv -> /opt/openv/
   ```

2. In the non-global zone, create a writable directory where the `/usr/openv` points to.

   For example:

   ```
   # mkdir /opt/openv
   ```

3. Client push-install or local install can now be done normally according to guides.

NetBackup LiveUpdate

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

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

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

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

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

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

Secure push install

The installation methods (`ssh` and `sftp`) of pushing UNIX client software from a UNIX master server to a UNIX client host consist of running the `install_client_files` script on the command line. Both of these methods are based on the usage of the `SunSSH` and `OpenSSH` products and these products must be at specific version and patch levels.

For more information about these patches, refer to Table 3-1 in Chapter 3, NetBackup product dependencies.

NetBackup cluster

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

- New NetBackup 7.1 media server installations cannot be clustered. However, you can upgrade existing NetBackup 6.x clustered media servers to version 7.1 and they remain clustered.
- When a fault occurs in a cluster resource group for NetBackup in a SunCluster configuration, failover of the NetBackup resource group does not occur. The failure in this situation could happen if the NIC (network) or other resources could not come online.
- 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.
- 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://entsupport.symantec.com/docs/278307` 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://entsupport.symantec.com/docs/288471`.
- When you configure disk storage units, only basic disk supports the use of application clusters. When you configure disk pools or storage servers, application clusters are not supported.

- 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
```

- If you install NetBackup 7.1 on the HP Service Guard v11.18 (or 11.17) on more than one node, the NetBackup cluster resource group may become unmanageable when the NetBackup package (Virtual IP) fails to come online or offline. Offline and failover of the cluster package does not occur.

  If you encounter this issue, do the following after you install NetBackup, and all cluster nodes:
  - Open the NetBackup package configuration file (`/etc/cmcluster/netbackup/netbackup.config`).
  - Change the name of the configuration entry for subnet mask from **MONITORED_SUBNET** to **SUBNET** on all of the nodes in the cluster. You do not need to update the cluster because the configuration has not changed.
  - Open the package control script `/etc/cmcluster/netbackup/netbackup`.
  - Uncomment the following parameters on all of the nodes in the cluster:

    - `SERVICE_NAME[0]="netbackup"`
    - `SERVICE_CMD[0]="/etc/cmcluster/netbackup/monitor"`
    - `SERVICE_RESTART[0]="-r 2"`

    Remove the hash symbol ('#') from the beginning of each of these three lines to uncomment the parameter.

NetBackup Documentation Notes

The following list identifies some known inconsistencies in the NetBackup documentation that has been released with NetBackup 7.1.

- The following was found in the *NetBackup Administrator's Guide, Volume I*.
  In Chapter 15, Figure 15-8 (Storage lifecycle policy (in Domain 2) with intermediary duplication destination) should show that the import destination and the first duplication destination are two different storage units. Note that when the storage units are PureDisk disk pools, (either MSDP or PDDO), PureDisk does not allow the duplication copy to be copied to the same disk volume as the import copy.
- On page 148 of the NetBackup OpsCenter administrator guide , there are two steps that contain different install commands.
  Step 4 of the upgrade procedure in the "Upgrading from NetBackup Operations Manager to OpsCenter on UNIX" section is incorrect. You must ignore Step 4 in the procedure. This step is listed on page 148 in the Symantec OpsCenter administrator guide.
  Step 4 of the upgrade procedure states the following:
  ```
  Type the following command:./installOpsCenterServer. Press Enter.
  ```
- The following was found in the *NetBackup LiveUpdate Guide*.
  In the *NetBackup LiveUpdate Guide*, on pages 12-13, the following statement appears:
  "To correct this problem, you must first install "unlimited strength jurisdiction policy files" into your NetBackup Java JRE. NetBackup does not deliver Java JRE with these files. They must be downloaded from the Sun Microsystems Website and installed in your NetBackup Java JRE location manually."
  The reference to the Sun Microsystems Web site is incorrect. The files must be downloaded from the IBM Web site.
- A change is required in a note within a procedure on page 369 of the *Symantec OpsCenter Administrator's Guide* is incorrect.
  The note in Step 3 of the "Configuring the Breakup Jobs option for master servers" procedure on page 369 of the *Symantec OpsCenter Administrator's Guide* is incorrect. The note states the following:

  ```
  Note: To disable the Breakup Jobs option for
  7.1 master servers, add the following text to scl.conf file:

  #nbu.scl.collector.enableBreakupJobDataCollection=false
  ```

  The text should not include the # character. The proper string of text to add to the scl.conf file is as follows:

```
nbu.scl.collector.enableBreakupJobDataCollection=false
```

- Table 2-4 in the Symantec OpsCenter Administrator's Guide lists the supported versions for Linux SUSE 11 as 2.6.5-*, 2.6.9-*, 2.6.16-*, 2.6.18-*,2.6.27-*, 2.6.32-* where * is the `kernel-smp` version. That is incorrect.

  The supported versions for SUSE Linux are 2.6.5-*, 2.6.16-*, 2.6.27-*, 2.6.32-*
  In addition, the supported versions for Red Hat Linux are 2.6.9-* and 2.6.18-*.

- To remove PureDisk files when you remove the NetBackup server software.
  In the NetBackup 7.1 Installation Guide for UNIX and Linux, the procedures for removing PureDisk files include a step with an incomplete command. When you remove NetBackup server software from the systems that support PureDisk, you should add the `-forceclean` option to the following command to remove the PureDisk files.

  `/opt/pdde/pddeuninstall.sh -basedir` *`base`* `-ostdir`
  `ostdir``[-forceclean] [-32bit]`

  The `-forceclean` option cleans everything. It ensures that the configuration files are not saved for upgrades.

- The following was found on page 175 of the *NetBackup Administrator's Guide, Volume I*.

  "`0/0 </> Matches the address of any family.`"

  The characters "`</>`" should not appear. The correct value should only be, "`0/0`".

- The following was found on page 175 of the *NetBackup Administrator's Guide, Volume I*.

  The following statement is not accurate:
  "If a host name is specified as the network, then the address that is used is the first returned by the DNS resolver."
  A more accurate statement should be documented as follows:
  "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."

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 caused by the Sun Microsystems™ issue, 6901233.
  See, `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 user interface corruption or a possible data loss.
- 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:

  - Hostname (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

About general NetBackup 7.1 notes

The following items describe general NetBackup 7.1 operational notes.

- 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 7.1 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, so if the time is not correctly synchronized, it may not appear in the correct order at the Activity Monitor.

- 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.

- This release of NetBackup contains several new error status codes.
  This release of NetBackup introduces 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.

- You may encounter an issue if you try to recover the deduplication storage that has a separate database path.
  In the deduplication environments that use separate paths for the storage and for the database, you must edit several configuration files after you recover the storage and the database.
  To work around this issue, see the following Technote on the Symantec Support Web site:
  http://symantec.com/docs/TECH152451

- If you select a large number of volumes for a point-in-time rollback restore from an Instant Recovery backup with verification enabled, the restore may fail. It fails because the `bpbrm` process on the master server and the `bppfi` process on the client or alternate client hangs. The issue occurs when 48 volumes were selected for a point-in-time rollback restore on a Solaris system.

The following output was obtained using the `truss` command. Use the same command to produce a similar output and compare your results to the following results to determine if the same issue exists.

```
The bpbrm process (pid: 1383) is still alive on "globalqe-sol4".

-bash-3.00# ps -ef | grep bpbrm
   root  1383   1   0   Jan 06 ?    0:01 bpbrm -restore -mt 0 -mst 0 -
k 1 -c globalqe-sol3 -hostname globalqe-sol3 -rcln

-bash-3.00# truss -p 1383
write(8, 0xFFFFFFFF7FFCB7D0, 549) (sleeping...)

-bash-3.00# ps -ef | grep bppfi

    root  1399   1   0   Jan 06 ?   0:00 bppfi -verbose -rollback -to
300 -locale C -keep -snpverify -altclient

-bash-3.00# truss -p 1399
write(2, 0xFFFFFFFF7FFFD8D0, 83) (sleeping...)
```

- 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.
- A Windows system may not come up after a disaster recovery.
  A Windows computer would not come up after a disaster recovery restore was performed after an ALL_LOCAL_DRIVES backup.
  If you encounter an error that is related to the `lsass.exe` executable, you should first attempt to perform a restore. Next, shut down the NetBackup client service from the services windows and then restart the system.
- An upgrade to SQLAnywhere 11.0.1 was made in NetBackup 7.0.
  An upgrade to SQLAnywhere 11.0.1 was made in NetBackup 7.0. However, there is a restriction within that version that requires the database server name to be less or equal to 31 characters. NetBackup has been modified to change the server name, from *VERITAS_NB_hostname.domain_name* to *NB_hostname* in `/usr/openv/db/bin/servername`. NetBackup also trims the name to 31 characters if necessary.
- 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 7.1, 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.
- Optimized duplication fails between PDDO to PDDO with media write error (84) on AIX and Solaris 10 x86_64.
  That issue applies to environments that run NetBackup 7.1 with a PureDisk 6.6.1 or PureDisk 6.6.1.1 deduplication agent on AIX or Solaris 10 x86_64 platforms. In these environments, optimized duplication fails with a media write error of 84.
  If you encounter this issue, contact Symantec Technical Support to request a fix.
- Do not use a **LIMIT_BANDWIDTH (IPv4)** configuration or a **THROTTLE_BANDWIDTH (IPv6)** configuration in the initial release of NetBackup 7.1. If you use either of these configuration options, you can encounter a sever performance degradation.
  An EEB will be available to fix the issues.
- When you perform a Duplicate to Remote Master operation, it is possible that the source image spans volumes within a single disk pool, which do not replicate to an equivalent set of volumes, within the same disk pool, in every target domain.
  That means that if you create an image to be duplicated to a Remote Master, and you run out of disk on the volume that you want to write to, then the job fails. The job is tried again when there is enough space to duplicate the backup image from of a single volume.

This issue will be addressed in the first available Release Update for NetBackup 7.1, and spanning will be disabled for the source copy of a duplication to remote master operation.

- The deduplication rate is low during a multistream backup of SQL2005 to PDDE. 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 PDDE 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 7.1.

  - BasicDisk
  - AdvancedDisk
  - PureDisk

  The following list indicates the disk storage units that do **not** support Granular Recovery in NetBackup 7.1.

  - NearStore
  - OpenStorage
  - SnapVault

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 NetBackup Administration Consoles should be able to handle a partial success error code.
  The Windows-Java and Windows user interfaces should be able to handle partial success error codes. That means they should be able to refresh the user interfaces as part of this process. Failing to refresh the user interfaces causes unexpected behaviors.
- The multiple-attribute values that were not modified were displayed with the modified attributes in the **Audit** record when the Disk Pool properties were updated.
  The **Audit** record listed the values of attributes that were not modified or updated for the DiskPool when the `setattribute` and `clearattribute` options were used. Only the values of the attributes that were modified or upgraded should have been displayed.
- The **Backup selection** is stored as a UTF-8 encoded string in the Audit database. The `nbauditreport` command does not convert the UTF-8 encoded string to the current locale; therefore, the command line interface may show unrecognizable characters for the backup selection output.
- Two audit records are created for each policy operation.

For each operation, the old and new values are first set from default values to blanks. Then these values are set from blanks to actual values. Thus, for every operation that occurred two audit records were created. Only one record should be created with the old and new values.

- Audit records may not show the values for the *reason* attribute in the `nbauditreport` detailed report.

  If you use the `bppolicynew -reason` command to rename or copy policies, the audit records that are created do not show the values for the *reason* attribute in `nbauditreport` detailed report.

- 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.

- The recurring **Weekdays** calendar is not scheduled because of an audit failure during a policy update operation.

  - The policy execution manager (PEM) registers with `BPDBM` for the policy update notifications. It also reschedules the policies based on the updates it received. If auditing of policy operations fail, `BPDBM` fails to send the notification to PEM which results in PEM not rescheduling the policies as desired.

    To work around this issue, disable the audit setting and update the policy after five minutes. you can use the policy adminstration command such as `bpplinfo` for example : `bpplinfo policy_name -modify`. Please ensure that the policy update operation was successful.

  - If auditing fails on on a policy delete operation, disable the audit setting and restart NetBackup.

NetBackup Bare Metal Restore

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

- The PHCO_40961 patch is required to create a BMR shared resource tree (SRT) on an HP-UX IA64 11.31 platform.

  The following 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).

  PHCO_40961

- 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.
- BMR recovery of Solaris operating system that has 5.1 VxVM installed and uses an SRT that contains a 5.1 VxVM package that does not work. It fails when the VxVM services start in a BMR restore environment.
  Please use the 5.0 VxVM package in SRT to restore the Solaris operating system that runs a 5.1 VxVM version.
  In case of any issues, please contact Symantec Support for additional help.
- BMR recovery of SUSE 10 client using SUSE 10 OS-based SRT created on SUSE 11 OS-based BMR Boot server may fail. While BMR booting of SUSE 10 client, it may fail during driver loading.
  User can import SUSE 10 SRT created on SUSE 10 OS-based BMR Boot server itself. DO PTR and BMR restore works.
  If SUSE 10 OS-based BMR Boot server is not available, please contact Symantec Support to get an EEB on this issue.
- A failure may occur during a VxFS7-based file creation.
  During a BMR restore, a failure can occur during a VxFS7-based file creation process. To work around this issue, use a `bmrsrtadm` to patch VxFS version with 5.0 release to edit the SRT. Attempt to restore again and start a client restore.
- The BMR restore does not work on IPv6 network channels.
  A `bmrsetupmaster` may fail while resolving BMR 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 7.1 only from NetBackup 7.0 and 6.x. You cannot directly upgrade an older standalone BMR product (BMR 4.7) to NetBackup 7.1, but it can be migrated to NetBackup 7.1.
  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 7.1 SRT does support restores of pre-7.1 NetBackup (for example, 6.5.X or 6.X) clients. The SRT that contains NetBackup 7.1 or a higher version NetBackup Client can be used to restore back-level NetBackup clients.

- About copying a pre-NetBackup 7.1 SRT
  The boot server does not support copying of 6.5.X and 6.X SRT.

- About importing a pre-NetBackup 7.1 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 back up 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 7.1 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 7.1.
- From the BMR Administration console, the source object is disabled in the user interface if mapping is successful.
  When you use the BMR Administration console to map an object, the source object is disabled in the user interface if mapping is successful. That indicates that it cannot be mapped again unless you un-map the object. For Solaris 10_x64 client configurations, when you map certain objects such as slices or volumes, even if the mapping completes successfully, the original object is not disabled. That does not mean that the mapping has failed. A BMR Restore using such a mapped configuration still completes successfully.
- The first boot after a successful restore may fail on a Linux client if the disk order in the BIOS is not correct.

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

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

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

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

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

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

- A `bmradmin`-user account that is created on a Windows boot server during a boot server installation is saved and not deleted later.

  A `bmradmin` account is created on a Windows BMR boot server during the boot server registration. (It is not created on non-Windows boot servers.) This account is created unconditionally because at the boot server installation and registration time, it is not clear whether you may require a Legacy SRT or not. Legacy SRTs require this account to perform legacy restores that use a CD or floppy boot option. FastRestore operations do not require this account. If you determine that you do not need to perform legacy restores, then you can remove this account. However, you if remove this account, and then decide that you need it to run a legacy restore, you must recreate the account manually. Manually creating this account requires assistance from Symantec Support because it is originally created with a predefined password and other attributes.

- The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while the BMR SRT is created.

  The `bmrsrtadm` command on AIX and HP-UX prompts you to enter the desired architecture (32/64) while the BMR SRT is created. If you want to install NetBackup client versions that are older than 7.1 into the SRT, the OS architecture type that you select should be 32-bit. For NetBackup 7.1, select 64-bit as the OS architecture type. While you install the NetBackup client into the SRT, `bmrsrtadm` gives the appropriate error message if there is any incompatibility between the SRT OS architecture type and the NetBackup client version.

- You can use a shared resource tree (SRT) that contains a version of the NetBackup client of 7.1 or higher restore the back-level NetBackup clients.

BMR support of SFW5 limitations

A NetBackup System state backup fails on certain Windows 2008 R2 systems with SFW 5.1 SP1. That is an issue that occurred on a system where the **System Reserved** partition did not have an assigned drive letter.

To avoid this issue, manually assign a drive letter to the **System Reserved** partition and run the backup again. The BMR configuration backup and NetBackup backup both complete successfully.

About database agent limitations

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 7.1 environments.
  In IPV6-enabled NetBackup 7.1 environments, granular recovery is not supported for Microsoft Exchange Server or Microsoft Sharepoint Server.
- NetBackup for Microsoft Exchange 2010 GRT backups and restores
  For Exchange 2010 GRT backups and restores, in addition to the NetBackup media server and the Exchange granular clients, also enable Services for Network File System on the CAS Server. For more information on configuring Services for Network File System (NFS), see the *NetBackup for Microsoft Exchange Administrator's Guide*.
- HP-UX PA-RISC checkpoints may not be unmounted on Oracle database agents.
  For HP-UX PA-RISC checkpoints to unmount and be cleaned up, create touch file `/usr/openv/netbackup/AIO_READS_MAX` that contains the value 1.
  See the *NetBackup for Oracle for UNIX and Linux Administrator's Guide* for more information.
- Sybase ASA performance is poor with an UltraSparc-T series processor.
  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 run your EMM server on this type of hardware.
- The `nbdb_move` command does not work in a remote EMM server configuration.
  When you use the command line interface, the `nbdb_move` command does not work in a remote EMM server configuration.

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 is empty if the restore is initiated from a node in the DAG.
  When you restore databases or granular items of a DAG backup, the restore status may be empty from the backup and restore user interface. The status is empty if the restore is initiated from a node in the DAG. You should initiate the restore from the active DAG node or a NetBackup server to properly see the activity status.
- User-initiated backups in a DAG environment fail if initiated from a node in the DAG that is not currently active for the virtual DAG name. Initiate the user backup from the active DAG node or manually start the backup from the NetBackup master to properly start the backup.
- An Exchange 2010 granular-item restore may result in duplicate message attachments.
  The Exchange 2010 granular-item restores may result in duplicate message attachments when you restore the mail items that were previously restored and then backed up with granular recovery.
- The **company** field of task objects does not get properly restored.
  The **company** field of task objects does not get properly restored with Exchange 2010 granular recovery.
- The `bpfis.exe` memory usage grows when a snapshot of multiple storage groups or Exchange 2010 databases is processed.
  In NetBackup testing, the `bpfis.exe` process memory usage grows by a few megabytes per storage group or Exchange 2010 database. If a single snapshot job processes a large number of storage groups or Exchange 2010 databases, the process virtual memory size can approach or exceed one gigabyte.
  The workaround is to make sure that you have sufficient virtual memory to accommodate this growth, or to break up your backup into smaller snapshots.
- Instant recovery backups are not supported for Exchange in a cluster environment.
  Instant recovery backups are not supported for Exchange in a cluster environment (Exchange 2007 cluster, Exchange 2007 CCR, or Exchange 2010 DAG).
- The progress log window does not display the proper messages when an Exchange backup is launched using the Snapshot Client off-host backup capability.
  When an Exchange backup is launched from the NetBackup Client user interface and uses the Snapshot Client off-host backup capability, the progress log window does not display the usual progress messages evident when a scheduled backup is executed. The lack of progress logging does not affect the backup operation. If detailed progress is desired, use the NetBackup

Administrator's user interface to launch a Manual Backup operation on an Exchange policy.
See the Testing Configurations Settings section in the *NetBackup for Exchange System Administrator's Guide* for instructions regarding a manual backup operation.

- Alternate client (off-host) backup of Exchange 2010 fails with a status 130 with NetBackup 7.1.
  An alternate client (off-host) backup of Exchange 2010 may fail with a status 130 error. That occurs if the Exchange management console (EMC) is not installed on the off-host client. This problem arises because the Exchange `eseutil` command is required on the alternate client if the EMC is not installed. For Exchange 2010, `eseutil` requires that the VC9 runtime DLLs be installed, and these DLLs are not automatically installed with NetBackup.
  From the `bpfis` log on the alternate client, the following error occurs.

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

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

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

- A backup image of pre-NetBackup 7.x versions that use a Mailbox backup can fail to restore attachments.

  Add support for wildcard characters in the file list for Exchange VSS backups (both DAG and standalone). That works for all versions of Exchange. The supported wildcard characters are a trailing * (it must be the last character) or one or more ?. Brackets are not supported. The following are valid file entries:

  - Exchange 2010 DAG
    Microsoft Database Availability Groups:`\Database*`
    Microsoft Database Availability Groups:`\Data??se`
  - Exchange 2010 standalone
    Microsoft Information Store:`\Database*`

Microsoft Information Store:`\Data??se`

- Exchange 2003 and 2007
  Microsoft Information Store:`\Storage Group*`
  Microsoft Information Store:`\Storage?G?oup`

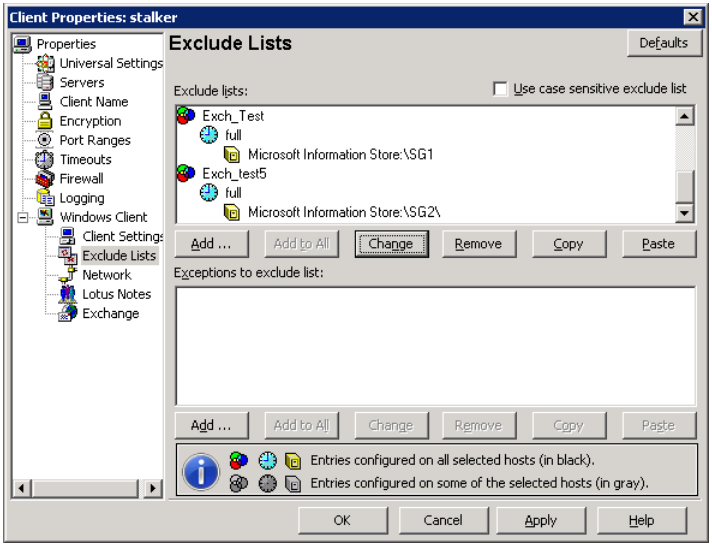
- The following inconsistency exists in the NetBackup 7.0.1 Release Notes pdf. The following statement in the NetBackup 7.0.1 Release Notes pdf is not correct. The following is not supported in either NetBackup 7.0.1 or NetBackup 7.1.
  VCS 5.1 SP1 AP1 support on Windows Server 2008 x64 with Microsoft Exchange Agent (Exchange 2010 support)

The following item applies to Exchange 2003 and 2007:

You must specify the exclude list entry as **Microsoft Information Store:\Storage_Group_Name**. Entering a database is not valid, because Exchange requires that VSS backups contain the entire storage group (for log truncation purposes). You can specify the exclude list entry under the **All Policies**, or under a specific policy and schedule.

The following item applies to Exchange 2010:

The exclude list entry is **Microsoft Information Store:\Database_Name**, even for the databases that exist in a DAG. You can specify the exclude list entry under the **All Policies**, or under a specific policy and schedule. However, if **All Policies** is entered for a database in a DAG, the discovery phase of the backup detects the exclude entry, and ignores it. If you enter a specific policy for a database in a DAG, the discovery phase does not detect it. The snapshot phase detects it and ignores it. In this situation, if that is the only database in the `bpfis` job, it causes the snapshot phase to fail with a status 69 error. The entire backup finishes with an error.



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.
- 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.
- 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.
- An initial backup of SharePoint may result in a Status 71 after you have installed on a clean system. Subsequent backups are successful
  Retry the backup. The failure is due to the registry entries that are not initialized.
- 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).

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 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/business/support/index?page=content&id=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 AdvancedDisk option

NetBackup does not support clustering of AdvancedDisk media servers.

NetBackup Media Server Deduplication Option

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/openv/netbackup/bin/bp.kill_all
  ```

- The `netbackup start` script may return a status 2 error on UNIX and Linux systems.
  On UNIX and Linux systems on which a deduplication storage server is not configured, the `netbackup start` script returns status 2. The status 2 indicates that the script cannot start the deduplication daemons. Because a storage server is not configured, the daemons cannot be started. The error is spurious; you can ignore it.
- 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 213 or status code 2074.
  Deduplication backup jobs may fail with status code 213 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.
- NetBackup 7.1 retains the existing `pd.conf` files on your deduplication hosts.

For upgrades from 7.0 and 7.0.1 to 7.1, NetBackup retains the existing pd.conf files on your deduplication hosts. For a description of `pd.conf` file parameters that are new for 7.1, see the *NetBackup Deduplication Guide* for the 7.1 release.

- Antivirus software may delete files required by the NetBackup Media Server Deduplication Option, causing it to fail to start. Deleted files may also result in corrupt, unrestorable images.
  See http://www/symantec.com/docs/TECH128891

NetBackup OpenStorage Option limitations

The following list contains the operational note information that pertains to NetBackup OpenStorage option.

- The NetBackup OpenStorage Options do not support clustering in some instances.
  The NetBackup OpenStorage Options does not support clustering of the media servers that function as data movers.
- NetBackup performs a regular duplication on images where optimized duplication is not possible.
  NetBackup performs optimized duplication until it encounters an image for which optimized duplication is not possible. For that image and all subsequent images, NetBackup performs a regular duplication.
- NetBackup requires OpenStorage vendor plug-ins to be 64-bit.
  Beginning with NetBackup 7.0 and going forward, NetBackup binaries are compiled in 64-bit. Therefore, NetBackup requires OpenStorage vendor plug-ins to be 64-bit. When you upgrade a media server that is used for OpenStorage to NetBackup 7.0, you also must update the vendor plug-in to a 64-bit version.

SharedDisk support in NetBackup 7.0 and later

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.

About SAN Client and Fibre Transport

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.

About OpsCenter limitations

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`.
  - Installing OpsCenter components in a location that is mounted from a remote host is not supported.
  - OpsCenter 7.1 does not support Internet Explorer (IE) 6.x.

- On page 148 of the NetBackup OpsCenter administrator guide , there are two steps that contain different install commands.
  Step 4 of the upgrade procedure in the "Upgrading from NetBackup Operations Manager to OpsCenter on UNIX" section is incorrect. You must ignore Step 4 in the procedure. This step is listed on page 148 in the Symantec OpsCenter administrator guide .
  Step 4 of the upgrade procedure states the following:
  `Type the following command:./installOpsCenterServer. Press Enter.`

- OpsCenter may not recognize a VMWare client if it has a name other than the display name.
  The **Virtual Client Summary** report may give inaccurate results when you configure a NetBackup policy for backing up a VMWare client using a name other than a display name. That happens when you provide names like UUID, DNS, or host name in the **Client Selection** drop-down list. If you provide a

UUID, DNS, or host name in the **Client Selection** drop-down list, you must use object merger functionality to merge these clients.

- 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).

- Table 2-4 in the Symantec OpsCenter Administrator's Guide lists the supported versions for Linux SUSE 11 as 2.6.5-*, 2.6.9-*, 2.6.16-*, 2.6.18-*,2.6.27-*, 2.6.32-* where * is the `kernel-smp` version. That is incorrect.

  The supported versions for SUSE Linux are 2.6.5-*, 2.6.16-*, 2.6.27-*, 2.6.32-*

  In addition, the supported versions for Red Hat Linux are 2.6.9-* and 2.6.18-*.

- 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.

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

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

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

  If an uninstallation process for OpsCenter Server or Agent is canceled or interrupted on UNIX, then the uninstall script (`uninstallOpsCenterServer`and`uninstallOpsCenterAgent`) is removed from

`/opt/VRTS/install`. If you want to uninstall the OpsCenter Server again, you can use the uninstall scripts from the OpsCenter DVD.

- Consider the following best-practice suggestions about report names in OpsCenter 7.1

  Review the following points about report names in OpsCenter 7.1:

  - 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 7.1. For example, a **media*summary**report in OpsCenter 7.0 is renamed as **media_summary** report in OpsCenter 7.1.

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

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

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

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

- May need to restart the AT service if you uninstall VBR after you have upgraded from VBR to OpsCenter 7.1.

  If you uninstall VBR after upgrading from VBR to OpsCenter 7.1 Server on Solaris, then you may not be able to log on to the OpsCenter console. To resolve that, you must start the AT process manually by running `/opt/VRTSat/bin/vxatd`.

- Ensure that data collection occurs properly after you upgrade a VBR server to OpsCenter 7.1.

  If a VBR server that collects NetBackup data through a remote VBR Agent is upgraded to OpsCenter 7.1 Server, then after the upgrade you must first configure the master servers to allow server access and data collection by OpsCenter.

  See "Adding a master server in OpsCenter" section in the *NetBackup OpsCenter Administrator's Guide*.

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

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

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

- The **Library Summary** report might display negative values.
  The **Library Summary** report might display negative values. These negative values are a result of negative slot counts. If the user added -1 NetBackup is unable to connect to the media. If the slot count is 0 NetBackup only calculates data for TLD and TLD8 media leading to negative values in the report. The user must enter the media slot count from **Settings > Configuration > Tape Library**.
- The color of an icon that is next to an error message on an Installation Status screen is misleading.
  When you install OpsCenter 7.1 on a Windows cluster and VCS is not configured properly, then a green icon with the following error message is displayed on the **Installation Status** screen:
  `Pre install cluster configuration failed to complete.`
  The green icon is misleading. The icon should be red for an installation failure. When you click **Next**, the correct red icon is shown.
- The `NetBackupOpsCenterVCS` resource is offline after you have installed an OpsCenter cluster.
  After installing an OpsCenter cluster on a Windows 2008 R2 x64 system, you must manually bring the `NetBackupOpsCenterVCS` resource online. You can bring the `NetBackupOpsCenterVCS` resource online from the command line interface or by using the cluster user interface.
  You can use the following command:
  `hares -online <resource name> -sys <Name of the active node>`
  `Example: hares -online newonelatest-OpsCenter -sys OPS-CLUSTER-1`
- On Windows systems, the `log.conf` file is not created properly. That causes the `vxlogview` to return a `No logs to be displayed` message.
  Use the following commands to view logs for OpsCenter GUI (OID-147) and Infrastructure components (OID-761):
  - OpsCenter GUI:
    - `<INSTALL_PATH>\OpsCenter\server\bin\vxlogview -p 58330 -o 147 -G`

- <*INSTALL_PATH*>\OpsCenter\gui\logs

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

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

- An Alert description for the **Media server unreachable** alert is not accurate.
  In the alert policy description for the **Media server unreachable** alert it states the following:

  ```
  An alert is generated when OpsCenter loses contact with the master server.
  ```

  Ideally the description should read as follows:

  ```
  An alert is generated when the media server loses contact with the master server.
  ```

  Media server always holds connection with NetBackup master server not the OpsCenter server. And OpsCenter also collects data for NetBackup master server and not the media server.

- A change is required in a note within a procedure on page 369 of the *Symantec OpsCenter Administrator's Guide* is incorrect.
  The note in Step 3 of the "Configuring the Breakup Jobs option for master servers" procedure on page 369 of the *Symantec OpsCenter Administrator's Guide* is incorrect. The note states the following:

  ```
  Note: To disable the Breakup Jobs option for
  7.1 master servers, add the following text to scl.conf file:

  #nbu.scl.collector.enableBreakupJobDataCollection=false
  ```

  The text should not include the # character. The proper string of text to add to the scl.conf file is as follows:

  ```
  nbu.scl.collector.enableBreakupJobDataCollection=false
  ```

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

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

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

- The WLA report displays the same date twice due to Daylight Saving Time (DST).

  The WLA report displays the same date twice due to Daylight Saving Time (DST). The report displays the same date twice only for that week when daylight saving.

  Normally, the report fetches data for a complete week. When you run the report for the first week of October (when daylight saving is still on), the report displays data for the first seven days. The same report displays different results when generated on the day when daylight saving ends. Let us consider the week of November 5th to 11th for year 2010. When daylight saving ends on November 7th and you generate the report, the report repeats the date 7th. The report displays data column headers for 5th, 6th, 7th, 7th, 8th, 9th, and 10th (seven days as 7th is repeated). Ideally the report carries correct data, but the data is displayed across incorrect date columns.

  The data for the last hour of November 7th is displayed in the first cell of the repeated date (November 7th) and the remaining cells display the data for 8th. Data for 9th, 10th, and 11th is displayed under November 8th, November 9th, November 10th column respectively.

- When you apply a language pack to OpsCenter 7.0 or 7.0.1 and then upgrade to OpsCenter 7.1, most components of the language pack get uninstalled during the upgrade.

  However, the Default Locale drop-down list in OpsCenter 7.1 continues to show the languages that are associated with the Language Pack. The Default Locale drop-down list can be accessed by clicking Settings > User Preferences > General in the OpsCenter console. When you select a language that is associated with the language pack from the Default Locale drop-down list, OpsCenter continues to show English text.

To resolve this issue, you must install the appropriate language pack for OpsCenter 7.1.

- The OpsCenter server can stop receiving events from the master server after a NetBackup 7.1 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 7.1.

  - 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 7.1 upgrade.

- A set of NetBackup Operations Manager (NOM) reports were not migrated to OpsCenter 7.1.

  The following NetBackup Operations Manager (NOM) reports (and the schedules that are created for these reports) are not migrated to OpsCenter 7.1:

  - Job Summary by Status
  - Jobs Scheduled to Run
  - Media Expiration Details
  - Drive usage details
  - Window Utilization by Policy
  - Job Summary by Client for master server
  - Job Summary by Client for media server
  - Cycle Dashboard
  - Successful clients job summary for schedule type
  - Partially successful clients job summary for schedule type
  - Failed clients job summary for schedule type
  - Cycle Dashboard by Job Type
  - Cycle Dashboard by media server
  - Successful clients job summary for schedule type and media server

- Partially successful clients job summary for schedule type and media server
- Failed clients job summary for schedule type and media server
- Running versus Queued Jobs
- Rolling an eight-day summary
- Rolling an eight-day summary by media server
- Job details for client and media server
- Job details for client on the reporting day
- Jobs between Timeframe
- Running Jobs
- Queued Jobs
- Job details of selected client and server context.
- Job details of selected client and server context.
- Job details for client (From Rolling Summary)
- Week at a glance

- A set of Veritas Backup Reporter (VBR) reports were not migrated to OpsCenter 7.1.

  The following Veritas Backup Reporter (VBR) reports (and the schedules that are created for these reports) are not migrated to OpsCenter 7.1:

  - Forecast - File Count
  - Job Duration - Historical
  - Job Duration - Distribution
  - Master server Count
  - Active job Count
  - Skipped File Report
  - Drive Throughput
  - Success Rate vs. Amount backed up
  - Success Rate vs. Client Count
  - Success Rate vs. Job Count
  - Success Rate vs. File Count
  - File Factor - Historical

- File Factor - Ranking
- File Savings - Historical
- File Savings - Ranking
- Protected files vs. backed up Files
- NetBackup storage lifecycle Map
- Tape Count by Volume Pool (Bar Chart)
- Tape Count by Retention Level (Bar Chart)
- Tape Used Capacity by Retention Level

- 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 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.
- In the **Job Count Workload Analyzer**, the sum of the occurrences for each cell differs from the total that is shown in the first column when time basis that is selected is Active. That is expected because a job can be active and span across a multiple-hours time frame. Hence, the same job is counted for all the hours. But the count in the first column shows the exact count of jobs that were active for these seven days. That is different from the implementation of Time basis=**Start** or **End**. In these cases, the sum of the occurrences in the cell match with the number displayed in first column.
- When a user upgrades from NOM to OpsCenter 7.0, some reports are not migrated. That happened because OpsCenter failed to migrate these reports. As a result, when a user upgrades from OpsCenter 7.0 to 7.1, the same issue is repeated. The reason for that is because the OpsCenter application does not have its own intelligence to correct the issues that are reported when the user migrates from NOM to OpsCenter 7.0.
  These issues are not seen when a user directly upgrades from NOM to OpsCenter 7.1.
- The **Master server job throughput** report appears without a report output in **My dashboard** after a user upgrades from NOM to OpsCenter. The reason is that it is an SQL query-based report and is a part of composite report that is not migrated in the dashboard.
- Daylight savings time (DST) support for Historical reports in OpsCenter
  If data for the historical reports is synchronized during the hour when daylight savings time begins, it can cause problems in a distributed database system. The user can also lose data.

A workaround to avoid this is to use Universal Time (UTC) as time zone or to use those time zones that do not have daylight savings time.
To set the time zone, refer to the Symantec OpsCenter Administrator's Guide.

NetBackup Hyper-V

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

- Data is restored to the Hyper-V server system drive if restore path is incorrectly specified (Windows only)
  When you restore selected files by means of a shared location on the virtual machine (using the Backup, Archive, and Restore interface on Windows), an incorrectly specified UNC path (share name) for the destination should cause the restore to fail, with status code 5. Instead, the files are restored to the system drive of the Hyper-V server.
  An example of an incorrect path is:
  `\server_name\drive_name\directory_name` (path has only one leading slash)
  Correct path format would be:
  `\\server_name\drive_name\directory_name`
  The files are restored to the Windows system drive on the Hyper-V server (such as the C drive). The restore location on the system drive includes the server name and drive name as specified in the UNC path.
  This issue will be fixed in a future NetBackup release, so that NetBackup fails the restore when a path is incorrectly specified.
- Symantec has identified an issue when performing NetBackup for VMware/Hyper-V based full VM restores at the target domain when the "Duplicate to remote master" option is used. For more information and a solution, see the following tech note:
  `http://www.symantec.com/business/support/index?page=content&id=TECH150176`
  A NetBackup EEB is being developed to address this problem and should be available in the near future.

Known IPv6 limitations

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

- In IPV6-enabled NetBackup 7.1 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 "About NetBackup for VMware" on page 108.

- 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 hostname 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 7.1, 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 hostname 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 hostname that resolves to one address with REQUIRED_INTERFACE or replacing it with the PREFERRED_NETWORK equivalent in NetBackup 7.1.

- 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.

About NetBackup Snapshot Client limitations

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.

- For this release, NetBackup does not support Snapshot Client VSS off-host file backups using a Storage Foundation for Windows (SFW) VSS provider.
- 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 7.1 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.

About NetBackup for VMware

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.

- Incremental backup of a virtual machine with BLIB may fail if the virtual machine has an independent disk.

  A virtual machine incremental backup may fail (or not work correctly) in the following case:

  - The incremental backup is configured to use BLIB (the "Perform block level incremental backups" option on the policy Attributes tab)
  - The virtual machine has an independent disk.

  In this case, the backup either fails with NetBackup status code 13, or the backup succeeds but also includes unnecessary data. If the backup includes unnecessary data, files can be successfully restored from the backup.

  A NetBackup EEB to address this problem and should be available in the near future.

- An issue may occur during NetBackup for VMware/Hyper-V based, full VM restores at the target domain when the "Duplicate to remote master" option is used. For more information and a solution, see the following tech note:

  `http://www.symantec.com/business/support/index?page=content&id=TECH150176`

  A NetBackup EEB is being developed to address this problem and should be available in the near future.

- 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.

- NetBackup 7.1 contains a new feature for automatic selection of virtual machines.

  NetBackup 7.1 contains a new feature for automatic selection of virtual machines for backup. You create rules for selection of virtual machines by means of the Query Builder in the **NetBackup Policy Clients** tab. The Query builder contains several drop-down fields for creating rules.

  Note: In the Java Administration Console (on UNIX and Linux master servers), the Query Builder browse function for the Value(s) field does not return any values. As a work-around, you can use the consoles on a Windows master server or media server to configure the policy.

- The Pre-Recovery Check may not detect a missing folder in the restore location.
  If a virtual machine was in a folder when the backup occurred, that folder must exist when you restore the virtual machine to its original location. If you restore to an alternate location and use the default (original) folder for the restore, the same is true: the folder must exist in the restore location. (The Recovery Options screen has an option for selecting a different folder.)
  If the folder no longer exists, the restore fails. The NetBackup Perform Recovery screen contains a "Pre-Recovery Check" to verify restore requirements before the restore occurs. The Pre-Recovery Check, however, does not detect a missing folder.
  In a future release, the Pre-Recovery Check will be enhanced to detect a missing folder in the restore location.
- 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.

  A VMware support request has been filed for this issue, SR number 1606121431.
- Certain characters within a VM's datastore name may mean you cannot restore a backup.

  If a virtual machine's datastore name contains any of the following characters, a backup of the virtual machine cannot be restored:

  - & (ampersand)
  - < (less than)
  - > (greater than)
- VMware Tools can add a disk controller prefix to the name of each restored .vmdk file.
  During a virtual machine restore, VMware Tools can add a disk controller prefix to the name of each restored `.vmdk` file. The prefix identifies the virtual disk controller (type and number) of the virtual machine when the backup occurred. The disk controller information can be useful when you want to debug problems with the restore.
  For example, a file name of `scsi-1-acmevm9.vmdk` indicates that the virtual disk controller of virtual machine `acmevm9` was SCSI controller number 1.
  Note: To enable VMware Tools to add the prefix, the following Windows registry key is required on the VMware backup host:

HKEY_LOCAL_MACHINE\Software\VERITAS\NetBackup\CurrentVersion\Config\BACKUP\UseDiskControllerPrefix

If the **UseDiskControllerPrefix** key does not exist, you can add it to the registry.

- The restore fails if ESX servers are configured with short host names and the backup and restore are done through a vCenter server

  In the following case, the attempt to restore the virtual machine fails:

  - The ESX servers in your VMware environment are configured with short host names (not fully qualified)
  - The backup was performed through a vCenter server, not directly from the ESX server
  - And the restore is directed through a vCenter server, not directly to an ESX server

  If these are true, NetBackup cannot find the ESX server for the restore. Restore of the virtual machine fails, and the following message appears in the `bpvmUtil` log:

  `FAILED_TO_GET_MOR_BY_NAME`

  To restore virtual machines through a vCenter server in environments with short ESX server host names:

  - On the Windows desktop of the backup host, click **Start > Run** and enter `regedit`.
  - Make a backup of the current registry (**File > Export**).
  - Go to **HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > Config** and create a key called **BACKUP**.
  - Right-click in the right pane and click **New > DWORD** Value. Enter `disableFQDN` as the name.

- Virtual machine restore to an internal datastore fails if the virtual machine has thin provisioned disks or Create thin provisioned disks is selected. When you attempt to restore a VMware virtual machine, the restore job fails in the following case:

  - Either **Try san then nbd** or **Try all types** is selected as the transfer type for the restore
  - The virtual machine that you want to restore has a thin-provisioned disk or you select Create thin provisioned disks on the **Recovery Options** dialog.
  - The target datastore is on a directly attached device (not on a networked device, SAN device, or iSCSI device).

In this case, the restore job fails with NetBackup status code 2817. The Detailed Status tab contains the message, `Virtual machine restore: file write failed`.

To restore the virtual machine, select **nbd** or **nbdssl** as the transfer type on the **Recovery Options** dialog in the NetBackup Backup, Archive, and Restore interface.

VMware has identified the cause of this problem in its virtual disk Development Kit (VDDK), as SR# 1512877431.

- NetBackup does not support the metablock group feature of Linux ext file systems in the following cases:
  - For policies that are configured with the Mapped full VM backup option.
  - For policies that are configured with the Full VM Backup option and with the Exclude unused and deleted blocks option enabled.
  - For file-level recovery.
    In these cases, if the ext file system on a virtual machine volume is configured with metablock groups, the virtual machine backup fails with the following errors and logs:

```
Error:
3/2/2011 11:54:40 AM - Error bpbrm(pid=748) from client
RHEL%205.4_x86_donotdelete: ERR - Unable to create fvv_table
for mapping: status 1.

3/2/2011 11:54:45 AM - end writing; write time: 00:00:17 file
read failed(13)
3/2/2011 11:54:50 AM - Info bpbkar32(pid=0) done.
status: 13: file read failed

Event Log:
Source: VxMS Ext2fs Mapping Plugin
Error: 0x00000001, in file .\RvpExt2fsFileSystem.cpp, line 148

Recommended action: configure the policy as follows and rerun the backup:
```

  - For the Virtual machine backup option under **Snapshot Client Options**, select **Full VM backup** instead of Mapped full VM backup.
  - Under **Snapshot Client Options**, disable **Exclude unused and deleted blocks**.
    This problem will be addressed in a future release.

To verify that the ext file system on the virtual machine is configured with the metablock group feature, use the debugfs command on the virtual machine.

For example.

```
echo show_super_stats | debugfs -c /dev/sdb1 | grep Filesystem
```

where `/dev/sdb1` designates the partition that contains the ext file system.

- VMware virtual machine templates are for cloning virtual machines; they cannot be powered on and used as functioning VMs. As a result, VMware has imposed the following restrictions on NetBackup backup and restore of virtual machine templates.
  - A virtual machine template cannot be captured in a snapshot. A NetBackup backup of the template skips the snapshot portion of the job and backs up the template to the storage unit that is designated in the policy.
  - A virtual machine template cannot be backed up or restored over a SAN. You must configure the NetBackup policy to use a local network transfer type, such as nbd. Likewise, the restore of a template must be conducted over a local network.
  - Block level incremental backup (BLIB) cannot be used when backing up a virtual machine template.

  Note that the Virtual Machine Intelligent Policy feature in NetBackup 7.1 allows for automatic selection of virtual machine templates for backup. You can use the Query Builder in the **Clients** tab of the NetBackup policy to create rules for automatic selection of virtual machine templates.

Chapter 5

End-of-life notifications

This chapter includes the following topics:

NetBackup 7.1 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 of NetBackup 7.1. Therefore, Symantec recommends that you refer to the following Technote on the Symantec Support Web site to view the latest NetBackup 7.1 release information.

http://www.symantec.com/docs/DOC3412

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:

- In the next major release after 7.0, support for all of the active and the passive media server clusters that use the NetBackup clustering agents is withdrawn.
- Starting with the next major release of NetBackup, the NetBackup-Java Administration Console is no longer ed.
- 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.
- At the next major release of NetBackup, the NetWare client is no longer compatible.

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

- NetBackup 7.1 no longer supports OpenAFS.
- OpsCenter 7.1 does not support Internet Explorer 6.x.

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 table lists the operating systems that may not be supported in the next major release of NetBackup. For the most recent list of supported platform information, download the NetBackup operating system compatibility List from the Support Web site with the following URL.

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

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.

Operating system	CPU Architecture	Comment
AIX 5.3	POWER	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
FreeBSD 6.x	X86-32	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
FreeBSD 6.x	X86-64	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
HP-UX 11.11	PA-RISC	The operating system on this CPU Architecture is no longer supported as a master or media server at the next major release. This platform will only be supported as a client.
HP-UX 11.23	PA-RISC	The operating system on this CPU Architecture is no longer supported as a master or media server at the next major release. This platform will only be supported as a client.

Operating system	CPU Architecture	Comment
HP-UX 11.31	PA-RISC	The operating system on this CPU Architecture is no longer supported as a master or media server at the next major release. This platform will only be supported as a client.
Red Hat Enterprise Linux 4.0	X86-64	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture.
Red Hat Enterprise Linux 4.0	IA64	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
Red Hat Enterprise Linux 4.0	POWER	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
Red Hat Enterprise Linux 5.0	POWER	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
Red Hat Enterprise Linux 4.0	z/Architecture	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, support for this operating system can change if the market position or vendor support position changes.
SUSE Linux Enterprise Server 10.0	X86-64	Support for this operating system can change if the market position or vendor support position changes.
SUSE Linux Enterprise Server 9.0	IA64	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
SUSE Linux Enterprise Server 9.0	POWER	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
SUSE Linux Enterprise Server 10.0	POWER	The operating system on this CPU Architecture is not supported at the next major release. However, support for this operating system can change if the market position or vendor support position changes.
SUSE Linux Enterprise Server 9.0	z/Architecture	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, support for this operating system can change if the market position or vendor support position changes.

Operating system	CPU Architecture	Comment
Mac OS X 10.5	POWER PC	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, support for this operating system can change if the market position or vendor support position changes.
Mac OS X 10.5	X86-32	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, support for this operating system can change if the market position or vendor support position changes.
Mac OS X 10.5	X86-64	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, support for this operating system can change if the market position or vendor support position changes.
Windows Server 2003 R2	IA64	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, NetBackup 7.0 and 7.1 will support this operating system , CPU Architecture, and associated components through the life of Windows Server 2008.
Windows Server 2003 SPI	IA64	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, NetBackup 7.0 and 7.1 will support this operating system , CPU Architecture, and associated components through the life of Windows Server 2008.
Windows Server 2008	IA64	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, NetBackup 7.0 and 7.1 will support this operating system , CPU Architecture, and associated components through the life of Windows Server 2008.
Windows Server 2008 R2	IA64	The next release that follows NetBackup 7.1 does not support this operating system on this CPU Architecture. However, NetBackup 7.0 and 7.1 will support this operating system , CPU Architecture, and associated components through the life of Windows Server 2008.

Chapter 6

Related Documents

This chapter includes the following topics:

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 for UNIX, Linux, and Windows*
  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 for UNIX, Linux, and Windows*
  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).
- *Symantec NetBackup Security and Encryption Guide for UNIX, Windows, and Linux*
  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 administrator's guides - agents and options

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

- *Symantec NetBackup Deduplication Guide*
  NetBackup_Dedupe_Guide.pdf
  Explains how to configure and use NetBackup media server deduplication and NetBackup client deduplication.
- *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 Shared Storage Guide*
  NetBackup_SharedStorage_Guide.pdf
  Explains how to configure and use shared storage in NetBackup. Shared storage includes AdvancedDisk, OpenStorage, and the Shared Storage Option.
- *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.
- *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 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 Snapshot Client Quick Start Guide*
  NetBackup_QuickStart_SnapshotClient.pdf
  Provides the first-time instructions for installing and configuring the Snapshot Client.
- *Symantec NetBackup for Hyper-V Guide for UNIX, Windows, and Linux*
  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 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 DB2 Administrator's Guide for UNIX*
  NetBackup_AdminGuide_DB2_Unix.pdf
  Explains how to install, configure, and use NetBackup for DB2.
- *Symantec NetBackup for DB2 Administrator's Guide for Windows*
  NetBackup_AdminGuide_DB2_Win.pdf
  Explains how to install, configure, and use NetBackup for DB2.
- *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_Win.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 Windows client.
- *Symantec NetBackup for Lotus Notes Administrator's Guide for UNIX*
  NetBackup_AdminGuide_LotusNotes_Unix.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 UNIX 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 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.

- *NetBackup for Oracle for UNIX, Windows, and Linux 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 for UNIX*
  NetBackup_AdminGuide_SAP_Unix.pdf
  Explains how to install, configure, and use NetBackup for SAP on UNIX.
- *Symantec NetBackup for SAP Administrator's Guide for Windows*
  NetBackup_AdminGuide_SAP_Win.pdf
  Explains how to install, configure, and use NetBackup for SAP on Windows-based servers.
- *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.
- *Symantec NetBackup for SYBASE Administrator's Guide for UNIX*
  NetBackup_AdminGuide_Sybase_Unix.pdf
  Explains how to install, configure, and use NetBackup for Sybase to back up and restore Sybase databases that are on a UNIX NetBackup client.
- *Symantec NetBackup for SYBASE Administrator's Guide on Windows*
  NetBackup_AdminGuide_Sybase_Win.pdf
  Explains how to install, configure, and use NetBackup for Sybase to back up and restore Sybase databases that are on a Windows NetBackup client.
- *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 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 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 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 NetBackup NetWare Media Server Option Administrator's Guide for UNIX and Windows*
  NetBackup_AdminGuide_NetWareServer.pdf
  This comprehensive manual provides detailed information and procedures for installing, configuring, and using the Symantec NetBackup NetWare Media Server Option.

About user's guides

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

- *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 Administrator's Guide for Novell NetWare Client*
  NetBackup_AdminGuide_NetWare_Client.pdf
  Explains how to install and use the NetBackup's NetWare Client software. With the NetWare Client, full and incremental backups can be scheduled to occur automatically and unattended under the control of the NetBackup master server. The NetWare Client also provides two methods for performing user-directed backups and restores: Target, which uses a character-based, menu-driven interface running on the NetWare server, and NonTarget, which uses the NetBackup for NetWare NonTarget Browser that is installed and run from a Windows computer.

About the device configuration guide

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

- *Symantec NetBackup Device Configuration Guide*
  NetBackup_DeviceConfig_Guide.pdf

Explains how to add device drivers and perform other system-level configurations for the operating systems of NetBackup servers that host storage devices. Also includes information about configuring several types of tape libraries.

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.

About NetBackup command documents

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

- *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.

Appendix A

Windows Logo Certification information

This appendix includes the following topics:

About Windows Server 2008 R2 Logo Certification

This topic contains information about Windows Server 2008 R2 Logo Certification and how it applies to NetBackup. The tables contain the following types of information:

- Files that have invalid file version information (Company, Product Name, and Product Version)
  See Table A-1 for a list of these files.
- Third-party files and tools that do not include or create requested ExecutionLevel tags
  See Table A-2 for a list of these files and tools.
- Files that NetBackup uses that are not signed
  See Table A-3 for a list of these files.
- Files that remain after an uninstall
  The NetBackup uninstall may leave files behind that other Symantec applications use. NetBackup 7.1 uses Veritas Authentication (VxAT) as a common security infrastructure component that can be shared between Symantec applications on the same host. For example, Veritas Storage Foundation (VxFS) and NetBackup can reside on the same host.
  If you uninstall NetBackup from a Windows Server 2008 R2 host and remove the VxAT files in the common directory, then the remaining application ceases

to function. However, the following files remain in the Security folder (C:\Program Files\Veritas\Security\...) after the uninstall completes. See Table A-4 for a list of files that remain after an uninstall has occurred.

Table A-1 NetBackup installs the following files that do not have valid file version information

Third-party file locations	File names
Third-party files located in Program Files\Veritas\NetBackup\bin	pxhpinst.exe
	pxsetup.exe
	vxblock.dll
Third-party files located in of Program Files\Common Files\VERITAS\VxMS\shared\VDDK	diskLibPlugin.dll
	gvmomi.dll
	libcurl.dll
	libeay32.dll
	liblber.dll
	libldap.dll
	libldap_r.dll
	libxml2.dll
	ssleay32.dll
	types.dll
	zlib1.dll
Third-party files located in any of the following paths: ■ Program Files\Veritas\pdde ■ Program Files\Veritas\pdde\pddb\bin ■ Program Files\Veritas\pdde\pddb\lib	_int.dll
	adminpack.dll
	ascii_and_mic.dll

Table A-1 NetBackup installs the following files that do not have valid file version information *(continued)*

Third-party file locations	File names
	autoinc.dll
	btree_gist.dll
	chkpass.dll
	cube.dll
	cyrillic_and_mic.dll
	dblink.dll
	dict_int.dll
	dict_snowball.dll
	dict_xsyn.dll
	earthdistance.dll
	euc_cn_and_mic.dll
	euc_jis_2004_and_shift_jis_2004.dll
	euc_jp_and_sjis.dll
	euc_kr_and_mic.dll
	euc_tw_and_big5.dll
	fuzzystrmatch.dll
	hstore.dll
	insert_username.dll
	int_aggregate.dll
	isn.dll
	latin_and_mic.dll
	latin2_and_win1250.dll
	libecpg.dll
	libecpg_compat.dll

Table A-1 NetBackup installs the following files that do not have valid file version information *(continued)*

Third-party file locations	File names
	libpgtypes.dll
	libpq.dll
	libxml2.dll
	libxslt.dll
	lo.dll
	ltree.dll
	moddatetime.dll
	oid2name.exe
	pageinspect.dll
	pg_buffercache.dll
	pg_freespacemap.dll
	pg_regress.exe
	pg_regress_ecpg.exe
	pg_standby.exe
	pg_trgm.dll
	pgbench.exe
	pgcrypto.dll
	pgrowlocks.dll
	pgstattuple.dll
	pgxml.dll
	plperl.dll
	plpgsql.dll
	plpython.dll
	pltcl.dll

Table A-1 NetBackup installs the following files that do not have valid file version information *(continued)*

Third-party file locations	File names
	refint.dll
	regress.dll
	seg.dll
	sslinfo.dll
	tablefunc.dll
	test_parser.dll
	timetravel.dll
	tsearch2.dll
	utf8_and_ascii.dll
	utf8_and_big5.dll
	utf8_and_cyrillic.dll
	utf8_and_euc_cn.dll
	utf8_and_euc_jis_2004.dll
	utf8_and_euc_jp.dll
	utf8_and_euc_kr.dll
	utf8_and_euc_tw.dll
	utf8_and_gb18030.dll
	utf8_and_gbk.dll
	utf8_and_iso8859.dll
	utf8_and_iso8859_1.dll
	utf8_and_johab.dll
	utf8_and_shift_jis_2004.dll
	utf8_and_sjis.dll
	utf8_and_uhc.dll

Table A-1 NetBackup installs the following files that do not have valid file version information *(continued)*

Third-party file locations	File names
	utf8_and_win.dll
	uuid-ossp.dll
	vacuumlo.exe
	vacuumlo.exe
	zlib1.dll

Table A-2 NetBackup uses the following third-party files and tools that do not include or create requested ExecutionLevel tags

Third-party file locations	File names
Third-party files located in Program Files\Veritas\NetBackupDB\java	java.exe
	javaw.exe
	keytool.exe
	policytool.exe
	rmid.exe
	rmiregistry.exe
	tnameserv.exe
Third-party files located in Program Files\Veritas\NetBackup\bin	pxhpinst.exe
	pxsetup.exe
	uconv.exe
Third-party files located in any of the following paths: ■ Program Files\Veritas\pdde ■ Program Files\Veritas\pdde\pddb\bin ■ Program Files\Veritas\pdde\pddb\lib	clusterdb.exe
	createdb.exe

Table A-2 NetBackup uses the following third-party files and tools that do not include or create requested ExecutionLevel tags *(continued)*

Third-party file locations	File names
	createlang.exe
	createuser.exe
	createuser.exe
	dropdb.exe
	droplang.exe
	dropuser.exe
	ecpg.exe
	initdb.exe
	oid2name.exe
	pg_config.exe
	pg_controldata.exe
	pg_ctl.exe
	pg_dump.exe
	pg_dumpall.exe
	pg_regress.exe
	pg_regress_ecpg.exe
	pg_resetxlog.exe
	pg_restore.exe
	pg_standby.exe
	pgbench.exe
	postgres.exe
	psql.exe
	reindexdb.exe
	vacuumdb.exe

Table A-2 NetBackup uses the following third-party files and tools that do not include or create requested ExecutionLevel tags *(continued)*

Third-party file locations	File names
	`vacuumlo.exe`
	`zic.exe`

Table A-3 NetBackup uses and installs the following files that are not signed.

Third-party file locations	File names
Third-party files located in `Program Files\Veritas\NetBackupDB\java`	`awt.dll`
	`cmm.dll`
	`dcpr.dll`
	`dt_socket.dll`
	`fontmanager.dll`
	`hpi.dll`
	`hprof.dll`
	`ioser12.dll`
	`java.dll`
	`java.exe`
	`javaw.exe`
	`jawt.dll`
	`JdbcOdbc.dll`
	`jdwp.dll`
	`jpeg.dll`
	`jsound.dll`
	`keytool.exe`
	`net.dll`
	`policytool.exe`

Table A-3 NetBackup uses and installs the following files that are not signed. *(continued)*

Third-party file locations	File names
	rmid.exe
	rmiregistry.exe
	tnameserv.exe
	verify.dll
	zip.dll
The following Microsoft runtime libraries	mfc*.dll
	msvc*.dll
Third-party files located in Program Files\Veritas\NetBackup\bin\x86	PrimoSDK.dll
	px.dll
	pxdrv.dll
	pxhpinst.exe
	pxmas.dll
	pxsetup.exe
	pxwave.dll
	vxblock.dll
Third-party files located in Program Files\Veritas\NetBackup\bin	diskLibPlugin.dll
	glib-2.0.dll
	gobject-2.0.dll
	gthread-2.0.dll
	gvmomi.dll
	iconv.dll
	intl.dll

Table A-3 NetBackup uses and installs the following files that are not signed. *(continued)*

Third-party file locations	File names
	libcurl.dll
	libeay32.dll
	liblber.dll
	libldap.dll
	libldap_r.dll
	libxml2.dll
	ssleay32.dll
	types.dll
	vixDiskLib.dll
	vixDiskLibVim.dll
	vixMntapi.dll
	vmacore.dll
	vmomi.dll
	zlib1.dll
Third-party files located in any of the following paths: ■ Program Files\Veritas\pdde ■ Program Files\Veritas\pdde\pddb\bin ■ Program Files\Veritas\pdde\pddb\lib	_int.dll
	adminpack.dll
	ascii_and_mic.dll
	autoinc.dll
	btree_gist.dll
	chkpass.dll
	clusterdb.exe
	comerr32.dll

Table A-3 NetBackup uses and installs the following files that are not signed. *(continued)*

Third-party file locations	File names
	createdb.exe
	createlang.exe
	createuser.exe
	createuser.exe
	cube.dll
	cyrillic_and_mic.dll
	dblink.dll
	dict_int.dll
	dict_snowball.dll
	dict_xsyn.dll
	dropdb.exeS
	droplang.exe
	dropuser.exe
	earthdistance.dll
	ecpg.exe
	euc_cn_and_mic.dll
	euc_jis_2004_and_shift_jis_2004.dll
	euc_jp_and_sjis.dll
	euc_kr_and_mic.dll
	euc_tw_and_big5.dll
	fuzzystrmatch.dll
	gssapi32.dll
	hstore.dll
	iconv.dll

Table A-3 NetBackup uses and installs the following files that are not signed. *(continued)*

Third-party file locations	File names
	initdb.exe
	insert_username.dll
	int_aggregate.dll
	isn.dll
	k5sprt32.dll
	krb5_32.dll
	latin_and_mic.dll
	latin2_and_win1250.dll
	libeay32.dll
	libecpg.dll
	libecpg_compat.dll
	libiconv-2.dll
	libintl-8.dll
	libpgtypes.dll
	libpq.dll
	libxml2.dll
	libxslt.dll
	lo.dll
	ltree.dll
	moddatetime.dll
	oid2name.exe
	pageinspect.dll
	pg_buffercache.dll
	pg_config.exe

Table A-3 NetBackup uses and installs the following files that are not signed. *(continued)*

Third-party file locations	File names
	pg_controldata.exe
	pg_ctl.exe
	pg_dump.exe
	pg_dumpall.exe
	pg_freespacemap.dll
	pg_regress.exe
	pg_regress_ecpg.exe
	pg_resetxlog.exe
	pg_restore.exe
	pg_standby.exe
	pg_trgm.dll
	pgbench.exe
	pgcrypto.dll
	pgevent.dll
	pgrowlocks.dll
	pgstattuple.dll
	pgxml.dll
	plperl.dll
	plpgsql.dll
	plpython.dll
	pltcl.dll
	postgres.exe
	psql.exe
	refint.dll

Table A-3 NetBackup uses and installs the following files that are not signed. *(continued)*

Third-party file locations	File names
	regress.dll
	reindexdb.exe
	seg.dll
	ssleay32.dll
	sslinfo.dll
	tablefunc.dll
	test_parser.dll
	timetravel.dll
	tsearch2.dll
	utf8_and_ascii.dll
	utf8_and_big5.dll
	utf8_and_cyrillic.dll
	utf8_and_euc_cn.dll
	utf8_and_euc_jis_2004.dll
	utf8_and_euc_jp.dll
	utf8_and_euc_kr.dll
	utf8_and_euc_tw.dll
	utf8_and_gb18030.dll
	utf8_and_gbk.dll
	utf8_and_iso8859.dll
	utf8_and_iso8859_1.dll
	utf8_and_johab.dll
	utf8_and_shift_jis_2004.dll
	utf8_and_sjis.dll

Table A-3 NetBackup uses and installs the following files that are not signed. *(continued)*

Third-party file locations	File names
	utf8_and_uhc.dll
	utf8_and_win.dll
	uuid-ossp.dll
	vacuumdb.exe
	vacuumlo.exe
	zic.exe
	zlib1.dll

Table A-4 Files that remain after NetBackup is uninstalled

File locations	Files
C:\Program Files\Veritas\Security\	Authentication
C:\Program Files\Veritas\Security\systemprofile\	SessionStore.lock
	VRTSatlocal.conf
	CRTSatlocal.conf.lock
C:\Program Files\Veritas\Security\systemprofile\certstore\	CertStore.lock
C:\Program Files\Veritas\Security\systemprofile\certstore\keystore\	KeyStore.lock
	SessionEncrKey.pem
	SessionHMACKey.pem
C:\Program Files\Veritas\Security\systemprofile\sessions\	default.db
	log.0000000001
	sdefault.db
	__db.001

Table A-4 Files that remain after NetBackup is uninstalled *(continued)*

File locations	Files
	__db.002
	__db.003
	__db.004
	__db.005
	__db.006
	__db.register
C:\Program Files\Veritas\Security\systemprofile\systruststore\	CertStore.lock