NetBackup™ Release Notes

Release 11.1.0.2

VERITAS
now part of Cohesity

NetBackup™ Release Notes

Last updated: 2026-02-23

Legal Notice

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 Cohesity 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
Japan	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 Cohesity website.

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity 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

Contents

Chapter 1

About NetBackup 11.1.0.2

This chapter includes the following topics:

About the NetBackup 11.1.0.2 release

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 9.

About EEBs and release content

NetBackup 11.1.0.2 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. 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 11.1.0.2 can be found on the Cohesity Operations Readiness Tools (SORT) website and in the *NetBackup Emergency Engineering Binary Guide*.

See "About Cohesity Services and Operations Readiness Tools" on page 34.

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 3.1 is based on NetBackup 8.1 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.veritas.com/docs/000002217

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.veritas.com/docs/000040237

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

https://www.veritas.com/support/en_US/15143.html

About NetBackup third-party legal notices

NetBackup products may contain third-party software for which Cohesity 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:

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

Chapter 2

New features, enhancements, and changes

This chapter includes the following topics:

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, Cohesity routinely backdates platform support to previous versions of NetBackup. Refer to the NetBackup Compatibility List for all Versions for the most up-to-date platform support listings.

See "About the NetBackup 11.1.0.2 release" on page 7.

See "About NetBackup compatibility lists and information" on page 42.

NetBackup 11.1.0.2 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 11.1.0.2 are grouped below by category. Select a link to read more information about the topic.

New features

- Changes in Cohesity terminology
- Support for malware scanning of hypervisor backups on OST targets
- Simplified Cloud Scale upgrade

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 11.1.0.2 from a release earlier than 8.1, make sure that you read and understand the *NetBackup Read This First for Secure Communications* document. NetBackup 8.1 includes many enhancements that improve the secure communications of NetBackup components. The *NetBackup Read This First for Secure Communications* document describes the features and benefits of these enhancements:

  NetBackup Read This First for Secure Communications

Support changes and enhancements

- NetBackup 11.1.0.2 support additions and changes
- NetBackup 11.1 and earlier support additions and changes
- Several shutdown commands to be deprecated in a future release
- BMR now uses Windows ADK 10.1.22621 (ADK 2022)

Cloud-related changes and enhancements

- Update cloud configuration file on the primary and media server immediately after install or upgrade to NetBackup 11.1.0.2

Other announcements

Changes in Cohesity terminology

To modernize our terminology, Cohesity has begun to replace certain outdated terms with more current terms.

Note: As Cohesity continues to update its terminology, the deprecated terms and the new terms may be used interchangeably.

Deprecated term	New term
Master	Primary
Slave	Secondary or media server
Whitelist or white list	Allowed list
Blacklist or black list	Blocked list
White hat	Ethical
Black hat	Unethical

Update cloud configuration file on the primary and media server immediately after install or upgrade to NetBackup 11.1.0.2

If you use cloud storage in your NetBackup environment, you may need to update your cloud configuration file on the NetBackup primary server immediately after you install or upgrade to NetBackup 11.1.0.2. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 11.1.0.2, related operations fail.

Cohesity continuously adds new cloud support to the cloud configuration files between releases. Updating your cloud configuration files is necessary only if your cloud storage provider was added to the cloud configuration package after version 2.13.6.

The following cloud support has been added to version 2.13.7 and later but was not included in the NetBackup 11.1.0.2 final build:

- HPE Alletra Storage MP X10000 - Object Lock (S3)
- Cloud Object store protection (COSP) - HPE Alletra Storage MP X10000
- Secsmart HyperProtect Data Lake Storage (S3)
- Cloud Object store protection (COSP) Nutanix Objects
- Cloud Object store protection (COSP) - PSPACE InfiniStor
- Samsung Cloud Platform (S3)
- Cloud Object store protection (COSP) - Samsung Cloud Platform
- FortKnox for NetBackup AWS (S3) regions

  - Asia Pacific (Taipei)
  - Asia Pacific (Malaysia)
  - Asia Pacific (New Zealand)
  - Asia Pacific (Thailand)
- Amazon (S3) region
  - Asia Pacific (New Zealand)

https://www.veritas.com/content/support/en_US/downloads/update.UPD971796

For additional information on adding cloud storage configuration files, refer to the following technical article:

http://www.veritas.com/docs/100039095

Several shutdown commands to be deprecated in a future release

A new, fully documented command for shutting down NetBackup processes and daemons will be provided in an upcoming release. At that point, the following commands will no longer be available:

- `bp.kill_all`
- `bpdown`
- `bpclusterkill`

Please plan accordingly. The new command will be announced in future release notes and in the *NetBackup Commands Reference Guide*.

NetBackup 11.1.0.2 support additions and changes

Note: This information is subject to change. See the NetBackup Compatibility List for all versions for the most recent product and services support additions and changes.

NetBackup 11.1 and earlier support additions and changes

Note: This information is subject to change. See the NetBackup Compatibility List for all Versions for the most recent product and services support additions and changes.

The following products and services are supported for NetBackup 11.1 and earlier versions:

Platforms

- Primary, Media, and Client
  - Rocky Linux 9.7
  - Red Hat Enterprise Linux 9.7
- Client
  - Red Hat Enterprise Linux 10.1
  - Rocky Linux 9.7
  - Alma Linux 9.7
  - Alma Linux 10.1
  - AIX 7.3 TL4
  - Lustre File System 2.16.x – Red Hat Enterprise Linux 9.x

Database

- PostgreSQL 17.x – Red Hat Enterprise Linux 10
- SQLite 3.4.x – Red Hat Enterprise Linux 10
- PostgreSQL 18.x – Red Hat Enterprise Linux 9.x
- PostgreSQL 17.x – Red Hat Enterprise Linux 8.10
- PostgreSQL 18.x – Oracle Linux 8.x
- PostgreSQL 18.x – Rocky Linux 9.x
- PostgreSQL 18.x – Red Hat Enterprise Linux 8.x
- PostgreSQL 18.x – Oracle Linux 9.x
- PostgreSQL 18.x – SUSE 15SP7
- PostgreSQL 18.x – Windows Server 2022
- PostgreSQL 18.x – Rocky Linux 10.x
- HCL Domino 14.x – Windows Server 2025
- Microsoft SQL Server 2025 – Windows Server 2025
- Microsoft SQL Server 2022 – Windows Server 2025
- Exchange SE – Windows 2019
- Exchange SE – Windows 2022

- Exchange SE – Windows 2025
- PostgreSQL 17.x – SUSE Linux Enterprise Server 15.x
- MySQL 9.x – Debian 13
- MySQL 9.x – Red Hat Enterprise Linux 10
- Oracle Database 23ai – Windows Server 2025
- MariaDB 11.x – Debian 12.x
- PostgreSQL 18.x – Red Hat Enterprise Linux 10.x
- MariaDB 11.x – Debian 13
- SAP HANA 2.0 SPS 08 – SUSE Linux Enterprise Server 15 SP7
- PostgreSQL 18.x – Ubuntu 24.04
- PostgreSQL 18.x – Rocky Linux 8.10

NDMP

- Dell EMC Unity OS 5.5 NDMP – Red Hat Enterprise Linux 9.x

OpenStorage

- Dell EMC Data Domain DDVE 8.4 OpenStorage plug-in 8.4

Virtualization

- Azure Local 24H2 – Build 2510
- VMware Cloud Foundation 9
- Amazon Elastic VMware Service (Amazon EVS)
- Nutanix AOS 7.5
- Kubernetes – Vanilla 1.34
- Kubernetes – Vanilla 1.35

CloudStorage

- IDrive e2 Cloud storage region Paris – Red Hat Enterprise Linux 9.x
- Oracle Cloud Infrastructure (OCI) regions Indonesia North (Batam), Israel Central (Jerusalem), Saudi Arabia Central (Riyadh)
- Samsung Cloud Platform Cloud Storage (Standard)

CloudObjectStoreProtection

- Samsung Cloud Platform Cloud Object Store Protection (COSP)

Cluster Primary Server

- InfoScale 8.0.2 – SUSE Linux Enterprise Server 15 SP7

TapeLibraries

- Quantum Scalar i7

Support for malware scanning of hypervisor backups on OST targets

NetBackup 11.1.0.2 now supports malware scanning for hypervisor backup images stored on OpenStorage Technology (OST) targets. Media servers with Instant Access capability are supported for VMware, Nutanix AHV, and Hyper-V workloads. For more information, see the *NetBackup Security and Encryption Guide*.

Simplified Cloud Scale upgrade

This release of NetBackup 11.1.0.2 introduces a simplified Cloud Scale upgrade process using the `kubectl` plugin. The enhanced workflow significantly streamlines upgrades compared to NetBackup versions earlier than 11.1, reducing complexity and operational effort.

For more information, refer to *Cohesity Cloud Scale Technology Manual Deployment Guide for Kubernetes Clusters.*

BMR now uses Windows ADK 10.1.22621 (ADK 2022)

Bare Metal Recovery (BMR) now uses a newer, supported version of the Windows Assessment and Deployment Kit (ADK), providing improved security, better compatibility with modern Windows environments, and longer-term support for customers.

BMR now supports **Windows ADK 2022 (version 10.1.22621).**

Warning: The exact same versions of Windows ADK and WinPE listed below must be used when creating the System Recovery Tool (SRT).

Other ADK or WinPE versions are **not supported**.

Both components must be pre installed before creating a new SRT.

Note: Use only the following Microsoft provided installers:

- Windows ADK (Deployment Tools):
  Windows Preinstallation Environment (WinPE)
- Windows ADK – Windows Preinstallation Environment (WinPE)

Windows Preinstallation Environment

Chapter 3

Operational notes

This chapter includes the following topics:

About NetBackup 11.1.0.2 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 Cohesity 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 Cohesity Support website:

NetBackup Release Notes, Administration, Installation, Troubleshooting, Getting Started, and Solutions Guides

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 11.1.0.2.

If NetBackup 11.1.0.2 upgrade fails on Windows, revert to previous log folder structure

The legacy log folder structure for non-root or non-admin invoked process logs has changed. The new folder structure is created under the process log directory name. For more information, refer to the *File name format for legacy logging* section from the NetBackup Logging Reference Guide.

For Windows, if the upgrade to NetBackup 11.1.0.2 fails and rollback occurs, run the following command to continue working on an earlier NetBackup version:

```
mklogdir.bat -fixFolderPerm
```

For more information, refer to the `mklogdir` command from the NetBackup Commands Reference Guide.

Native installation requirements

In NetBackup 8.2, a change was made to initial installs such that the answer file is now required. This change may have some negative effect on users who want to use the native packages to create VM templates or otherwise install the NetBackup packages without configuring the product. On Linux, one possible way of obtaining the previous behavior is with the `-noscripts` option of the RPM Package Manager. Providing this option when installing the `VRTSnbpck` package avoids the configuration steps. This option does not need to be provided when you install other packages. The answer file must still exist, but the only value that must be provided is the role of the machine, either a client or a media server. For example:

```
echo "MACHINE_ROLE=CLIENT" > /tmp/NBInstallAnswer.conf
rpm -U --noscripts VRTSnbpck.rpm
rpm -U VRTSpbx.rpm VRTSnbclt.rpm VRTSpddea.rpm
```

NetBackup servers must use a host name that is compliant with RFC 1123 and RFC 952

Starting with NetBackup 8.0, all NetBackup server names must use a host name that is complaint with RFC 1123 ("Requirements for Internet Hosts - Application and Support") and RFC 952 ("DOD Internet Host Table Specification") standards. These standards include the supported and unsupported characters that can be used in a host name. For example, the underscore character (_) is not a supported character for host names.

More information is available about these standards and about this issue:

RFC 952

RFC 1123

http://www.veritas.com/docs/000125019

These standards should be applied to all computing hosts, including all NetBackup hosts. To accommodate legacy environments and functionality, features of NetBackup that were implemented before 2010 continue to allow some non-compliant characters. But newer features, as well as more recently integrated 3rd-party components, are not tested with nor expected to be compatible with host names that do not adhere to the industry standards.

In some situations, it may be possible to configure name services with a network hostname alias that is standards-compliant, and then use the alias when you configure NetBackup. But using host names that are standards-compliant is the only way to ensure compatibility with all features.

About support for HP-UX Itanium vPars SRP containers

Hewlett-Packard Enterprise (HPE) 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 run 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.

NetBackup only supports installing into the global view. NetBackup installation fails if you try to install into an HPE Itanium SRP container (private file system, shared file system, or workload).

Change in the default path for NetBackup installation

Starting with NetBackup 11.1, the default path for NetBackup installation is as follows:

`C:\Program Files\Cohesity NetBackup\NetBackup`

The default installation path for NetBackup 11.0.0.1 and earlier versions is as follows:

`C:\Program Files\Veritas`

In a cluster, you must ensure that installation paths for all cluster nodes are the same. In case of an upgrade from NetBackup 11.0.0.1 or earlier to NetBackup 11.1, you must check the default installation path of the older cluster nodes and use the same path for the new node that you want to add.

For example, if old cluster nodes have the default installation path, you must use `C:\Program Files\Veritas` as installation path for the new node after the upgrade.

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 11.1.0.2.

For more information about the specific NetBackup administration interfaces, refer to the *NetBackup Web UI Administrator's Guide* or 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 Cohesity Support website.

See “About NetBackup compatibility lists and information” on page 42.

Intermittent issues with X forwarding of NetBackup Administration Console

Intermittent issues may occur with X forwarding of the NetBackup 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.

NetBackup Administration Console fails in Simplified Chinese UTF-8 locale on Solaris SPARC 64-bit systems with Solaris 10 Update 2 or later

The NetBackup 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 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 11.1.0.2.

After PIT restore, "The host ID does not exist" error appears

After a point-in-time (PIT) restore operation (which may include either a Full File System restore or a BMR restore), the error message **The hostID does not exist** appears.

In this scenario, a full backup is taken when a SERVICE_USER as root/administrator account is configured. This account takes the backup of the NetBackup installed binaries with root/administrator ownership.

Before a restore, SERVICE_USER is configured with an account other than root/administrator, and then an incremental backup is taken where the service user is backed up as part of `bp.conf`. In a PIT restore operation with the incremental backup, the SERVICE_USER entry gets restored. However, the binaries are restored in the root account ownership.

Workaround

After changing the service user, you must take a full backup, whether it is a MS-Windows\Standard Policy for File System or BMR policy configuration.

NetBackup services may not start automatically after BMR restore on a Linux client

NetBackup services may not start automatically after a Bare Metal Restore (BMR) restore operation is performed on the Linux client.

The NetBackup services may run for a while after a BMR restore operation, and the BMR post-restore scripts may complete successfully. Later, however, NetBackup services may stop.

This issue happens only if a service user is different than the root user that is defined on the NetBackup Linux client.

Workaround

Start the NetBackup services manually on the Linux client.

To start the services, run the following command:

```
/usr/openv/netbackup/bin/bp.start_all
```

NetBackup Bare Metal Restore on AWS hangs when restoring a Windows 2025 client

On AWS, Windows 2025 uses NVMe disks by default. Bare Metal Restore does not support NVMe disks.

Workaround:

No workaround for this issue.

Mirrored dynamic volume may not receive a drive letter after Windows BMR DDR restore

In Windows Bare Metal Restore (BMR) environments that use Dissimilar Disk Restore (DDR), mirrored (RAID-1) dynamic volumes may not automatically receive a drive letter after the restore. This behavior is expected due to the way Windows Disk Management and DDR handle dynamic disks during disk reconstruction and system startup.

Cause

During a BMR DDR restore, disk and volume reconstruction is prioritized over drive-letter assignment. The BMR process focuses on restoring the disk layout, partition structure, and dynamic disk metadata. Drive letters for non-system volumes are not guaranteed to be reassigned during this stage.

After the restore, mirrored dynamic volumes may appear in the following states:

- Resynching
- Degraded
- Healthy (no drive letter assigned)

Windows may delay drive-letter assignment until the dynamic mirror is fully recognized and stabilized. Additionally, if the original drive letter is already reserved, temporarily assigned, or conflicting with another volume during boot, Windows may withhold letter assignment to avoid collision.

In DDR scenarios that involve dissimilar hardware, changed disk order, or other mapping differences, only the system volume (C:) is guaranteed to be auto-mapped. Other volumes may be restored successfully but remain unmounted. In Disk Management, the mirrored volume typically appears as:

- Healthy
- Dynamic
- No drive letter

The volume is accessible but not mounted, and applications may fail until a drive letter is manually assigned.

Workaround

After the system boots, manually assign the drive letter using Windows Disk Management:

1. Open **Disk Management**.
2. Right-click the mirrored volume.
3. Select **Change Drive Letter and Paths**.
4. Assign the desired drive letter.

After the letter is assigned, the volume becomes fully functional. No rebuild, reformat, or additional restore operation is required.

BMR Restore Failure for ReFS Volumes on Windows (2016–2025)

Cause

During a Bare Metal Restore (BMR) on Windows Server 2016, 2019, 2022, or 2025, ReFS volumes fail to restore and appear in an “Unformatted” state.

This occurs because **no version of ADK/WinPE supports bare-metal or block-level restore of ReFS volumes**, due to incompatibilities between ReFS versions.

ReFS Versions Used in Installed Operating Systems

Table 3-1

Windows Version	ReFS Version
Windows Server 2016	3.1
Windows Server 2019	3.4
Windows Server 2022	3.7
Windows Server2025	3.14

ReFS Version in SRT / WinPE Environment

Table 3-2

Environment	ReFS Version
SRT / ADK WinPE	3.9

Important Compatibility Note

The **WinPE ReFS driver (3.9)** cannot be **downgraded** or made backward compatible with OS-specific ReFS versions (3.1, 3.4, 3.7, 3.14).

Microsoft provides no workaround for this downgrade limitation.

As a result:

- Restored ReFS volumes appear **Unformatted**
- The target OS cannot read WinPE-created ReFS 3.9 metadata
- The volume becomes unusable after BMR restore

Cause

ReFS versions are not backward compatible at the metadata level.

Key Rules:

- A lower ReFS driver cannot recreate or replay metadata from a higher version
- WinPE’s ReFS driver is read-mostly, not designed for reconstruction
- BMR restore requires metadata replay, allocation maps, and integrity stream handling—operations that fail on version mismatch

Compatibility Matrix

All combinations below fail due to version mismatch:

Table 3-3

Source Volume (ReFS)	Target OS	WinPE ReFS (3.9)	Result
3.14 (Windows 2025)	Server 2025	3.9	Fail
3.7 (Winodws 2022)	Server 2022	3.9	Fail
3.4 (Winodws 2019)	Server 2019	3.9	Fail
3.4 (Windows 2016)	Server 2016	3.9	Fail

Why it fails:

- WinPE cannot create the required ReFS metadata structures
- Version mismatch prevents metadata replay
- Restore tools fall back to unsupported APIs

Solution

There is **no direct solution**.

Microsoft has not provided any method to upgrade or downgrade ReFS versions during BMR workflows.

Workaround

To ensure ReFS volumes are restored with the correct 3.x version matching the original operating system, perform the following steps:

1. Right-click the BMR configuration and create a copy using **New Client Configuration**.
2. Edit the copied configuration and **exclude all ReFS volumes** from volume mapping.
3. Run **Prepare to Restore** and proceed with the system restore.
4. After the machine boots into the restored operating system:
   - Create the ReFS volumes excluded in step 2
   - Format them using **Disk Management** or **DISKPART**
   - Windows will automatically create the ReFS volume using the correct version for that OS
5. Verify the ReFS version using: `fsutil fsinfo refsinfo <DriveLetter:>`
6. Restore the data for these volumes from **Recovery** tab in **NetBackup Web UI**.

Post Bare Metal Restore (BMR) operation, windows Start Menu and Search not functioning

Problem

Post Bare Metal Restore (BMR) operation, windows **Start Menu** and **Search** not functioning.

This behavior has been observed on the **Windows Server 2019 (2K19) EFI** client.

Cause

The most probable cause is that the AppX State Repository database was not properly updated during the recovery process.

While application files were successfully restored, the system's internal registration database was not synchronized, leading to failures in initializing built-in Windows components.

Solution

Follow the Microsoft's documentation and recommendations for registering the Appx Package.

Apart from official documentation, the following procedure may assist in resolving registration-related inconsistencies.

Recovery Procedure

1. Open PowerShell as an administrator.
2. Run the following command:

```
Get-AppXPackage -AllUsers | Foreach {
  Add-AppxPackage -DisableDevelopmentMode -Register
"$($_.InstallLocation)\AppXManifest.xml"
}
```

   This command re-registers all installed AppX packages by reading their respective `AppXManifest.xml` files and rebuilding the associated registration data

Functional Impact

Executing this command performs the following actions:

- Enumerates all installed AppX packages across all user profiles
- Parses each `AppXManifest.xml`
- Rebuilds package activation and identity mappings

- Re-indexes packages in the Windows State Repository
- Re-applies required security identifiers (including **ALL APPLICATION PACKAGES**)
- Reconstructs AppX deployment metadata

This process helps resolve AppX package registration mismatches and related shell initialization issues.

Post-Registration Action

After completing the re-registration:

- Restart the Windows Shell by restarting the `explorer.exe` process to ensure the updated registrations are applied.

Preconditions and Validation Checks

Before performing AppX package re-registration, verify the following:

AppLocker Configuration

- Ensure no AppLocker Deny rules are blocking packaged applications.
- Open secpol.msc and navigate to: `Application Control Policies → AppLocker`
- Confirm that no rules deny execution of Packaged Apps.

Required Directories

Ensure the following directories exist:

- `C:\Windows\System32\AppLocker`
- `C:\Windows\AUInstallAgent`

If missing, create them.

Do not delete these directories if they already exist.

AppReadiness Directory

- Verify that `C:\Windows\AppReadiness` exists.
- If missing, create the directory.

This location is required for AppX staging operations.

Registry Validation

- Navigate to: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Appx`

- Confirm that the PackageRoot registry value points to:`C:\Program Files\WindowsApps`

Optional Service Restart

If required, restart the AppX deployment service before or after package re-registration:

```
Restart-Service AppXSVC -Force
```

Official Error Context

- **0x80073CF9 (Install Failed)**: Officially defined as "The package deployment failed because the staging operation could not be completed.".
  In a BMR Scenario:
  This typically indicates that:
  The Staging Operation is the process where Windows prepares the application before committing it to the State Repository.
  - The AppReadiness directory is missing
  - The AUInstallAgent staging directory is missing
  - Directory permissions are incorrect
- **0x80070003 (Path Not Found)**: Officially refers to a "Deployment Target Access failure."
  In a BMR Scenario:
  This confirms that: may be missing or inaccessible due to stripped or incorrect SIDs.
  This indicates that the database contains registration references, but the physical directory structure is either missing or inaccessible.
  - The AppX database cannot locate the required directory structure
  - `C:\Windows\SystemApps` or
  - `C:\Program Files\WindowsApps`

Warning message after BMR restore on Windows

After performing a Bare Metal Restore (BMR) restore on Windows clients, users may see the following warning message:

The Recycle Bin on c:\ is corrupted. Do you want to empty the Recycle Bin for this drive?.

Behavior details

- The warning may appear for each drive present on the restored system, not just the C: drive.
- The hidden system folders `$Recycle.Bin` and `System Volume Information` may be visible on all drives.
- This message may appear even when the Recycle Bin does not contain any user data.

NetBackup Cloud Object Store Workload operational notes

This topic contains some of the operational notes and known issues that are associated with the NetBackup Cloud Object Store Workload in version 11.1.0.2.

Full backup after upgrading from a version prior to NetBackup 11.1

Amazon S3 is discontinuing support for the Display name parameter in the Owner object for some APIs and regions. This change may affect how NetBackup identifies backups. If the Display name parameter is missed from the previous backups, NetBackup treats the backup as new instead of incremental.

Workaround:

There is no workaround. After upgrade, NetBackup performs a full backup initially. The subsequent backups are incremental backups, if configured in the policy.

Note the following:

- Plan for this behavior when you upgrade from NetBackup versions prior to 11.1.
- Review backup schedules and storage capacity to accommodate a potential full backup post-upgrade.

Supported version of RHEL media server as backup host

The supported RHEL media server version as backup host for the Cloud Object Store workload in NetBackup 11.1.0.2 is RHEL 9.5 or earlier.

Auto Image Replication (AIR) from NetBackup version 11.1.0.2 requires NetBackup 10.2 or later

You cannot run Auto Image Replication (AIR) from a computer with NetBackup version 11.1.0.2 to a target computer with a NetBackup version that is earlier than version 10.2.

Workaround:

None. Upgrade the target computer to NetBackup version 10.2 or later.

Backup jobs become unresponsive and consume significant space on the temporary staging location.

NetBackup Cloud object store data protection feature uses the `ListObjects S3` API to iterate over the list of objects to further read and back up the objects in a bucket. The `ListObjects S3` API returns up to 1000 objects per request in lexicographical order, based on their key names and the NextContinuationToken. This NextContinuationToken is used for pagination. For example, for a `ListObjects S3` API call, to get the next set of 1000 objects and a new NextContinuationToken is used to get the subsequent page.

For certain Cloud object store providers, like Hitachi, the NextContinuationToken does not work correctly if the object names contain certain special characters, potentially hinders backup performance.

This behavior disrupts the `cos_sqllite` database that NetBackup uses in the temporary staging area. This database stores the object list for a backup job that is in progress. Because of this disruption, the `cos_sqllite` database drastically grows in size, filling up the disk space in the temporary staging area. This leads the NetBackup jobs to slow down and eventually fail.

Workaround:

1. Reconfigure the NextContinuationToken in the `ListObjects S3` API calls to return the proper value for each batch.
2. Cancel the existing backup job and retry backup.

NetBackup NAS operational notes

NetBackup Snapshot Manager and NDMP V4 snapshot extension can make snapshots of client data on a NAS host. A NAS snapshot is a point-it-time disk image. You can retain the Snapshots on the disk for any duration. Using the Instant Recovery feature in NetBackup, you can efficiently restore the data from the disk. Broadly, in NetBackup, snapshot-based data protection for NAS can be performed

using NAS-Data-Protection policy and NDMP policy. This topic contains some of the operational notes and known issues that are associated with NetBackup NAS in NetBackup 11.1.0.2.

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 Cohesity Support website:

http://www.veritas.com/docs/000095049

NetBackup Cloud workload operational notes

This topic contains some of the operational notes and known issues that are associated with the NetBackup Cloud workload in version 11.1.0.2.

VMs and other OCI assets with CMK-encrypted disks are marked as deleted in NetBackup UI.

If the KMS service at the OCI provider is down, the VMs and other assets with CMK-encrypted disks are marked as deleted in NetBackup UI. Once the KMS service is restored, the deleted status is cleared after a successful plug-in level discovery, and the assets or VMs become eligible for backup. No further action is required.

Workaround:

Ensure that the KMS service at the OCI provider-end is running.

NetBackup 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 11.1.0.2.

Support for localized environments in database and application agents

Non-ASCII characters are supported in the following fields for NetBackup database and application agents.

- Oracle:
  Datafile path, Tablespace name, TNS path
- DB2:
  Datafile path, Tablespace name
- SAP:
  English SAP runs on localized OS. (No specific SAP fields are localized.)
- Exchange:
  Mailboxes, Mails, Attachment names and contents, Public folders, Contacts, Calendar, Folders and Database paths
- SharePoint:
  Site Collection Names, Libraries and lists within the site collection
- Lotus Notes:
  Emails data /.nsf files
- Enterprise Vault (EV) agent:
  Vault store, Partitions, Data
- VMWare:
  Username, Password, VM display name, DataCenter, Folder, Datastore, Resource pool, VApp, Network name, VM disk path

Certain 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 (primary server, media server, Enterprise Media Manager (EMM) server, volume database host, media host, client, instance group)
- 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
- Token name
- Storage lifecycle policy (SLP) names

Appendix A

About SORT for NetBackup Users

This appendix includes the following topics:

About Cohesity Services and Operations Readiness Tools

Cohesity Services and Operations Readiness Tools (SORT) is a robust set of standalone and web-based tools that support 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.
- **NetBackup Future Platform and Feature Plans**
  Use this tool to determine what items you can expect to see replaced with newer and improved functionality. The tool also provides insight about what items you can expect to see discontinued without replacement. Some of these items include certain NetBackup features, functionality, 3rd-party product integration, other 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

Appendix B

NetBackup installation requirements

This appendix includes the following topics:

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 Installation Guide* and the *NetBackup Upgrade Guide*.

See "NetBackup installation and upgrade operational notes" on page 18.

- Before you upgrade the NetBackup server software, you must back up your NetBackup catalogs and verify that the catalog backup was successful.
- Before upgrading to NetBackup 11.1.0.2, you must ensure that you have the free disk space that is twice the size of the NetBackup relational database. That means for default installations of the primary server, you are required to have that amount of free space on the file system containing the `/usr/openv/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.

- Primary 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 articles on the Cohesity Support website:
  http://www.veritas.com/docs/000013512
- NetBackup primary 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.
- Cohesity recommends that you have the primary 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 for All Versions. 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, and so on) 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, Cohesity recommends that you install the latest OS updates on your servers and clients before you install or upgrade NetBackup.

The most up-to-date required OS patch information for NetBackup 11.1.0.2 and other NetBackup releases can be found on the Cohesity Services and Operational Readiness Tools (SORT) website and in the NetBackup Compatibility Lists for All Versions. 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.

See "About NetBackup compatibility lists and information" on page 42.

See "About Cohesity Services and Operations Readiness Tools" on page 34.

NetBackup 11.1.0.2 binary sizes

The following table contains the approximate binary sizes of the NetBackup 11.1.0.2 primary server, media server, and client software for the various supported operating systems. These binary sizes indicate the amount of disk space occupied by the product after an initial installation. Note that for the sizes listed in the table, 1 MB equals 1024 KB.

Note: The table lists only 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 Services and Operations Readiness Tools (SORT) website, or the NetBackup Compatibility List for all Versions.

Table B-1 NetBackup binary sizes for compatible platforms

OS	CPU Architecture	64-bit client	64-bit server	Notes
AIX	64-bit client	1978 MB	No longer supported	
Alma Linux		1978 MB		
Amazon Linux		1971 MB		
BC-Linux		1978 MB		
Canonical Ubuntu	x86-64	1978 MB		

Table B-1 NetBackup binary sizes for compatible platforms *(continued)*

OS	CPU Architecture	64-bit client	64-bit server	Notes
CentOS	x86-64	1978 MB	7353 MB	
Debian GNU/Linux	x86-64	1978 MB		
Kylin Linux Advanced Server 10.0		1978 MB		
NeoKylin Linux Advanced Server		1978 MB		
Oracle Linux	x86-64	1978 MB	7353 MB	
Red Hat Enterprise Linux Server	POWER 8/9 client	503 MB		
Red Hat Enterprise Linux Server	x86-64	1978 MB	7353 MB	
Red Hat Enterprise Linux Server	z/Architecture	710 MB	No longer supported	Media server or client compatibility only.
Rocky Linux client		1978 MB		
Solaris	SPARC	1090 MB	No longer supported	
Solaris	x86-64	1047 MB	No longer supported	
SUSE Linux Enterprise Server	POWER 8/9 client	508 MB		
SUSE Linux Enterprise Server	x86-64	1399 MB	6614 MB	

Table B-1 NetBackup binary sizes for compatible platforms *(continued)*

OS	CPU Architecture	64-bit client	64-bit server	Notes
SUSE Linux Enterprise Server	z/Architecture	483 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64	1210 MB	5898 MB	Covers all compatible Windows x64 platforms.

Appendix C

NetBackup compatibility requirements

This appendix includes the following topics:

About compatibility between NetBackup versions

You can run mixed versions of NetBackup between primary 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.

NetBackup supports only certain combinations of servers and clients. In mixed version environments, certain computers must be the highest version. Specifically, the version order is: NetBackup Snapshot Manager computer, primary server, media server, and then clients. For example, the scenario that is shown is supported: 11.0 NetBackup Snapshot Manager > 10.2 primary server > 10.0 media server > 9.1.0.1 client.

All NetBackup versions are four digits long. The NetBackup 11.0 release is the 11.0.0.0 release. Likewise, the NetBackup 10.2 release is the NetBackup 10.2.0.0 release. For the purposes of supportability, the fourth digit is ignored. A 10.2 primary server supports a 10.2.0.1 media server. An example of what is not supported is a 10.2.0.1 primary server with a 11.0 media server.

The NetBackup catalog resides on the primary server. Therefore, the primary 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 primary server to perform a catalog backup.

For complete information about compatibility between NetBackup versions, refer to the Cohesity SORT website.

Review the End of Support Life information available online.

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 Cohesity Operations Readiness Tools (SORT) for NetBackup website.

See "About Cohesity Services and Operations Readiness Tools" on page 34.

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, Cohesity has made available a variety of compatibility lists to help customers quickly reference up-to-date compatibility information for NetBackup:

NetBackup Compatibility Lists for All Versions

Note: For information about which versions of NetBackup are compatible with each other, select a **Software Compatibility List (SCL)**, and then select **Compatibility Between NetBackup Versions** from within the SCL.

About NetBackup end-of-life notifications

Cohesity 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. Cohesity 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 Cohesity 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.

Cohesity provides advance notification to better help its customers to plan for upcoming changes to the support status of the various features in NetBackup. Cohesity 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. Cohesity 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 Cohesity Services and 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.veritas.com/nbufutureplans

NetBackup end-of-support-life (EOSL) information is also available at the following location:

https://sort.veritas.com/eosl/show_matrix

See “About Cohesity Services and Operations Readiness Tools” on page 34.

About changes in platform compatibility

The NetBackup 11.1.0.2 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 9.

http://www.netbackup.com/compatibility

Appendix D

Other NetBackup documentation and related documents

This appendix includes the following topics:

About related NetBackup documents

Cohesity releases various guides that relate to NetBackup software. Unless otherwise specified, the NetBackup documents can be downloaded in PDF format or viewed in HTML format from the NetBackup Documentation Landing Page.

Not all documents are published with each new release of NetBackup. In the guides, you may see references to other documents that were not published for NetBackup 11.1.0.2. In these cases, refer to the latest available version of the guide.

Note: Cohesity assumes no responsibility for the correct installation or use of PDF reader software.

All references to UNIX also apply to Linux platforms unless otherwise specified.
