NetBackup™ Release Notes

Release 11.2

VERITAS
now part of Cohesity

NetBackup™ Release Notes

Last updated: 2026-06-09

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1

About NetBackup 11.2

This chapter includes the following topics:

About the NetBackup 11.2 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 10.

About EEBs and release content

NetBackup 11.2 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 11.2 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 53.

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:

https://support.cohesity.com/s/article/article-100040113

About NetBackup Late Breaking News

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

https://support.cohesity.com/s/article/article-100022065

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.cohesity.com/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 11.2 release” on page 8.

See “About NetBackup compatibility lists and information” on page 61.

NetBackup 11.2 new features, changes, and enhancements

New features, changes, and enhancements in NetBackup 11.2 are grouped below by category. Select a link to read more information about the topic.

New features

Secure communication features, changes, and enhancements

- **Note:** Before you install or upgrade to NetBackup 11.2 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 11.2 support additions and changes
- NetBackup 11.1.0.2 and earlier support additions and changes qualified in NetBackup 11.2
- Several shutdown commands to be deprecated in a future release

Installation, upgrade, and configuration changes and enhancements

- Flexible Version Compatibility for Kubernetes Operator

Cloud-related changes and enhancements

- Update cloud configuration file on the primary and media server immediately after install or upgrade to NetBackup 11.2

Workload and database agent changes and enhancements

- Enhanced Log Collection in NetBackup Web UI
- MS Exchange Recovery from NetBackup Web UI
- Backup Selections Tab in Policies in NetBackup Web UI
- Change job priority for quewed jobs in Activity Monitor
- Enhanced report time selection and control
- Enhanced Backup Capabilities for MongoDB Ops Manager

Other important announcements

- EOL of NetBackup Administration Console (Java UI) starting with 11.2
- Knowledge Base article updates
- About the new Cohesity Unified Documentation Portal

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

About the new Cohesity Unified Documentation Portal

You can access all Cohesity product documentation using the new Unified Documentation Portal (UDP):

docs.cohesity.com

The NetBackup documentation is available on the new UDP on the following location:

https://docs.cohesity.com/docs/netbackup

Knowledge Base article updates

Knowledge Base Articles (tech notes) have transitioned from the Veritas domain to the Cohesity domain. As a result, users will now need a MyCohesity account to access these articles. If you already have an account, simply log in to continue accessing the content.

To create a new MyCohesity account, visit the following website:

https://my.cohesity.com

EOL of NetBackup Administration Console (Java UI) starting with 11.2

Starting with NetBackup 11.2, the NetBackup Administration Console (Java UI) on Windows and Unix/Linux, and the Java Remote Administration Console (RAC) will no longer be delivered. These components will not be available for installation. The components will be removed during NetBackup 11.2 upgrade.

However, the Java Backup, Archive and Restore (BAR) GUI will be available on the platforms that currently support it. The Windows MFC BAR GUI will also be available.

NetBackup 11.2 documents have references to the NetBackup Administration Console (or Java UI) and its functions with respect to their old versions. These references will be removed eventually.

File hash calculation for threat detection

NetBackup now supports hash calculation for files stored in backup images, including files inside compressed and archive formats.

This feature generates SHA-256 hashes after backup and stores them for use in threat detection. These hashes can be matched against known malicious indicators to help identify potential threats in backup data.

For more information, refer to the *NetBackup™ Security and Encryption Guide*.

Update cloud configuration file on the primary and media server immediately after install or upgrade to NetBackup 11.2

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 11.2. If a cloud provider or related enhancement is not available in the cloud configuration file after you upgrade to NetBackup 11.2, 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 2.14.1 and later but was not included in the NetBackup 11.2 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)

For the latest cloud configuration package, see the following article:

https://support.cohesity.com/s/update-detail?c__updateId=UPD971796

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

https://support.cohesity.com/s/article/article-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*.

RESTful APIs included in NetBackup 11.2

NetBackup 11.2 includes both updated and new RESTful application programming interfaces (APIs). These APIs are built on the Representational State Transfer

(REST) architecture. They provide a web-service-based interface that lets you configure and administer NetBackup in your environments.

API documentation

You can find documentation for the NetBackup APIs in on SORT and on your primary server. Make sure to review the *Versioning* topic and the *What's New* topic in the *Getting Started* section.

- On SORT:
  NetBackup API documentation is available on SORT:
  HOME > KNOWLEDGE BASE > Documents > Product Version > 11.2
  Look under **API Reference**. A *Getting Started* document provides background information about using NetBackup APIs. The API YAML files are also available for reference, however, they are not functional. You cannot test the APIs from the documents on SORT.
- On your primary server:
  APIs are stored in YAML files on the primary server:
  `https://<primary_server>/api-docs/index.html`
  The APIs are documented in Swagger format. This format lets you review the code and test the functionality by making actual calls with the APIs. You must have the appropriate security permissions to access the primary server and APIs to use the Swagger APIs.

  Caution: Cohesity recommends that you test APIs only in a development environment. Because you can make actual API calls from the Swagger files, you should not test the APIs in a production environment.

NetBackup 11.2 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.

The following products and services are supported starting with NetBackup 11.2:

Platforms:

- FTMS Server - Red Hat Enterprise Linux 8.10 [Qlogic]
- Primary Server - Oracle Linux 10.1 (UEK/RHCK)
- Media Server - Oracle Linux 10.1 (UEK/RHCK)

- Primary Server - Rocky Linux 10.1
- Media Server - Rocky Linux 10.1

Databases:

- PostgreSQL - Red Hat Enterprise Linux 9 [z/Architecture]
- PostgreSQL - Red Hat Enterprise Linux 8 [z/Architecture]
- MySQL - Red Hat Enterprise Linux 9 [z/Architecture]
- MySQL - Red Hat Enterprise Linux 8 [z/Architecture]
- Oracle Database 19c - Red Hat Enterprise Linux 9.x [z/Architecture]
- Informix 15.x - AIX 7.3 [POWER]
- Informix 15.x - Red Hat Enterprise Linux 10
- SAP ASE 16.1 - Red Hat Enterprise Linux 10 [x86-64]

OpenStorage:

- Dell EMC Data Domain OpenStorage plug-in 8.6 - Oracle Linux 10.x
- Dell EMC Data Domain OpenStorage plug-in 8.6 - Rocky Linux 10.x

NetBackupSnapshotManager:

- NetBackup Snapshot Manager - Rocky Linux 10

Bare Metal Restore (BMR):

- Primary/Client/Boot Server - Red Hat Enterprise Linux 9.7
- Primary/Client/Boot Server - Red Hat Enterprise Linux 9.6

NetBackup 11.1.0.2 and earlier support additions and changes qualified in NetBackup 11.2

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 11.1.0.2 and earlier versions and qualified with NetBackup 11.2.

Platforms:

- Client
  - Client – Ubuntu 26.04

- VxFS File System Qualification – Red Hat Enterprise Linux 9.7
- VxFS File System Qualification – Red Hat Enterprise Linux 10.1
- GPFS File System 6.0.0.1 – Red Hat Enterprise Linux 8.10
- GPFS File System 6.0.0.1 – Red Hat Enterprise Linux 9.6
- GPFS File System 6.0.0.1 – Ubuntu 22.04
- GPFS File System 6.0.0.1 – Ubuntu 24.x
- Lustre File System 2.17.x – Red Hat Enterprise Linux 9.x
- Lustre File System 2.17.x – Red Hat Enterprise Linux 10.x
- Lustre File System 2.17.x – SUSE 15 SP7
- VxFS File System Qualification – Oracle Linux 9.7
- VxFS File System Qualification – Oracle Linux 10.1

Database:

- SAP HANA 2.0 SP08 – Red Hat Enterprise Linux 10.x
- SAP ASE 16.1 – Red Hat Enterprise Linux 10
- Oracle Database 26ai – SUSE Linux 15.x
- PostgreSQL 18.x – Ubuntu 22.04
- PostgreSQL 18.x – Oracle Linux 10.x
- PostgreSQL 17.x – Rocky Linux 10
- PostgreSQL 17.x – Oracle Linux 10
- PostgreSQL 18.x – Windows Server 2025
- DB2 12.x – Ubuntu 24.04
- DB2 12.x – Red Hat Enterprise Linux 10.x
- DB2 12.x – Windows Server 2025
- SQLite 3.51.x – Windows Server 2025
- SQLite 3.46.x – Rocky Linux 10.x
- MySQL 8.x – Oracle Linux 9

NDMP:

- NetApp ONTAP 9.18.x NDMP
- Dell EMC PowerScale OneFS 9.11 NDMP

OpenStorage:

- Dell EMC Data Domain OpenStorage plug-in 8.6 – Oracle Linux 9.x
- Dell EMC Data Domain OpenStorage plug-in 8.6 – Rocky Linux 9.x
- Dell EMC Data Domain OpenStorage plug-in 8.6 – Red Hat Enterprise Linux 10.x

CloudStorage:

- FortKnox for NetBackup – Azure region Chile Central
- FortKnox for NetBackup – AWS region Asia Pacific (Malaysia)
- FortKnox for NetBackup – AWS region Israel (Tel Aviv)

Cluster Primary Server:

- InfoScale 9.1 – Windows Server 2022
- InfoScale Cluster 9.1 – Red Hat Enterprise Linux 9.7

TapeLibraries:

- Quantum Scalar i3

TapeDrives:

- HPE LTO8 tape drive with MR216i SAS card
- HPE LTO9 tape drive with MR216i SAS card
- IBM LTO-9 Tape Drive

Support for STIG compliance for NetBackup MSDP

Starting with NetBackup11.2, MSDP supports Security Technical Implementation Guides (STIG) compliance by enabling verification for the following RPM packages on BYO:

- VRTSpddea
- VRTSpddeu
- VRTSpddes

Support for verification of the images stored in the archive tier

NetBackup now supports verification of the backup images that are stored in archive tiers, including Amazon Glacier, Amazon Glacier Deep Archive, and Azure Archive. For more information, see the *NetBackup Deduplication Guide*.

Enhanced MSDP deduplication and performance

NetBackup 11.2 improves MSDP deduplication efficiency and performance across backup, optimized duplication and replication.

Enhancements include better data locality and performance for parallel processing of image fragments in optimized duplication and replication jobs, more effective use of predictive fingerprint cache for MSDP-C, background population of the fingerprint cache with recent backups, and support for dynamic selection of last images to improve client-side deduplication efficiency.

For more information, see the *NetBackup Deduplication Guide*.

Local WORM cache support for MSDP cloud

NetBackup 11.2 introduces local WORM cache support for MSDP Cloud through the Open Cloud Storage Daemon (OCSD). This enhancement reduces cloud API calls by caching relevant cloud metadata locally, helping lower cloud costs when using object-level immutability (WORM) with MSDP cloud volumes. The cache is automatically rebuilt if it is disabled and re-enabled to ensure data consistency. This feature is not supported for DBPaaS workloads, and the cloud bucket lifecycle policies that remove non-current object versions must not be enabled.

For more information, see the following article:

https://support.cohesity.com/s/article/MSDP-Cloud-OCSD-WORM-Cache

Change job priority for quewed jobs in Activity Monitor

You can now change the execution priority of queued backup jobs directly from the NetBackup Web UI, without canceling or restarting the job.

This enhancement gives administrators finer control over workload scheduling, allowing critical jobs to run ahead of lower-priority workloads when system resources are constrained.

Key benefits:

- Adjust job scheduling dynamically without disrupting job execution
- Prioritize urgent backup jobs during peak workloads
- Manage multiple queued jobs in a single action

For more information, see *NetBackup Web UI Administrator's Guide > Monitoring and notifications > Job monitoring > Jobs: cancel, suspend, restart, resume, delete, or change job priority* section.

Enhanced Backup Capabilities for MongoDB Ops Manager

The following enhancements are incorporated in this release:

- **Incremental Snapshot Backups** (INCR) Support for incremental snapshot backups that capture only data changes since the last full backup, reducing backup overhead for MongoDB Ops Manager workloads.
- **Transaction Log (TLOG) Backups** Support for transaction log (oplog) backups to enable point-in-time recovery in conjunction with full and incremental backups.
- **Preferred Node Selection for Backups** Support for selecting preferred nodes in replica sets and shards to control which nodes are used for MongoDB Ops Manager backup operations.

For more information:

- see *NetBackup for MongoDB Ops Manager Administrator's Guide* > *Backup* > *Policies* section.
- See "MongoDB Ops Manager upgrade behavior" on page 32.

Enhanced Log Collection in NetBackup Web UI

NetBackup now provides an enhanced log collection experience that offers greater flexibility and reliability when gathering logs for Cohesity Technical Support.

Administrators can choose between collecting diagnostic information, debug logs, or only specific debug log files from selected hosts.

The enhanced workflow introduces automatic host-level and primary server disk space validation to prevent log collection failures and disk exhaustion.

When a Job ID is provided, NetBackup automatically selects the relevant hosts, logs, and time range. Administrators can also manually select specific log files to reduce log size and collection time.

For more information, see *NetBackup Logging Reference Guide* > *Using the Log collection utility* > *Add a record and collect logs* section.

See "Unable to cancel log collection after web service restart" on page 34.

Backup Selections Tab in Policies in NetBackup Web UI

The NetBackup Web UI now includes a Backup selections tab within the Policies workflow. This enhancement provides clear visibility into the backup selection lists configured for each policy, helping administrators quickly verify what data is included in backups.

Key highlights

- View existing backup selections per policy directly from the Web UI
- See multiple backup selections listed individually for the same policy
- Improve policy reviews, audits, and troubleshooting by validating backup scope in one place

Important behavior details

- Backup selections are displayed only for policies that already have backup selections configured
- Policies without configured backup selections do not appear in the Backup selections tab
- Backup selections are scoped per policy, not per client
- Existing policies automatically populate the tab after feature enablement; visibility depends on the policy cache sync interval

Permissions

- No additional role is required
- Users must have view access to the policy to see its backup selections

For more information, see *NetBackup Web UI Administrator's Guide* > *Configuring backups* > *Managing policies* > *About the Policies utility* section

Enhanced report time selection and control

Reports now provide more precise control over the reporting window and execution:

- Specify both start and end date and time when generating reports.
- Use quick-select options such as Earliest available, Last 24 hours, or Current time.
- Cancel a running report using the new Stop option.

These enhancements improve accuracy and flexibility when generating Web UI reports.

NetBackup integration with Helios

In this release, NetBackup extends beyond domain-level management by integrating natively with Helios, enabling centralized visibility, analytics, and operational control across multiple NetBackup environments.

Pre-requisite Configuration for NetBackup Web UI Access – Authorization

Before accessing the NetBackup Web UI on the primary server, ensure that the user is authorized through Helios (NetBackup-Alta).

- Assign a NetBackup-Alta canned role to the Helios user:
  Assign one of the following predefined roles based on the required access level:
  - **NetBackup Admin**: Provides administrator-level access to the NetBackup Primary server.
  - **NetBackup Viewer**: Provides read-only access to the NetBackup Primary server.
- Create a NetBackup-Alta custom role for Web UI access
  If more controlled access is required, create a custom role with Web UI permissions:.
  - Enable the NetBackup WebUI Access permission.
  - Select the scope (Primary servers) for which access is required.
  - Choose the appropriate canned or custom role for the selected NetBackup Primary server.
  - Create the custom role and assign it to the user.

  A custom role can inherit permissions from roles defined on the NetBackup Primary server and can be assigned to users as needed

You can now:

- Register multiple NetBackup domains and manage them from a single cloud-based console
- Gain global visibility into jobs, policies, assets, connectivity, and versions
- Monitor cyber resiliency using risk scores, anomaly detection, and malware insights
- Perform policy, job, and recovery operations centrally, without switching dashboards
- Use Copilot, a generative AI assistant, for guided troubleshooting, reporting queries, and operational insights

This integration requires minimal NetBackup-side changes and uses outbound-only secure communication, ensuring ease of deployment while enhancing operational efficiency.

For more information, see Helios documentation.

See “NetBackup integration with Helios – operational notes” on page 51.

Accelerator support for Oracle Cloud Infrastructure (OCI)

OCI backups now support NetBackup Accelerator for incremental backups.

For more information, see *NetBackup™ Web UI Cloud Administrator's Guide*.

Dynamic multi-streaming support for Standard and Catalog policies

Dynamic multi-streaming is now supported as part of Standard and Catalog policies in NetBackup.

For more information, see the respective topics in the *NetBackup Web UI Administrator's Guide*.

Auto-resume for Cloud object store backups

In check-point restart enabled backups, auto-resume for incomplete backup jobs is now supported for Cloud object store backups.

For more information, see *NetBackup™ for Cloud Object Store Administrator's Guide*.

Flexible Version Compatibility for Kubernetes Operator

The NetBackup Kubernetes operator no longer requires the NetBackup Primary Server and Media Server to be on the same NetBackup version. The operator can run on an earlier NetBackup version than the servers it connects to.

The Kubernetes operator can be:

- Up to one NetBackup version older than the Media Server
- Up to two NetBackup versions older than the Primary Server

The operator supports the features available in its own version. This supported configuration provides greater flexibility during phased upgrade scenarios.

During this upgrade model, existing Kubernetes policies continue to run backups. However, restore operations must be performed manually until the Kubernetes operator is upgraded.

For more information, see *NetBackup for Kubernetes Administrator's Guide > Deploying and configuring the NetBackup Kubernetes operator > Upgrade the NetBackup Kubernetes operator* section

MS Exchange Recovery from NetBackup Web UI

You can now recover Microsoft Exchange workloads directly from the NetBackup Web UI.

This release introduces Web UI–based recovery for Microsoft Exchange backups, allowing administrators to perform recovery operations without using legacy interfaces.

Key capabilities include:

- Start Microsoft Exchange recovery from the NetBackup Web UI
- Perform granular recovery by selecting individual items from backups
- Restore data to the original location or an alternate destination
- Choose recovery behaviors such as roll-forward recovery or point-in-time recovery
- Monitor restore jobs directly from the Activity Monitor in the Web UI

This enhancement simplifies Exchange recovery workflows by centralizing recovery operations within the NetBackup Web UI.

For more information, see *NetBackup for Microsoft Exchange Server Administrator's Guide > Performing recovery using NetBackup Web UI for MS-Exchange* section

Cloud Scale enhancements and deployment updates

In this release of NetBackup11.2, Cloud Scale Technology includes changes related to enhancements and deployment updates. For more information, refer to *Cohesity Cloud Scale Technology Manual Deployment Guide for Kubernetes Clusters*.

Support for NVMe Local Storage as MSDP Cloud Cache

MSDP-C now supports using local NVMe storage on Kubernetes worker nodes as cloud cache for MSDP engine pods. This enhancement improves performance and helps reduce cloud storage costs in cloud-backed MSDP deployments. You can configure this capability by specifying annotations on the MSDP Scaleout custom resource (CR) and updating the cloud cache configuration to use NVMe-backed mount points.

Enhanced certificate management and troubleshooting for Cloud Scale deployments

Certificate management in NetBackup Cloud Scale Kubernetes deployments has been enhanced to improve reliability and visibility. The updated certificate distribution mechanism removes dependency on shared NFS storage, ensuring more consistent certificate availability across pods. These improvements also provide better visibility

into certificate-related errors and simplify recovery from issues that affect pod communication and startup.

Debug tool container for Kubernetes troubleshooting

NetBackup introduces a debug tool container that provides a dedicated, ephemeral environment for troubleshooting Kubernetes deployments. This container can be dynamically attached to running pods or nodes using the `kubectl debug` command, without modifying existing NetBackup container images.

Parallel restore for cloud virtual machines

NetBackup 11.2 introduces parallel restore for cloud virtual machines to reduce restore time. Instead of restoring disks one by one, NetBackup now restores multiple disks at the same time. This improves restore performance and helps complete recoveries faster, especially for virtual machines with multiple disks. The feature is supported on AWS and Microsoft Azure and is enabled by default.

For more information, refer to the *NetBackup™ Web UI Cloud Administrator's Guide*.

Support for protecting Azure disks with DENY_ALL network policy

NetBackup Snapshot Manager now supports protecting Azure managed disks that use the **DENY_ALL** network access policy.

When this feature is enabled, NetBackup automatically creates and manages the required disk access resources and private endpoints during backup and snapshot operations. This removes the need for manual setup and simplifies protection of secure disks. For more information, refer to the *NetBackup Snapshot Manager for Cloud Install and Upgrade Guide*.

Job resiliency for Oracle and MS-SQL-Server policies

NetBackup 11.2 introduces resilient backup jobs for Oracle and MS-SQL-Server policies. If the connection to the primary server is lost, the backup retries the failed activity until it succeeds or until the configured timeout is reached.

When the timeout is reached, the job is marked as failed. The storage unit that is associated with the policy must target a media server running NetBackup 11.2 or later.

Multiplexing is not supported for these jobs.

See the *NetBackup Administrator's Guide, Volume I*, for the new resilient backup settings.

Enhancements in KVM support

NetBackup for KVM now supports Accelerator, single-file restore (SFR), raw-formatted disks, block type disks.

See the *NetBackup for KVM Administrator's Guide*.

SAP HANA intelligent policy

You can configure an intelligent policy to protect SAP HANA instances and databases.

See the *NetBackup for SAP Administrator's Guide*.

Role elevation feature

Role elevation allows authorized users in NetBackup to temporarily elevate their privileges so they can perform administrative or security-sensitive actions that are normally restricted.

This feature supports the principle of least privilege by eliminating the need to permanently grant powerful roles to users.

See the *NetBackup Web UI Administrator's Guide*.

KMS configuration and management using web UI

You can configure and manage key management servers (KMS) using NetBackup web UI.

You can add keygroups and keys for KMS server so that the storage server can use the keygroup and its active key for encrypting and decrypting the backup data.

See the *NetBackup Web UI Administrator's Guide*.

Troubleshooter in web UI

You can now troubleshoot job failures using the **Activity monitor > Troubleshooter** web UI. You can see the troubleshooting information such as error details and recommended actions for a specific NetBackup status code, using the troubleshooter UI.

See the *NetBackup Web UI Administrator's Guide*.

Enhancements in EEB management web UI

You can manage engineering binaries (EEB) at scale using the NetBackup web UI. You can remove EEBs from multiple clients and media servers, and update the existing EEBs.

See the *NetBackup Web UI Administrator's Guide*.

Chapter 3

Operational notes

This chapter includes the following topics:

About NetBackup 11.2 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 11.2.

If NetBackup 11.2 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 11.2 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

https://support.cohesity.com/s/article/article-100033400

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.

MongoDB Ops Manager upgrade behavior

After upgrading to NetBackup 11.2 or later:

- Existing MongoDB Ops Manager policies and backup images that were created before the upgrade remain available and unchanged.
- If an existing MongoDB Ops Manager policy contains a Differential Incremental backup type, that backup type runs as an Incremental backup after the upgrade.
- To continue running oplog backups (referred to as Transaction log (TLOG) backups in NetBackup 11.2+), you must manually update any pre-existing MongoDB Ops Manager policies and change the Differential Incremental backup type to Transaction log (TLOG).
- Oplog backup images that were created before the upgrade continue to appear as Differential Incremental backup images in the restore view.
- Oplog (Transaction log/TLOG) backup images created using NetBackup 11.2 or later appear as Transaction log backup images in the restore view.

MongoDB Ops Manager transaction log (TLOG) backup continuity considerations

MongoDB Ops Manager transaction log (oplog) backups rely on continuous oplog metadata to support point-in-time recovery. NetBackup validates oplog continuity during backup and restore operations to ensure recovery consistency.

If **any oplog or incremental backup fails**, the continuity of the oplog chain required for point-in-time recovery may be broken.

MongoDB Ops Manager logs may report messages such as:

- Observed non-continuous sets of oplog files
- Gap overlap observed for this set of oplog files

Impact

- After an oplog or incremental backup failure, **subsequent oplog or incremental backups (including retry and auto-retry operations) may report success**; however, **successful completion does not indicate point-in-time recoverability** if oplog continuity was previously broken. .
- Until a new Full backup is performed, the affected backup chain **cannot be used for log-based (point-in-time) recovery**.
- Snapshot-based restores (Full or Incremental without logs) remain available.

Operational guidance

If an oplog or incremental backup failure occurs:

1. Treat the current Full + oplog backup chain as unavailable for point-in-time recovery.
2. Perform a new Full backup to establish a new recovery baseline.
3. Review MongoDB Ops Manager logs for oplog continuity or retention warnings.
4. Verify oplog retention sizing and ensure backup schedules align with the required recovery window.

Warning: NetBackup validates oplog continuity but does not generate, repair, or reconcile MongoDB oplog metadata. Continuous oplog retention and accurate metadata reporting by MongoDB Ops Manager are required for successful log-based recovery.

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 11.2.

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 61.

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.

Unable to cancel log collection after web service restart

If NetBackup web services are restarted while a log collection is in progress, the log collection cannot be cancelled from the NetBackup Web UI.

This happens because log collection requests that were already running are not retained after the web services restart. As a result, the **Cancel** option in the Web UI displays **No Entity Found** error message.

Workaround: The log collection can still be cancelled using the NetBackup command line.

```
./nblogadm --action cancelcollection --recid {collectionId} --api
```

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 11.2.

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`

Recycle Bin Corruption Warning Observed After Windows Bare Metal Restore

Issue

After performing a Bare Metal Restore (BMR) on Windows client, the following warning message may appear after login or when accessing the desktop.

Error Message

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

- The prompt continues to appear until “Yes” is selected..
- 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.

Cause

This issue occurs because the **$RECYCLE.BIN** folder may not be fully synchronized or correctly reinitialized during the Bare Metal Restore process.

This behavior is cosmetic and does not indicate any corruption of the operating system or restored user data .

Resolution

The issue can be resolved by recreating the Recycle Bin folder on the affected volume(s).

Steps to resolve the issue.

1. Log in to the restored system.
2. Open Command Prompt with Administrator privileges.
3. Run the following command for each affected drive:

   ```
   RD C:\$Recycle.bin /s /q
   ```

   Note: Replace C: with the appropriate drive letter if other volumes are also affected.

4. Restart the system.

Additional Information

- Ensure that the SYSTEM account has Full Control permissions on the root of each restored NTFS volume.
- This issue does not impact system functionality or data integrity outside of the Recycle Bin.
- Any data deleted by accepting the prompt is limited to the Recycle Bin contents only.

Data Recovery

If data existed in the Recycle Bin at the time of backup, it can be recovered using a redirected restore:

1. Navigate to the Recovery tab in the NetBackup console.
2. Select the affected Windows client.

3 Browse to the following path:

```
C:\$RECYCLE.BIN
```

4 Select the “$RECYCLE.BIN” folder.

5 5. Choose “**Restore everything to original location**” and start the restore. The data will get restored in Recycle bin.

Additional Information

- Ensure that the SYSTEM account has Full Control permissions on the root of each restored NTFS volume.
- This issue does not impact system functionality or data integrity outside of the Recycle Bin.
- Any data deleted by accepting the prompt is limited to the Recycle Bin contents only.

Thin Logical Volumes Are Not Restored After BMR When LVM PVs Are Created on Raw Disks

Problem

After a successful NetBackup Bare Metal Restore (BMR) of a Linux client using LVM thin provisioning, **thin logical volumes (thin LVs) are missing or unusable after system boot**.

The BMR restore job completes without fatal errors, but **data stored on thin-provisioned logical volumes is not restored or mounted**.

This behavior occurs when **LVM Physical Volumes (PVs) were created directly on raw disks** (for example, /dev/sdb) rather than on partition-based devices (for example, /dev/sdb1).

Environment

- Product: Veritas NetBackup Bare Metal Restore (BMR)
- Client OS: Linux (for example, RHEL 9.x)
- Storage Configuration:
  - LVM with thin provisioning
  - Physical Volumes created on raw disks (no disk partitions)
- Restore Type: Bare Metal Restore (BMR)

Symptoms

After a completed BMR restore and system reboot:

- Thin pools may exist, but:
  - Thin logical volumes are missing OR
  - File systems are not present OR
  - Volumes are not mounted OR
  - Mounted volumes are empty
- No fatal errors are reported during the BMR restore job

Cause

The BMR restore workflow **does not fully support thin-provisioned LVM configurations where Physical Volumes are created directly on raw disks**.

BMR restore logic **expects thin provisioning to be backed by partition-based PVs**. When PVs are created on raw disks, BMR:

- Recreates the volume group and thin pool metadata
- Does NOT recreate or populate thin logical volumes
- Does NOT restore file system data contained within thin LVs

Workaround

Warning: The following procedure removes and recreates thin logical volumes. Incorrect execution can cause permanent data loss. Perform only if you understand your LVM layout and have valid backups.

Preconditions

- Volume Group exists
- Thin pool exists
- NetBackup backup contains data from the thin logical volume

Recovery Steps

1. Unmount the thin logical volume (if mounted):

   ```
   umount <MOUNT_POINT> 2>/dev/null
   ```

2. Remove the existing thin logical volume:

   ```
   lvremove -y <VG_NAME>/<THIN_LV_NAME>
   ```

3 Verify logical volumes in the volume group:

```
lvs <VG_NAME>
```

4 Recreate the thin logical volume:

```
lvcreate -V <VIRTUAL_SIZE> -T <VG_NAME>/<THINPOOL_NAME> -n
<THIN_LV_NAME>
```

5 Verify logical volumes again:

```
lvs <VG_NAME>
```

6 Create a file system on the thin logical volume:

```
mkfs.xfs -f /dev/<VG_NAME>/<THIN_LV_NAME>
```

7 Verify the block device:

```
blkid /dev/<VG_NAME>/<THIN_LV_NAME>
```

8 Create the mount point and mount the volume:

```
mkdir -p <MOUNT_POINT>
```

```
mount /dev/<VG_NAME>/<THIN_LV_NAME> <MOUNT_POINT>
```

9 Verify the mount:

```
df -lh
```

10 Perform a redirected restore of the required data into `<MOUNT_POINT>`.

Best Practice Recommendation (Strongly Advised)

To prevent this issue in future BMR restores:

- Always create partitions on data disks
- Create LVM Physical Volumes on partition devices (for example, /dev/sdb1)
- Avoid creating PVs directly on raw disks

Status

This is a known limitation in the current BMR restore workflow for thin-provisioned LVM configurations created on raw disks.

Use the documented workaround to recover thin logical volumes and restore 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 11.2.

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 11.2 requires NetBackup 10.2 or later

You cannot run Auto Image Replication (AIR) from a computer with NetBackup version 11.2 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 11.2.

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:

https://support.cohesity.com/s/article/article-100031122

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 11.2.

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 11.2.

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

Japanese and Chinese characters display incorrectly in the NetBackup BAR GUI on RHEL 10

On RHEL 10 systems, Japanese and Chinese text may appear garbled in the NetBackup Java Backup, Archive, and Restore (BAR) GUI. This issue occurs because the required CJK font packages are not installed by default on RHEL 10.

To resolve this issue, perform the following steps:

1. Install the required CJK font package.

   ```
   sudo dnf install google-noto-sans-cjk-fonts
   ```

2. Refresh the font cache.

   ```
   fc-cache -fv
   ```

3. Verify the font installation.

   ```
   LANG=ja_JP.UTF-8 fc-match
   ```

NetBackup integration with Helios – operational notes

Note: Applies to: NetBackup 11.2 and later when accessed through Helios

Table 3-4 Known limitations and unsupported operations

Area	Limitation	Workaround
Reporting	Tape content report is not available in Helios	Use NetBackup Web UI
Authentication	SSO and Smart Card users not supported	Login via NetBackup Web UI
Log collection	Download of collected logs disabled	Use NetBackup Web UI
Restore	File/folder download disabled	Use NetBackup Web UI
File operations	Large file downloads not supported	Use NetBackup Web UI
Job monitoring	Updates are near real time, not real time	Use NetBackup Web UI
Session management	Cannot terminate user sessions	Use NetBackup Web UI
API access	Swagger docs unavailable	Use NetBackup Web UI
MFA	Cannot configure MFA	Not supported
API keys	Cannot add API keys	Not supported

Table 3-4 Known limitations and unsupported operations *(continued)*

Area	Limitation	Workaround
RBAC	Helios users cannot be added to NetBackup RBAC	Not supported
Updates	Uploading EEB/patches from a local computer is disabled in Helios	Use NetBackup Web UI
Cloud operations	Adding snapshot server extensions and performing cloud agent operations are disabled in Helios	Use NetBackup Web UI

Sheltered Harbor connection failure

The Sheltered Harbor project is discontinued. Therefore, the NetBackup Sheltered Harbor solution will be unable to connect to the Sheltered Harbor monitoring log services.

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/cohesity/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 30.

- 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 11.2, 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:
  https://support.cohesity.com/s/article/article-100006242
- 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 on UNIX/Linux systems. For installation, gunzip and gzip must be installed on the host before you attempt to install NetBackup. These utilities are not required on Windows hosts. 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 11.2 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 61.

See "About Cohesity Services and Operations Readiness Tools" on page 53.

NetBackup 11.2 binary sizes

The following table contains the approximate binary sizes of the NetBackup 11.2 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	1530 MB	No longer supported	
Alma Linux		2020 MB		
Amazon Linux		2020 MB		
BC-Linux		2020 MB		
Canonical Ubuntu	x86-64	2020 MB		

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

OS	CPU Architecture	64-bit client	64-bit server	Notes
CentOS	x86-64	2020 MB	7534 MB	
Debian GNU/Linux	x86-64	2020 MB		
Kylin Linux Advanced Server 10.0		2020 MB		
NeoKylin Linux Advanced Server		2020 MB		
Oracle Linux	x86-64	2020 MB	7534 MB	
Red Hat Enterprise Linux Server	POWER 8/9 client	509 MB		
Red Hat Enterprise Linux Server	x86-64	2020 MB	7534 MB	
Red Hat Enterprise Linux Server	z/Architecture	718 MB	No longer supported	Media server or client compatibility only.
Rocky Linux client		2020 MB		
Solaris	SPARC	1103 MB	No longer supported	
Solaris	x86-64	1058 MB	No longer supported	
SUSE Linux Enterprise Server	POWER 8/9 client	507 MB		
SUSE Linux Enterprise Server	x86-64	1445 MB	6776 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	736 MB	No longer supported	Media server or client compatibility only.
Windows	x86-64	894 MB	5109 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 53.

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

See “About Cohesity Services and Operations Readiness Tools” on page 53.

About changes in platform compatibility

The NetBackup 11.2 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 10.

NetBackup Compatibility Lists for All Versions

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 11.2. 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.
