

Symantec NetBackup™ Release Notes

Release 7.7

Document Version 2



Documentation version: 7.7

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

About Symantec Operations Readiness Tools

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

Access SORT from the following webpage:

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

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

- Installation and Upgrade Checklist
Use this tool to create a checklist to see if your system is ready for a NetBackup installation or an upgrade. This report contains all the software and the hardware

compatibility information specific to the information provided. The report also includes product installation or upgrade instructions, as well as links to other references.

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

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

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Technical Support	3
Chapter 1	About NetBackup 7.7 18
	About the NetBackup 7.7 release 18
	About NetBackup Late Breaking News 19
	About NetBackup third-party legal notices 19
Chapter 2	New features, enhancements, and changes 21
	About new enhancements and changes in NetBackup 21
	NetBackup 7.7 new features and enhancements 22
	General support enhancements 22
	User interface enhancements 25
	Logging enhancements 29
	NetBackup security and encryption 30
	NetBackup for NDMP 31
	NetBackup for Replication Director 31
	NetBackup Search 31
	NetBackup for SQL Server 32
	NetBackup virtualization 33
	NetBackup language packs 34
Chapter 3	Operational notes 38
	About NetBackup 7.7 operational notes 39
	NetBackup installation and upgrade operational notes 39
	No appliance upgrade path to NetBackup 7.7 until Appliance 2.7.1 patch is released 39
	Do not install from the menu that appears when the installation DVD is inserted 40
	Cannot install server software to root environment of separate host that is mounted on Solaris system 40
	After upgrading to 7.6, changes to Object IDs in nblog.conf are not preserved 40

After upgrade to 7.x, interface entry may change for configurations that previously listed an IP address as REQUIRED_INTERFACE	40
About support for HP-UX Itanium vPars SRP containers	41
Extra steps are required to perform NetBackup 7.6 client push installations from an HP PA-RISC media server	41
A successful install may return an unsuccessful exit status (non-zero) for an upgrade of a pre- 7.0 NetBackup client to version 7.6	42
A Java error can occur on AIX 7.1	42
Character restrictions for database server name	43
Uninstalling NetBackup from FreeBSD	43
Considerations for Oracle backup policies when upgrading from NetBackup 7.1 and earlier	43
NetBackup administration and general operational notes	43
NetBackup supports two optimized duplication methods for OpenStorage	44
Export file shows incorrect properties while exporting properties of multiple hosts with different versions	45
Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms	45
NetBackup Management > Catalog search results display a single image even if there is more than one image present on the system	46
Java Windows Administration console throws status code 521 on Windows Vista/Server 2008 and later	46
Radio buttons may render incorrectly in the NetBackup Administration Console when using Remote Desktop Connection (RDC) on Mac OS X	47
NetBackup limitations when using IPv6 address as client name or image name	47
IPv6 link-local addresses not supported in NetBackup	47
Intermittent issues with X forwarding of NetBackup Java Administration Console	47
Image extension files remain in catalog when using NetBackup Administration Console to expire NetBackup images	48
Reduced functionality during the initialization of the NetBackup-Java Administration Console	48
Memory requirements to run the NetBackup Administration Console	48
Remote display of the NetBackup-Java Administration Console in multi-byte locale environments is not supported	48

Performance issues may occur with NetBackup 7.x master servers on UltraSPARC T-series or SPARC T3 architecture	49
A multistream backup may fail if DFSR is active on the client	49
The backup script path field is not active for an automatic backup schedule	49
Migration to a simplified client name for Windows clients	49
The swapfile.sys file needs to be manually excluded from Windows 8 client backups	50
A newly-added NetBackup appliance media server may get added to the EMM database as a master server	50
Restore may fail for the clients that have both WAN Resiliency and client direct deduplication enabled	50
Issues with SUSE 11 running on kernel versions later than 2.6	51
Certain file names in the Windows system drive root directory prevent NetBackup from functioning properly	51
Time differences between NetBackup hosts causes display issues in the Activity Monitor	51
NetBackup administration interface operational notes	51
Information at the Activity Monitor may not appear in the correct order	52
Logs are deleted even though the Keep logs up to GB option is enabled	52
Java Administration Console may encounter a core dump issue when the Simplified Chinese UTF-8 locale is used on a Solaris SPARC 64-bit system with Solaris 10 Update 2 or later	52
NetBackup Java user interface may fail to start in HP-UX 11.31 environments	53
NetBackup Accelerator operational notes	53
Accelerator version requirements for master, media, client, and media servers	53
Accelerator and Replication Director support for virtualized servers cannot be configured together	53
Accelerator does not support the VxFS File Change Log	53
The bpverify operation can fail with status code 191 for certain NetBackup Accelerator images	54
Accelerator backups for VMware intermittently fail with an incorrect checksum error	54
Accelerator policy creation can fail because it does not recognize a valid storage unit group	54
NetBackup auditing operational notes	55
Two restore audit records are created in a catalog restore instead of three	55

The command line interface may show unrecognizable characters for the backup selection output	55
Action with parent jobs does not generate audit records for children	55
NetBackup Bare Metal Restore operational notes	55
A new BMR user prompt has been added to choose between multiple kernel levels	56
NetBackup 7.6.0.2 clients on Windows x86-32 cannot be used as Virtual Instance Converters	56
Legacy Restore is not supported on Windows 8/Server 2012 and later	56
Other file systems on ZFS volumes are not supported	56
BMR does not support restoring the Remote Installation Folder location of an RIS Server	57
NetBackup BMR can only restore IPv6 information using an IPv4 network connection	57
Inconsequential message may appear during BMR recovery of an RHEL client that has RAID1 volumes	57
An extra step is required after restoring a Windows client with EFI boot system	57
If the boot server has a base installation of Solaris 10 update 11, the creation of SRTs can fail	57
A devfsadm error may occur on Solaris 11 and newer	58
Many services on Solaris 11 print warning messages during a system boot and during BMR first boot	58
Solaris Zone recovery on Solaris 11 and newer takes time to reconfigure after a BMR restore during first boot	59
A Solaris BMR restore operation fails if the text-installer package is not present in the customized AI ISO	59
The OS takes time for configuration after a client to virtual machine conversion	59
BMR restores of encrypted file systems on RHEL are restored without encryption	59
When the /etc/mke2fs.conf file is restored, the restore task is shown as partially completed in the Activity Monitor	60
ZFS temporary mount can fail during a BMR restore	60
Issues may occur after a BMR restore is performed on RHEL 6	60
BMR fails to create a media SRT when a Basic Server installation is performed on an RHEL system	60
The system relabels all of the file systems after a BMR restore during the first startup	61

The /boot partition must be on a separate partition for a multiple device-based OS configuration	61
Multiple error messages might be displayed during the first boot after the restoration of a client with ZFS storage pools	61
BMR may not format or clear the ZFS metadata	62
Coexistence of two BMR-supported multi-path solutions can cause issues	62
A BMR restore may fail during a Linux DDR scenario between internal disk and SAN disk	63
BMR backups may fail on Citrix XenCenter virtualization due to disk naming	63
A NetBackup system state backup can fail on certain Windows Server 2008 R2 systems with SFW	63
Specifying the short name of the client to protect with Auto Image Replication and BMR	64
A restore task may remain in a finalized state in the disaster recovery domain even after the client restores successfully	64
Patch required to create an SRT on HP-UX 11.31 IA64	65
IPv6 support for BMR	65
A failure may occur during a VxFS7-based file creation	65
Automatic boot may fail for HP-UX after a restore	66
Prepare to Restore may not work for a Solaris client	66
An issue can occur when you use bmrsetupmaster in the CLI to configure a BMR master server on AIX	66
The first boot after a successful restore may fail on a Linux client if the disk order in the BIOS is not correct	67
Restoring back-level clients	68
The non-critical or non-system ZFS storage pool of an original client may become unavailable	68
The spare devices and cache devices under the ZFS root pool may become unavailable	68
Mount failure of ZFS file systems	68
A BMR restore of a Solaris client may fail if the client has a ZFS root pool containing alternate boot environments	68
NetBackup Cloud operational notes	69
Verizon cloud storage servers do not support buckets created in NetBackup	69
Synthetic (TIR) backups fail with status code 87 in Hitachi cloud configurations with encryption enabled	69
Master server installation on platforms not supported by NetBackup Cloud may result in cloud storage server configuration issues	69

Network connection issues may occur when the Rackspace plug-in is used on a host running Windows Server 2008 R2 with IPv6 enabled	70
NetBackup cluster operational notes	70
A virtual name cannot resolve to both IPv4 and IPv6 addresses in clustered environments	71
NetBackup cluster installation notes	71
NetBackup database and application agent operational notes	73
NetBackup for DB2 operational notes	73
NetBackup for Exchange and NetBackup for SharePoint operational notes	73
NetBackup for Microsoft Active Directory operational notes	75
SQL Server restore fails when you restore a SQL Server compressed backup image as a single stripe or with multiple stripes	76
NetBackup deduplication operational notes	77
New versions of NetBackup may significantly modify MSDP deduplication database	77
Internationalization and localization operational notes	77
Certain NetBackup user-defined strings must not contain non-US ASCII characters	77
Restricted support for localized environments in database and application agents for all supported platforms	78
Do not run language packs that are not at the same version level as the English version	78
NetBackup LiveUpdate operational notes	79
LiveUpdate is not compatible with OpenVMS (UNIX) or Novell operating systems	79
Attempts to use LiveUpdate to install or upgrade to NetBackup 7.7 can fail because the target host has an incompatible version of Java JRE installed	79
The push and silent installation methods do not install the LiveUpdate agent as part of the package	79
Error during upgrade of an HP PA-RISC client to NetBackup 7.6 using LiveUpdate	80
NetBackup Logging Assistant operational notes	81
Modifying logging levels in the NetBackup Administration Console can change the global logging level and VxUL debug levels	81
NetBackup for NDMP operational notes	81
NDMP multiplexed (MPX) restores may generate excessive log messages and cause Activity Monitor to hang	81

Parent directories in the path of a file may not be present in an NDMP incremental image	82
NetBackup OpsCenter operational notes	82
OpsCenter no longer supports NetBackup 6.x	82
database.conf overwritten by non-default installation location	82
NetBackup OpsCenter branding and name changes in NetBackup 7.6	83
NetBackup 7.6 Support Changes	83
Unable to set different alert.conf water mark thresholds	83
Language packs cause OpsCenter upgrade from 7.1 or 7.5 to 7.6 to fail	83
Incomplete uninstall of maintenance releases	84
Report export location determined by web browser	84
Ampersand prevents user from being edited	84
Add and monitor NetBackup 2.6 appliances	84
Accessing OpsCenter console using Internet Explorer	84
Unable to log in to OpsCenter on UNIX system if Korn shell is not installed	85
Cloud metering data collection failure due to unreachable server	85
Nodes with attached objects in View Builder temporarily disappear when moved	85
Data collection fails if storage unit path is more than 256 characters	85
Blank report when only Include Accelerator Job Only is selected	86
Browse functionality is not supported on IE8	86
Browse and Select client functionality displays NetApp volume as client name for Replication Director VM backups	86
Cannot collect data from unsupported EV, TSM, or EMC servers	86
database.conf should contain only database location string	87
Report emails fail to deliver if attachments are too large	87
Cannot assign alerts to new users until they log on	87
New users not visible in Copy User Profile	87
Backup Exec data collection fails if server password contains HTML characters	87
OpsCenter Monitor File List tab shows empty for active jobs	88
Special characters in subgroup name prevent users from being authorized	88
Undefined JAVA_HOME or JRE_HOME variables after you run a third-party utility	88

Duplicate entries in Monitor and Views interfaces	89
Alert email for each volume if OpenStorage alert policy is configured	89
Job collection fails on master server if port 1556 is not open bi-directionally	90
Support for 64-bit software on Windows	90
Running Capacity Licensing reports	90
Data format in SFR Timeline shown as "unknown"	90
OpsCenter does not support creating or editing multiple reports simultaneously for the same user session from different tabs or windows	90
Deduplication reports show no data when Report On is set as Storage unit Name	91
Search and Restore operations in VMware and Hyper-V	91
OpsCenter installation and deployment information and best practices	91
File selection lists with more than 50 items do not appear in OpsCenter	91
OpsCenter does not provide the option to purge breakup jobs	92
Canceled or interrupted uninstall removes uninstall script	92
Some result sets for a stored procedure that has multiple result sets may not appear	92
Character limitation for virtual host names on Windows	92
Some reports may only consider Full and Incremental schedule type jobs	92
NetBackup OpsCenter must be brought online manually	93
Missing log.conf file on Windows systems	93
OpsCenter object merger utility fails on master server	93
Custom Tabular Backup and Custom-Client count report returns no data	94
OpsCenter server stops receiving events from master server after NetBackup upgrade	94
Users can now search for clients from the Monitor>Hosts>Clients page (but not by attribute)	95
Job Count Workload Analyzer summation rules	95
Upgrading from NOM to OpsCenter causes Master server job throughput report to appear without an output	95
Daylight Savings Time support for historical reports in OpsCenter	95
When you upgrade from OpsCenter 7.0.x to 7.x, the Installation Choice screen displays available space on system drive	96

OpsCenter cannot monitor IPv6-only servers	96
OpsCenter interface returns non-specific error after it fails to connect to a master server	96
The NetBackup Disk Pool Size vs. Percentage Full report may show incorrect data	97
OpsCenter reports display IP addresses for some VMs	97
OpsCenter displays incorrect OS level for Windows Server 2012 R2	97
Issues accessing an OpsCenter Server from the remote OpsCenter View Builder on a Windows computer	97
NetBackup OpsCenter no longer supports Search & Hold	98
Dropped support for Solaris and UNIX clusters	98
NetBackup Replication Director operational notes	98
Replications fail after point-in-time restore with NBUPugin 1.1	99
NBUPugin 1.1 replication fails with error code 84	99
Database system error when browsing files in "Backup, Archive, and Restore" interface	100
Indexing logs grow very large when log level set to 4 or higher	100
Discovery fails on VMs running vCenter 2.5 or ESX 3.5 and older	100
Hardware snapshot generated on boot disk even when "Virtual disk selection" is set to "Exclude boot disk"	100
Backup in SLP using NetBackup Accelerator fails with status code 13 if storage read speed is very slow	100
Instance group names cannot be localized for Oracle Intelligent Policy	101
Volume GUID not supported for VSS	101
Activity Monitor may show wrong Kilobytes value for snapshot jobs if policy has alternate client configuration	101
Snapshot of NFS mount fails with status code 20 on Linux	101
Test Query option in Query Builder may incorrectly display VMs which will not be selected for backup job	101
NetApp Plug-in for NetBackup 1.0.1 crashes under certain circumstances	102
Replication may fail on NetApp Plug-in for NetBackup 1.0.1 under certain conditions	102
Snapshot leaks when cleaning up all images for policies with Primary > Mirror topologies	103
Incremental backups created with Replication Director may throw error: "unable to obtain list of files using specified search criteria"	103

If VM and its datastore have identical names, the Backup, Archive, and Restore client interface displays two separate images	103
BAR interface accesses files directly from snapshot if storage lifecycle policy is not configured to index VM (or if indexing does not complete)	104
Backups and restores from snapshots on RHEL 5.3 operating systems do not work properly due to lack of support from NetBackup 7.6	104
Restoring from a differential incremental backup at the volume level can result in data loss	104
SnapVault replication may result in data loss if the qtree has not been updated in the DFM server	105
Replication Director policy validation takes a long time to complete	105
Resilient network operational notes	106
NetBackup Search operational notes	106
NetBackup Search functionality not supported in 7.7 and later	106
NetBackup Snapshot Client operational notes	106
Logs for legacy processes are less verbose than in previous releases	107
FlashBackup is not supported with Storage Foundation 6 or greater volume manager	107
A Standard policy that is configured with certain selections causes the Policy Execution Manager to crash and generate a core dump with an assertion failure	107
Cannot create a disk array snapshot if a VxVM disk group on the array contains a software-based snapshot of the VxVM volume	107
Multi-stream policy backups fail due to missing files	108
NetBackup virtualization operational notes	108
NetBackup for VMware operational notes	108
NetBackup for Hyper-V operational notes	114
NetBackup Add-in for Microsoft System Center Virtual Machine Manager (SCVMM) Console operational notes	114
Appendix A About SORT for NetBackup Users	117
About Symantec Operations Readiness Tools	117
Recommended SORT procedures for new installations	118
Recommended SORT procedures for upgrades	122

Appendix B	NetBackup installation requirements	124
	About NetBackup installation requirements	124
	Required operating system patches and updates for NetBackup	125
	NetBackup 7.7 binary sizes	129
Appendix C	NetBackup compatibility requirements	132
	About NetBackup release types and versioning	132
	About compatibility between NetBackup versions	133
	About Auto Image Replication compatibility	136
	About NetBackup compatibility lists and information	136
	About NetBackup end-of-life notifications	138
Appendix D	Other NetBackup documentation and related documents	140
	About related NetBackup documents	140
	About NetBackup release notes documents	141
	About NetBackup administration documents	141
	About administration of NetBackup options	142
	About administration of NetBackup database agents	144
	About NetBackup installation documents	145
	About NetBackup configuration documents	145
	About NetBackup troubleshooting documents	146
	About other NetBackup documents	146

About NetBackup 7.7

This chapter includes the following topics:

- [About the NetBackup 7.7 release](#)
- [About NetBackup Late Breaking News](#)
- [About NetBackup third-party legal notices](#)

About the NetBackup 7.7 release

Symantec is pleased to announce the release of NetBackup 7.7. This release introduces significant features, enhancements, and performance improvements to NetBackup and its associated options. These new features and enhancements improve and expand NetBackup's capability to protect mission-critical data and applications in physical and virtualized environments.

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

See [“About new enhancements and changes in NetBackup”](#) on page 21.

About EEBs and release content

NetBackup 7.7 incorporates fixes to many of the known issues that affected customers in previous versions of NetBackup. Some of these fixes are associated with the customer-specific issues that have been documented in the form of Titan or Salesforce.com (SFDC) cases. Several of the customer-related fixes that were incorporated into this release were also made available as emergency engineering binaries (EEBs).

Listings of the EEBs and Etracks that document the known issues that have been fixed in NetBackup 7.7 can be found on the Symantec Operations Readiness Tools (SORT) website and in the [NetBackup Emergency Engineering Binary Guide](#).

See “[About Symantec Operations Readiness Tools](#)” on page 117.

About NetBackup appliance releases

The NetBackup appliances run a software package that includes a preconfigured version of NetBackup. When a new appliance software release is developed, the latest version of NetBackup is used as a basis on which the appliance code is built. For example, NetBackup Appliance 2.6 is based on NetBackup 7.6. This development model ensures that all applicable features, enhancements, and fixes that were released within NetBackup are included in the latest release of the appliance.

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

Appliance-specific documentation is available at the following location:

<http://www.symantec.com/docs/DOC2792>

About NetBackup Late Breaking News

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

<http://www.symantec.com/docs/TECH74904>

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

go.symantec.com/nb

About NetBackup third-party legal notices

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

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

<http://www.symantec.com/about/profile/policies/eulas/>

New features, enhancements, and changes

This chapter includes the following topics:

- [About new enhancements and changes in NetBackup](#)
- [NetBackup 7.7 new features and enhancements](#)

About new enhancements and changes in NetBackup

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

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

See [“About the NetBackup 7.7 release”](#) on page 18.

See [“About NetBackup compatibility lists and information”](#) on page 136.

NetBackup 7.7 new features and enhancements

The following lists contain some of the general new features, enhancements, and changes that can be found in NetBackup version 7.7:

General support enhancements

The following support has been added for NetBackup 7.7:

- Support for the backup and restore of the following General Parallel File System (GPFS) metadata attributes: storage pools, metadata replication, and data replication. More information about this feature is available:
 See [“Support for GPFS metadata attributes: storage pools, metadata replication, and data replication”](#) on page 23.

- Enterprise Vault 11

Note: You do not need to make any modifications to your backup policy in order to upgrade to Enterprise Vault 11 from Enterprise Vault 8 and newer.

- SAP High-Performance Analytic Appliance (HANA) SPS 09 on SUSE Linux 11 SP3 and SAP High-Performance Analytic Appliance (HANA) SPS 09 on Red Hat Enterprise Linux (RHEL) 6.5

Note: NetBackup 7.7 does not support the redirected restore of a database instance on these platforms. However, this functionality is supported in NetBackup 7.6.1.2 and will be supported in NetBackup 7.7.1 and later releases.

- Complete support for Red Hat Enterprise Linux (RHEL) 7.0 on Bare Metal Restore (BMR) master servers, clients, and boot servers. Complete support includes self-restore, Dissimilar Disk Recovery (DDR), and Dissimilar System Recovery (DSR) scenarios in physical and virtual environments.
- Support for Lotus Notes 9 on Red Hat Enterprise Linux (RHEL) 6.5

The following are not supported in NetBackup 7.7:

- NetBackup 7.7 is not supported on Windows Server 2003.
- The following robot types:
 - TL4 - Tape library 4mm
 - TL8 - Tape library 8mm
 - TLM - Tape library multimedia

For the current and most comprehensive list of supported software and hardware, see the [NetBackup Master Compatibility List](#).

More information about support and end-of-life notifications is available:

See “[About NetBackup end-of-life notifications](#)” on page 138.

Security updates to the NetBackup database

As a part of security changes in NetBackup, Symantec may make changes to your NetBackup (NBDB) database password. If you changed the password on the NetBackup database from the default value, no changes to the password are made. Any existing NetBackup databases which still have the default password are updated with a new, randomly generated password. All new installations of NetBackup have a randomly generated password assigned to the NetBackup database for improved security. This password is not provided to the user during installation or upgrade. You can use the `nbdb_admin` command to change this randomly generated password. See the *Symantec NetBackup Commands Reference Guide* for more information about the `nbdb_admin` command.

About security certificates for NetBackup media servers

NetBackup requires that media servers have a digital security certificate so that they function correctly in the following use cases:

NetBackup Administration Console authorization for Enhanced Auditing	In the Enhanced Auditing mode, a security certificate is mandatory when a user wants to connect to a media server through the NetBackup Administration Console . See the <i>NetBackup Security and Encryption Guide</i> : http://www.symantec.com/docs/DOC5332
For cloud storage	The NetBackup CloudStore Service Container requires that a certificate be installed on the media server. If one is not installed, the Service Container cannot start. See the <i>NetBackup Cloud Administrator's Guide</i> : http://www.symantec.com/docs/DOC5332

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

Support for GPFS metadata attributes: storage pools, metadata replication, and data replication

NetBackup has added support for the backup and restore of the following GPFS metadata attributes: storage pools, metadata replication, and data replication. By default, NetBackup backs up and restores the ACLs, the extended attributes, and

these additional metadata attributes for GPFS volumes. No additional configuration is necessary.

The following information is pertinent if, after restoring a file, the `illplaced` or the `illreplicated` flags display in the status of the file. (View the status of the file by using the GPFS `mmlsattr` command.)

The `illplaced` flag displays if the file was restored to a different GPFS storage pool than where it was when it was backed up. The change could be due to a change in creation rules or the result of migration rules in the GPFS file placement policy. Or the GPFS administrator may have used the `mmchattr` command to manually move the file to a different storage pool.

The `illreplicated` flag displays when the storage pool containing the restored file has fewer failure groups than required by the data replication setting or the system pool has fewer failure groups than the metadata replication setting.

The GPFS administrator can rebalance the replication factor of the file and resolve the `illplaced` or `illreplicated` flags by running one of two GPFS commands, depending on the number of the files that are involved and the network traffic:

- For a single file: `mmrestripefile`
- For the complete file system: `mmrestripefs`

Note: Restoring files with GPFS attributes and ACLs to an alternate platform does not restore the metadata attributes or the ACLs. For example, backing up files from an RHEL system and restoring to an AIX system. The restore may generate an error such as “Invalid system call.” (Extended attributes can be restored to the alternate platform, however.)

Notes about support for GPFS metadata attributes

- Restoring files with GPFS attributes and ACLs to an alternate platform does not restore the metadata attributes or the ACLs. For example, backing up files from an RHEL system and restoring to an AIX system. The restore may generate an error such as “Invalid system call.” (Extended attributes can be restored to the alternate platform, however.)
- When NetBackup 7.6.1 is used to restore a backup that was created with a NetBackup 7.6.1.1 client, any GPFS Extended Attributes or newly supported GPFS metadata attributes that were backed up are not restored. (ACLs are restored, however.) Depending on the verbose logging level used, the progress log may display a message similar to the following:

```
Unknown extended attribute (3 - META_GPFS) - information will be lost
```


User interface enhancements

Starting with version 7.7, NetBackup no longer includes a native Windows version of the NetBackup Administration Console. Instead, the Java-based version of the console has been updated and enhanced to provide unified performance and functionality across all supported Windows and UNIX platforms. Unless otherwise noted, all uses of the term NetBackup Administration Console within the product documentation are in reference to the latest Java-based version.

Multiple base versions of the NetBackup Administration Console are installed when you install NetBackup server software. You may need to reinstall a previous base version to apply patch updates of the NetBackup Administration Console. For example, when you install or upgrade to NetBackup 7.7, base versions from 7.0 through 7.7 of the console are all installed. For more information about using the NetBackup Administration Console, refer to the *NetBackup Administrator's Guide, Volume I*.

Note: The standalone Backup, Archive, and Restore (BAR) interface for Windows is still included with NetBackup 7.7.

General changes and enhancements for the Java-based NetBackup Administration Console:

- The NetBackup Administration Console is now installed as the default administrative interface when you install NetBackup server packages. You can continue installing the NetBackup Administration Console as a standalone installation (Remote Administration Console) on a host with no existing NetBackup software. However, there is no option to install a native Remote Administration Console for Windows.
- The default NetBackup server installation on Windows includes multiple versions of the new Java-based NetBackup Administration Console. These multiple versions are provided to manage older versions of NetBackup servers as far back as version 7.0.
You can find these consoles under **Start > Programs > NetBackup > Back-level Admin Consoles**.
- The NetBackup Administration Console now provides better and faster performance for bulk image expiration. Any errors that are encountered during the operation for multiple backup images are now displayed together in a single error message box. The details include **Backup ID**, **Copy Number**, and **Error Message**.
- Two commands that operated only on UNIX systems have been removed and replaced with the NetBackup Administration Console: `bpadm` and `vmadm`.

The `bpadm` utility provided a menu interface that administrators used to configure NetBackup and monitor its operations. The `vmaadm` utility presented a menu of operations from any terminal.

- **Images On Media** reports now differentiate true image restore (TIR) backup images. The following reports now specify the TIR type of backup images under the **Fragment Number** column:
 - Images on Media
 - Images on Tape
 - Images on Disk
 - Images on Disk – PureDisk disk pool
- Several enhancements have been made to the **Activity Monitor**. Some of these enhancements include faster loading of data after login, better background refresh performance, and faster response to user inputs such as scrolling, sorting, and keyboard shortcuts.
- A new status, **Disabled**, is introduced for services in the Activity Monitor to explicitly indicate the services that are disabled for the monitored NetBackup server.
- Keyboard shortcuts have been assigned for the **Filter** and **Clear Filter** options. The **Ctrl+T** key combination opens the **Filter** dialog. The **Ctrl+U** key combination clears the applied filters in the tabular data.

GUI enhancements and changes

- **Browse** functionality has been added to the following interfaces:
 - The **Import Clients** dialog in the LiveUpdate policy
 - The **Catalog Recovery Wizard** to select the catalog backup file for disaster recovery
 - The **Backup Selection** panel of the **Backup Policy Configuration Wizard** for all policy types.
 - The **New Storage Unit** dialog
 - The **Disaster Recovery** tab of the NBU-Catalog policy type
 - The **Catalog Disaster Recovery File** panel of the **Backup Policy Configuration Wizard**
 - The **Clients** tab on the **Add New Policy** dialog
 - The **Clients** tab on the **Change Policy** dialog
 - The **Add Backup Selection** dialog for the MS-Exchange-Server policy type

- The **Add Backup Selection** dialog for the MS-SharePoint policy type
- The **Policy > Backup Selection** tab. When you browse a client, you can select multiple directories and files for backup.
- The **Add Path** dialog when adding or changing a tape drive
- The following dialogs, which available for Windows Clients from Client Host Properties:
 - **Add to Exclude List**
 - **Change to Exclude List**
 - **Add Exceptions to Exclude List**
 - **Change Exceptions to Exclude List**
- The NetBackup Administration Console now displays the **Drives** tab in Activity Monitor. You can use the **Drives** tab to manage drives, device paths, and service requests for operators. For more information, refer to the *NetBackup Administrator's Guide, Volume I*.
- A message is displayed on the **Change Policy** dialog when you try to save a policy that another process or another instance of the interface is currently modifying.
- You can now seamlessly switch between the tabs on the **Change Policy** dialog. The data that you enter is not discarded when you switch between the tabs. The **Apply** button has been removed, and the data is saved when you click **OK**.
- You can copy textual information to the Clipboard from all tables like Activity Monitor, Policies, and Storage servers by using the new menu called **Copy to Clipboard**. You can paste the information into other applications like Microsoft Excel and Notepad for further analysis. The new menu **Copy to Clipboard** is available in the right-click menu, under the **Edit** menu, and also in the toolbar menu.
- In the Backup, Archive and Restore (BAR) interface, under the **Task Progress** tab, you can now view the Job ID of the backup and restore tasks.
- The BAR interface now lets you browse, back up, and restore files and folders containing non-English name characters without restarting the console.
- The NetBackup Administration Console now provides an option to adjust the column size to accommodate the data. This enhancement applies to instances of data that is displayed in a flat tabular view, such as with policies, wizards, and the Activity Monitor. This adjustment is also available in the Activity Monitor's hierarchical view.
 To adjust the size of a column, you can either right-click in the table and select **Column > Size to Data**, or click **View** in the menu bar and select **Column >**

Size to Data. Note that these selections are persistent across consecutive logins.

- A new option, **Clear Filter**, has been added to the **View** menu on the toolbar and in the right-click menu. The **Clear Filter** option is used to clear the filters that you applied to the tabular data in NetBackup. This option is enabled only when a filter is applied to the data.
- The **Filter** button has been added in the toolbar that opens the **Filter** dialog. The **Filter** dialog is used to select and apply filters to the tabular data in the selected pane.
- The **Progress log filename** text box (used to specify an alternate path for backup and restore jobs progress log files) has been removed. The option is removed from the **Backup Files and Marked Restore Files** dialogs from the Backup, Archive, and Restore (BAR) interface. The backup and restore job progress logs are stored in the default log files. The path for the default log file of a job is displayed in the **Results of the Task Selection Above** pane in the **Task Progress** tab.
- The **Logging** tab is added to the **Options** dialog box (**View > Options**). By using this tab you can set the parameters for console logging. The settings available on the **Logging** tab are similar to the `Debug.properties` file. For more information, see NetBackup online Help.

New features

- You can now change multiple schedules of multiple policies at one time. For more information, refer to the *NetBackup Administrator's Guide, Volume I*.
- You can now copy policy attributes, clients, schedules, and backup selections from one policy to another or from one server to another. For more information, refer to the *NetBackup Administrator's Guide, Volume I*.
- You can now change multiple clients of multiple policies at one time. For more information, refer to the *NetBackup Administrator's Guide, Volume I*.
- Two new methods of connecting to NetBackup hosts have been added to the **Host Properties**.
- When performing restores, the source client that you select is populated as the destination client for restore. You can change the destination client for restore. You can also add, edit, and remove clients in the **Edit Client List** dialog.
- You can now detect the operating system and hardware of the client that you add or change when configuring a backup policy. To use this feature, enable the **Detect client operating system** check box in the **Add Client** dialog and **Change Client** dialog.

This feature is also available when you configure the LiveUpdate policy type and also when you use the **Policy Configuration Wizard** to configure a policy. To use the auto-detect feature, the master server name must be included in the `bp.conf` file on the client. This task is accomplished when you enter the master server name during the installation of the client software on the host.

Logging enhancements

Logging UI changes in NetBackup 7.7:

- Starting from NetBackup 7.7, the following properties are moved from the **Clean-up** host properties to the **Logging** host properties: **Keep logs** and **Keep Vault logs**. On the **Logging properties** screen, these properties are referred to as **Keep logs for days** and **Keep Vault logs for** respectively.
- Starting with NetBackup 7.7, the **Enable Robust Logging** option is removed from the NetBackup Administration Console **Logging Host Properties** dialog box, because the option is now always enabled. The error logs are always created based on the robust logging configuration parameters. However, the following configuration parameter still appears when you run the `nbgetconfig` command: `ENABLE_ROBUST_LOGGING = NO`

This is a known issue in NetBackup 7.7. Irrespective of the value of the `ENABLE_ROBUST_LOGGING` configuration parameter, robust logging is always enabled.

New logging features in NetBackup 7.7:

- The legacy log file name format is changed beginning with this release. If you use scripts to parse legacy log files, you may have to modify them to read the new log file names. For information about the log file names, see “File name format for legacy logging” in the *Symantec NetBackup™ Logging Reference Guide*:
<http://www.symantec.com/docs/DOC5332>
- The following parameters are added in the configuration file (the Windows registry or the `bp.conf` file in UNIX):
 - `MAX_LOGFILE_SIZE`
It indicates the maximum size of a log file. When the log file size in NetBackup matches the `MAX_LOGFILE_SIZE` setting, the next logs are stored in a new log file.
 - `MAX_NUM_LOGFILES`
It indicates the maximum number of log files that can be created in NetBackup. When the number of log files matches the `MAX_NUM_LOGFILES` setting, the older log files are purged.

- The following new options are added on the **Logging** dialog in the NetBackup Administration Console:
 - **Enable**

This option creates logs for critical NetBackup processes. In previous NetBackup versions, logging starts once you have created the log directories for the required processes. After you select **Enable**, the log directories are automatically created for the critical NetBackup processes and logging begins. The following critical NetBackup processes are logged when you select the **Enable** option:

Master server processes:

 - bprd
 - bpdbm

Media server processes:

 - bpbm
 - bptm
 - bpdm

Client processes:

 - bpfis
 - **Keep logs up to GB**

This option specifies the size of the NetBackup logs that you want to retain. When the NetBackup log size grows to this value, the older logs are deleted. To set the log size in gigabytes (GB), select the check box and specify the value in GB.

NetBackup security and encryption

The following list contains some of the new features and enhancements associated with NetBackup security and encryption starting in NetBackup 7.7:

- NetBackup has enhanced the auditing capability that helps to audit user information. With this feature, you can audit user information without having to enable NBAC. Refer to the *NetBackup Security and Encryption Guide* for details about the enhanced auditing feature.

Note: For this release, enhanced auditing is supported only for Policy and Job operations.

- The NetBackup Key Management Service (KMS) can now be operated in the FIPS mode, wherein the encryption keys generated are FIPS approved. The functionality of exporting and importing keys in KMS is also available. The import and export of keys allows the user to quickly sync multiple NetBackup domains to use the same set of keys or quickly move a set of keys from one domain to another. Along with the above functionalities, the version of NetBackup consumed OpenSSL is upgraded to 1.0.1j. Refer to the *NetBackup Security and Encryption Guide* for more details.

NetBackup for NDMP

The following list contains some of the new features and enhancements associated with NetBackup for NDMP starting in NetBackup 7.7:

- NetApp cDOT filer support
NetBackup for NDMP supports NetApp cDOT filers. See the following guide for information about configuring NetBackup to work with NetApp cDOT filers:
[NetBackup for NDMP Administrator's Guide](#)

NetBackup for Replication Director

The following list contains some of the new features and enhancements associated with NetBackup Replication Director starting in NetBackup 7.7:

- Replication Director now supports the NetApp Clustered Data ONTAP (cDOT) operating system. This enhancement lets you protect the data in your cDOT environment using NetBackup Replication Director. You can use Replication Director to snap, replicate, or back up volumes on Storage Virtual Machines (vservers) within a NetApp Clustered Data ONTAP Cluster.
More information about this feature is available in the [NetBackup Replication Director Solutions Guide](#)

NetBackup Search

The following list contains some of the new features and enhancements associated with NetBackup Search starting in NetBackup 7.7:

- Starting with Release 7.7, NetBackup no longer supports the NetBackup Search functionality. When you upgrade to NetBackup 7.7, the information related to NetBackup Search, including indexing of backup images is deleted. You might continue to see old indexing jobs in the Activity Monitor. The Hold functionality and the existing holds are retained.
Symantec recommends that you uninstall the NetBackup Search software from the indexing servers.

When you upgrade OpsCenter to 7.7, the legal holds are converted to user holds, which can be managed by using the `nbholdutil` command. If a legal hold is found to have the same name as that of an existing user hold, all the hold names are renamed to avoid conflicts. For more information about conversion of hold names and managing holds, see *NetBackup Administrator's Guide, Volume II*.

NetBackup for SQL Server

The following list contains some of the new features and enhancements associated with NetBackup for SQL Server starting in NetBackup 7.7:

- This release of NetBackup includes SQL Server Intelligent Policy. This feature improves the end-user experience for protecting SQL Server environments with NetBackup. Typically NetBackup administrators are responsible for protecting SQL Server environments but have little knowledge of SQL Server internals. Database administrators (DBAs) on the other hand have extensive knowledge of SQL Server but little or no experience using NetBackup. That requires coordination between the NetBackup administrator and the DBA to configure NetBackup properly to protect their SQL Server environment. A number of design deficiencies existed in the SQL Server legacy backup policies that made this process difficult and prone to user error.

To address these issues, SQL Server Intelligent Policy includes the following improvements:

- Fewer policies are required to protect SQL Server instances. You can create a single policy to protect multiple instances that are spread over multiple clients.
- A new discovery service discovers SQL Server instances throughout the NetBackup environment. Newly discovered instances are displayed in the **Applications > Microsoft SQL Server > Instances** node of the NetBackup Administration Console. You can also use the `nbsqladm` command to manage the instances.
- Batch files do not need to be created for backups because they are automatically generated at run-time.
- Improved reporting in the Job Details of the Activity Monitor.
- Enhanced error codes enable faster identification, troubleshooting, and correction of problems. You can easily restart a failed job.
- The Application backup schedule is not used with SQL Server Intelligent Policy. Backup schedules now include full, differential, and transaction log backups.

- You can manually back up any number of instances or databases.
- Performance tuning options with policy configuration, including the following: backup stripes, transfer size, buffer usage, and the option to skip any databases that are unavailable.
- You can create a new transaction log schedule that backs up the transaction logs in intervals of minutes.
- The database administrator can control all instance credentials with the `nbsqladm` command, providing improved security throughout the system.

Legacy SQL Server policies (configured with clients and batch files) can still be used, but cannot be upgraded to a SQL Server Intelligent Policy. If you want to protect the instances in a legacy policy with an Intelligent Policy instead, you must configure a new Intelligent Policy.

For more detailed information about NetBackup for SQL Server, see the [NetBackup for SQL Server Administrator's Guide](#).

NetBackup virtualization

The following list contains some of the new features and enhancements associated with virtualization starting in NetBackup 7.7:

- Enhancement of Instant Recovery (IR) in NetBackup plug-in for VMware vSphere Web Client

In addition to the instant recovery of virtual machines using the command line interface, the Symantec NetBackup Plug-in for VMware vSphere Web Client introduces instant recovery wizard on the user interface. This wizard enables the administrator to perform single as well as simultaneous multiple virtual machines' recovery, instantly, to a single destination. The wizard initiates the instant recovery by exposing the virtual machine's backup image as a datastore to the destination ESX server. The recovered virtual machine(s) are made accessible to the user immediately.

- NetBackup Add-in for Microsoft SCVMM Console

From the Microsoft System Center Virtual Machine Manager (SCVMM) console, you can use the NetBackup Add-in to recover virtual machines from NetBackup backup images.

You can use the Add-in to do the following in the SCVMM console:

- Recover the full virtual machine to its original location or to an alternate location.
- Monitor the progress of recovery jobs that the Add-in initiated.

For complete installation, configuration, and usage details, see the *NetBackup Add-in for Microsoft SCVMM Console Guide*.

- **Hyper-V Intelligent Policy**

NetBackup can automatically select Hyper-V virtual machines for backup by means of filtering rules in the policy. The policy **Clients** tab includes a **Query Builder** for creating the rules. NetBackup makes a list of the virtual machines that currently meet the rules, and adds those virtual machines to the backup.

Automatic selection of virtual machines has these advantages:

- Simplifies the policy configuration for sites with large Hyper-V environments, including clustered environments.
- Allows the backup list to stay up-to-date, in spite of changes in the virtual environment.
- Virtual machine selection takes place dynamically at the time of the backup.

NetBackup language packs

NetBackup language packs are available for download at the Symantec Enterprise Technical Support site and on Symantec File Connect. The NetBackup French, Japanese, and Simplified Chinese media kits also include language pack media. Please contact your Symantec sales representative or reseller for more details about how to obtain NetBackup language packs.

This section describes expansions that have been made to the language packs for NetBackup and OpsCenter in NetBackup 7.7. For more details, please refer to the Symantec NetBackup 7.7 Language Pack Read This First and the Symantec OpsCenter 7.7 Language Pack Read This First provided with each language pack.

Platform support

NetBackup language packs now support Red Hat Enterprise Linux and SUSE Linux Enterprise Linux.

OpsCenter language packs now support the same Linux distributions as NetBackup language packs.

Language pack platform support in 7.7 is summarized below. New platform support for 7.7 is marked with an asterisk (*).

Table 2-1 Supported server and client platforms

	Solaris SPARC	Solaris x86-64	AIX Power	HP-UX IA	Red Hat x86-64	SUSE x86-64	Windows
NetBackup	Localized	No	Localized	Localized	Localized*	Localized*	Localized
OpsCenter	N/A	N/A	N/A	N/A	Localized*	Localized*	Localized

Character encoding support

Language packs now support UTF-8 encoding in addition to non-Unicode encodings for UNIX/Linux platforms. Language pack encoding support in 7.7 is summarized below. New encoding support for 7.7 is marked with an asterisk (*).

Table 2-2 Supported character encoding, character sets, and code pages

	French	Japanese	Simplified Chinese
Solaris SPARC	ISO 8859-1 ISO-8859-15 UTF-8*	Shift_JIS EUC-JP UTF-8*	GB-2312 GBK GB-18030 UTF-8*
AIX Power	ISO 8859-1 ISO-8859-15 UTF-8*	Shift_JIS EUC-JP UTF-8*	GB-2312 GBK GB-18030 UTF-8*
HP-UX IA	ISO 8859-1 ISO-8859-15 UTF-8*	Shift_JIS EUC-JP UTF-8*	GB-2312 GBK GB-18030 UTF-8*
Red Hat x86-64	ISO 8859-1* ISO-8859-15* UTF-8*	Shift_JIS* EUC-JP* UTF-8*	GB-2312* GBK* GB-18030* UTF-8*
SUSE x86-64	ISO 8859-1 ISO-8859-15 UTF-8	Shift_JIS* EUC-JP* UTF-8*	GB-2312* GBK* GB-18030* UTF-8*
Windows	CP1252	CP1252	CP1252

Localization component support

NetBackup language packs now support the following components in 7.7:

- NetBackup for Windows language packs now support the Java-based administration console.
- NetBackup for Windows language packs now support the Backup, Archive, Restore interface if it is installed to a NetBackup server.
- NetBackup for Linux language packs now provide the same localization coverage as NetBackup for UNIX language packs.
- OpsCenter Linux language pack provides the same localization coverage as Windows language pack.

NetBackup and OpsCenter language pack component support for 7.7 is summarized below. New support introduced in 7.7 is marked with an asterisk (*).

Table 2-3 Localized NetBackup components

	Java-based Administration Console	Java-based Backup Archive, Restore Console	Microsoft Foundation Class –based Backup Archive, Restore Console	Command line interface commands	Menu interface
Solaris SPARC	Localized	Localized	N/A	Localized	No
AIX Power	Localized	Localized	N/A	Localized	No
HP-UX IA	Localized	Localized	N/A	Localized	No
Red Hat x86-64	Localized*	Localized*	N/A	Localized*	No
SUSE x86-64	Localized*	Localized*	N/A	Localized*	No
Windows	Localized*	Localized*	Localized	Localized	No

Table 2-4 Localized OpsCenter components

	Web-based administration console	Command line interface commands
Red Hat x86-64	Localized*	No
SUSE x86-64	Localized*	No
Windows	Localized*	No

Note: For NetBackup 7.7, the NetBackup server must be installed on a computer before you can install a language pack for the Java-based Windows Administration Console on that same computer. Remote installations of the Administration Console, which are installed on computers which do not have the NetBackup server also installed, cannot be localized.

Operational notes

This chapter includes the following topics:

- [About NetBackup 7.7 operational notes](#)
- [NetBackup installation and upgrade operational notes](#)
- [NetBackup administration and general operational notes](#)
- [NetBackup administration interface operational notes](#)
- [NetBackup Accelerator operational notes](#)
- [NetBackup auditing operational notes](#)
- [NetBackup Bare Metal Restore operational notes](#)
- [NetBackup Cloud operational notes](#)
- [NetBackup cluster operational notes](#)
- [NetBackup database and application agent operational notes](#)
- [NetBackup deduplication operational notes](#)
- [Internationalization and localization operational notes](#)
- [NetBackup LiveUpdate operational notes](#)
- [NetBackup Logging Assistant operational notes](#)
- [NetBackup for NDMP operational notes](#)
- [NetBackup OpsCenter operational notes](#)
- [NetBackup Replication Director operational notes](#)
- [Resilient network operational notes](#)

- [NetBackup Search operational notes](#)
- [NetBackup Snapshot Client operational notes](#)
- [NetBackup virtualization operational notes](#)

About NetBackup 7.7 operational notes

NetBackup operational notes describe and explain important aspects of various NetBackup operations that may not be documented elsewhere in the NetBackup documentation set or on the Symantec Support website. The operational notes can be found in the *NetBackup Release Notes* for each version of NetBackup. Typical operational notes include known issues, compatibility notes, and additional information about installation and upgrade.

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

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

See [“About related NetBackup documents”](#) on page 140.

NetBackup installation and upgrade operational notes

NetBackup can be installed and upgraded in heterogeneous environments using a variety of methods. NetBackup is also compatible with a mixture of servers and clients that are at various release levels in the same environment. This topic contains some of the operational notes and known issues that are associated with the installation, upgrade, and software packaging of NetBackup 7.7.

See [“About NetBackup release types and versioning”](#) on page 132.

No appliance upgrade path to NetBackup 7.7 until Appliance 2.7.1 patch is released

At the General Availability of NetBackup 7.7, the NetBackup Appliance has no upgrade path to support NetBackup 7.7 clients or media servers. If you currently have a NetBackup Appliance in your environment, Symantec recommends the following workarounds until the NetBackup Appliance 2.7.1 patch is released:

- Do not upgrade a client to NetBackup 7.7 if the client's media server is an appliance.

- Do not upgrade a media server to NetBackup 7.7 if the master server is an appliance.

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

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

Cannot install server software to root environment of separate host that is mounted on Solaris system

In previous releases, you could install NetBackup server software to the root environment of a separate host that was mounted on a Solaris system. For example, if Host B's file systems are mounted to Host A at a specific location, this option let you log into Host A, specify that location in the NetBackup installer, and thus install NetBackup onto Host B.

This feature has been removed in NetBackup 7.7 and no longer appears as an option in the NetBackup installer.

After upgrading to 7.6, changes to Object IDs in nblog.conf are not preserved

After an upgrade to NetBackup 7.6, changes to individual Object IDs in the `nblog.conf` file are not preserved. However, the major default settings are preserved.

After upgrade to 7.x, interface entry may change for configurations that previously listed an IP address as REQUIRED_INTERFACE

Upon upgrading to NetBackup 7.x, a configuration that lists an IP address for the `REQUIRED_INTERFACE` entry may experience a +change on the choice of interfaces after the upgrade. (For example, `REQUIRED_INTERFACE = IP_address`.)

If the host name that is associated with the IP address resolves to more than one IP address, each of those addresses is used, rather than the first address.

Symantec recommends the use of a host name that resolves to one address with `REQUIRED_INTERFACE` or replacing it with the `PREFERRED_NETWORK` equivalent in NetBackup 7.x.

About support for HP-UX Itanium vPars SRP containers

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

Starting with version 7.6.1, NetBackup installation aborts if you try to install into an HP Itanium SRP container (private file system, shared file system, or workload). If you install into the global container, a parameter is added to all `swremove` and `swinstall` commands to install only to the global view.

Extra steps are required to perform NetBackup 7.6 client push installations from an HP PA-RISC media server

Extra steps are required to perform NetBackup 7.6 client push installations from an HP PA-RISC media server to clients that support NetBackup-Java applications.

During the installation, `/usr/opensv/java/nbj.conf` ends up empty on the receiving client. This issue applies to the `ssh`, `rsh`, `ftp`, `sftp`, and `update_clients` remote installation methods for both initial installations and upgrades.

On the receiving client, `/usr/opensv/java/nbj.conf` has zero length. From the pushing server, you encounter a message similar to the following:

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

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

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

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

To work around this issue, see the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH210951>

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

A successful install may return an unsuccessful exit status (non-zero) for an upgrade of a pre- 7.0 NetBackup client to version 7.6

If the following `ssh` command is used to upgrade a pre- 7.0 NetBackup client to version 7.6, a successful install may return an unsuccessful exit status (non-zero):

```
/usr/opensv/netbackup/bin/install_client_files ssh <client>
```

If the installation encountered this particular issue, rerunning the command to the client should return a successful exit status. To work around this issue altogether, use a different remote installation method such as `rsh`, `ftp`, `sftp`, or `update_clients` to upgrade pre- 7.0 NetBackup clients.

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

For more information, see "Installing client software with the `ssh` method" in the [NetBackup Installation Guide](#).

A Java error can occur on AIX 7.1

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

```
WARNING: Installation of Java LiveUpdate agent failed.  
Refer to file /tmp/JLU-Log/JavaLiveUpdate-Install.log on bmaix57 for more information.
```

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

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

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

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

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

Character restrictions for database server name

An upgrade to SQL Anywhere 11.0.1 was made in NetBackup 7.0. However, there is a restriction within that version that requires the database server name to be less or equal to 31 characters. NetBackup has been modified to change the server name, from `VERITAS_NB_hostname.domain_name` to `NB_hostname` in `/usr/opensv/db/bin/servername`. NetBackup also trims the name to 31 characters if necessary.

Uninstalling NetBackup from FreeBSD

The procedure given in the NetBackup 7.7 Install Guide to uninstall NetBackup from a FreeBSD client is incorrect. Instead of uninstalling PBX, you should perform the following commands in FreeBSD:

1. `/opt/VRTSpx/bin/vxpbx_exchanged stop`
2. `rm -rf /opt/VRTSpx`
3. `rm -rf /etc/vx/VxICS`
4. `rm -r /usr/share/man/man1/pbxcfg.1`

Considerations for Oracle backup policies when upgrading from NetBackup 7.1 and earlier

For upgrades from NetBackup 7.1 or earlier to NetBackup 7.5 or later, special care may be required for the Oracle backup policies before the upgrade is performed.

Consideration is required if an Oracle policy uses snapshots and directs the backup to a storage lifecycle policy: The SLP processing for all of the images that are associated with that policy must be brought to a complete state before the upgrade.

See the *NetBackup Upgrade Guide* for more information.

NetBackup administration and general operational notes

NetBackup provides a complete, flexible data protection solution for a variety of platforms. The platforms include Windows, UNIX, and Linux systems. In addition to a standard set of data protection features, NetBackup can also utilize several

other licensed and non-licensed components to better protect a variety of different systems and environments. This topic contains some of the general operational notes and known issues that are associated with the administration of NetBackup 7.7.

NetBackup supports two optimized duplication methods for OpenStorage

NetBackup supports two optimized duplication methods for OpenStorage. The optimized duplication method that NetBackup uses depends on the capability that the vendor's OpenStorage plug-in exposes, as follows:

Optimized duplication NetBackup optimized duplication is extent-based; NetBackup transfers data in 256-KB chunks.

For optimized duplication, the NetBackup `bpstsinfo` command output that shows the storage server capabilities shows the following flag:

```
STS_SRVC_COPY_EXTENT
```

Whole image optimized duplication Whole image optimized duplication uses the storage unit **Maximum fragment size** for the data chunk size. Symantec refers to this type of operation as *whole image* optimized duplication because an entire NetBackup image fragment is transferred.

Because larger chunks of data are transferred, fewer copy management requests occur and performance improves. Also, the storage device controls progress reporting. The storage device may report progress when system load is low rather than consume the resources that are better used for duplication. Or, the storage device may report progress at short intervals, updating the NetBackup user as frequently as NetBackup would for extent-based optimized duplication.

For whole image, optimized duplication, the NetBackup `bpstsinfo` command output that shows the storage server capabilities shows the following two flags:

```
STS_SRVC_COPY_EXTENT
STS_SRVC_COPY_EXTENT_WHOLEIMAGE
```

The following is the syntax for the `bpstsinfo` command that shows the storage server capabilities:

```
bpstsinfo -servercap -storage_server host_name -stype vendor_string
```

More information about the `bpstsinfo` command is available.

See the *NetBackup Commands Reference Guide*:

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

More information about OpenStorage is available.

See the *NetBackup OpenStorage Solutions Guide for Disk*:

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

Export file shows incorrect properties while exporting properties of multiple hosts with different versions

While exporting properties of multiple NetBackup hosts with different versions, the export file may show properties that are not applicable for a particular NetBackup version.

Consider the following scenario: You have exported host properties of multiple NetBackup Master Servers with versions 7.5, 7.6.1, and 7.7. The export file may show the NetBackup 7.7-specific property 'Logging for critical processes: YES' also for the 7.6.1 and 7.5 master servers.

Workaround:

To export properties of NetBackup hosts with multiple versions, you need to select the hosts of the same NetBackup version while exporting and create a separate export file for each NetBackup version.

To export host properties, do the following: In the NetBackup Administration Console, expand **NetBackup Management > Host Properties > Master Servers, Media Servers, or Clients**. To select multiple hosts, hold down the SHIFT or CTRL key, select hosts, right-click and click Export.

Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms

Using X forwarding to launch the NetBackup Administration Console can fail on certain Linux platforms, particularly Red Hat Enterprise Linux 6.0 (RHEL 6.0) on VMware. The issue is a result of incompatibilities between the default GNU C Library (`glibc`) and Advanced Vector Extensions (AVX) on newer hardware. The issue should be fixed in a future release of `glibc`.

Workaround: Run the `export LD_BIND_NOW=1` command before you execute `runInstaller`.

NetBackup Management > Catalog search results display a single image even if there is more than one image present on the system

In some cases, **NetBackup Management > Catalog** search results display a single image even if there is more than one image present on the system.

Workaround: Run the following command to display the images:

- UNIX

```
/usr/opensv/netbackup/bin/admincmd/nbstlutil stlilist -U
```

- Windows

```
\Program Files\Veritas\NetBackup\bin\admincmd\nbstlutil.exe  
stlilist -U
```

Use the exact timestamp of an image to see it in the catalog.

Java Windows Administration console throws status code 521 on Windows Vista/Server 2008 and later

Beginning with Windows Vista/Server 2008 and up, you might encounter status code 521 (NB-Java Configuration file *file_name* does not exist) when you run the Java Windows Administration Console. This error occurs in User Access Control (UAC)-enabled environments because of inadequate permissions. If you run the Java Windows Administration Console or its installer (*Setup.exe*) while UAC is enabled, a warning and a prompt to disable UAC is displayed.

To work around this issue, Symantec recommends that you disable UAC before you run the Java Windows Administration Console. If UAC is not disabled adequately, non-built-in administrators are required to launch the Java Windows Administration Console by choosing the **Run as administrator** option.

Although a warning is displayed, you can still run the Java Windows Administration Console installer in a UAC-enabled environment. The error only occurs when you run the console itself.

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

Radio buttons may render incorrectly in the NetBackup Administration Console when using Remote Desktop Connection (RDC) on Mac OS X

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

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

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

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

The following two NetBackup limitations can occur if an IPv6 address is used as a client name or an image name:

- Using IPv6 addresses as client names in a policy do not work with Instant recovery (IR) snapshots on Windows systems. That can cause a backup to fail. Specify a host name instead of an IPv6 address.
Image names are created automatically in NetBackup, and consist of a combination of the client name and a timestamp. If the client name is configured in the policy as the IPv6 address, the result is an image name (in the image catalog) that includes the IPv6 address. That causes the backup to fail.
- Using IPv6 addresses as image names under the catalog do not work with Instant recovery (IR) snapshots on Windows systems.

IPv6 link-local addresses not supported in NetBackup

The use of IPv6 link-local addresses is not supported in NetBackup. IPv6 link-local addresses are the addresses that start with fe80::.

Intermittent issues with X forwarding of NetBackup Java Administration Console

Intermittent issues may occur with X forwarding of the NetBackup Java Administration Console. This behavior only occurs when you use X forwarding. This issue does not occur at the local console. The issue is most commonly seen on Linux servers, but not exclusively. The issue generally occurs when older versions of X viewers are used, such as Xming and XBrowser.

The use of MobaXterm seems to minimize or eliminate the issue. If you experience issues with X forwarding, consider upgrading your X viewer and retrying the operation or access the server from the local console.

Image extension files remain in catalog when using NetBackup Administration Console to expire NetBackup images

If you use the NetBackup Administration Console to expire NetBackup images, the image extension files remain in the catalog. However, NetBackup expires the image extension files, usually within 12 hours.

Reduced functionality during the initialization of 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.

Memory requirements to run the NetBackup Administration Console

Memory requirements to run the NetBackup Administration Console.

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

Remote display of the NetBackup-Java Administration Console in multi-byte locale environments is not supported

No remote display of the NetBackup-Java Administration Console in multi-byte locale environments.

Remote display of the NetBackup-Java Administration Console in multi-byte locale environments is not supported.

Performance issues may occur with NetBackup 7.x master servers on UltraSPARC T-series or SPARC T3 architecture

You might experience performance issues if you use UltraSPARC T-series or SPARC T3 architecture as a NetBackup master server in large environments. These issues include the following problems:

- No response from storage lifecycle policy (SLP) requests (`nbslutil` stops responding)
- Delays accessing database contents
- Delays with catalog verify and validate queries
This issue occurs when pending database queries take longer than CORBA timeout values.

Additional issues have been reported as well. More information is available:

<http://www.symantec.com/docs/TECH204332>

A multistream backup may fail if DFSR is active on the client

A Windows multistream backup of all local disks may fail if Microsoft Distributed File System Replication (DFSR) is active on the client.

Workaround: Disable multistreaming for the Windows clients that have DFSR enabled.

The backup script path field is not active for an automatic backup schedule

When you configure an MS-SQL-Server policy with the **Backup Policy Configuration Wizard** and select the **Backup Type**, the field to specify the backup script path is not active after you select **Automatic Backup**. This issue only affects the NetBackup-Java Administration Console.

For more information and workarounds for this issue, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH222312>

Migration to a simplified client name for Windows clients

NetBackup is migrating to a simplified client name for Windows clients.

The new client selection **Windows** will be used for all supported Windows clients, regardless of the specific Windows version of the client. In future releases, specific Windows version choices will be eliminated. As part of this migration, the client

selection **Windows** may or may not appear in the client selection menus. Please choose the new **Windows** menu selection for the appropriate architecture (x86 or x64). If the **Windows** selection is not available, please select the specific Windows version.

Note: If the **Windows** selection is not available when adding a Windows 8/Server 2012 through any of the NetBackup interfaces, choose the Windows 7 or Windows 2008 menu selection.

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

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

A newly-added NetBackup appliance media server may get added to the EMM database as a master server

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

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

Restore may fail for the clients that have both WAN Resiliency and client direct deduplication enabled

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

Issues with SUSE 11 running on kernel versions later than 2.6

Live browse and backup problems can occur on SUSE 11 operating systems that have a kernel version later than 2.6. The issues occur because the `nbfirescan` process in NetBackup 7.7 does not support kernel versions later than 2.6.

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

Certain file names in the Windows system drive root directory prevent NetBackup from functioning properly

If any file named `program` exists in the root directory of the Windows system drive (such as `C:\`), NetBackup does not function properly. Any such file must be removed or renamed before NetBackup can execute command lines and process creation options.

Time differences between NetBackup hosts causes display issues in the Activity Monitor

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 Activity Monitor provides more information for each job execution and it prints the information from media server and client processes. The timestamp information for those messages originates on the media server and client. Therefore, if the time is not correctly synchronized, it may not appear in the correct order at the Activity Monitor.

NetBackup administration interface operational notes

The NetBackup administrator has a choice of several interfaces to use to administer NetBackup. All of the interfaces have similar capabilities. This topic contains some of the operational notes and known issues that are associated with these interfaces in NetBackup 7.7.

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

See [“About NetBackup compatibility lists and information”](#) on page 136.

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

Information at the Activity Monitor may not appear in the correct order

The precision that the Activity Monitor uses is measured in seconds. Starting with NetBackup 7.1, more information is printed into the Activity Monitor. Messages from the master server, media server, and clients that generate at the same second may display out of the order that they occurred.

Logs are deleted even though the Keep logs up to GB option is enabled

Logging Assistant is a helpful tool that you can use to significantly shorten the time required to set up, collect, and upload debug logs and other information to Symantec Technical Support.

While the Logging Assistant tool collects NetBackup logs, the total NetBackup log size may increase. If you have enabled the new **Keep logs up to GB** option on the **Host Properties > Logging** dialog box and the total NetBackup log size reaches its maximum capacity, logs are deleted. Logs that you want to retain may also be deleted. To avoid the deletion of logs that you want to retain, you must disable the **Keep logs up to GB** option while you collect logs using Logging Assistant.

Alternatively, you can set the **Keep logs up to GB** option to a value higher than the current value, so that the important logs are not deleted before the log collection is complete.

Java Administration Console may encounter a core dump issue when the Simplified Chinese UTF-8 locale is used on a Solaris SPARC 64-bit system with Solaris 10 Update 2 or later

The NetBackup Java Administration Console may encounter a core dump issue when the Simplified Chinese UTF-8 locale is used on a Solaris SPARC 64-bit system with Solaris 10 Update 2 and later installed. For more information, refer to Bug ID 6901233 at the following URL on the Oracle Technology Network website:

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6901233

If you encounter this issue, apply the appropriate Solaris patches or upgrades that Oracle provides for this issue.

NetBackup Java user interface may fail to start in HP-UX 11.31 environments

The NetBackup Java user interface may not start in environments that run the HP-UX 11.31 operating system. To start properly, the Java user interface requires up-to-date patches to the HP-UX 11.31 operating system.

Workaround: Before you launch the NetBackup Java user interface, you must install the HP-UX 11.31 patches that are required for Java™ 8.0 for the Quality Pack that you have installed on your system. For more information, see the following HP site:

<ftp://ftp.hp.com/pub/softlib/hpuxjava-patchinfo/index.html>

NetBackup Accelerator operational notes

NetBackup Accelerator increases the speed of full backups. The increase in speed is made possible by change detection techniques on the client. The client uses the change detection techniques and the client's current file system to identify the changes that occurred since the last backup. This topic contains some of the operational notes and known issues that are associated with NetBackup Accelerator in version 7.7.

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

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

Accelerator and Replication Director support for virtualized servers cannot be configured together

NetBackup Accelerator and Replication Director support for virtualized servers cannot be configured together. The Block Level incremental backup settings do not currently allow the combination.

Accelerator does not support the VxFS File Change Log

The NetBackup Accelerator does not support the VxFS File Change Log.

The bpverify operation can fail with status code 191 for certain NetBackup Accelerator images

If you use the `bpverify` command to verify an Accelerator image that was taken using NetBackup 7.5.0.4 or earlier, then the verify operation can fail with a status code 191. The failure can occur because the total size of the image in media may not match the size of the image that was recorded in the catalog metadata.

This issue specifically pertains to an incorrect image size in the catalog metadata. It does not mean that the image is corrupt or stop you from restoring the image. The following error can appear in the logs:

```
/usr/opensv/netbackup/logs/bpdm/112112_00011.log ---
02:32:36.278 [28530] <2> verify_image_frgsizes:
validating abcd12.xxxx.xxx.symantec.com:
wxyz.xxx.xxx.symantec.com_1352283783_C1_F1 imo_size=6130472960
613...
(Kbytes=5986790 remainder=512 diff=-512)

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

Accelerator backups for VMware intermittently fail with an incorrect checksum error

Accelerator backups for VMware intermittently fail with status code 84 and an `incorrect checksum` error when you use the `hotadd` transport method on a Windows proxy.

Further information and potential workarounds for this issue can be found at the following location on the Symantec Support website:

<http://www.symantec.com/docs/TECH222588>

Accelerator policy creation can fail because it does not recognize a valid storage unit group

The creation of a NetBackup Accelerator policy can fail because it does not recognize a valid storage unit group. The issue is a result of uninstalling and then reinstalling the NetBackup Administration Console with a different host name (domain).

For more information and workarounds for this issue, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH209889>

NetBackup auditing operational notes

An audit trail is a record of user-initiated actions in a NetBackup environment. Essentially, auditing gathers the information to help answer who changed what and when they changed it. This topic contains some of the operational notes and known issues that are associated with auditing and audit trails in NetBackup 7.7.

Support notes

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 command line interface may show unrecognizable characters for the backup selection output

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.

Action with parent jobs does not generate audit records for children

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.

NetBackup Bare Metal Restore operational notes

NetBackup Bare Metal Restore (BMR) automates and streamlines the server recovery process, making it unnecessary to reinstall operating systems or configure hardware manually. This topic contains some of the operational notes and known issues that are associated with BMR in NetBackup 7.7.

A new BMR user prompt has been added to choose between multiple kernel levels

An additional user prompt has been added to let you choose the appropriate kernel when you create a Bare Metal Restore (BMR) shared resource tree (SRT) for a Linux client using operating system installation media that have multiple kernels.

For example, the following prompt is displayed when you create an Oracle Linux 6.4 client:

```
Choose appropriate SRT kernel version for your SRT :
```

1. vmlinuz-2.6.39-400.17.1.el6uek.x86_64
2. vmlinuz-2.6.32-358.el6.x86_64

```
Enter your selection [1] :
```

In the example, the default kernel selection is the Oracle Linux UEK kernel (`vmlinuz-2.6.39-400.17.1.el6uek.x86_64`) and gets added in the SRT by default. However, you may need to select a different kernel depending on your requirements. In this example, you must select the Red Hat Enterprise Linux (RHEL) kernel (`vmlinuz-2.6.32-358.el6.x86_64`) when an SRT is created for Oracle Linux 6.4 running on a Windows Hyper-V VM. After the BMR recovery, you must select the appropriate kernel to boot the server.

NetBackup 7.6.0.2 clients on Windows x86-32 cannot be used as Virtual Instance Converters

NetBackup 7.6.0.2 Windows x86-32 clients cannot be used as Virtual Instance Converters (VICs) for BMR physical to virtual (P2V) conversions. Note that NetBackup 7.6.0.2 uses VMware VDDK 5.5 libraries, which do not support the Windows x86-32 bit platform.

Legacy Restore is not supported on Windows 8/Server 2012 and later

Legacy Restore is not supported on Windows 8/Server 2012 and later.

Other file systems on ZFS volumes are not supported

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

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.

NetBackup BMR can only restore IPv6 information using an IPv4 network connection

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.

Inconsequential message may appear during BMR recovery of an RHEL client that has RAID1 volumes

During a Bare Metal Restore (BMR) recovery of a Red Hat Enterprise Linux (RHEL) client that has RAID1 volumes configured, you may receive the following message on the client screen:

```
INFO: task mdadm:<pid> blocked for more than 120 seconds
```

You can safely ignore this message. The message is the result of the `mdadm` utility taking longer than expected. However, the utility eventually finishes and the restore completes successfully.

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

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

10 update 11 has a kernel patch ID that is lower than the ID for previous Solaris 10 updates.

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

A devfsadmd error may occur on Solaris 11 and newer

During a BMR restore on Solaris 11 and newer, the following error message may be displayed:

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

During a BMR restore, the service that is related to the `devfsadmd` daemon is stopped temporarily to manipulate the `/dev` and `/devices` links. As a result, when the operating system wants to do internal communication with the `devfsadmd` daemon it generates the error message.

This message is not for BMR and it does not have any effect on a BMR restore or on the overall system. The message can be ignored. Once the system boots up after the BMR restore, the `devfsadmd` daemon restarts and the message does not display again.

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

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

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

```
sendmail/filesys_update failed
```

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

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

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

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

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

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

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

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

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

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

The OS takes time for configuration after a client to virtual machine conversion

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

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

BMR restores of encrypted file systems on RHEL are restored without encryption

If a backed-up file system is encrypted for Red Hat Enterprise Linux (RHEL) and then restored with the BMR option, the existing encryption is removed.

When the `/etc/mke2fs.conf` file is restored, the restore task is shown as partially completed in the Activity Monitor

When the `/etc/mke2fs.conf` file is restored, the restore task is shown as partially completed in the **Activity Monitor**. The issue occurs on Red Hat Enterprise Linux (RHEL) 6 Update 2 and later even though the Bare Metal Restore (BMR) recovery of the client completes successfully. The issue occurs because the security properties contain some incorrect settings for the `/etc/mke2fs.conf` file in a BMR environment after the file is restored.

ZFS temporary mount can fail during a BMR restore

During a Bare Metal Restore (BMR) restore, the Zeta file system (ZFS) temporary mount fails. This issue occurs if any ZFS is not mounted or the `canmount` value is set to `OFF` during a backup.

To restrict the disk or the disk pool, edit the BMR configurations. The edits ensure that the disk is not overwritten and the data that it contains is not erased during the restore process.

For more information on how to edit the configurations, refer to the following sections of the *Bare Metal Restore Administrator's Guide*:

- Managing Clients and Configurations
- Client Configuration Properties

Issues may occur after a BMR restore is performed on RHEL 6

After the completion of a Bare Metal Restore (BMR) Linux restore task, the system may display "Kernel Panic" when it looks for a grub menu. The system may also go into maintenance mode during the first restart. These issues occur because the UDEV daemon dynamically detects devices, causing discrepancies with disk names and ordering in various configuration files across restarts.

If you encounter this issue, please contact Symantec Support and have your support representative reference the following tech notes: TECH201332 and TECH179048.

BMR fails to create a media SRT when a Basic Server installation is performed on an RHEL system

A Basic Server installation of Bare Metal Restore (BMR) on a Red Hat Enterprise Linux (RHEL) system fails to create a media shared resource tree (SRT). This issue occurs because the package that contains a command that is used for ISO creation

is missing. This issue does not occur with a normal Desktop installation on RHEL clients.

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

The system relabels all of the file systems after a BMR restore during the first startup

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

That is a necessary process that is related to SELinux:

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

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

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

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

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

```
SUNW-MSG-ID: ZFS-8000-D3, TYPE: Fault, VER: 1, SEVERITY: Major
EVENT-TIME: Mon May 23 13:10:09 CDT 2011
PLATFORM: SUNW,Sun-Fire-V215, CSN: -, HOSTNAME: bmrso1101.vxindia.veritas.com
SOURCE: zfs-diagnosis, REV: 1.0
EVENT-ID: c257eb38-495e-cdb6-9a52-a4d9c2ae38be
DESC: A ZFS device failed. Refer to http://sun.com/msg/ZFS-8000-D3 for more information.
AUTO-RESPONSE: No automated response will occur.
```

IMPACT: Fault tolerance of the pool may be compromised.

REC-ACTION: Run 'zpool status -x' and replace the bad device.

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

```
all pools are healthy
```

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

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

BMR may not format or clear the ZFS metadata

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

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

Coexistence of two BMR-supported multi-path solutions can cause issues

Coexistence of two Bare Metal Restore (BMR)-supported multi-path solutions (EMC PowerPath and Linux native multi-path) with both actively configured on a client can cause issues and is not supported by BMR.

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

A BMR restore may fail during a Linux DDR scenario between internal disk and SAN disk

A Bare Metal Restore (BMR) restore may fail during a Linux dissimilar disk restore (DDR) scenario from internal disk to SAN disk and vice versa.

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

If you remove SAN disks before restoration, then the restore may work properly with the existing BIOS ordering.

BMR backups may fail on Citrix XenCenter virtualization due to disk naming

Bare Metal Restore (BMR) can only support disk naming conventions such as `hdX`, `sdX`, `cXDn`, and so forth.

BMR backups can fail on Citrix XenCenter virtualization for the following reasons:

- BMR does not recognize disk names such as `xvdX`, which are newly introduced on Citrix XenCenter virtualization. This issue is due to the Xen para-virtual drivers that are introduced in this type of virtual environment.
- For modern versions of BMR that Linux systems such as SLES 11 SP1 support, the client computers show `hda` and `sda` disk naming conventions at the same time. BMR does not support this behavior.

To work around this issue, make sure that you use the **Other** media install because it is the only template that BMR supports for a Citrix XenCenter virtual machine. Do not use the systems that BMR does not support. For example, BMR does not support SLES 11 SP1 and RHEL6.1 and onwards on Citrix XenCenter virtualization.

A NetBackup system state backup can fail on certain Windows Server 2008 R2 systems with SFW

A NetBackup system state backup can fail on certain Windows Server 2008 R2 systems with Storage Foundation for Windows (SFW) 5.1 SP1. This issue occurred on a system where the System Reserved partition did not have an assigned drive letter. The following SFW 5.1 SP1 hot fix resolves the issue:

sfw-Hotfix_5_1_10064_584_2496270

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

This issue is also resolved in SFW 5.1 SP2 CP7.

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

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

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

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

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

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

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

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

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

Patch required to create an SRT on HP-UX 11.31 IA64

The PHCO_40961 patch is required to create a Bare Metal Restore (BMR) shared resource tree (SRT) on an HP-UX11.31 IA64 platform.

The same patch is required to create a BMR SRT on an HP-UX 11.31 IA64 platform with Veritas Storage Foundation packages (VxVM, VxFS).

IPv6 support for BMR

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

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

Example

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

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

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

A failure may occur during a VxFS7-based file creation

During a Bare Metal Restore (BMR) restore, a failure can occur during a VxFS7-based file creation process. To work around this issue, use `bmrstadm` to patch VxFS version with version 5.0 to edit the SRT. Attempt to restore again and start a client restore.

Automatic boot may fail for HP-UX after a restore

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

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

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

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

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

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

Prepare to Restore may not work for a Solaris client

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

To work around this issue, perform the following:

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

An issue can occur when you use `bmrsetupmaster` in the CLI to configure a BMR master server on AIX

An issue can occur when you use `bmrsetupmaster` in the command line interface (CLI) to configure a NetBackup 7.0 or greater Bare Metal Restore (BMR) master server on an AIX platform. This issue occurs because the stack size, data segment size, and max memory size `ulimit` parameters on the system are set too small. As a result, 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:

- 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` using the following commands:
 - `ulimit -s unlimited`
 - `ulimit -d unlimited`
 - `ulimit -m unlimited`
- Run `bmrsetupmaster -redo` to configure the BMR master server. You can permanently change the resource limits by manipulating the `/etc/security/limits` file on the system.

The first boot after a successful restore may fail on a Linux client if the disk order in the BIOS is not correct

The first boot after a successful restore may fail on a Linux client if the disk order in the BIOS is not the following:

Primary Master > Primary Slave > Secondary Master > Secondary Slave

For example, the order of the disks on a live client might be the following:

- `/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.

Restoring back-level clients

You can use a shared resource tree (SRT) that contains a version of the NetBackup client of 7.x or higher to restore back-level NetBackup clients.

The non-critical or non-system ZFS storage pool of an original client may become unavailable

After a system-only restore, the non-critical or non-system ZFS storage pool of the original client may be unavailable or incorrect.

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

<http://www.symantec.com/docs/TECH179039>

The spare devices and cache devices under the ZFS root pool may become unavailable

After a Bare Metal Restore (BMR) restore of a ZFS root pool, the spare devices and cache devices under the ZFS root pool may be unavailable.

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

<http://www.symantec.com/docs/TECH179040>

Mount failure of ZFS file systems

After the first boot, you may come across some issues that are related to the mount failure of ZFS file systems.

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

<http://www.symantec.com/docs/TECH179042>

A BMR restore of a Solaris client may fail if the client has a ZFS root pool containing alternate boot environments

A Bare Metal Restore (BMR) restore of a Solaris client may fail if the client has a ZFS root pool containing alternate boot environments.

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

<http://www.symantec.com/docs/TECH179043>

NetBackup Cloud operational notes

NetBackup Cloud Storage enables you to back up and restore data from cloud Storage as a Service (STaaS) vendors. NetBackup Cloud Storage is integrated with Symantec OpenStorage. This topic contains some of the operational notes and known issues that are associated with the NetBackup Cloud in NetBackup 7.7.

Verizon cloud storage servers do not support buckets created in NetBackup

When you configure a disk pool for Verizon cloud storage server, the **Add Volume** option is available to add buckets or volumes. However, Verizon does not support the buckets that are created in NetBackup. For more details about creating buckets through the Verizon portal, contact your Verizon cloud provider.

Synthetic (TIR) backups fail with status code 87 in Hitachi cloud configurations with encryption enabled

In the case of Hitachi cloud configurations, the true image restore (TIR) or synthetic backups do not work if you have enabled the encryption option. To successfully run the TIR or synthetic backups, you need to enable the versioning option for buckets (or namespaces) through the Hitachi cloud portal. For more details on how to enable the versioning option, contact Hitachi cloud provider.

Master server installation on platforms not supported by NetBackup Cloud may result in cloud storage server configuration issues

If the master server is installed on a platform that NetBackup Cloud does not support (such as Solaris x86 or Windows 2008), you may observe the following issues during cloud storage server configuration.

For the operating systems that NetBackup supports for cloud storage, see the NetBackup operating system compatibility list available through the following URL:

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

- Backup, restores, storage server properties settings, and other operations on existing Amazon S3AT&T, and Rackspace cloud storage servers using NetBackup 7.7 media server are not successful.

However, all NetBackup backups, restores, storage server properties settings, and other operations on the existing Amazon S3, AT&T, and Rackspace cloud storage servers are successful using media servers with the version older than NetBackup 7.7.

- Cloud storage server configuration for any cloud provider is not successful.

In the case of Solaris x86 master server, carry out the following steps to work around this problem:

- Identify one of the NetBackup 7.7 cloud supported media servers as *cloud_master_server_host*.
- Note that going forward, this media server does not hold the master copy of the `CloudProvider.xml` file (contains details of all supported cloud storage providers), which all media servers require while configuring the cloud storage and running operations such as backup, restore, and so on.
- Run the following command on all NetBackup 7.7 cloud supported media servers including the one that is selected as *cloud_master_host*:

```
nbcssc-t-a NetBackup  
nbcssc-s-a NetBackup-mcloud_master_host-f
```

- Make sure that the values of `CSSC_PORT` and `CSSC_IS_SECURE` as mentioned in `cloudstore.conf` file from *cloud_master_host* are copied as `CSSC_MASTER_PORT` and `CSSC_MASTER_IS_SECURE` in `cloudstore.conf` file on all other NetBackup 7.7 cloud supported media servers.
- Note that once you select *cloud_master_host*, you should not change the name again to point to another media server. If in certain scenarios, you need to do so, you should contact Symantec Technical Support.

Caution: There is no workaround for Windows 2008 to enable the support for cloud storage. You must choose a master server that has the supported cloud platform.

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

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

NetBackup cluster operational notes

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

some of the operational notes and known issues that are associated with cluster technologies in NetBackup 7.7.

A virtual name cannot resolve to both IPv4 and IPv6 addresses in clustered environments

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.

NetBackup cluster installation notes

ssh command on UNIX clusters in 7.5

UNIX `ssh` command

Starting with NetBackup 7.5, UNIX clusters can run the `ssh` command. The root user guidelines for the `ssh` command are the same as those for the `rsh` command.

UNIX cluster upgrade order

UNIX cluster node upgrade order

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

Install patch 278307 for VCS Windows before installing or upgrading to 7.1

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. For more information, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH43003>

Log on to server using virtual name

When you launch the NetBackup Administration Console, you should log into the server using the virtual name that is associated with NetBackup.

NetBackup Access Control can be configured in a clustered server environment

NetBackup Access Control (NBAC) can be configured in a clustered server environment. For more information, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH51483>

Increase resource offline timeout after installing or upgrading on non-Solaris UNIX clusters

After you install or upgrade NetBackup on UNIX clusters other than Solaris Cluster, you should increase the NetBackup resource offline timeout to at least 600 seconds.

Normal error messages when upgrading clustered servers to 7.0

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

NetBackup VCS agent's argument is not populated

During NetBackup 7.6 installation on a new Storage Foundation for Windows (SFW) VCS cluster, the NetBackup VCS agent's argument is not populated. As a result, after installation VCS cannot successfully **ONLINE** the NetBackup service group and the service group is seen in an offline state. For more information and workaround instructions, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH213303>

NetBackup resource group tuning parameters for Solaris Cluster

When you install or upgrade NetBackup on Solaris 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.

To accomplish these changes, use the following commands:

- # `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`

Note: Running these commands causes shutdown and restart of NetBackup.

NetBackup database and application agent operational notes

NetBackup offers several methods of protecting various database and application technologies, such as Oracle, Microsoft SQL Server, and Microsoft Exchange Server. This topic contains some of the operational notes and known issues that are associated with the protection of database technologies in NetBackup 7.7.

NetBackup for DB2 operational notes

NetBackup for DB2 integrates the database backup and recovery capabilities of DB2 with the backup and the recovery management capabilities of NetBackup. This topic contains some of the operational notes and known issues that are associated with NetBackup for DB2 in NetBackup 7.7.

ROLLFORWARD operation may fail for DB2 version 10 and newer if `bprestore` log directory does not exist

If the NetBackup `bprestore` log directory does not exist, a `ROLLFORWARD` operation may fail for DB2 version 10 and newer.

If you use the `USEREXIT` program to protect the DB2 archive logs and attempt to perform a restore and a `ROLLFORWARD` operation, the roll-forward may fail.

Workaround: Manually create the NetBackup `bprestore` log directory (`/usr/opensv/netbackup/logs/bprestore`).

NetBackup for Exchange and NetBackup for SharePoint operational notes

NetBackup for Exchange Server and NetBackup for SharePoint Server extend the capabilities of NetBackup to include online backups and restores of Exchange and

SharePoint databases. This topic contains some of the operational notes and known issues that are associated with NetBackup for Exchange and NetBackup for SharePoint in NetBackup 7.7.

Granular restores skip versioned documents or files that are checked out

With SharePoint 2010 and SharePoint 2013, when a document or file is enabled for versioning and is checked out at the time of backup, granular restore of such documents or files is skipped.

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

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

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

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

Restored wiki pages may not be correct

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

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

A SharePoint GRT restore of a blog post results in orphaned comments

When you use Granular Recovery Technology (GRT) to restore a blog post on SharePoint 2013, comments are restored, but they are not linked to the appropriate blog post.

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

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

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

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

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

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

GRT live browse error of a SharePoint application-aware VMware image

When you perform a live browse of VMware SharePoint application-aware backups where the Primary VM identifier is not a NetBIOS name (for example, display name or UUID), a client name like `client SP2010` becomes `client%20SP2010`. The result is that the SharePoint live browse fails with a database system error because `client%20SP2010` is not recognized as a valid client name.

Use the following workaround for this issue:

- In the NetBackup Administration Console, add an entry to **NetBackup Management > Host Properties > Master Servers > Distributed Application Restore Mapping** where the Primary VM identifier is the name of the application host, and the front-end client name is the name of the component host. If the Primary VM identifier cannot be added under **Distributed Application Restore Mapping** using the NetBackup Administration Console on the master server, then manually add the entry. For UNIX master servers, add the `SPS_REDIRECT_ALLOWED` entry to the `bp.conf` file. For Windows master servers, add an `SPS_REDIRECT_ALLOWED` registry entry.

NetBackup for Microsoft Active Directory operational notes

NetBackup for Active Directory lets you restore individual objects and attributes in the Active Directory instead of restoring the entire Active Directory. This topic contains some of the operational notes and known issues that are associated with NetBackup for Active Directory in NetBackup 7.7.

Restoring a deleted Active Directory user account using GRT restores it in a disabled state

If you perform a granular (GRT) restore of a deleted Active Directory user account, the user account is disabled. User accounts in the **Built-in** folder are not affected.

To work around this issue, open **Active Directory Users > Computers** and manually reset the password for the account and then enable the account.

SQL Server restore fails when you restore a SQL Server compressed backup image as a single stripe or with multiple stripes

This issue occurs when SQL Server is busy with the buffer of compressed data and cannot process all the data that is sent within a certain length of time. By default in Windows Server, TCP connections must close after the TCP connection state has been set to `FIN_WAIT_2` for two minutes. Refer to the following Microsoft article for more information:

<https://support.microsoft.com/en-us/kb/923200/>

Note: If the **TCPFinWait2Delay** value does not exist, you must create it as a `REG_DWORD` registry value. Otherwise, Windows uses the default value of **240**.

To increase the time that TCP connections may remain in the `FIN_WAIT_2` state

- 1 On the NetBackup media server, open `regedit.exe`.
- 2 Locate and select the following registry subkey:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
- 3 Double-click on **TCPFinWait2Delay**.
- 4 Enter a value of **300**.
- 5 Restart the media server.
- 6 After the restore completes successfully, remove the registry setting or change the setting to its original value.

When you increase the value of this setting it has an adverse effect for all TCP/IP connections. This higher value could cause port exhaustion for other applications that run on the media server.

- 7 Restart the media server.

NetBackup deduplication operational notes

NetBackup provides several deduplication options that let you deduplicate data everywhere, as close to the source of data as you require. Deduplication everywhere lets you choose at which point in the backup process to perform deduplication. NetBackup can manage the deduplication of environments that use the NetBackup Deduplication Engine. This topic contains some of the operational notes and known issues that are associated with the NetBackup Deduplication Engine in NetBackup 7.7.

For the most up-to-date compatibility information for MSDP, see the *NetBackup Enterprise Server and Server OS Software Compatibility List* at the following location:

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

New versions of NetBackup may significantly modify MSDP deduplication database

New versions of NetBackup may occasionally introduce significant changes to the underlying MSDP technologies. These types of changes often result in major modifications to the MSDP deduplication database during and after upgrade. Examples of these types of changes include the switch over to LZO compression in NetBackup 7.1 and the database conversions that occurred in NetBackup 7.6 and 7.6.1.

Internationalization and localization operational notes

This topic contains some of the operational notes and known issues that are associated with internationalization, localization, and non-English locales in NetBackup 7.7.

Certain NetBackup user-defined strings must not contain non-US ASCII characters

Specific NetBackup user-defined strings must not contain non-US ASCII characters.

The following NetBackup user-defined strings must not contain non-US ASCII characters:

- Host name (master server, media server, Enterprise Media Manager (EMM) server, volume database host, media host, client)
- Policy name

- Policy KEYWORD (Windows only)
- Backup, Archive, and Restore KEYWORD (Windows only)
- Storage unit name
- Storage unit disk pathname (Windows only)
- Robot name
- Device name
- Schedule name
- Media ID
- Volume group name
- Volume pool name
- Media description
- Vault policy names
- Vault report names
- BMR Shared Resource Tree (SRT) name

Restricted support for localized environments in database and application agents for all supported platforms

Database and application agents have restricted support of localized environments for all supported platforms.

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

- Any database object names. For example, database, tablespace, file group, data files, portals, etc.
- Any path names of database files, directories, transaction logs, or other database storage locations.
- Any path names that are specified in the policy backup selection. For example, notification script, template, or batch file.

Do not run language packs that are not at the same version level as the English version

Symantec does not recommend running any language packs that are not at the same level as the English version. For example, do not run the NetBackup 7.6

Language Pack with the English version of NetBackup 7.7. Please remove any previously installed language packs before updating the English version.

NetBackup LiveUpdate operational notes

NetBackup LiveUpdate provides a cross-platform, policy-driven method to distribute NetBackup Release Updates and hot fix downloads to NetBackup hosts at version 6.5 and later. Starting with NetBackup 7.1, NetBackup LiveUpdate also supports upgrades to major releases and minor releases for NetBackup clients. This topic contains some of the operational notes and known issues that are associated with LiveUpdate in NetBackup 7.7.

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

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

Attempts to use LiveUpdate to install or upgrade to NetBackup 7.7 can fail because the target host has an incompatible version of Java JRE installed

Attempts to use LiveUpdate to install or upgrade to NetBackup 7.7 can fail because the target host has an incompatible version of Java JRE installed.

The Java LiveUpdate (JLU) agent requires that a minimum version of Java JRE be installed. For most UNIX platforms, NetBackup delivers a Java JRE version that meets or exceeds this minimum requirement. However, Java is no longer included in the NetBackup installation packages for a few specific UNIX platforms. Upgrading NetBackup with one of these packages results in the removal of Java versions that NetBackup might have previously installed.

The push and silent installation methods do not install the LiveUpdate agent as part of the package

The push and silent installation methods do not install the LiveUpdate agent as part of the package. To install the LiveUpdate agent, Symantec recommends that you copy the LiveUpdate binaries to the local host and install the LiveUpdate agent manually. The LiveUpdate binaries are available at the following location:

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

For more information about 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.

Error during upgrade of an HP PA-RISC client to NetBackup 7.6 using LiveUpdate

When using NetBackup LiveUpdate to upgrade an HP PA-RISC client to NetBackup 7.6, you can encounter an error if that client has the following configuration:

- The directories `/dev/random` and `/dev/urandom` exist.
- The default system Java JDK/JRE level is between version 1.6.0 and 1.6.0.16. To verify the current JDK/JRE version level, run the following command:

```
java -version
```

If you want to use LiveUpdate to upgrade an HP PA-RISC client to NetBackup 7.6, you can perform either of the following two options to avoid this issue:

- Option 1:
In the default system java security file (for example, `/opt/java6/jre/lib/security/java.security`), change the following:
`securerandom.source=file:/dev/urandom`
To:
`securerandom.source=file:/dev/random`
- Option 2:
Upgrade the default system Java JDK/JRE level to version 1.6.0.16 or later.

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

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

You should make sure that `/usr/opencv/java/jre/bin/java` is a symbolic link to the default system Java binary. Then perform one of the two previous options or rerun the failed NetBackup LiveUpdate job.

NetBackup Logging Assistant operational notes

This topic contains some of the operational notes and known issues that are associated with the Logging Assistant in this release of NetBackup.

Modifying logging levels in the NetBackup Administration Console can change the global logging level and VxUL debug levels

Under certain conditions in NetBackup 7.6, modifying logging levels in the NetBackup Administration Console can result in unintentional changes to the global logging level and VxUL debug levels. These changes can cause information not to be logged as expected.

Note: If you upgrade to NetBackup 7.6, logging continues to work normally. An upgrade by itself does not change logging levels and you should encounter no issues.

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

<http://www.symantec.com/docs/TECH212610>

NetBackup for NDMP operational notes

NetBackup for NDMP is an optional NetBackup application. It enables NetBackup to use the Network Data Management Protocol (NDMP) to initiate and control backups and restores of Network Attached Storage (NAS) systems. This topic contains some of the operational notes and known issues that are associated with NetBackup for NDMP in NetBackup 7.7.

NDMP multiplexed (MPX) restores may generate excessive log messages and cause Activity Monitor to hang

NetBackup NDMP multiplexed (MPX) restores may generate excessive numbers of messages to the `bptm` log and cause the `bptm` program and the Activity Monitor to hang. This issue can occur when a `NON_MPX_RESTORE` touch file exists on the NetBackup master server. This issue applies only to NDMP MPX restores on both UNIX and Windows platforms.

For information on a workaround for this issue, please see the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH207556>

Parent directories in the path of a file may not be present in an NDMP incremental image

An issue can occur if a NetBackup Network Data Management Protocol (NDMP) backup policy is configured with the directive `set type=tar` in the backup selection. Parent directories in the path of a file that an incremental NDMP backup saves may not be present in the backup image. For more information on this issue, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH202412>

NetBackup OpsCenter operational notes

NetBackup OpsCenter is a web-based software application that helps organizations by providing visibility into their data protection environment. By using NetBackup OpsCenter, you can track the effectiveness of backup operations by generating comprehensive reports. This topic contains some of the operational notes and known issues that are associated with OpsCenter in NetBackup 7.7.

Note: OpsCenter is a convergence of NetBackup Operations Manager (NOM) and Veritas Backup Reporter (VBR) and is available in the following two versions: Symantec NetBackup OpsCenter and Symantec NetBackup OpsCenter Analytics. Starting with NetBackup 7.0, NOM has been replaced with OpsCenter. If your current NetBackup environment includes NOM or VBR, you must first upgrade to OpsCenter 7.0 or 7.1 before you can upgrade to a later version of OpsCenter.

For more information about upgrading OpsCenter, refer to the *NetBackup OpsCenter Administrator's Guide*.

OpsCenter no longer supports NetBackup 6.x

Starting with version 7.6.1, NetBackup OpsCenter no longer supports NetBackup 6.x.

database.conf overwritten by non-default installation location

During an upgrade to NetBackup OpsCenter 7.6 or 7.6.1, if you want to use a non-default location for installation, make sure that the installation directory that you choose is different than the backup directory. If both directories are the same, the `database.conf` (a backup file) is overwritten and the OpsCenter services do not start.

NetBackup OpsCenter branding and name changes in NetBackup 7.6

The following NetBackup OpsCenter branding and name changes take effect in NetBackup 7.6:

- Symantec OpsCenter has been changed to Symantec NetBackup OpsCenter.
- Java View Builder has been changed to Symantec NetBackup OpsCenter Analytics View Builder.

NetBackup 7.6 Support Changes

The following list contains some of the Symantec NetBackup OpsCenter support changes which take effect in NetBackup 7.6:

- NetBackup OpsCenter Server is no longer supported on HP-UX 11.31 IA64.
- NetBackup OpsCenter Server is no longer supported on AIX 6.1 and 7.1 64-bit POWER.

Unable to set different alert.conf water mark thresholds

The water mark threshold in the `alert.conf` file is a global setting and is applicable for all disk pools for all selected NetBackup master servers in Disk Full alert policies. You cannot set up different thresholds for different master servers or different alert policies.

For more information, refer to the following HOWTO article:

<http://www.symantec.com/docs/HOWTO94997>

Note: Note: If you select individual disk pools when you configure a Disk Pool Full alert policy, no alerts are generated. You should select a master server instead of individual disk pools.

Language packs cause OpsCenter upgrade from 7.1 or 7.5 to 7.6 to fail

On 64-bit Windows systems, if OpsCenter language packs or maintenance (triple-dot) releases are installed on top of an installation of version 7.1 or version 7.5, an upgrade to OpsCenter 7.6 may fail. For example, if you upgrade OpsCenter 7.5 to version 7.5.0.6, an upgrade to OpsCenter 7.6 may fail.

For upgrade and workaround instructions, please see the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH211070>

Incomplete uninstall of maintenance releases

Uninstalling OpsCenter software may not completely uninstall maintenance releases on Windows. OpsCenter maintenance releases may still be visible in the Windows system program uninstaller.

For more information and workaround instructions for this issue, see the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH211299>

Report export location determined by web browser

The **Settings > Configuration > Report Export Location** determines where scheduled reports are saved. However, when you select **Export Report** in the OpsCenter console, your web browser settings determine the export location. For example: The location that is specified in **Firefox > Options > General > Save files to** determines where non-scheduled reports are saved.

Ampersand prevents user from being edited

OpsCenter user names that contain an ampersand (&) cannot be edited after an upgrade to version 7.6. After upgrade, user edits such as reset password, enable and disable, and change user role can fail. For fresh installations of version 7.6, the issue only prohibits resetting the user's password. In both cases, the edits fail with the following message:

```
Error performing User action.
```

During a password reset operation, the user name only displays with the characters before the ampersand.

Add and monitor NetBackup 2.6 appliances

In OpsCenter 7.6, you can add and monitor NetBackup 2.6 appliances. You can also collect certain hardware information from the appliances.

Accessing OpsCenter console using Internet Explorer

Extra steps are required to access the OpsCenter console using Internet Explorer version 6, 7, or 8 on a 32-bit Windows computer. For more information, see "About web browser considerations" in the *NetBackup OpsCenter Administrator's Guide*, available from the following location:

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

Unable to log in to OpsCenter on UNIX system if Korn shell is not installed

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

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

Cloud metering data collection failure due to unreachable server

A cloud metering data collection failure can occur if one or more media servers with credentials to access a cloud storage server (data movers) is unreachable for some reason.

Workaround: From the unreachable media server, use `tpconfig` to remove the credentials of that media from all cloud storage servers on the master. Cloud metering data collection should then succeed. All the cloud metering data from the media servers that were missed earlier can now be collected.

Nodes with attached objects in View Builder temporarily disappear when moved

In the OpsCenter Analytics View Builder, if you move a node that has any objects that are assigned to it within a view, the object may seem to appear missing after the move operation. In this case, the object is temporarily invisible and becomes visible over time.

To work around the issue, Symantec recommends that you wait for some time and then log back in to the view builder to see the updated view.

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

Data collection fails if storage unit path is more than 256 characters

In NetBackup OpsCenter 7.6 and earlier releases, data collection by OpsCenter fails if the specified basic-disk storage unit (STU) path is more than 256 characters.

To work around the issue, you must create a storage unit path that has 256 characters or less.

Blank report when only Include Accelerator Job Only is selected

Certain reports do not show any data when the **Include Accelerator Job Only** filter is applied for a NetBackup master server at Version 7.5 or 7.5.0.x. These reports include any Tabular Backup reports or any Custom reports that include accelerator data-related columns. The reports do not show any data because NetBackup Accelerator support is enabled in NetBackup OpsCenter 7.6.

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

Browse functionality is not supported on IE8

The Browse functionality in Operational Restore is not usable with some variants of the Internet Explorer 8 browser. To use the Browse functionality in Operational Restore, Symantec recommends Internet Explorer 9 or newer, or Firefox.

Browse and Select client functionality displays NetApp volume as client name for Replication Director VM backups

For OpsCenter restore, the **Browse and Select client** functionality result displays the NetApp volume as the client name for Replication Director VM backups. This selection does not display any files. For browsing the files and directories and for performing an operational restore, it is necessary to select the actual VM client name.

Cannot collect data from unsupported EV, TSM, or EMC servers

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

For more detailed information on product support in OpsCenter 7.6, see the *NetBackup OpsCenter Administrator's Guide*.

database.conf should contain only database location string

During an OpsCenter database upgrade, if you have customized the `database.conf` file, make sure that it contains only the database location string. If the file contains characters or strings other than the database location, a database upgrade does not succeed. If you want to change the database path, you should replace the original path with the new one instead of commenting out the original path. If you need a reference, you can create a backup copy of the original `databases.conf` file with a different file name.

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

- <http://www.symantec.com/docs/TECH205138>

Report emails fail to deliver if attachments are too large

The reports email may not be received when the reports are scheduled in bulk.

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

Cannot assign alerts to new users until they log on

In OpsCenter 7.6, you cannot assign any alerts to a newly added OpsCenter user. The new users are not listed on the **Monitor > Alerts** page in the **Assigned To** column. New users must log on to OpsCenter first before they appear in the **Assigned To** column. Once a user appears in the column, you can then assign the alerts to that specific user.

New users not visible in Copy User Profile

A newly created user is not listed in the drop-down list for **Copy User Profile**

As a new user, to work around this issue you need to log into OpsCenter with the newly-created user name and then log out. The new user name is registered with **Copy User Profile** after it has logged on at least once. The user name should then appear in the **Copy User Profile** drop-down list.

Backup Exec data collection fails if server password contains HTML characters

If the Backup Exec server password contains HTML characters such as `&`, `<`, `>`, or `/`, and you make edits to the Backup Exec data collector on OpsCenter, it causes the data collection to fail.

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

- Change the password of the Backup Exec server to a non-HTML character password.
- Delete the existing entry of the Backup Exec data collector and add a new entry.

OpsCenter Monitor File List tab shows empty for active jobs

When jobs are viewed from OpsCenter Monitor, the **File List** tab shows up empty for active jobs.

In OpsCenter 7.5 and forward, the **File List** tab appears to be empty when the job is in progress. The **File List** tab gets populated only when the job is successfully completed.

Special characters in subgroup name prevent users from being authorized

Users that are part of a subgroup with special characters do not get authorized.

If a subgroup name has special characters, then the authorization fails to return the parent or chain-of group names. The parent or chain-of group names are required to determine if any of the parents is an OpsCenter user. Therefore, users who are part of subgroup that contains special characters like "PD_#QE%" do not get authorized.

Undefined JAVA_HOME or JRE_HOME variables after you run a third-party utility

After you install OpsCenter, if you run a third-party utility, such as `version.sh` in Tomcat, you get the following error message:

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

If you encounter this issue, use the following workarounds:

- For Windows: After you install OpsCenter, you have to first execute the command `setEnv.bat` and then run any third-party utility.
The path for `setEnv.bat` is `INSTALL_PATH\OpsCenter\server\bin`.
- For UNIX: After you install OpsCenter you have to first execute the command `setEnv.sh` and then run any third-party utility.
The path for `setEnv.sh` is `<INSTALL_PATH>/SYMCopsCenterServer/bin`.

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

Duplicate entries in Monitor and Views interfaces

In certain scenarios, duplicate entries of a client are displayed on the **Monitor** and **Views** interfaces.

This issue is seen in any of the following scenarios:

- A NetBackup master server is used as a client in one or more policies.
- Some NetBackup policies refer to a NetBackup master server with a fully qualified domain name (FQDN) while others refer to it with a short name.
- The actual name of the master server does not match its network name or display name that is used in OpsCenter.

The following is an example scenario of the issue:

The actual name of the NetBackup master server is `abc.xyz.com`. The network name or display name that is used in OpsCenter is `xyz`.

In this scenario, if `abc.xyz.com` is used as a client in one or more NetBackup policies, duplicate entries of this client are displayed on the following OpsCenter screens:

- **Monitor > Host > Client**
- **Settings > Views > Manage Nodes and Objects > Objects not in selected view**

Alert email for each volume if OpenStorage alert policy is configured

If an OpenStorage alert policy is configured, then OpsCenter generates an alert (email) for each volume.

To work around this issue, you can filter the volume type alert by specifying the text (for example: With volume name, not protected for any volume, and as required) in the field that is provided for the **Event message contains word(s)** selection. OpsCenter generates the alert only when the NTAP event contains the text that is specified in **Event message contains word(s)** selection.

Job collection fails on master server if port 1556 is not open bi-directionally

OpsCenter job collection from master servers could fail if port 1556 is not opened bi-directionally on both the NetBackup and OpsCenter sides.

Support for 64-bit software on Windows

As of OpsCenter 7.5, Symantec OpsCenter Agent supports 64-bit software on Windows systems. 32-bit Agent software is not supported on 64-bit Windows systems in versions 7.5 and later. The installer automatically installs 64-bit Agent software on a 64-bit Windows system.

Running Capacity Licensing reports

To run a Capacity Licensing report in NetBackup 7.7, a user name and password are required for each master server. To successfully run a report for any master servers that were added to OpsCenter in versions previous to 7.5.0.5, an extra step is required. The user name and password credentials for each master server must be entered manually in the NetBackup configuration settings. If the credentials are not added in the configuration settings, a user name and password error is returned when the report is run.

Additionally, for Capacity Licensing to work correctly, please refer to the following tech note and install the specified EEBs:

<http://www.symantec.com/docs/TECH148678>

Data format in SFR Timeline shown as "unknown"

In the SFR Timeline View, for the images that are collected in OpsCenter, the data format is shown as `unknown` because of the lack of data.

OpsCenter does not support creating or editing multiple reports simultaneously for the same user session from different tabs or windows

OpsCenter does not support creating or editing multiple reports simultaneously for the same user session from different tabs or windows. You cannot open the same OpsCenter console in two or more browser tabs or windows and create or edit standard and custom reports simultaneously. That causes an exception to occur.

Deduplication reports show no data when Report On is set as Storage unit Name

The Deduplication reports do not show any data when you select the **Report On** parameter as **Storage Unit Name**.

Search and Restore operations in VMware and Hyper-V

For VMware or Hyper-V clients, the search and restore operations work only if the client name is the same as host name. If the client name is the same as display name, UUID, or DNS name then only the Search functionality is available. You cannot perform restore operations in this case. The following table provides details on whether Search and Restore functionality is available when the client name is the host name, display name, etc.:

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

OpsCenter installation and deployment information and best practices

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

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

File selection lists with more than 50 items do not appear in OpsCenter

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

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

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

OpsCenter does not provide the option to purge breakup jobs

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

Canceled or interrupted uninstall removes uninstall script

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

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

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

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

Character limitation for virtual host names on Windows

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 must contain fewer than 15 characters.

Some reports may only consider Full and Incremental schedule type jobs

When the user applies a 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

NetBackup OpsCenter must be brought online manually

The `NetBackupOpsCenter` resource is offline after you have installed an OpsCenter cluster.

After installing an OpsCenter cluster on a Windows 2008 R2 x64 system, you must manually bring the `NetBackupOpsCenter` resource online. You can bring the `NetBackupOpsCenter` resource online from the command line interface or by using the cluster user interface.

You can use the following command:

```
hares -online <resource name> -sys <Name of the active node> Example:  
hares -online newonlatest-OpsCenter -sys OPS-CLUSTER-1
```

Missing log.conf file on Windows systems

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`

OpsCenter object merger utility fails on master server

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.

Custom Tabular Backup and Custom-Client count report returns no data

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.

OpsCenter server stops receiving events from master server after NetBackup upgrade

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

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

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

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

Users can now search for clients from the Monitor>Hosts>Clients page (but not by attribute)

An enhancement has been made in OpsCenter to maintain VBR parity.

You can now search for clients from the **Monitor > Hosts > Clients** page. You can use host names or substrings to accomplish that.

However, you can only search for clients and not other attributes such as, **CPU Count**, **CPU Speed**, **Discovered Agent Server**, and others.

Job Count Workload Analyzer summation rules

An issue occurs in the **Job Count Workload Analyzer**: For each cell, the sum of occurrences differs from the total in the first column when the time basis that is selected is **Active**. That is expected because a job can be active and span across a multiple-hours time frame. Hence, the same job is counted for all the hours. But the count in the first column shows the exact count of jobs that were active for these 7 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.

Upgrading from NOM to OpsCenter causes Master server job throughput report to appear without an output

The **Master server job throughput** report appears without a report output in **My dashboard** after an upgrade from NOM to OpsCenter. The reason is that it is an SQL query-based report and is a part of composite report that is not migrated in the dashboard.

Daylight Savings Time support for historical reports in OpsCenter

Daylight savings time (DST) support for Historical reports in OpsCenter

If data for the historical reports is synchronized during the hour when daylight savings time begins, it can cause problems in a distributed database system. The user can also lose data.

A workaround is to use Universal Time (UTC) as the time zone, or use a time zone that does not have daylight savings time.

To set the time zone, refer to the *Symantec OpsCenter Administrator's Guide*.

When you upgrade from OpsCenter 7.0.x to 7.x, the Installation Choice screen displays available space on system drive

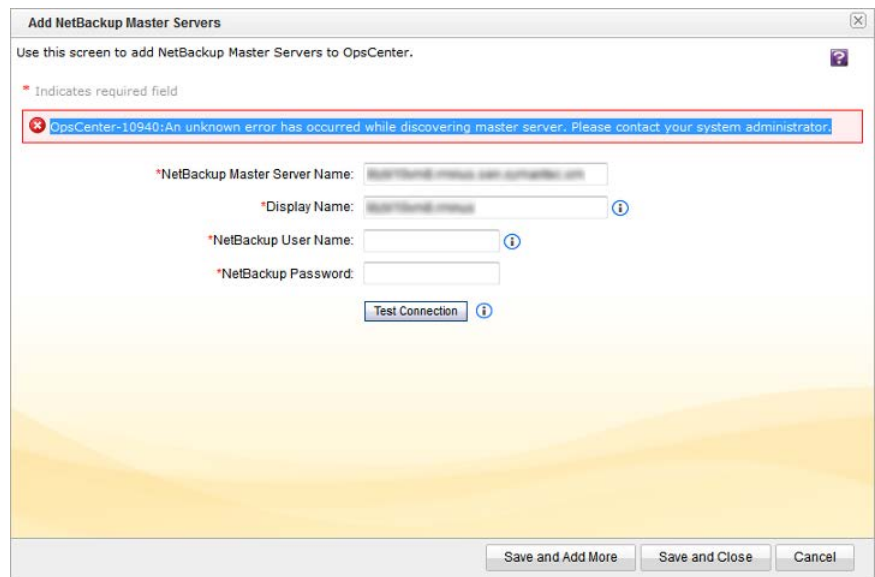
When you upgrade from OpsCenter 7.0.x to OpsCenter 7.x, the Installation Choice screen displays the available space on the system drive. This issue occurs even if your previous installation is on a different drive (a drive other than the system drive).

OpsCenter cannot monitor IPv6-only servers

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.

OpsCenter interface returns non-specific error after it fails to connect to a master server

If the NetBackup OpsCenter server cannot connect to the specified master server under **Getting Started > Add NetBackup Master Servers**, OpsCenter returns an unknown error.



The screenshot shows a window titled "Add NetBackup Master Servers". Inside, there is a message box with a red "x" icon and the text: "OpsCenter-10940: An unknown error has occurred while discovering master server. Please contact your system administrator." Below the message box, there are four input fields, each with an asterisk indicating it is required: "NetBackup Master Server Name:", "Display Name:", "NetBackup User Name:", and "NetBackup Password:". Each field has a placeholder text "XXXXXXXXXX" and an information icon (i) to its right. Below the fields is a "Test Connection" button with an information icon. At the bottom of the window are three buttons: "Save and Add More", "Save and Close", and "Cancel".

Make sure that you have specified the correct **NetBackup Master Server Name** and that the master server is connected to the network.

The NetBackup Disk Pool Size vs. Percentage Full report may show incorrect data

OpsCenter's NetBackup Disk Pool Size vs. Percentage Full report may show incorrect data when OpsCenter does not have disk pool size data for one or more days.

This issue occurs because the report calculates disk pool sizes every day and shows the average values in report. Missing data for any day that falls within the selected report time frame generates incorrect average data.

OpsCenter reports display IP addresses for some VMs

OpsCenter reports display IP addresses for some of the listed virtual machines (VMs). OpsCenter tries to alias these IP addresses with their respective VM names and host names when that information is available. For this aliasing to reflect in the reports, OpsCenter services need to be restarted. Please note that if a VM's name and host name are not available in the OpsCenter database, then that VM's IP will still appear in the reports.

OpsCenter displays incorrect OS level for Windows Server 2012 R2

NetBackup OpsCenter displays an incorrect operating system for a Windows Server 2012 R2 master server host. Instead of Windows Server 2012 R2, OpsCenter displays "Windows Server 2012" in the **Operating System** column under **Settings > Configuration > NetBackup**.

Issues accessing an OpsCenter Server from the remote OpsCenter View Builder on a Windows computer

If you use a remote OpsCenter View Builder on a Windows computer that does not host the OpsCenter database, you may encounter database connection issues.

This problem can arise in any of the following scenarios:

- When the network name and the host name of the OpsCenter Server do not match
- When the OpsCenter Server host and the remote View Builder host are in different domains

To work around this issue, do the following:

1. Add the OpsCenter Server host name to the View Builder's `etc/hosts` file.
2. Add the View Builder host name to the OpsCenter Server's `etc/hosts` file.

Note: Ensure that you add both the short name and the fully qualified domain name (FQDN) of the host to the `etc/hosts` file.

NetBackup OpsCenter no longer supports Search & Hold

When you upgrade to OpsCenter version 7.7, you cannot perform a search (related to Search & Hold) for backup images. The existing saved searches and their corresponding results are deleted. OpsCenter continues to show certain hold related information about backup images and media. You cannot create new legal holds from OpsCenter. Upgrade NetBackup master server to version 7.7 after you upgrade OpsCenter to version 7.7 to convert the existing legal holds to user holds. The user holds can then be managed by using the `nbholdutil` command in NetBackup 7.7. For more information about the command, see the Symantec NetBackup Commands Reference Guide.

The following changes are carried out for OpsCenter reports in 7.7:

- The predefined reports that are related to Search & Holds are deleted.
- The columns that are related to Indexing for Search in the saved custom reports might show incorrect data. Symantec recommends that you edit such reports to delete those columns.
- The columns that are related to Indexing for Search in the custom SQL reports might show incorrect data. Symantec recommends that you edit such reports to delete those columns. For more information, see the Symantec NetBackup OpsCenter Reporting Guide.

For more information, see the Symantec NetBackup OpsCenter Reporting Guide.

Dropped support for Solaris and UNIX clusters

NetBackup OpsCenter 7.7 no longer supports Solaris and UNIX clusters.

For a complete list of supported software and hardware, see the NetBackup master compatibility list: <https://www.netbackup.com/compatibility>

NetBackup Replication Director operational notes

Replication Director is the implementation of NetBackup OpenStorage-managed snapshots and snapshot replication, where the snapshots are stored on the storage systems of partnering companies. Replication Director uses an OpenStorage plug-in on the media server to communicate with the disk array (through the storage server) and to make requests to move data. The OpenStorage partner also hosts a software plug-in that allows communication between NetBackup and the disk array. This

topic contains some of the operational notes and known issues that are associated with Replication Director and its associated plug-ins in NetBackup 7.7.

Replications fail after point-in-time restore with NBUPlugin 1.1

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

This issue relates to replication job failures for the policies that are configured for Replication Director. This issue occurs when NBUPlugin 1.1 is used under the following circumstances:

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

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

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

The replication jobs fail because the PIT restore deletes the base snapshot (given that the specified option was enabled for the restore). The Replication operation did not have the base snapshot to replicate.

To return to successful replication jobs, resynchronize the relationship between the primary volumes and the target volumes using the NetApp CLI.

NBUPlugin 1.1 replication fails with error code 84

For NBUPlugin 1.1, replication can fail with error code 84 (media write error) if both of the following conditions are true:

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

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

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

Database system error when browsing files in "Backup, Archive, and Restore" interface

When you browse the files in the **Backup, Archive, and Restore** user interface, the following error may be reported:

```
ERROR: database system error
```

This message can indicate a variety of issues, such as an unsupported file system, a snapshot mount failure, or other hardware or networking problems.

Indexing logs grow very large when log level set to 4 or higher

The size of the `ncflbc` and `ncfnbhf` logs that are generated as a result of an indexing job can be very large. The size of the log files can grow rapidly when the log level is set to 4 or higher.

To work around this issue, you can lower the NCF logging level (to 3 or less). In addition, you can adjust the log file rollover mode, maximum log file size, or number of log files if you want to continue to accommodate a higher NCF logging level.

Discovery fails on VMs running vCenter 2.5 or ESX 3.5 and older

Discovery can fail on virtual machines running vCenter 2.5 or ESX 3.5 and older. Note that vCenter versions before version 4 are not officially supported.

Hardware snapshot generated on boot disk even when "Virtual disk selection" is set to "Exclude boot disk"

A hardware snapshot occurs on a boot disk even when **Virtual disk selection** is set to **Exclude boot disk** on the **Advanced** options of the **VMware** policy tab.

This option only applies when a Backup From Snapshot operation is performed and a tar image is created of the VM in the snapshot.

Backup in SLP using NetBackup Accelerator fails with status code 13 if storage read speed is very slow

A NetBackup Accelerator-enabled Backup operation in an SLP can fail with status code 13 (file read failed) if it encounters very slow storage read speeds. In particular,

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

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

Instance group names cannot be localized for Oracle Intelligent Policy

For Oracle Intelligent Policy, instance group names cannot be localized.

Volume GUID not supported for VSS

For VSS, the Volume GUID is not supported.

Activity Monitor may show wrong Kilobytes value for snapshot jobs if policy has alternate client configuration

For policies with alternate client configuration, the Activity Monitor may show the wrong value in the **Kilobytes** column for snapshot jobs.

Snapshot of NFS mount fails with status code 20 on Linux

A snapshot job of an NFS mount can fail with status code 20 on Linux due to an NFS remount failure. However, subsequent runs of the snapshot job may succeed.

Test Query option in Query Builder may incorrectly display VMs which will not be selected for backup job

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

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

Review the Test Query results carefully. Note that only VMs on an NFS datastore get backed up by Replication Director.

NetApp Plug-in for NetBackup 1.0.1 crashes under certain circumstances

The NetApp Plug-in for Symantec NetBackup version 1.0.1 can crash under the following circumstances:

- Running an NDMP storage lifecycle policy
- Export workflow (indexing, backup, restore, or browse)
- Export for copy 2 or 3 (not for copy 1)

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

Replication may fail on NetApp Plug-in for NetBackup 1.0.1 under certain conditions

You may experience replication failures if you use the NetApp Plug-in for Symantec NetBackup version 1.0.1. Replication can fail if all the following conditions are met:

- Multiple volumes are present in the backup selections
- The destination is SnapMirror
- At least 60% of the volume is full
- NAS storage is used

The following are some of the symptoms that may indicate failures:

- In the NetBackup Activity Monitor:

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

- In the `bpdm` logs:

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

- In the NetApp Management Console:

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

Snapshot leaks when cleaning up all images for policies with Primary > Mirror topologies

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

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

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

Incremental backups created with Replication Director may throw error: "unable to obtain list of files using specified search criteria"

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

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

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

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

If VM and its datastore have identical names, the Backup, Archive, and Restore client interface displays two separate images

Replication Director for virtual machines:

If the virtual machine and its datastore have identical names, the Backup, Archive, and Restore client interface displays two separate images when you browse to restore the virtual machine or its files. The image with an `OST_FIM` image format should not be displayed. If the virtual machine has more than one datastore, this `OST_FIM` image may not present all the data that the virtual machine contains. Do not use the `OST_FIM` image: Select the other image for restore.

This issue will be fixed in a future NetBackup release.

BAR interface accesses files directly from snapshot if storage lifecycle policy is not configured to index VM (or if indexing does not complete)

If the storage lifecycle policy (SLP) was not configured to index the virtual machine (or indexing is not complete), the BAR interface accesses the files directly from the snapshot. When you browse the files, the message `ERROR: database system error` may appear. This message can indicate a variety of issues, such as an unsupported file system, a snapshot mount failure, or other hardware or networking problems.

Backups and restores from snapshots on RHEL 5.3 operating systems do not work properly due to lack of support from NetBackup 7.6

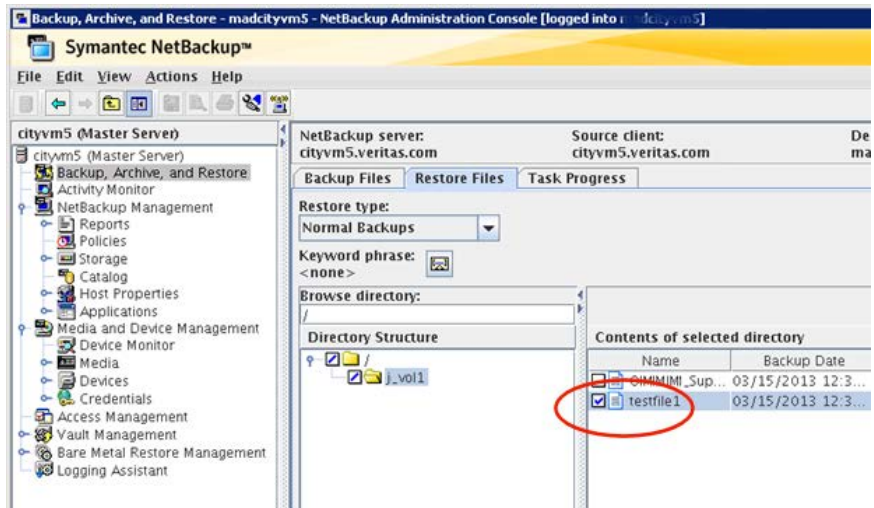
Problems with backups and restores exist on RHEL 5.3 operating systems with kernel version 2.6.18-128.el5. Backups and restores from snapshots do not work properly because of an issue with the `kobject_add` process. The issue occurs because NetBackup 7.6 does not support this kernel version. This kernel version is supported with the release of RHEL 5.9.

For more information, refer to the *NetBackup Replication Director Solutions Guide*.

Restoring from a differential incremental backup at the volume level can result in data loss

Normally, when a single file is restored from an incremental backup, only the file that is selected from that backup is restored. In certain situations using Replication Director, however, not only is the selected file restored, but all of the other files in the backup are restored as well. The restore can possibly overwrite the files that have changed since the incremental backup was performed, leading to data loss.

To avoid unintentionally overwriting the files that have changed since the last incremental backup, do not select the entire volume in the **Backup, Archive, and Restore** interface. Instead, select only the file that you want to restore. In the following example, `testfile1` is correctly selected for restore.



SnapVault replication may result in data loss if the qtree has not been updated in the DFM server

A qtree that has been newly added to a volume may not be protected by a Replication Director policy if the storage lifecycle policy indicates a **Snapshot-to-Replication** (SnapVault) topology.

Before the Replication Director policy runs, use the DataFabric Manager server interface to verify that any new qtrees in a volume have been updated. The new qtrees in the volume are not updated frequently due to a restriction on the NetApp DFM server.

The Replication Director policy may run without incident, but the qtree may not appear in the vaulted replica when browsing with the NetBackup **Backup, Archive, and Restore** interface.

For more information, see the *NetApp Plug-in 1.1 for Symantec NetBackup*:

https://library.netapp.com/ecm/ecm_download_file/ECMP1140478

(Access to the NetApp site requires a logon.)

Replication Director policy validation takes a long time to complete

The Replication Director policy validation can take a long time to complete. You cannot perform other operations until this operation completes. Open a new instance of the NetBackup Administration Console to perform other operations.

Resilient network operational notes

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

- Resilient network connections are not supported in a NetBackup cluster environment.

NetBackup Search operational notes

NetBackup Search provides a mechanism to index the file system metadata that is associated with NetBackup backup images. With indexed backup images, searching for relevant information is simple, powerful, and fast.

NetBackup Search functionality not supported in 7.7 and later

Starting with Release 7.7, NetBackup no longer supports the NetBackup Search functionality. When you upgrade to NetBackup 7.7, the information related to NetBackup Search, including indexing of backup images is deleted. You might continue to see old indexing jobs in the Activity Monitor. The Hold functionality and the existing holds are retained.

Symantec recommends that you uninstall the NetBackup Search software from the indexing servers.

When you upgrade OpsCenter to 7.7, the legal holds are converted to user holds, which can be managed by using the `nbholdutil` command. If a legal hold is found to have the same name as that of an existing user hold, all the hold names are renamed to avoid conflicts. For more information about conversion of hold names and managing holds, see *Symantec NetBackup Administrator's Guide, Volume I*.

NetBackup Snapshot Client operational notes

NetBackup Snapshot Client provides a variety of snapshot-based features for NetBackup. It supports clients on UNIX, Linux, and Windows platforms, on Fibre Channel networks (SANs) or traditional LANs. Each snapshot method relies on the snapshot technology that is built into the storage subsystem where the data is stored. This topic contains some of the operational notes and known issues that are associated with Snapshot Client in NetBackup 7.7.

Logs for legacy processes are less verbose than in previous releases

In NetBackup 7.7, logs for legacy processes will be less verbose than they were in previous releases. The default logging level in NetBackup 7.7 is 0, which is the minimum logging level. To restore the same level of verbosity seen in previous releases, set the logging level higher than 0. This issue does not impact Unified logging processes.

FlashBackup is not supported with Storage Foundation 6 or greater volume manager

FlashBackup is not currently supported with Storage Foundation 6 or greater volume manager.

A Standard policy that is configured with certain selections causes the Policy Execution Manager to crash and generate a core dump with an assertion failure

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

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

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

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

Cannot create a disk array snapshot if a VxVM disk group on the array contains a software-based snapshot of the VxVM volume

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.

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."

Multi-stream policy backups fail due to missing files

When using snapshot backups, if a multi-stream policy backup fails with error code 71 or 227 due to missing files, subsequent retries do not detect the missing files even if they become available during the designated Job Retry Delay period.

NetBackup virtualization operational notes

NetBackup offers several methods of protecting virtual environments. The two primary virtualization technologies that NetBackup can protect are VMware and Hyper-V, although NetBackup can protect other virtualization technologies as well. This topic contains some of the operational notes and known issues that are associated with the protection of virtualization technologies in NetBackup 7.7.

NetBackup for VMware operational notes

NetBackup for VMware provides backup and restore of the VMware virtual machines that run on VMware ESX servers. Additionally, the NetBackup plug-in for VMware vCenter (vCenter plug-in) allows the vSphere Client to monitor virtual machine backups and recover a virtual machine from a backup. This topic contains some of the operational notes and known issues that are associated with NetBackup for VMware and the vCenter plug-in in NetBackup 7.7.

VMware web client does not allow SAN restores

The 6.0 release of the Virtual Disk Development Kit (VDDK) introduced an issue with SAN backups and restores and the BIOS UUID. With SAN transport mode, VDDK 6.0 tries to find requested virtual machines by looking up their BIOS UUID.

See “SAN mode VDDK 6.0 searches for virtual machines by BIOS UUID” in the Virtual Disk Development Kit 6.0 Release Notes:

<https://www.vmware.com/support/developer/vddk/vddk-600-releasenotes.html>

To prevent data loss because of this VDDK 6.0 issue, NetBackup 7.7 fails the backup and the restore jobs that meet all of the following conditions:

- Use only the SAN transport mode.
- Target a VM for which a duplicate BIOS UUID exists.
- Restore the BIOS UUID.

NetBackup 7.7 also removes the SAN transport mode as an option in this situation when multiple transport modes are selected.

vCloud Director keywords do not select appropriate computers

For a policy that uses the Query Builder to automatically select VMs in vCloud Director, the `vCDIsExpired` keyword does not operate as expected. The `vCDIsExpired` keyword correctly selects VMs that have expired. However, it also selects VMs in a vApp that has a run-time lease setting of Never Expire. This issue will be fixed in a future release.

Hotadd or SAN restore may fail if the backup image disk geometry differs from VM default values

A restore of a VM with the hotadd transport mode or the SAN transport mode may not succeed if the VM's disk geometry in the backup image differs from the VM's default values. VM disk geometry refers to the layout of the virtual disk (cylinders, heads, sectors) as specified in the vmdk file.

The NetBackup restore job reports partial success with status code 1 (the requested operation was partially successful). For more information about this issue and available workarounds, see the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH210611>

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

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

Virtual Machine restore fails with status code 220 (database system error)

A restore of the virtual machine can fail with status code 220 (database system error) if all of the following are true of the backup:

- The backup was run from an incremental schedule and **Enable block-level incremental backup** was enabled on the policy VMware tab.
- **Enable file recovery from VM backup** was disabled on the policy VMware tab.
- At the time of the incremental backup, the data in the VM had not changed since the previous backup.

To work around this issue, restore from the full image rather than the incremental image. Because there is no change of data since the full backup, a restore from the full image is exactly the same as a restore from the incremental backup.

Unsupported vSphere VM configuration

The following VMware configuration for High Availability (HA) is not supported for virtual machine backup: vSphere 5.1 with Single Sign On Server in an HA configuration that is behind an F5 load balancer (or any other load balancing software).

NetBackup recognizes the name case of VMs

In VMware vSphere, virtual machine (VM) display names, resource pool names, and vApp names are case-sensitive. For example, `vm1` is a different virtual machine from one that is named `VM1`. In version 7.5 and earlier, NetBackup does not recognize case when it selects virtual machines for backup automatically through a query. It considers `VM1` and `vm1` to be the same virtual machine.

Starting with version 7.6, NetBackup recognizes case in VM display names, resource pool names, and vApp names. A backup policy that uses automatic selection through a query is now case-sensitive. The same is true of the new **Search Virtual Clients** function in the Backup, Archive, and Restore interface. Now, `vm1` is identified as a different virtual machine than `VM1`.

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

For a VMware VM with Windows dynamic disks, a restore from incremental backup fails with a Windows restore host and the hotadd transport mode

A restore of a Windows virtual machine by means of the hotadd transfer mode may fail in the following case:

- A backup is taken of a Windows virtual machine that has a dynamic disk group.
- After the backup, another dynamic disk is added to the virtual machine's disk group.
- After the dynamic disk is added, an incremental backup is taken of the virtual machine.
- A Windows restore host is used with the hotadd transport mode to restore the virtual machine from the incremental backup.

For more information and potential workarounds, refer to the following tech note on the Symantec Support website:

<http://www.symantec.com/docs/TECH224707>

A restored VM may not boot up or its file system(s) may not be accessible

A restored VM may not boot up or its file system(s) may not be accessible in the following case:

- The VM's guest operating system is Windows 8,
- The VM is restored from a block-level incremental backup image,
- And the restore uses the hotadd transport mode.

As a result of a VMware issue in VDDK 5.5.x, the Windows NTFS Master File Table on the restored VM may be corrupted.

As a workaround, use a different transport mode to restore the VM (not hotadd).

Hotadd transport backups of 2-TB VMDKs on a VVol datastore fail

Backups of a VMware Virtual Machine Disk (vmdk) fail under the following conditions:

- The vmdk is larger than 2 TBs.
- The vmdk resides on a VMware vSphere Virtual Volumes (VVol) datastore.
- The transport method is hotadd.

The NetBackup software functions correctly under these conditions. Symantec advises customers to contact their VMware support representative about this issue.

To back up a larger than 2-TB vmdk on a VVol datastore, use an NBD transport method or an NBDSSL transport method.

If you encounter the problem, errors similar to the following may appear in the **Job Details** for the backup job.

```
Error bpbrm (pid=xxxx) from client <hostname>: ERR - Error opening
the snapshot disks using given transport mode: hhotadd Status 23
Critical bpbrm (pid=xxxx) from client <hostname>: FTL - cleanup()
failed, status 6
Error bptm (pid=xxxx) media manager terminated by parent process
```

Compressed drive inaccessible after hotadd restore of vmdk from a cumulative incremental backup

After a hotadd restore of a VMware Virtual Machine Disk (vmdk) from a NetBackup cumulative incremental backup, the file system of the vmdk may be corrupt.

The NetBackup software functions correctly under these conditions. Symantec advises customers to contact their VMware support representative about this issue.

To avoid potential file system corruption after a restore, use one of the following alternate transport methods: NBD, NBDSSL, or SAN.

If you encounter the problem, errors similar to the following may appear in the **Job Details** for the restore job:

```
Error bpbrm (pid=<xxxx>) from client <hostname>:
ERR - Error opening the snapshot disks using given transport
mode: hotadd Status 23
Error bptm (pid=<xxxx>) cannot write data to socket, 10054
Info bptm (pid=<xxxx>) EXITING with status 24 <-----
Info tar32 (pid=<xxxx>) done. status: 24: socket write failed
Error bpbrm (pid=<xxxx>) client restore EXIT STATUS 24: socket
write failed
```

Virtual machine recovery using the VMware vSphere Web Client Plug-in may fail if initiated from the Monitoring screen

If you initiate a recovery operation in the NetBackup vSphere Web Client by right-clicking on a successful backup event, the operation may fail with the following error:

NetBackup master server <master server name> not found in the list of added master server.

. This issue occurs when the backup events in **Monitoring** tab of the vSphere plug-in contain the master server name that is specified as a short name and not as an FQDN (fully qualified domain name).

Workaround:

- 1 Initiate the recovery operation using the Recovery Wizard by manually selecting the virtual machine and the image.
- 2 If you want to recover the backup image by right-clicking on the backup event, remove the existing master server name from the list and then add the master server name again using a short name. Make this change using the **Register Master Server** option in the vSphere plug-in.

VM restore to standalone ESXi 6.0 host fails if virtual machine display name contains a period (.)

A VM restore to a standalone ESXi 6.0 host may fail if the VM's display name contains a period character (.). The restore job reports NetBackup status 2820, and messages similar to the following appear in the Activity Monitor's job details:

```
05/19/2015 10:56:30 - Info bpVMutil (pid=6884) INF - vmwareLogger:
  WaitForTaskComplete: SYM_VMC_ERROR: TASK_REACHED_ERROR_STATE
05/19/2015 10:56:30 - Info bpVMutil (pid=6884) INF - vmwareLogger:
  WaitForTaskComplete: The file already exists <249>
05/19/2015 10:56:30 - Info bpVMutil (pid=6884) INF - vmwareLogger:
  CreateVm: SYM_VMC_ERROR: TASK_REACHED_ERROR_STATE
05/19/2015 10:56:30 - Info bpVMutil (pid=6884) INF - vmwareLogger:
  CreateVirtualMachineExAPI: SYM_VMC_ERROR: TASK_REACHED_ERROR_STATE
05/19/2015 10:56:30 - end Restore; elapsed time 0:00:17
NetBackup VMware policy restore error (2820)
```

The ESXi server's **Task** list shows the "Create virtual machine" task failing with status "The file already exists."

As a workaround, restore the VM with a display name that does not contain a period (.).

Note: This problem occurs only when the VM is restored to a standalone ESXi 6.0 server. It does not occur if the VM is restored through a vCenter server.

NetBackup for Hyper-V operational notes

NetBackup for Hyper-V provides snapshot-based backup of the virtual machines that run on various versions of Windows Server. This topic contains some of the operational notes and known issues that are associated with NetBackup for Hyper-V in NetBackup 7.7.

Character restrictions in .vhd or .vhdx names in the “Enable file recovery from VM backup” option

For Hyper-V policies that include the **Enable file recovery from VM backup** option, non-ASCII characters are not supported in the vhd or vhdx name. Examples of non-ASCII characters are Japanese or Chinese characters (multi-byte). If the vhd or vhdx name contains non-ASCII characters, the backup job completes but the VM's files cannot be individually restored from the backup.

As an alternative, you can restore the entire VM.

NetBackup Add-in for Microsoft System Center Virtual Machine Manager (SCVMM) Console operational notes

NetBackup Add-in for Microsoft System Center Virtual Machine Manager (SCVMM) Console lets you recover virtual machines from NetBackup backup images. This topic contains some of the operational notes and known issues that are associated with the NetBackup Add-in for Microsoft SCVMM Console in NetBackup 7.7.

Next button in Recovery Wizard is enabled even though required input has not been entered

In the Recovery Wizard of the NetBackup Add-in for SCVMM, the Next button is enabled even though required input has not been entered. In the following case, the Recovery Wizard of the NetBackup Add-in for SCVMM enables the Next button prematurely:

- On the Add-in's Manage Master Servers screen, an authentication token was added for an invalid master server. For example: the token was generated for an existing master server, but the server name was entered incorrectly on the Manage Master Servers screen.
- A second master server and its authentication token are added, and the master server's name is entered correctly.

When you select the second master server in the wizard's Virtual Machine Selection screen, you can click Next without selecting a VM identifier. The wizard lets you progress from screen to screen without completing the input for each screen. If you

continue without making the required input, the Recovery button on the wizard's last screen is grayed out.

Note: The wizard's Next button should remain grayed out until the input for each screen is completed.

To run the restore, go back through the wizard and make the required entries. You should also delete the invalid master server.

VM Identifier field mislabeled as Display Name

On the **Restore Options** screen of the Add-in's **Recovery Wizard**, the **Display Name** field should instead be labeled **VM Identifier**.

Space characters in virtual machine display names appear as %20 in SCVMM Recovery Wizard

On the **Review Settings** screen of the Add-in's **Recovery Wizard**, spaces in a virtual machine display name are displayed as %20.

The Recovery Wizard of the NetBackup Add-in for SCVMM does not prompt to overwrite the VM, and the recovery fails

The NetBackup Add-in for Microsoft SCVMM Console does not complete a VM recovery in the following situation:

- On the Virtual Machine Selection screen of the Add-in Recovery Wizard, the VM is identified by its GUID or host name (not its display name).
- On the Restore Options screen of the wizard, the Overwrite existing virtual machine option is not selected.
- The same VM exists at the recovery destination.

When you click Recover, the wizard should detect the VM at the recovery destination and then prompt you to select the overwrite option. However, the prompt does not appear; the recovery job starts but then fails with status 2821.

To recover the VM, select Overwrite existing virtual machine on the Restore Options screen and rerun the recovery.

SCVMM Rollup 5 and 6 cannot restore VM to alternate location on Hyper-V server

The NetBackup Add-in for Microsoft SCVMM supports restore of a VM to its original location or to an alternate location. The Add-in supports the System Center 2012

R2 Virtual Machine Manager, including Rollups 1 to 6. If your SCVMM version is Rollup 5 or 6 however, the Add-in cannot restore the VM to an alternate location on the target Hyper-V server. When you click Browse to specify the restore location on the Add-in's Restore Options screen, the following message appears:

Exception has been thrown by the target of an invocation.

The NetBackup administrator can restore the VM to an alternate location by means of the NetBackup Backup, Archive, and Restore interface.

About SORT for NetBackup Users

This appendix includes the following topics:

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

About Symantec Operations Readiness Tools

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

Access SORT from the following webpage:

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

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

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

Use this tool to find out whether a release that you plan to install contains the hot fixes that you need.

- **Custom Reports**

Use this tool to get recommendations for your system and Symantec enterprise products.

- **NetBackup Future Platform and Feature Plans**

Use this tool to get information about what items Symantec intends to replace with newer and improved functionality. The tool also provides insight about what items Symantec intends to discontinue without replacement. Some of these items include certain NetBackup features, functionality, 3rd-party product integration, Symantec product integration, applications, databases, and the OS platforms.

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

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

Recommended SORT procedures for new installations

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

Table A-1

Procedure	Details
Create a SymAccount profile on the SORT webpage	See “To create a SymAccount profile on the SORT page” on page 119.
Create generic installation reports	See “To create a generic installation checklist” on page 119.
Create system-specific installation reports	See “To create a system-specific installation report for Windows” on page 120. See “To create a system-specific installation report for UNIX or Linux” on page 121.

To create a SymAccount profile on the SORT page

- 1 In your web browser, navigate to:
<https://sort.symantec.com/netbackup>
- 2 In the upper right corner, click **Register**.
- 3 Enter the requested login and contact information:

Email address	Enter and verify your email address
Password	Enter and verify your password
First name	Enter your first name
Last name	Enter your last name
Company name	Enter your company name
Country	Enter your country
Preferred language	Select your preferred language
CAPTCHA text	Enter the displayed CAPTCHA text. If necessary, refresh the image.

- 4 Click **Submit**.
- 5 When you receive your login information, you can log into SORT and begin uploading your customized information.

To create a generic installation checklist

- 1 In your web browser, navigate to:
<https://sort.symantec.com/netbackup>
- 2 Find the **Installation and Upgrade Checklist** widget.

3 Specify the requested information

Product	Select the appropriate product from the drop-down menu. For NetBackup select NetBackup Enterprise Server or NetBackup Server .
Product version you are installing or upgraded to	Select the correct version of NetBackup. The most current version is always shown at the top of the list.
Platform	Select the operating system that corresponds to the checklist you want generated.
Processor	Select the correct processor type for your checklist.
Product version you are upgrading from (optional)	For new installations, do not make any selections. For upgrades, you can select the currently installed version of NetBackup.

4 Click **Generate Checklist**.

- 5 A checklist corresponding to your choices is created. You can modify your selections from this screen, and click **Generate Checklist** to create a new checklist.

You can save the resulting information as a PDF. Numerous options are available for NetBackup and many of them are covered in the generated checklist. Please spend time reviewing each section to determine if it applies to your environment.

To create a system-specific installation report for Windows

- 1 Go to the SORT website:
<https://sort.symantec.com/>
- 2 Select **SORT > SORT for NetBackup**
- 3 In the **Custom Reports Using Data Collectors**, select the **Data Collector** tab.
- 4 Select the radio button for **Graphical user interface** and download the correct data collector for your platform.

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.
- 5 Launch the data collector after it finishes downloading.

- 6 On the **Welcome** screen, select **NetBackup** from the product family section and click **Next**.
- 7 On the **System Selection** screen, add all computers you want analyzed. Click **Browse** to see a list of computers you can add to the analysis. Symantec recommends starting the tool with an administrator or a root account.
- 8 When all systems are selected, review the **System names** section and click **Next**.
- 9 In the **Validation Options** screen, under **Validation options**, select the version to which you plan to upgrade.
- 10 Click **Next** to continue
- 11 The utility performs the requested checks and displays the results. You can upload the report to My SORT, print the results, or save them. Symantec recommends that you upload the results to the My SORT website for ease of centralized analysis. Click **Upload** and enter your My SORT login information to upload the data to My SORT.
- 12 When you are finished, click **Finish** to close the utility.

To create a system-specific installation report for UNIX or Linux

- 1 Go to the SORT website:
<https://sort.symantec.com/>
- 2 Select **SORT > SORT for NetBackup**
- 3 Change to directory that contains downloaded utility.
- 4 In the **Custom Reports Using Data Collectors**, select the **Data Collector** tab.
- 5 Download the appropriate data collector for your platform.

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.
- 6 Run `./sortdc`

The utility performs checks to confirm the latest version of the utility is installed. In addition, the utility checks to see it has the latest data. The utility then lists the location of the log file for this session.
- 7 If requested, press **Enter** to continue.
- 8 Select the **NetBackup Family** at the **Main Menu**.

- 9 Select **Installation/Upgrade report** when prompted **What task do you want to accomplish?**

You can select multiple options by separating your response with commas.

- 10 Specify the system or systems you want included in the report.

If you previously ran a report on the specified system, you may be prompted to run the report again. Select **Yes** to re-run the report.

The utility again lists the location of the log files for the session.

The progress of the utility is displayed to the screen.

- 11 Specify **NetBackup** when prompted for the product you want installation or upgrade reports.

- 12 Enter the number that corresponds to the version of NetBackup you want to install.

The utility again lists the location of the log files for the session.

The progress of the utility is displayed to the screen.

- 13 The utility prompts you to upload the report to the SORT website if you want to review the report online. The online report provides more detailed information than the text-based on-system report.

- 14 When your tasks are finished, you can exit the utility. You have the option to provide feedback on the tool, which Symantec uses to make improvements to the tool.

Recommended SORT procedures for upgrades

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

Table A-2

Procedure	Details
Create a SymAccount profile on the SORT webpage	See "To create a SymAccount profile on the SORT page" on page 119.

Table A-2 (continued)

Procedure	Details
Create a system-specific upgrade report	See “To create a system-specific installation report for Windows” on page 120. See “To create a system-specific installation report for UNIX or Linux” on page 121.
Review the future platform and feature plans. Review the hot fix and emergency engineering binary release auditor information.	See “To review future platform changes and feature plans” on page 123. See “To review hot fix and emergency engineering binary information” on page 123.

To review future platform changes and feature plans

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

To review hot fix and emergency engineering binary information

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

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

NetBackup installation requirements

This appendix includes the following topics:

- [About NetBackup installation requirements](#)
- [Required operating system patches and updates for NetBackup](#)
- [NetBackup 7.7 binary sizes](#)

About NetBackup installation requirements

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

See [“NetBackup installation and upgrade operational notes”](#) on page 39.

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- Database rebuilds are likely to occur in each major, minor (single-dot), and release update (double-dot) version of NetBackup. Therefore, before upgrading to NetBackup 7.7, you must ensure that you have an amount of free disk space available that is equal to or greater than the size of the NetBackup database. That means for default installations, you are required to have that amount of free space on the file system containing the `/usr/opensv/db/data` (UNIX) or `<install_path>\Veritas\NetBackupDB\data` (Windows) directories. If you have changed the location of some of the files in either of these directories, free

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

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

- Master and media servers must have a minimum soft limit of 8000 file descriptors per process for NetBackup to run correctly.
For more information about the effects of an insufficient number of file descriptors, refer to the following tech notes on the Symantec Support website:
<http://www.symantec.com/docs/TECH168846>
- 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.
- NetBackup master and media servers exchange server version information at startup, and every 24 hours. This exchange occurs automatically. During startup after an upgrade, the upgraded media server uses the `vmd` service to push its version information to all of the servers that are listed in its server list.
- Symantec recommends that you have the master server services up and available during a media server upgrade.
- All compressed files are compressed using gzip. The installation of these files requires gunzip and gzip, so make sure that they are installed on the computer before you attempt to install NetBackup. For all UNIX platforms except HP-UX, the binaries are expected to be in `/bin` or `/usr/bin` and that directory is a part of the root user's `PATH` variable. On HP-UX systems, the `gzip` and `gunzip` commands are expected to be in `/usr/contrib/bin`. Installation scripts add that directory to the `PATH` variable. These commands must be present to have successful UNIX installations.

Required operating system patches and updates for NetBackup

NetBackup server and client installations are only supported on a defined set of operating systems (OSs) that are listed in the NetBackup compatibility lists. Most

OS vendors provide patches, updates, and service packs (SPs) for their products. The best practice of NetBackup Quality Engineering is to test with the latest SP or update level of the OS when a platform is tested. Therefore, NetBackup is supported on all vendor GA updates (n.1, n.2, etc.) or SPs (SP1, SP2, and so on). However, if a known compatibility issue exists on a specific SP or updated OS level, this information is identified in the compatibility lists. If no such compatibility issues are noted, Symantec recommends that you install the latest OS updates on your servers and clients before you install or upgrade NetBackup.

The compatibility lists include information about the minimum OS level that is required to support a minimum NetBackup version in the latest major release line. In some cases, new releases of NetBackup may require specific vendor OS updates or patches. [Table B-1](#) includes the OS updates and patches that are required for NetBackup 7.7. However, this information may sometimes change in between releases. The most up-to-date required OS patch information for NetBackup 7.7 and other NetBackup releases can be found on the Symantec Operations Readiness Tools (SORT) website.

See [“About NetBackup compatibility lists and information”](#) on page 136.

See [“About Symantec Operations Readiness Tools”](#) on page 117.

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

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

Table B-1
Required operating system patches and updates for NetBackup 7.7

Operating system type and version	NetBackup role	Patch	Notes
AIX 6.1	Master, media, client	AIX run-time libraries 9.0.0.3 or later	The run-time libraries need to be at 9.0.0.3 or later. You may need to restart after you change to version 9.0.0.3.

Table B-1 Required operating system patches and updates for NetBackup 7.7
(continued)

Operating system type and version	NetBackup role	Patch	Notes
AIX 7.1	Master, media, client	AIX 7.1 TL1 SP2 (7100-01-02-1150)	This patch is required for the NetBackup-Java Administration Console to function properly. https://www-304.ibm.com/support/docview.wss?uid=isg1fixinfo134913
HP-UX	Master, media, client	COMPLIBS.LIBM-PS32	If you install AT on an HP-UX platform, this patch is required.
HP-UX IA-64	Master, media, client	Networking.NET-RUN: /usr/lib/libip6.sl	
	Master, media, client	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.1	
	Master, media, client	Networking.NET-RUN-64: /usr/lib/pa20_64/libip6.sl	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux32/libip6.so.1	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so	
	Master, media, client	Networking.NET2-RUN: /usr/lib/hpux64/libip6.so.1	
	Master, media, client	Networking.NET2-RUN: /usr/lib/libip6.1	
HP-UX 11.31	Media	QPK1131 (B.11.31.1003.347a) patch bundle	This patch bundle is required for NetBackup media server support. It is an HP-UX March 2010 patch bundle.
Red Hat Enterprise Linux 6	Master, media, client	glibc-2.12-1.107 or higher	
Windows Vista x86-32	Client	KB936357	Microsoft microcode reliability update.

Table B-1 Required operating system patches and updates for NetBackup 7.7
(continued)

Operating system type and version	NetBackup role	Patch	Notes
	Client	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Vista x86-64	Client	KB936357	Microsoft microcode reliability update.
	Client	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Server 2008 x86-32	Client	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Server 2008 x86-64	Client	KB952696	Contains the necessary updates to ensure that you can back up encrypted files.
Windows Server 2008 (SP2)	Master, media, client	KB979612	Hot fix to improve TCP loopback latency and UDP latency
Windows Server 2008 R2	Master, media, client	KB2265716	Hot fix for when a computer randomly stops responding. Note that this patch is also contained in Windows Server 2008 R2 SP1.
	Master, media, client	KB982383	Hot fix for a decrease in I/O performance under a heavy disk I/O load. Note that this patch is also contained in Windows Server 2008 R2 SP1.
	Master, media, client	KB983544	Update for the "Modified time" file attribute of a registry hive file. Note that this patch is also contained in Windows Server 2008 R2 SP1.

Table B-1 Required operating system patches and updates for NetBackup 7.7
(continued)

Operating system type and version	NetBackup role	Patch	Notes
	Master, media, client	KB979612	Hot fix to improve TCP loopback latency and UDP latency Note that this patch is also contained in Windows Server 2008 R2 SP1.

- 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 Vista: (suggested) <http://support.microsoft.com/?kbid=936357>
 - Symantec AntiVirus. Update to latest version and latest update (required).
 - The `Symevent` driver updates (required). Update to latest driver version.

NetBackup 7.7 binary sizes

[Table B-2](#) contains the approximate binary sizes of the NetBackup 7.7 master server, media server, and client software for the various supported operating systems. This information is meant to help you determine if you have allocated enough disk space on your computers to safely and efficiently back up and restore all of the data in your NetBackup environment.

Note: [Table B-2](#) and [Table B-3](#) only list the supported operating systems. For up-to-date information about the specific operating system versions that NetBackup currently supports, check the Installation and Upgrade Checklist on the Symantec Operations Readiness Tools (SORT) website, or the *NetBackup Operating System Compatibility List* document at <http://www.netbackup.com/compatibility>.

See “[About Symantec Operations Readiness Tools](#)” on page 117.

Table B-2 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	32-bit client	64-bit client	32-bit server	64-bit server	Notes
AIX	POWER		2430MB		6750MB	
Canonical Ubuntu	x86-64		1548MB			
CentOS	x86-64		1548MB		4952MB	Media server or client compatibility only.
Debian GNU/Linux	x86-64		1548MB			
FreeBSD	x86-64		300MB			
HP-UX	IA-64		2761MB		7525MB	
Mac OS X	x86-64		248MB			
Novell Open Enterprise Server	x86-64		1540MB		4946MB	
OpenVMS	IA-64		128MB			The listed sizes are for the NetBackup 7.5 binaries. No NetBackup 7.7 binaries for OpenVMS are provided.
Oracle Linux	x86-64		1548MB		4952MB	
Red Hat Enterprise Linux Server	x86-64		1548MB		4952MB	
Red Hat Enterprise Linux Server	z/Architecture		1175MB		2318MB	Media server or client compatibility only.
Solaris	SPARC		1532MB		4789MB	
Solaris	x86-64		1593MB		4990MB	
SUSE Linux Enterprise Server	x86-64		1540MB		4946MB	
SUSE Linux Enterprise Server	z/Architecture		1095MB		2207MB	Media server or client compatibility only.
Windows	x86-32	750MB				Covers all compatible Windows x86 platforms
Windows	x86-64		1050MB		2700MB	Covers all compatible Windows x64 platforms

The following space requirements also apply to some NetBackup installations on Windows:

- If you install NetBackup in a custom location on a Windows system, some portions of the software are installed on the system drive regardless of the primary application folder location. The space that is required on the system drive generally accounts for 40 to 50 percent of the total binary size that is listed in [Table B-2](#).
- If you install NetBackup server on a Windows cluster, some portions of the software are installed on the cluster shared disk. Note, the space that is required on the cluster shared disk is in addition to the binary size that is listed in [Table B-2](#). The additional required space is equivalent to 15 to 20 percent of the total binary size.

NetBackup OpsCenter

[Table B-3](#) contains the approximate binary sizes of the OpsCenter Agent, Server, and **ViewBuilder** for the various operating systems that are compatible with NetBackup OpsCenter 7.7.

Table B-3 NetBackup OpsCenter binary sizes for compatible platforms

OS	CPU Architecture	Agent	Server	ViewBuilder
Oracle Linux	x86-64		713MB	
Red Hat Enterprise Linux Server	x86-64		713MB	
SUSE Linux Enterprise Server	x86-64		713MB	
Windows Server	x86-64	245MB	643MB	201MB

NetBackup plug-ins

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

NetBackup compatibility requirements

This appendix includes the following topics:

- [About NetBackup release types and versioning](#)
- [About compatibility between NetBackup versions](#)
- [About NetBackup compatibility lists and information](#)
- [About NetBackup end-of-life notifications](#)

About NetBackup release types and versioning

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

The NetBackup family of software and appliance products uses the following release types and version number schemes:

- A major release is the first in a series of releases. This release type contains new features, enhancements, platform support, and a complete set of the latest product documentation.
- A minor release is a single-dot release that follows a major release, for example 2.6 or 7.6. This release type contains much of the same requirements as a major release. It contains a smaller set of new features and enhancements, new platform support, and a complete set of the latest product documentation.
- A software update release is a double-dot release, for example 2.6.1 or 7.6.1. This release type may contain a few new features and enhancements along

with many product fixes. Only those documents that are applicable to the new features or enhancements are updated and republished.

- A maintenance release is a triple-dot release, for example 2.6.0.2 or 7.6.0.2. This release type is primarily comprised of a number of fixes that are developed to address issues in major, minor, and software update releases. It may also contain a small number of new features, enhancements, and platform support. The only documentation that is provided for this release type is a readme text file and a new version of the *NetBackup Release Notes*. Both files are online-only and are made available on the Symantec Support website.

About compatibility between NetBackup versions

Note: The statements that are made in this topic do not override Symantec's standard End of Life and End of Support Life policies. Once a NetBackup version reaches its End of Support Life, no release of that product version is supported in any configuration.

Symantec recommends that you review the NetBackup End of Support Life information available online.

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

You can run mixed versions of NetBackup between master servers, media servers, and clients. This back-level support lets you upgrade NetBackup one server at a time, which minimizes the effect on overall system performance.

For compatibility between major versions, the latest available release of NetBackup is compatible with media servers and clients that run a release of NetBackup that is up to one major version behind. However, this compatibility ceases to be supported in any configuration once the previous major version has reached its End of Support Life.

The master server within a NetBackup environment must be at a version level that is equal to or greater than the version levels of the media servers and clients within that environment. However, NetBackup offers the flexibility of an environment where the clients and the media servers run different triple-dot releases than the master server. For example you can upgrade a media server or client to version 7.6.0.2 in an environment where the master server is running version 7.6 GA. Symantec recommends that you keep your entire NetBackup environment up-to-date with the latest maintenance (triple-dot) releases.

See [“About NetBackup release types and versioning”](#) on page 132.

NetBackup does not support any scenario where a media server or client runs a minor release version or software release update version that is higher than that of the parent server. For example:

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

Table C-1 shows the various compatibility schemes that are supported with the current NetBackup product line.

Table C-1 Release compatibility for the NetBackup product line

NetBackup master server	NetBackup media server	NetBackup client
7.7	7.7	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x, 7.6.1, 7.6.1.x, 7.7
7.7	7.6.1.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x, 7.6.1, 7.6.1.x
7.7	7.6.1	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x, 7.6.1, 7.6.1.x
7.7	7.6.0.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x
7.7	7.6	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x
7.7	7.5.0.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.7	7.5	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.7	7.1.0.x	7.0, 7.0.1, 7.1, 7.1.0.x
7.7	7.1	7.0, 7.0.1, 7.1, 7.1.0.x
7.7	7.0.1	7.0, 7.0.1
7.7	7.0	7.0
7.6.1.x	7.6.1.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x, 7.6.1, 7.6.1.x

Table C-1 Release compatibility for the NetBackup product line (*continued*)

NetBackup master server	NetBackup media server	NetBackup client
7.6.1.x	7.6.1	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x, 7.6.1, 7.6.1.x
7.6.1.x	7.6.0.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x
7.6.1.x	7.6	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x
7.6.1.x	7.5.0.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6.1.x	7.5	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6.1.x	7.1.0.x	7.0, 7.0.1, 7.1, 7.1.0.x
7.6.1.x	7.1	7.0, 7.0.1, 7.1, 7.1.0.x
7.6.1.x	7.0.1	7.0, 7.0.1
7.6.1.x	7.0	7.0
7.6	7.6.0.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x
7.6	7.6	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x, 7.6, 7.6.0.x
7.6	7.5.0.x	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6	7.5	7.0, 7.0.1, 7.1, 7.1.0.x, 7.5, 7.5.0.x
7.6	7.1.0.x	7.0, 7.0.1, 7.1, 7.1.0.x
7.6	7.1	7.0, 7.0.1, 7.1, 7.1.0.x
7.6	7.0.1	7.0, 7.0.1
7.6	7.0	7.0

Note: Support for the NetBackup 6.x product line has ended as of October, 2012. See [“About NetBackup end-of-life notifications”](#) on page 138.

Other NetBackup mixed version compatibility notes

The following list includes additional compatibility details you should take into consideration:

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

For more information about NetBackup compatibility, refer to the following article on the Symantec Support website:

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

About Auto Image Replication compatibility

In NetBackup 7.7, Auto Image Replication is supported for the servers that run version 7.5.0.3 or higher. For lower versions to accept replications from version 7.6, an Emergency Engineering Binary (EEB) for the NetBackup 7.1 master server is required.

Auto Image Replication is supported between NetBackup servers running 7.1.x.x and 7.5.x.x. However, an exception occurs in certain versions in which the replication of catalog backups may fail. For more information, refer to the following tech note on the Symantec Support website:

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

About NetBackup compatibility lists and information

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

See “[About Symantec Operations Readiness Tools](#)” on page 117.

For NetBackup, SORT provides an Installation and Upgrade Checklist report as well as the ability to collect, analyze, and report on host configurations across your environments. In addition, you can determine which release contains the hot fixes

or EEBs that you may have installed in your environment. You can use this data to assess whether your systems are ready to install or upgrade to a given release.

NetBackup compatibility lists

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

www.netbackup.com/compatibility

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

- *NetBackup Enterprise Server and Server 7.x OS Software Compatibility List*
This list contains information about the operating system (OS) level and the version that is required to be compatible with a NetBackup master server or media server. It also describes the OS level and the version that is required to be compatible with a NetBackup client. Predecessors and successors to the documented operating system levels may function without difficulty, as long as the release provides binary compatibility with the documented operating system.
This list contains compatibility information about several NetBackup Enterprise features, including the following:
 - NetBackup Enterprise server and client
 - Bare Metal Restore (BMR)
 - NetBackup Access Control (NBAC)
 - Network Data Management Protocol (NDMP)
 - NetBackup OpsCenter
 - NetBackup SAN media server and SAN client
 - Fibre Transport (FT) media server
 - NetBackup Media Server Deduplication Option
 - File system compatibility
 - NetBackup virtual system compatibility
 - NetBackup Media Server Encryption Option (MSEO)

NetBackup compatibility for a platform or OS version requires platform vendor support for that product. The platform compatibility lists that NetBackup maintains are subject to change as vendors add and drop platforms or OS versions.
- *NetBackup Enterprise Server and Server 7.x Hardware Compatibility List*

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

- NetBackup appliances
- AdvancedDisk arrays
- OpenStorage (OST) solutions
- Tape drives
- Fibre Transport media server host bus adapters (HBAs)
- Virtual tape libraries (VTLs)
- Network Data Management Protocol (NDMP) devices
- Tape libraries
- Encryption and security solutions
- *NetBackup 7.x Database and Application Agent Compatibility List*
This list contains the most current compatibility information for the database agents and application agents that are supported on specific operating systems and CPU architectures.
- *NetBackup 7.x Snapshot Client Compatibility List*
This list contains the most current server and client snapshot compatibility information, sorted by arrays, agents, operating systems, and VSS providers.
- *NetBackup 7.x Cluster Compatibility List*
This list contains the most current compatibility information for the cluster types and versions that are supported on specific operating systems and CPU architectures.
- *Support for NetBackup 7.x in virtual environments*
This list contains the most current compatibility information for NetBackup in virtual environments.

About NetBackup end-of-life notifications

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

- General availability releases

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

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

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

Using SORT

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

<https://sort.symantec.com/nbufutureplans>

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

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

See “[About Symantec Operations Readiness Tools](#)” on page 117.

About changes in platform compatibility

The NetBackup 7.7 release may contain changes in support for various systems. In addition to using SORT, you should make sure to review the *NetBackup Release Notes* document and the NetBackup compatibility lists before installing or upgrading NetBackup software.

See “[About new enhancements and changes in NetBackup](#)” on page 21.

See “[About NetBackup compatibility lists and information](#)” on page 136.

Other NetBackup documentation and related documents

This appendix includes the following topics:

- [About related NetBackup documents](#)
- [About NetBackup release notes documents](#)
- [About NetBackup administration documents](#)
- [About NetBackup installation documents](#)
- [About NetBackup configuration documents](#)
- [About NetBackup troubleshooting documents](#)
- [About other NetBackup documents](#)

About related NetBackup documents

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

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

See [“About NetBackup release types and versioning”](#) on page 132.

Unless otherwise specified, the NetBackup documents can be downloaded in PDF format from the following location:

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

Note: Symantec assumes no responsibility for the correct installation or use of PDF reader software.

About NetBackup release notes documents

The following release notes documents are published for NetBackup software:

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

About NetBackup administration documents

The following administrator guides are published for NetBackup software:

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

About administration of NetBackup options

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

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

virtual machines from backups, and monitor VM backup status and related messages.

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

This document describes how to use the NetBackup OpsCenter user interface to provide reporting, monitoring, and alerts for NetBackup and its agents and options.

- *NetBackup OpsCenter Reporting Guide*
This guide explains how to use NetBackup OpsCenter to generate and use comprehensive business-level reports to track the effectiveness of data backup and archive operations.
- *NetBackup OpsCenter Performance and Tuning Guide*
This performance and tuning guide is for administrators who want to analyze, evaluate, and tune OpsCenter performance. This document is intended to provide guidance on how to tune OpsCenter for maximum performance, which system configurations you should use for OpsCenter depending on your backup environment, and best practices to follow for increased OpsCenter performance.

About administration of NetBackup database agents

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

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

This guide explains how to configure and use the NetBackup for Microsoft SQL Server agent to back up and restore Microsoft SQL Server databases and transaction logs.

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

About NetBackup installation documents

The following installation documents are published for NetBackup software:

- *NetBackup Upgrade Guide*
This guide is provided to help assist you plan and accomplish your upgrade of NetBackup software. This guide is updated periodically to provide you with the most up-to-date information.
- *NetBackup Installation Guide*
This guide explains how to install NetBackup server, client, and administrative software on UNIX and Windows platforms.
- *NetBackup LiveUpdate Guide*
This guide explains how to set up a NetBackup LiveUpdate server to provide a policy-driven method of distributing NetBackup software releases within your environment.

About NetBackup configuration documents

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

- *NetBackup Device Configuration Guide*

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

About NetBackup troubleshooting documents

The following troubleshooting guides are published for NetBackup software:

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

About other NetBackup documents

The following documents are published for NetBackup software:

- *NetBackup Commands Reference Guide*
This guide contains detailed information on the commands that run on UNIX systems and Windows systems, including all of the NetBackup man page commands.
- *NetBackup Clustered Master Server Administrator's Guide*
This guide provides information on how to install and configure a NetBackup master server in a cluster.
- *NetBackup in Highly Available Environments Guide*
This guide discusses various methods for using NetBackup in highly available environments and provides guidelines for protecting NetBackup against single points of failure.
- *NetBackup Security and Encryption Guide*
This guide provides information about on how to secure NetBackup using access control, enhanced authorization and authentication, and encryption.
- *NetBackup Network Ports Reference Guide*
This guide provides a reference to NetBackup network ports, including master server and media server ports, client ports, default ports, and other ports that NetBackup uses.
- *NetBackup Getting Started Guide*
This guide provides a high-level description of preinstallation information that is related to this release of NetBackup. The guide also includes descriptions of

the NetBackup media kit, the NetBackup Electronic Software Distribution (ESD) images, and the NetBackup license key requirements.

- *NetBackup Backup, Archive, and Restore Getting Started Guide*
This guide provides basic information about backup and restore procedures for new users of NetBackup. These procedures include how to back up, archive, and restore files, folders or directories, and volumes or partitions that reside on a computer.
- *NetBackup Third-party Legal Notices*
This document contains proprietary notices for the Third-Party Programs and the licenses for the Third-Party Programs, where applicable, that pertain to the Symantec NetBackup and OpsCenter products.