

# Veritas NetBackup™ Emergency Engineering Binary Guide

Release 9.0 and 9.x

Document Version 1

**VERITAS™**

# Veritas NetBackup™ Emergency Engineering Binary Guide

Last updated: 2020-12-16

## Legal Notice

Copyright © 2020 Veritas Technologies LLC. All rights reserved.

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

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

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 Veritas Technologies LLC 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. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

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

Veritas Technologies LLC  
2625 Augustine Drive  
Santa Clara, CA 95054

<http://www.veritas.com>

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

## Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

[NB.docs@veritas.com](mailto:NB.docs@veritas.com)

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

## Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

Chapter 1	<b>NetBackup release content listings</b> .....	5
	About NetBackup release content listings .....	5
	About the NetBackup "known issues" documentation conventions .....	6
Chapter 2	<b>EEBs and other known issues resolved in NetBackup 9.0</b> .....	7
	Previous EEBs now resolved in NetBackup 9.0 .....	7
	Other known issues resolved in NetBackup 9.0 .....	13
Appendix A	<b>About SORT for NetBackup Users</b> .....	20
	About Veritas Services and Operations Readiness Tools .....	20
	Recommended SORT procedures for new installations .....	21
	Recommended SORT procedures for upgrades .....	25

# NetBackup release content listings

This chapter includes the following topics:

- [About NetBackup release content listings](#)
- [About the NetBackup "known issues" documentation conventions](#)

## About NetBackup release content listings

Each release of NetBackup incorporates fixes to several known issues that affected previous versions of NetBackup. Some of these fixes are associated with the customer-specific issues that have been documented in the form of customer cases. Several of the customer-related fixes that are incorporated into each release are also made available as emergency engineering binaries (EEBs).

The *NetBackup Emergency Engineering Binary Guide* contains the following information:

- Tables that list the EEBs that were incorporated into NetBackup releases
- Release content listings of some of the known issues that were fixed in NetBackup releases

The *NetBackup Emergency Engineering Binary Guide* is published for each major release and minor (single-dot) release. The guide is then periodically updated to include the EEB and release content listings for subsequent double-dot and triple-dot releases.

Much of the information that is found in the *NetBackup Emergency Engineering Binary Guide* can also be found on the Veritas Services and Operations Readiness Tools (SORT) website using the NetBackup Hot Fix and EEB Release Auditor widget.

See ["About Veritas Services and Operations Readiness Tools"](#) on page 20.

---

**Note:** If you do not see information about an EEB or a fixed issue that you expected to see in the *NetBackup Emergency Engineering Binary Guide* or in SORT, contact Veritas Support.

---

## About the NetBackup "known issues" documentation conventions

The following items describe the conventions used in the NetBackup known issues listings:

- **Etrack Incident**  
Notes the Etrack number that targets a release
- *Associated Primary Etrack*  
An additional Etrack number that exists in the incident hierarchy
- *Associated Service Request Etrack*  
The Etrack that is associated with the customer support service request
- *Description*  
Describes a particular issue that has been fixed in a release, as well as additional notes and workarounds (if available).  
Workarounds can be used instead of applying the patch, however, Veritas recommends the best practice of operating at the latest available NetBackup release level.
- **\*\*Description or \*\*Etrack number**  
Describes a critical issue or an issue that can lead to a potential data loss that has been fixed in this release  
Please read these issue descriptions carefully. In some cases, a Tech Alert link is provided.

# EEBs and other known issues resolved in NetBackup 9.0

This chapter includes the following topics:

- [Previous EEBs now resolved in NetBackup 9.0](#)
- [Other known issues resolved in NetBackup 9.0](#)

## Previous EEBs now resolved in NetBackup 9.0

[Table 2-1](#) contains a listing of known issues with NetBackup that were identified, fixed, and made available to customers in the form of an emergency engineering binary (EEB). NetBackup 8.3.0.1 resolves the issues that were fixed with each of these EEBs.

More information on the Etracks that are listed in this topic (and any other service request Etrack) can be found using the Veritas Services and Operations Readiness Tools (SORT) website.

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

**Table 2-1** Previous EEBs now resolved in NetBackup 9.0

Etrack Number	EEB Description
3980582	DB2 backups fail until restarted. DB2sys dumps during the process and no backups then take place.

**Table 2-1** Previous EEBs now resolved in NetBackup 9.0 (*continued*)

Etrack Number	EEB Description
3981134, version 23, 22, 21, 20, 19, 18, 17, 16	The EEB bundle contains common fixes for MSDP issues on NetBackup 8.2
3981837, version 17, 16	The EEB bundle contains fixes for Cloud Catalyst issues on NetBackup 8.2.
3985362	Encryption key is present in the key file in the client. Scheduled backups are configured for policy with encrypt option enabled. The files in backup selections are less than 256K. Delete the key in the keyfile. Scheduled backup jobs are successful.
3986713	Replaces vulnerable jars.
3986976	This EEB replaces vulnerable jars.
3987486, version 2	There are currently no limits on how many AIR jobs can run simultaneously. This can cause a lot of contention for NetBackup resources (such as overloading nbrb) and storage resource (too many jobs trying to write to the same replication target).
3988520, version 1	The EEB contains enhancements to have keyfile in a customized path. Add below entry in NetBackup Client Configuration using nbsetconfig command CLIENT_ENCRYPTION_KEY_PATH=/mypath/keyfilename
3988602	Vulnerable spring jars 4.3.5 were packaged with NetBackup.
3988653	The EEB contains enhancements to have keyfile in a customized path. Add below entry in NetBackup Client Configuration using nbsetconfig command CLIENT_ENCRYPTION_KEY_PATH=/mypath/keyfilename. Improving the efficiency and behavior of hostdb.cache.
3989188	This EEB will replaces vulnerable spring jars with non vulnerable spring jars.
3991153	Modify the encryption format of a tape, to encrypt all data except the media header. The media header and in-cartridge memory have several fields de-populated to avoid exposing information that could be useful to an attacker.
3993611	Upgrade to Tomcat version 8.5.53 on OpsCenter 8.2 Server is required due to security vulnerabilities.
3993893	Oracle backups are causing service restarts.
3994065	Backups fail with status 25 when more than 64 IP's configured on the client.
3994195	This EEB will replaces vulnerable spring jars with non vulnerable spring jars.
3994951	Backports nb_monitor_util - CLI utility - to monitor NetBackup events and fetch different information.



**Table 2-1** Previous EEBs now resolved in NetBackup 9.0 (*continued*)

Etrack Number	EEB Description
3994952	Backports nb_monitor_util - CLI utility - to monitor NetBackup events and fetch different information.
3996250	Upgrade to Tomcat version 8.5.53 on OpsCenter 8.1.2 Server is required due to security vulnerabilities.
3996536	NetBackup 8.2 GUI cannot expand the tablespace list when trying to browse DB2 database structure.
3996724	Backups fail with status 25 when more than 64 IP's configured on the client.
3996875	nbcertcmd on client runs hastatus -summary on cluster node to validate if it is an active node.
3999274	EEB contains the latest Sybase Anywhere patch #17.0.10.6127 to fix the issue of database server crashing due to corrupt index.
4000282	Windows 8.1.2 client backed up with multiple policies fails during BMR DSR to a HyperV VM with 1002 (Failed to verify backup).
4000294	The database contains a number of VM clients with inconsistencies that are causing the Week at a Glance and other reports to display incorrect data.
4001960	This EEB adds NetBackup for OpenStack enhancements: 1. Global Admin 2. Ceph based Cinder volume support 3. Save extra metadata
4002141	JRE needs to be upgraded to 1.8_251
4002163	Image clean up jobs are not getting initiated.
4002172, version 3	EEB Bundle containing two NBSL fixes: OpsCenter Data Collection is not working and the NBSL service is getting crash frequently on cluster master server.
4003077	DFSR backup fails while taking an excessive amount of time in preprocessing.
4004031	Corrects critical error for eval license shown in nbemm logs.
4004448	nbcatsync will stop working when resume number of the image is changed after replication.
4004732	A functionality exception occurs for BMR supporting a restore when the client is using two different networks to connect to master and media servers.
4004754	A stack overflow is often caused by bpbkar32 during VADP backup.
4004767	This EEB will replaces vulnerable spring jars with non-vulnerable spring jars.
4004911	Netbackup is connecting to old VMs which have been removed from all policies, but still exist in domain_PolicyClient table.

**Table 2-1** Previous EEBs now resolved in NetBackup 9.0 (*continued*)

Etrack Number	EEB Description
4004942	Backups with large number of files fail with status code 233 intermittently.
4005824	nbcomponentupdate failed to update JRE due to version check.
4005854	The Universal Share consumes more space than expected.
4005935, version 1	SLP processing jobs are not submitted as expected. While some SLP jobs may be submitted, others are not. As a result, the SLP backlog rises.
4005955	VMware backup of Windows Server 2019 causes backup host to become unresponsive.
4006076	Appropriate name was not configured against entity for the given client ID.
4006181	After JRE is upgraded using nbcomponentupdate and then clicking in jnbSA Admin GUI 'Configure Storage Devices', the cursor rotates but nothing happens.
4006226	Upgrade to Tomcat version 8.5.55 or later on the master server is required to address Tomcat vulnerability CVE 2020-9484.
4006544	Client Direct backups fail due to incorrect network interface being used.
4006681, version 3, 2, 1	Vault eject jobs intermittently hang during multi-MAP operation on NetBackup 8.2
4006761	Upgrade to Tomcat version 8.5.5 or later on OpsCenter is required to address Tomcat vulnerability CVE 2020-9484.
4006820	NetBackup is looking for the device in a different path.
4006997	Unexpected results after installation of an EEB which is a fix for Accelerator.
4007237	Correct error handling during SSL shutdown close notify processing within nbpxyhelper/vnetd-proxy.
4007299	Post March 8th (Daylight Savings Time), the current day can show zero (0) data depending on which Relative TimeFrame is used
4007318, version 1	Backup jobs are failing intermittently with error 'premature eof encountered (233)'
4007413	Mapping volumes fails if ESP is set to anything other than the first partition.
4008558	Upgrade to Tomcat version 8.5.56 or 9.0.36 later is required to address Tomcat vulnerabilities CVE-2020-11996 and CVE-2020-9484.
4008711	This EEB contains a newer Sybase SQL Anywhere patch - 17.0.10.6160 to fix the issue of database server crash.

**Table 2-1** Previous EEBs now resolved in NetBackup 9.0 (*continued*)

Etrack Number	EEB Description
4008911	Performance issues occur during VMware restore. The GUI takes some time to populate before the restore starts.
4009026	Editing policy displays bplpschedrep: must be superuser to execute.
4009029	Remote Java GUI SSO is case sensitive.
4009086	VMware backup of Windows Server 2019 causes backup host to become unresponsive.
4009098, version 1	This is bundled EEB
4009140	A security vulnerability is found in lower version of Tomcat.
4009303	VxUpdate EEB for NB 8.1.2 required for Java vulnerability.
4009313	Oracle backups are causing service restarts.
4009598	Policies taking too long to load from Laptop Java Console. Removed dependency of Oracle Instances loading on Policy loading.
4009785	Amazon cloud snapshot replica retention is not honored when it is different from the primary snapshot retention.
4009877, version 3, 2, 1	bpjobd optimization, and debugging, for update flush during JOBALL processing.
4009899	Fixes clustered vs. standalone ESXi hierarchy display for manual selection of VMware VMs.
4010158	Throttling functionality for classic cloud is not working properly.
4010272	When users duplicate an image from AdvanceDisk or other non-MSDP storage to Cloud Catalyst, no IM and TIR of images are created. Therefore, images in cloud storage cannot be listed by image sharing.
4010300	Microsoft is using '*.avs.azure.com' for domain name, which NetBackup does not support.
4010336	Amazon cloud snapshot replica retention is not honored when it is different from the primary snapshot retention.
4010434	Fixes issue in certmapinfo.json file corruption with '\u0000?' character and wrong/unrelated master server name entries in 'serverAltNames' field of certmapinfo.json file.
4010448	Microsoft is using '*.avs.azure.com' for domain name, which NetBackup does not support.
4010585	Fixes Netbackup FETB licensing metering issue for multistream backups.
4010741	After upgrading the NetBackup master server to 8.3, BMR backup jobs may report failure.

**Table 2-1** Previous EEBs now resolved in NetBackup 9.0 (*continued*)

Etrack Number	EEB Description
4010780	Proxy restores are failing when multiple users on a single machine are doing proxy backups.
4011035	A functionality exception occurs for BMR supporting a restore when the client is using two different networks to connect to master and media servers
4011100	CPU usage of spoold process always keeps 50%.
4011555	NetBackup web management console will not start after Java update to JRE 1.8.0_261
4011735	A restore of images in parallel (MPX) that have the same backup ID (share the same 'backup time') may run into severe performance degradation.
4011823	DFSR backup takes an excessive amount of time in preprocessing.
4011860	Mapping volumes fails if ESP is set to anything other than the first partition.
4012066, version 1	EEB to solve conflict of netbackup.war
4012128	8.2 OpsCenter is inaccessible after updating to JRE version 1.8.0_261 from JRE version 1.8.0_251.
4012263	Fix clustered vs. standalone ESXi hierarchy display for manual selection of VMware VMs
4012414	AIR imports fail after upgrade to NetBackup 8.3. Date and other fields appear to be missing from the IM fragments in the OST plugin logs.
4012433, version 1	Large bpdmbm logs and higher CPU utilization on master. Lots of 'database is locked' message in logs.
4012437	Queries on SQL backups generate unsuccessful attempts to connect with the wrong user.
4012473	NetBackup web management console will not start after Java update to JRE 1.8.0_261.
4012475	NetBackup web management console will not start after Java update to JRE 1.8.0_261.
4012550	When NAS-Data-Protection policy is in use, NBDeployUtil fails to generate the usage reports for traditional licensing. This applies to the manual mode and scheduled mode of NBDeployUtil.
4012619, version 1	EEB bundle to upgrade tomcat and resolve login error code.
4012682	After upgrading to NetBackup 8.3, NetBackup is unable to load the OST plugin.
4012875	Cumulative EEB to solve the conflict of netbackup.war while upgrading the Tomcat.
4013200, version 1	EEB bundle to upgrade tomcat and solve NDMP manual backup issue
4013363, version 1	Fix clustered vs. standalone ESXi hierarchy display for manual selection of VMware VMs (for use with Windows Gold EEB)

**Table 2-1** Previous EEBs now resolved in NetBackup 9.0 (*continued*)

Etrack Number	EEB Description
4013559	Nbdeployutil may fail to generate usage reports for traditional licensing. When 'NAS-Data-Protection' policy is in use, Nbdeployutil would fail to generate the usage reports for traditional licensing.
4013577	Unable to access OpsCenter console after upgrading JRE version to 1.8.0_261.
4013761	Problem updating remote Java console to latest JRE 1.8.0_261.
4013820	JVM crashes after updating the remote java console to the latest JRE 1.8.0_261.
4013835	RHV 4.4 support in 8.3
4015176	Java Upgrade causes NetBackup Administration Console (GUI Console) to crash after providing credentials
4015443	nbjm experienced a core dump issue from segfault.
4016087	RHV 4.4 support in 8.3.0.1
4016679, version 1	Cumulative EEB to fix the API issue along with fixes for tomcat upgrade issue
4016984	Security scanners detecting HSTS not being configured.
4017171	Filesystem backups fail with status code 233 intermittently.
4017319	Resolves security vulnerabilities for several Python modules.
4017722	Security scanners detecting HSTS not being configured. This change enables HSTS for NetBackup web services.
4017927	8.2 Gold EEB V4 doesn't contain the latest code for NBNioEndpoint.java related to Tomcat upgrade, which was causing the issue while restarting the webservices for those who installed Tomcat 8.5.50 and above
4018857	Security scanners detecting HSTS not being configured. This change enables HSTS for NetBackup web services.
4019187	Security scanners detecting HSTS not being configured. This change enables HSTS for NetBackup web services.

## Other known issues resolved in NetBackup 9.0

This topic contains a list of some of the known issues that were fixed and included in the NetBackup 9.0 release.

**Etrack Incident: 4000964**

- Associated Primary Etrack: 3998149
- Associated Service Request Etrack(s): 3998148
- Description:  
When attempting to move EMM DB files with the `nbdbb_move` command, the lock file `vxdbms_conf.lock` was not moved.

**Etrack Incident: 4003802**

- Associated Primary Etrack: 4003707
- Associated Service Request Etrack(s): 4003706
- Description:  
A MySQL backup left `.sqlx` dump files in the filesystem after the backup failed.

**Etrack Incident: 4006230**

- Associated Primary Etrack: 4005112
- Associated Service Request Etrack(s): 4005111
- Description:  
A NetBackup Administration Console pop-up window on login states: "6006: Unable to Connect To Server".

**Etrack Incident: 4006381**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
A few disk remains offline after the Bare Metal Restore (BMR) Windows recovery completed successfully.

**Etrack Incident: 4006549**

- Associated Primary Etrack: 4004511
- Associated Service Request Etrack(s): 4004510
- Description:  
Unable to segregate the DB name information from command output of `nbmariadb -o query` on the MariaDB database.

**Etrack Incident: 4006777**

- Associated Primary Etrack: 4006221
- Associated Service Request Etrack(s): 4006220
- Description:

After installation of Cloud Catalyst EEB bundle, new checks found duplicate inodes.

**Etrack Incident: 4006827**

- Associated Primary Etrack: 4006110
- Associated Service Request Etrack(s): 4006109
- Description:  
FT media server failed to start `nbftsrvr` and `nbfdrv64` processes after upgrade from NetBackup 8.0 to 8.1.2 (SUSE Linux).

**Etrack Incident: 4007463**

- Associated Primary Etrack: 4004748
- Associated Service Request Etrack(s): 4004747
- Description:  
One drive of a VM was not displayed when browsing for individual files.

**Etrack Incident: 4008054**

- Associated Primary Etrack: 4006514
- Associated Service Request Etrack(s): 4006513
- Description:  
An NetBackp Windows DLL file `log4net.dll` contained a vulnerability.

**Etrack Incident: 4008688**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
An OpenStack core dump was caused when an instance to be backed up was in a BUILD state.

**Etrack Incident: 4008731**

- Associated Primary Etrack: 4008600
- Associated Service Request Etrack(s): 4008599
- Description:  
Some jobs failed to backup to MSDP with status code 84 after a NetBackup appliance upgrade from 3.0 to 3.1.2.

**Etrack Incident: 4008750**

- Associated Primary Etrack: 4007682

- Associated Service Request Etrack(s): 4007681
- Description:  
filedel did not work properly for the MD5 algorithm.

**Etrack Incident: 4009184**

- Associated Primary Etrack: 3994887
- Associated Service Request Etrack(s): 3994886
- Description:  
Bpexpdate reported a status 0 when it fails to expire an image.

**Etrack Incident: 4009482**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
Catalog backup exited with partial success when there were non-existing users in the exported DR package.

**Etrack Incident: 4010215**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
NetBackup was unable to assign certificates for clients with hostnames longer than 64 characters.

**Etrack Incident: 4010759**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
Guava version in NBWSS differed from the one being used in web services.

**Etrack Incident: 4010881**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
OData server core version was not the latest version.

**Etrack Incident: 4011566**

- Associated Primary Etrack: 4010951



- Associated Service Request Etrack(s): 4010950
- Description:  
A CloudPoint upgrade or new installation failed if IPv6 is disable on the CloudPoint server.

**Etrack Incident: 4011750**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
`nbcert` and `nbwebservice` logs contained irrelevant information about ECA even when ECA was not configured. Also, secure inbound connections appeared in the Peer Host Validation report.

**Etrack Incident: 4011755**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
Secure inbound connections appeared in the Peer Host Validation report.

**Etrack Incident: 4012234**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
niversal Share BYO configuration failed if IPv6 was disabled.

**Etrack Incident: 4014231**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
When the operating system restarted on a media server, `spoold` would hang because it started before `spad` had not started.

**Etrack Incident: 4014342**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
APTARE reports displayed the Provider Generated ID instead of a user-friendly display name.

**Etrack Incident: 4015147**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
Many problems detected during SLP processing were logged only in the `nbstserv` log.

**Etrack Incident: 4016079**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
The inactivate SLP message was logged in the log file but did not appear in Problems report.

**Etrack Incident: 4017970**

- Associated Primary Etrack: 4017322
- Associated Service Request Etrack(s): 4017321
- Description:  
A Spring vulnerability was reported on a media server.

**Etrack Incident: 4017985**

- Associated Primary Etrack: 4017322
- Associated Service Request Etrack(s): 4017321
- Description:  
A Spring vulnerability was reported on a media server.

**Etrack Incident: 4018080**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
After a WORM backup with checkpoints enabled, a retry for an HDR image did not have WORM attributes enabled.

**Etrack Incident: 4018375**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:

The NetBackup web UI could not create a disk pool with more than one volume because the web UI did not support multiple disk volumes for the specified storage category.

**Etrack Incident: 4018382**

- Associated Primary Etrack: 4017387
- Associated Service Request Etrack(s): 4017386
- Description:  
Appliance media server upgrades failed if the `vm.conf` file was present.

**Etrack Incident: 4019071**

- Associated Primary Etrack: N/A
- Associated Service Request Etrack(s): N/A
- Description:  
Upgrades to NetBackup 8.3 reverted custom tuning parameters to default values in `OpsCenterServerService.xml` and `OpsCenterGUIService.xml` files.

# About SORT for NetBackup Users

This appendix includes the following topics:

- [About Veritas Services and Operations Readiness Tools](#)
- [Recommended SORT procedures for new installations](#)
- [Recommended SORT procedures for upgrades](#)

## About Veritas Services and Operations Readiness Tools

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

Access SORT from the following webpage:

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

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

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

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

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

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

## Recommended SORT procedures for new installations

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

**Table A-1**

Procedure	Details
Create a Veritas Account on the SORT webpage	See <a href="#">“To create a Veritas Account on the SORT page”</a> on page 22.
Create generic installation reports	See <a href="#">“To create a generic installation checklist”</a> on page 22.
Create system-specific installation reports	See <a href="#">“To create a system-specific installation report for Windows”</a> on page 23. See <a href="#">“To create a system-specific installation report for UNIX or Linux”</a> on page 24.

### To create a Veritas Account on the SORT page

- 1 In your web browser, navigate to:  
<https://sort.veritas.com/netbackup>
- 2 In the upper right corner, click **Login**, then click **Register now**.
- 3 Enter the requested login and contact information:

<b>Email address</b>	Enter and verify your email address
<b>Password</b>	Enter and verify your password
<b>First name</b>	Enter your first name
<b>Last name</b>	Enter your last name
<b>Company name</b>	Enter your company name
<b>Country</b>	Enter your country
<b>Preferred language</b>	Select your preferred language
<b>CAPTCHA text</b>	Enter the displayed CAPTCHA text. If necessary, refresh the image.

- 4 Click **Submit**.
- 5 When you receive your login information, you can log into SORT and begin uploading your customized information.

### To create a generic installation checklist

- 1 In your web browser, navigate to:  
<https://sort.veritas.com/netbackup>
- 2 Find and select the **Installation and Upgrade Checklist** widget.

**3** Specify the requested information

<b>Product</b>	Select the appropriate product from the drop-down menu. For NetBackup select <b>NetBackup Enterprise Server</b> or <b>NetBackup Server</b> .
<b>Product version you are installing or upgraded to</b>	Select the correct version of NetBackup. The most current version is always shown at the top of the list.
<b>Platform</b>	Select the operating system that corresponds to the checklist you want generated.
<b>Processor</b>	Select the correct processor type for your checklist.
<b>Product version you are upgrading from (optional)</b>	For new installations, do not make any selections. For upgrades, you can select the currently installed version of NetBackup.

**4** Click **Generate Checklist**.

- 5** A checklist corresponding to your choices is created. You can modify your selections from this screen, and click **Generate Checklist** to create a new checklist.

You can save the resulting information as a PDF. Numerous options are available for NetBackup and many of them are covered in the generated checklist. Please spend time reviewing each section to determine if it applies to your environment.

**To create a system-specific installation report for Windows**

- 1** Go to the SORT website:  
<https://sort.veritas.com/netbackup>
- 2** In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.
- 3** Select the **Data Collectors** tab
- 4** Select the radio button for **Graphical user interface** and download the correct data collector for your platform.

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.

- 5** Launch the data collector after it finishes downloading.

- 6 On the **Welcome** screen, select **NetBackup** from the product family section and click **Next**.
- 7 On the **System Selection** screen, add all computers you want analyzed. Click **Browse** to see a list of computers you can add to the analysis. Veritas recommends starting the tool with an administrator or a root account.
- 8 When all systems are selected, review the **System names** section and click **Next**.
- 9 In the **Validation Options** screen, under **Validation options**, select the version to which you plan to upgrade.
- 10 Click **Next** to continue
- 11 The utility performs the requested checks and displays the results. You can upload the report to My SORT, print the results, or save them. Veritas recommends that you upload the results to the My SORT website for ease of centralized analysis. Click **Upload** and enter your My SORT login information to upload the data to My SORT.
- 12 When you are finished, click **Finish** to close the utility.

**To create a system-specific installation report for UNIX or Linux**

- 1 Go to the SORT website:  
<https://sort.veritas.com/netbackup>
- 2 In the **Installation and Upgrade** section, select **Installation and Upgrade custom reports by SORT data collectors**.
- 3 Select the **Data Collector** tab.
- 4 Download the appropriate data collector for your platform.  

The data collector is OS-specific. To collect information about Windows computers, you need the Windows data collector. To collect information about UNIX computers, you need the UNIX data collector.
- 5 Change to directory that contains downloaded utility.
- 6 Run `./sortdc`  

The utility performs checks to confirm the latest version of the utility is installed. In addition, the utility checks to see it has the latest data. The utility then lists the location of the log file for this session.
- 7 If requested, press **Enter** to continue.
- 8 Select the **NetBackup Family** at the **Main Menu**.



- 9** Select **Installation/Upgrade report** when prompted **What task do you want to accomplish?**  
 You can select multiple options by separating your response with commas.
- 10** Specify the system or systems you want included in the report.  
 If you previously ran a report on the specified system, you may be prompted to run the report again. Select **Yes** to re-run the report.  
 The utility again lists the location of the log files for the session.  
 The progress of the utility is displayed to the screen.
- 11** Specify **NetBackup** when prompted for the product you want installation or upgrade reports.
- 12** Enter the number that corresponds to the version of NetBackup you want to install.  
 The utility again lists the location of the log files for the session.  
 The progress of the utility is displayed to the screen.
- 13** The utility prompts you to upload the report to the SORT website if you want to review the report online. The online report provides more detailed information than the text-based on-system report.
- 14** When your tasks are finished, you can exit the utility. You have the option to provide feedback on the tool, which Veritas uses to make improvements to the tool.

## Recommended SORT procedures for upgrades

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

**Table A-2**

Procedure	Details
Create a Veritas Account on the SORT webpage	See <a href="#">"To create a Veritas Account on the SORT page"</a> on page 22.

**Table A-2** (continued)

Procedure	Details
Create a system-specific upgrade report	See <a href="#">"To create a system-specific installation report for Windows"</a> on page 23. See <a href="#">"To create a system-specific installation report for UNIX or Linux"</a> on page 24.
Review the future platform and feature plans. Review the hot fix and emergency engineering binary release auditor information.	See <a href="#">"To review future platform changes and feature plans"</a> on page 26. See <a href="#">"To review hot fix and emergency engineering binary information"</a> on page 26.

**To review future platform changes and feature plans**

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

**To review hot fix and emergency engineering binary information**

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

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