Release notes

NetApp Backup and Recovery

NetApp
February 11, 2026

Table of Contents

Release notes . . . 1
What's new in NetApp Backup and Recovery . . . 1
09 February 2026 . . . 1
19 January 2026 . . . 2
08 December 2025 . . . 3
06 October 2025 . . . 3
25 August 2025 . . . 5
12 August 2025 . . . 6
28 July 2025 . . . 8
14 July 2025 . . . 9
09 June 2025 . . . 10
13 May 2025 . . . 11
16 April 2025 . . . 12
17 March 2025 . . . 13
21 February 2025 . . . 14
13 February 2025 . . . 15
22 November 2024 . . . 15
27 September 2024 . . . 16
Known limitations with NetApp Backup and Recovery for ONTAP volumes . . . 16
Replication limitations for ONTAP volumes . . . 17
Backup-to-object limitations for ONTAP volumes . . . 17
Restore limitations for ONTAP volumes . . . 19
Known limitations with NetApp Backup and Recovery for Microsoft SQL Server workloads . . . 19
Clone lifecycle support . . . 19
Standard deployment mode only . . . 20
Windows cluster name restriction . . . 20
SnapCenter migration issues . . . 20
Limited support for virtualization management software . . . 21
Known limitations with NetApp Backup and Recovery for VMware workloads . . . 21
Known limitations with NetApp Backup and Recovery for Hyper-V workloads . . . 22
Unsupported actions . . . 22
Known limitations with NetApp Backup and Recovery for KVM workloads . . . 22
Unsupported actions . . . 22
Unsupported configurations . . . 23
Troubleshooting notes . . . 23
Known limitations with NetApp Backup and Recovery for Oracle Database workloads . . . 23

Release notes

What's new in NetApp Backup and Recovery

Learn what's new in NetApp Backup and Recovery.

09 February 2026

This NetApp Backup and Recovery release includes the following updates.

Microsoft Hyper-V workloads supported in General Availability (GA)

Microsoft Hyper-V workload support is now generally available (GA) in NetApp Backup and Recovery.

KVM workloads supported in General Availability (GA)

KVM workload support is now generally available (GA) in NetApp Backup and Recovery.

Kubernetes workloads enhancements

This release of Kubernetes workloads introduces the following enhanced capabilities:

- **CR workflow support**: You can now perform common protection tasks using CRs as well as the Backup and Recovery web UI.
- **Cluster migration**: You can now add existing Kubernetes clusters protected with Trident Protect to Backup and Recovery.
- **Alerting framework support**: You can now receive email and UI alerts for certain Kubernetes workload events.
- **Restore tab integration**: You can now access the Kubernetes workload restore actions from the Restore menu.
- **Support for the 3-2-1 fanout backup architecture**: You can now use a 3-2-1 fanout architecture in your protection policy when protecting Kubernetes workloads.

For details about protecting Kubernetes workloads, refer to Protect Kubernetes workloads overview.

Oracle Database workloads enhancements

This release of Oracle Database workloads introduces the following enhanced capabilities:

- **Non-root user support**: Non-root users can now perform backup, restore, and clone operations, improving security and compliance.
- **Clone support**: Clone capabilities are now supported across primary and secondary NAS, SAN, and ASM environments using ASM library v2, enabling coordinated protection workflows.
- **Clone split support**: You can now split writable snapshots (clones) from their parent volumes, freeing up storage and enabling independent operations.
- **Backup and restore for object store**: Native backup and restore capabilities are now supported for object-based S3-compatible storage targets.
- **Clone Lifecycle Management (CLM)**: Clone refresh operations are supported on primary storage.

- **Clone to alternate host**: You can now clone databases to a different host (for testing or analytics) from both primary and secondary storage.
- **ONTAP consistency group support**: ONTAP consistency groups are now supported, ensuring application-consistent snapshots across multiple volumes.
- Backup and Recovery now supports the following protection policy architectures for Oracle Database workloads:
  - 3-2-1 fanout
  - Disk to disk
  - Disk to object storage
  - Cascading
  - Local snapshot

For details about protecting Oracle Database workloads, refer to Protect Oracle Database workloads overview.

19 January 2026

This NetApp Backup and Recovery release includes the following updates.

ONTAP volume workloads enhancements

This release of ONTAP volume workloads introduces the following enhanced capability:

Support for multiple buckets: (Private preview) Beginning with ONTAP 9.17.1 and newer, you can now protect the volumes within a system with up to 6 buckets per system across different cloud providers.

Learn more about backing up ONTAP volume data using NetApp Backup and Recovery.

VMware workloads enhancements

This release of VMware workloads introduces the following enhanced capabilities:

- VMware workload support is now generally available (GA) in NetApp Backup and Recovery.
- You can now restore guest OS files and folders.

Learn more about restoring guest files and folders.

Hyper-V workloads preview enhancements

This release of Hyper-V workloads introduces the following enhanced capabilities:

- You can now restore Hyper-V VM backups and snapshots to an alternate location. Use this feature to manage VM versions on different Hyper-V hosts.
- NetApp Backup and Recovery now supports Hyper-V virtual machines provisioned by System Center Virtual Machine Manager (SCVMM) and hosted on a CIFS share.
- You can now edit protection groups.

> In this release only, you cannot upgrade the NetApp plugins for Hyper-V or Windows using the **Upgrade** option in the Actions menu. Instead, remove each Hyper-V host and add it again to update the plugins.

Learn more about restoring Hyper-V VMs with NetApp Backup and Recovery.

KVM workloads preview enhancements

The KVM workloads preview now protects KVM hosts and virtual machines that are managed by Apache CloudStack.

For details about protecting KVM workloads, refer to Protect KVM workloads overview.

08 December 2025

This NetApp Backup and Recovery release includes the following updates.

VMware workloads preview enhancements

The preview release of VMware workloads introduces the following enhanced capabilities:

- You can now restore backups and snapshots to an alternate location. This is useful if you want to manage versions of a VM on different VMware vCenter deployments, VMware ESXi hosts, or VMware datastores.

Learn more about restoring VMware VMs with NetApp Backup and Recovery.

- You can now restore specific VMware virtual disks (VMDK images) from either a primary or secondary location, enabling more granular control over restoring VM data.

Learn more about restoring VMware virtual disks with NetApp Backup and Recovery.

06 October 2025

This NetApp Backup and Recovery release includes the following updates.

BlueXP backup and recovery is now NetApp Backup and Recovery

BlueXP backup and recovery has been renamed to NetApp Backup and Recovery.

BlueXP is now NetApp Console

The NetApp Console, built on the enhanced and restructured BlueXP foundation, provides centralized management of NetApp storage and NetApp Data Services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration that is highly secure and compliant.

For details on what's changed, see the NetApp Console release notes.

Hyper-V workload support as a private preview

This release of of NetApp Backup and Recovery introduces support for discovering and managing Hyper-V workloads:

- Backup and restore VMs on standalone instances as well as failover cluster instances (FCI)
- Protect VMs stored on SMB3 shares
- Bulk protection at virtual machine level
- VM and crash consistent backups

- Restore VMs from primary, secondary, and object storage
- Search and restore VM backups

For details about protecting Hyper-V workloads, refer to Protect Hyper-V workloads overview.

KVM workload support as a private preview

This release of of NetApp Backup and Recovery introduces support for discovering and managing KVM workloads:

- Back up and restore qcow2 VM images stored on NFS shares
- Back up storage pools
- Bulk VM and storage pool protection using protection groups
- VM consistent and crash consistent VM backups
- Search and restore VM backups from primary, secondary, and object storage
- Guided process to back up and restore KVM-based VMs and VM data

For details about protecting KVM workloads, refer to Protect KVM workloads overview.

Kubernetes preview enhancements

The preview release of Kubernetes workloads introduces the following enhanced capabilities:

- 3-2-1 Fan out backup architecture support
- Support for ONTAP S3 as a backup target
- New Kubernetes dashboard for easier management
- Enhanced role based access control (RBAC) configuration includes support for the following roles:
  - Backup and Recovery super admin
  - Backup and Recovery backup admin
  - Backup and Recovery restore admin
  - Backup and Recovery viewer
- Support for the SUSE Rancher Kubernetes distribution
- Multi-bucket support: You can now protect the volumes within a system with multiple buckets per system across different cloud providers

For details about protecting Kubernetes workloads, refer to Protect Kubernetes workloads overview.

VMware preview enhancements

The preview release of VMware workloads introduces the following enhanced capabilities:

- Support for restoring from object storage
- NetApp Console Dashboard now displays VMware workload status information
- Role-based access control (RBAC) support
- Email alert and notification support for job events
- Support for backing up and restoring to NVMe-based storage

- Edit protection groups
- Edit protection policies

For details about protecting VMware workloads, refer to Protect VMware workloads overview.

Oracle Database workload support as a private preview

This release of NetApp Backup and Recovery introduces support for discovering and managing Oracle Database workloads:

- Discover standalone Oracle databases
- Create protection policies for data only or data and log backups
- Protect Oracle databases with a 3-2-1 backup scheme
- Configure backup retention
- Mount and unmount ARCHIVELOG backups
- Virtualized databases
- Search and restore database backups
- Oracle dashboard support

For details about protecting Oracle Database workloads, refer to Protect Oracle Database workloads overview.

ONTAP volume workload enhancements

This release of ONTAP volume workloads introduces the following enhanced capability:

Beginning with ONTAP 9.17.1 and newer, DataLock is now supported with Google Cloud Platform. This complements existing DataLock support with Amazon AWS, Microsoft Azure, and NetApp StorageGRID.

25 August 2025

This NetApp Backup and Recovery release includes the following updates.

Support for protecting VMware workloads in Preview

This release adds preview support for protecting VMware workloads. Back up VMware VMs and datastores from on-premises ONTAP systems to Amazon Web Services and StorageGRID.

> Documentation about protecting VMware workloads is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

Learn more about protecting VMware workloads with NetApp Backup and Recovery.

High performance indexing for AWS, Azure, and GCP is generally available

In February 2025, we announced the preview of high performance indexing (Indexed Catalog v2) for AWS, Azure, and GCP. This feature is now generally available (GA). In June 2025, we provided it to all *new* customers by default. With this release, the support is available to *all* customers. High performance indexing improves the performance of backup and restore operations for workloads that are protected to object storage.

Enabled by default:

- If you are a new customer, high performance indexing is enabled by default.
- If you are an existing customer, you can enable reindexing by going to the Restore section of the UI.

12 August 2025

This NetApp Backup and Recovery release includes the following updates.

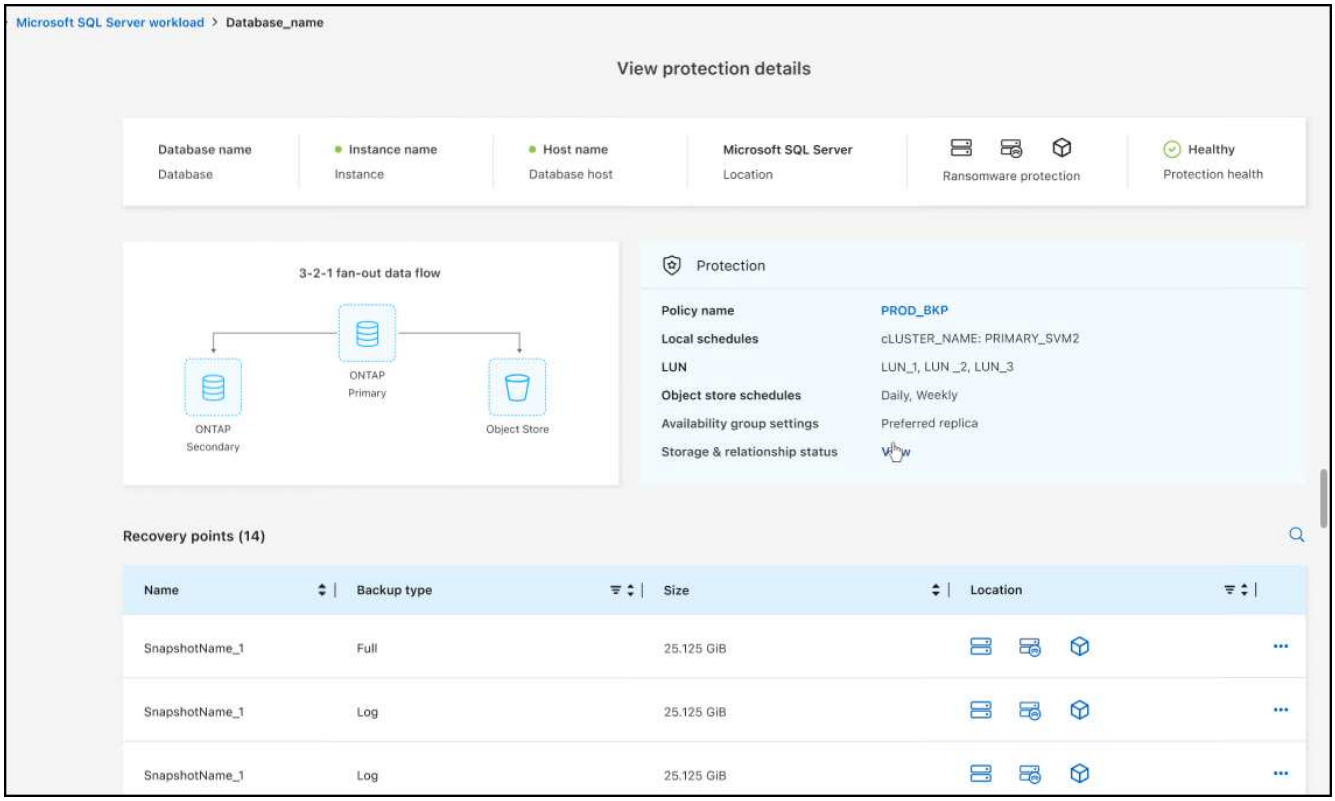
Microsoft SQL Server workload supported in General Availability (GA)

Microsoft SQL Server workload support is now generally available (GA) in NetApp Backup and Recovery. Organizations using an MSSQL environment on ONTAP, Cloud Volumes ONTAP, and Amazon FSx for NetApp ONTAP storage can now take advantage of this new backup and recovery service to protect their data.

This release includes the following enhancements to the Microsoft SQL Server workload support from the previous preview version:

- **SnapMirror active sync**: This version now supports SnapMirror active sync (also referred to as SnapMirror Business Continuity [SM-BC]), which enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. NetApp Backup and Recovery now supports protection of Microsoft SQL Server databases in a SnapMirror active sync and Metrocluster configuration. The information appears in the **Storage and relationship status** section of the Protection details page. The relationship information is displayed in the updated **Secondary settings** section of the Policy page.

  Refer to Use policies to protect your workloads.

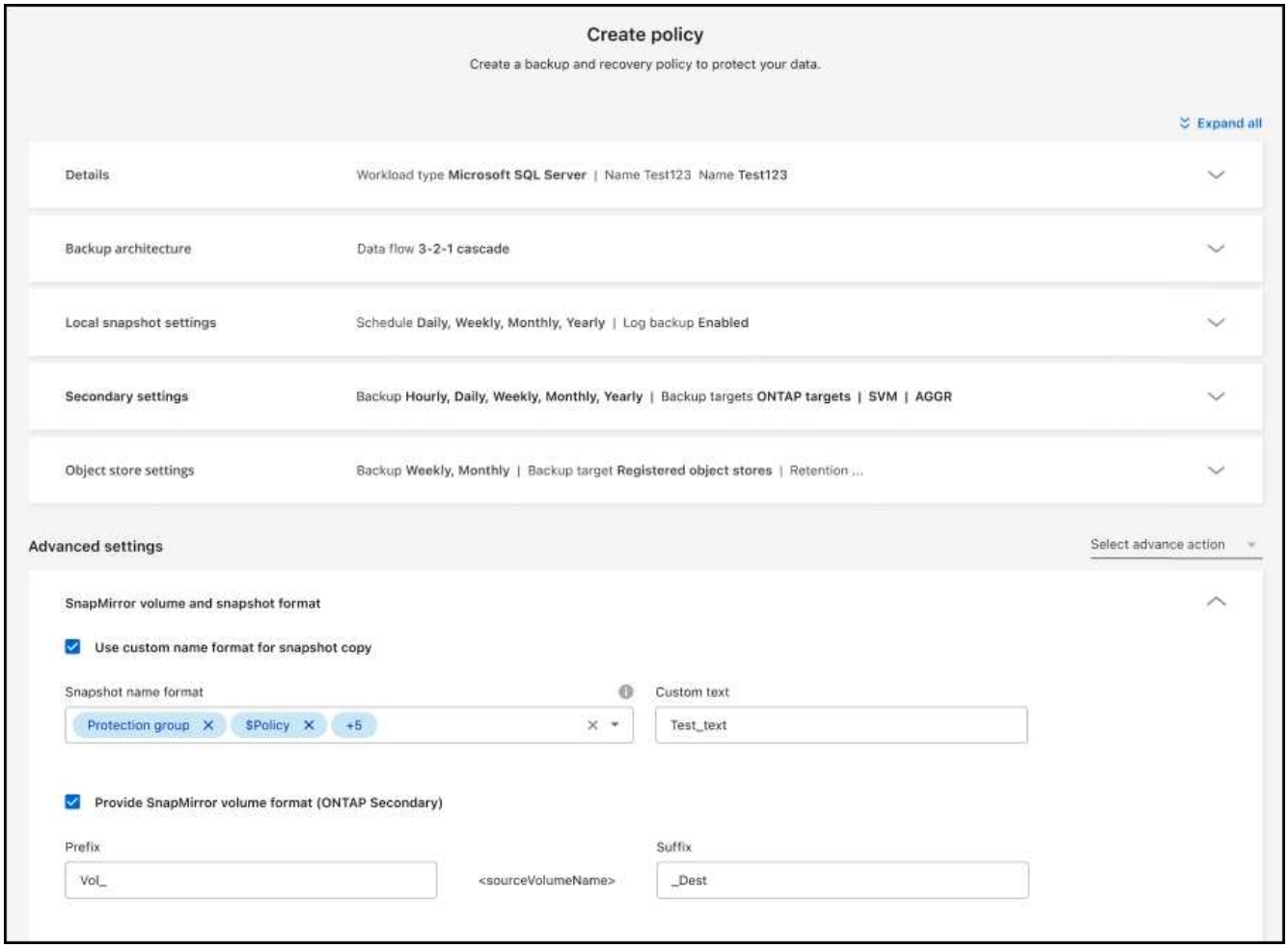


- **Multi-bucket support**: You can now protect the volumes within a working environment with up to 6 buckets per working environment across different cloud providers.

- **Licensing and free trial updates** for SQL Server workloads: You can now use the existing NetApp Backup and Recovery licensing model to protect SQL Server workloads. There is no separate licensing requirement for SQL Server workloads.

  For details, refer to Set up licensing for NetApp Backup and Recovery.

- **Custom snapshot name**: You can now use your own snapshot name in a policy that governs the backups for Microsoft SQL Server workloads. Enter this information in the **Advanced settings** section of the Policy page.

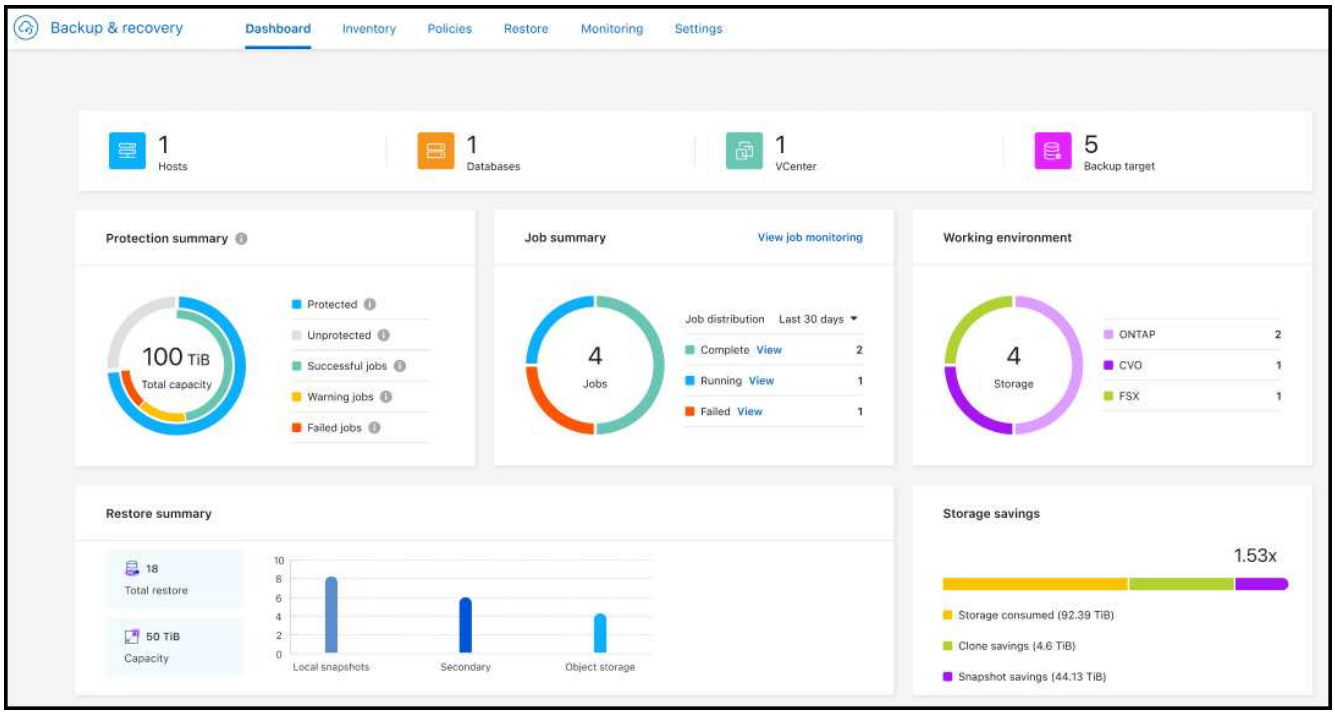


  Refer to Use policies to protect your workloads.

- **Secondary volume prefix and suffix**: You can enter a custom prefix and suffix in the **Advanced settings** section of the Policy page.
- **Identity and access**: You can now control users' access to features.

  Refer to Log in to NetApp Backup and Recovery and NetApp Backup and Recovery access to features.

- **Restore from object storage to an alternate host**: You can now restore from object storage to an alternate host even if the primary storage is down.
- **Log backup data**: The database protection details page now shows log backups. You can see the Backup type column that shows whether the backup is a full backup or a log backup.
- **Enhanced Dashboard**: The Dashboard now shows Storage and Clone savings.



ONTAP volume workload enhancements

- **Multi-folder restore for ONTAP volumes**: Until now, you could restore either one folder or multiple files at a time from the Browse and restore feature. NetApp Backup and Recovery now provides the ability to select multiple folders at a time using the Browse and restore feature.
- **View and manage backups of deleted volumes**: The NetApp Backup and Recovery Dashboard now gives an option to show and manage volumes that are deleted from ONTAP. With this, you can view and delete backups from volumes that no longer exist in ONTAP.
- **Force delete backups**: In some extreme cases, you might want NetApp Backup and Recovery not to have access to backups any longer. This might happen for example, if the service no longer has access to the backup bucket or backups are DataLock protected but you don't want them anymore. Previously, you could not delete these yourself and needed to call NetApp Support. With this release, you can use the option to force delete backups (at volume and work environment levels).

> Use this option carefully and only in extreme cleanup needs. NetApp Backup and Recovery will not have access to these backups any longer even if they are not deleted in the object storage. You will need to go to your cloud provider and manually delete the backups.

Refer to Protect ONTAP workloads.

28 July 2025

This NetApp Backup and Recovery release includes the following updates.

Kubernetes workload support as a Preview

This release of of NetApp Backup and Recovery introduces support for discovering and managing Kubernetes workloads:

- Discover Red Hat OpenShift and open-source Kubernetes clusters, backed by NetApp ONTAP, without sharing kubeconfig files.

- Discover, manage, and protect applications across multiple Kubernetes clusters using a unified control plane.
- Offload data movement operations for backup and recovery of Kubernetes applications to NetApp ONTAP.
- Orchestrate local and object-storage-based application backups.
- Back up and restore entire applications and individual resources to any Kubernetes clusters.
- Work with containers and virtual machines running on Kubernetes.
- Create application-consistent backups using execution hooks and templates.

For details about protecting Kubernetes workloads, refer to Protect Kubernetes workloads overview.

14 July 2025

This NetApp Backup and Recovery release includes the following updates.

Enhanced ONTAP volume Dashboard

In April 2025, we launched a preview of an enhanced ONTAP volume Dashboard that is much faster and more efficient.

This dashboard was designed to help enterprise customers with a high number of workloads. Even for customers with 20,000 volumes, the new dashboard loads in <10 seconds.

After a successful preview and great feedback from preview customers, we are now making it the default experience for all our customers. Be ready for a blazingly fast dashboard.

For details, see View protection health in the Dashboard.

Microsoft SQL Server workload support as a Public Technology Preview

This release of NetApp Backup and Recovery provides an updated user interface that enables you to manage Microsoft SQL Server workloads using a 3-2-1 protection strategy, familiar in NetApp Backup and Recovery. With this new version, you can back up these workloads to primary storage, replicate them to secondary storage, and back them up to cloud object storage.

You can sign up for the preview by completing this Preview Signup Form.

> This documentation about protecting Microsoft SQL Server workloads is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before general availability.

This version of NetApp Backup and Recovery includes the following updates:

- **3-2-1 backup capability**: This version integrates SnapCenter capabilities, enabling you to manage and protect your SnapCenter resources with a 3-2-1 data protection strategy from the NetApp Backup and Recovery user interface.
- **Import from SnapCenter**: You can import SnapCenter backup data and policies into NetApp Backup and Recovery.
- **A redesigned user interface** provides a more intuitive experience for managing your backup and recovery tasks.
- **Backup targets**: You can add buckets in Amazon Web Services (AWS), Microsoft Azure Blob Storage,

StorageGRID, and ONTAP S3 environments to use as backup targets for your Microsoft SQL Server workloads.

- **Workload support**: This version enables you to back up, restore, verify, and clone Microsoft SQL Server databases and availability groups. (Support for other workloads will be added in future releases.)
- **Flexible restore options**: This version enables you to restore databases to both original and alternate locations in case of corruption or accidental data loss.
- **Instant production copies**: Generate space-efficient production copies for development, testing, or analytics in minutes instead of hours or days.
- This version includes the ability to create detailed reports.

For details about protecting Microsoft SQL Server workloads, see Protect Microsoft SQL Server workloads overview.

09 June 2025

This NetApp Backup and Recovery release includes the following updates.

Indexed catalog support updates

In February 2025, we introduced the updated indexing feature (Indexed Catalog v2) that you use during the Search & Restore method of restoring data. The previous release significantly improved data indexing performance in on-premises environments. With this release, the indexing catalog is now available with Amazon Web Services, Microsoft Azure, and Google Cloud Platform (GCP) environments.

If you are a new customer, the Indexed Catalog v2 is enabled by default for all new environments. If you are an existing customer, you can re-index your environment to leverage the Indexed Catalog v2.

How do you enable indexing?

Before you can use the Search & Restore method of restoring data, you need to enable "Indexing" on each source working environment from which you're planning to restore volumes or files. Select the **Enable Indexing** option when you are performing a Search & Restore.

The Indexed Catalog can then track every volume and backup file, making your searches quick and efficient.

For more information, refer to Enable indexing for Search & Restore.

Azure private link endpoints and service endpoints

Typically, NetApp Backup and Recovery establishes a private endpoint with the cloud provider to handle protection tasks. This release introduces an optional setting that lets you enable or disable NetApp Backup and Recovery from automatically creating a private endpoint. This might be useful to you if you want more control over the private endpoint creation process.

You can enable or disable this option when you enable protection or start the restore process.

If you disable this setting, you must manually create the private endpoint for NetApp Backup and Recovery to function properly. Without proper connectivity, you might not be able to perform backup and recovery tasks successfully.

Support for SnapMirror to Cloud Resync on ONTAP S3

The previous release introduced support for SnapMirror to Cloud Resync (SM-C Resync). The feature streamlines data protection during volume migration in NetApp environments. This release add support for SM-

C Resync on ONTAP S3 as well as other S3-compatible providers such as Wasabi and MinIO.

Bring your own bucket for StorageGRID

When you create backup files in object storage for a working environment, by default, NetApp Backup and Recovery creates the container (bucket or storage account) for the backup files in the object storage account that you configured. Previously, you could override this and specify your own container for Amazon S3, Azure Blob Storage, and Google Cloud Storage. With this release, you can now bring your own StorageGRID object storage container.

See Create your own object storage container.

13 May 2025

This NetApp Backup and Recovery release includes the following updates.

SnapMirror to Cloud Resync for volume migrations

The SnapMirror to Cloud Resync feature streamlines data protection and continuity during volume migrations in NetApp environments. When a volume is migrated using SnapMirror Logical Replication (LRSE) from one on-premises NetApp deployment to another, or to a cloud-based solution such as Cloud Volumes ONTAP, SnapMirror to Cloud Resync ensures that existing cloud backups remain intact and operational.

This feature eliminates the need for a time-consuming and resource-intensive re-baseline operation, enabling backup operations to continue post-migration. This feature is valuable in workload migration scenarios, supporting both FlexVols and FlexGroups, and is available starting with ONTAP version 9.16.1.

By maintaining backup continuity across environments, SnapMirror to Cloud Resync enhances operational efficiency and reduces the complexity of hybrid and multi-cloud data management.

For details on how to perform the resync operation, see Migrate volumes using SnapMirror to Cloud Resync.

Support for third-party MinIO object store (Preview)

NetApp Backup and Recovery now extends its support to third-party object stores with a primary focus on MinIO. This new preview feature enables you to leverage any S3-compatible object store for your backup and recovery needs.

With this preview version, we hope to ensure robust integration with third-party object stores before the full functionality is rolled out. You are encouraged to explore this new capability and provide feedback to help enhance the service.

This feature should not be used in production.

Preview mode limitations

While this feature is in preview, there are certain limitations:

- Bring Your Own Bucket (BYOB) is not supported.
- Enabling DataLock in the policy is not supported.
- Enabling Archival mode in the policy is not supported.
- Only on-premises ONTAP environments are supported.

- MetroCluster is not supported.
- Options to enable bucket-level encryption are not supported.

Getting started

To begin using this preview feature, you must enable a flag on the Console agent. You can then enter the connection details of you MinIO third-party object store in the protection workflow by choosing **Third party Compatible** object store in the backup section.

16 April 2025

This NetApp Backup and Recovery release includes the following updates.

UI improvements

This release enhances your experience by simplifying the interface:

- The removal of the Aggregate column from the Volumes tables, along with the Snapshot Policy, Backup Policy, and Replication Policy columns from the Volume table in the V2 Dashboard, results in a more streamlined layout.
- Excluding non-activated working environments from the drop-down list makes the interface less cluttered, the navigation more efficient, and loading faster.
- While sorting on the Tags column is disabled, you can still view the tags, ensuring that important information remains easily accessible.
- The removal of labels on protection icons contributes to a cleaner look and decreases loading time.
- During the working environment activation process, a dialog box displays a loading icon to provide feedback until the discovery process is complete, enhancing transparency and confidence in the system's operations.

Enhanced Volume Dashboard (Preview)

The Volume Dashboard now loads in under 10 seconds, providing a much faster and more efficient interface. This preview version is available to select customers, offering them an early look at these improvements.

Support for third-party Wasabi object store (Preview)

NetApp Backup and Recovery now extends its support to third-party object stores with a primary focus on Wasabi. This new preview feature enables you leverage any S3-compatible object store for your backup and recovery needs.

Getting started with Wasabi

To begin using third-party storage as an object store, you must enable a flag within the Console agent. Then, you can enter the connection details for your third-party object store and integrate it into your backup and recovery workflows.

Steps

1. SSH into your connector.
2. Go into the NetApp Backup and Recovery cbs server container:

```
docker exec -it cloudmanager_cbs sh
```

3. Open the `default.json` file inside the `config` folder via VIM or any other editor:

```
vi default.json
```

4. Modify `allow-s3-compatible`: false to `allow-s3-compatible`: true.
5. Save the changes.
6. Exit from the container.
7. Restart the NetApp Backup and Recovery cbs server container.

Result

After the container is ON again, open the NetApp Backup and Recovery UI. When you initiate a backup or edit a backup strategy, you will see the new provider "S3 Compatible" listed along with other backup providers of AWS, Microsoft Azure, Google Cloud, StorageGRID, and ONTAP S3.

Preview mode limitations

While this feature is in preview, consider the following limitations:

- Bring Your Own Bucket (BYOB) is not supported.
- Enabling DataLock in a policy is not supported.
- Enabling Archival mode in a policy is not supported.
- Only on-premises ONTAP environments are supported.
- MetroCluster is not supported.
- Options to enable bucket-level encryption are not supported.

During this preview, we encourage you to explore this new feature and provide feedback about integration with third-party object stores before the full functionality is rolled out.

17 March 2025

This NetApp Backup and Recovery release includes the following updates.

SMB snapshot browsing

This NetApp Backup and Recovery update resolved an issue that prevented customers from browsing local snapshots in an SMB environment.

AWS GovCloud environment update

This NetApp Backup and Recovery update fixed an issue that prevented the UI from connecting to an AWS GovCloud environment due to TLS certificate errors. The issue was resolved by using the Console agent host name instead of the IP address.

Backup policy retention limits

Previously, the NetApp Backup and Recovery UI limited backups to 999 copies, while the CLI allowed more. Now, you can attach up to 4,000 volumes to a backup policy and include 1,018 volumes not attached to a backup policy. This update includes additional validations that prevent exceeding these limits.

SnapMirror Cloud resync

This update ensures that SnapMirror Cloud resync cannot be started from NetApp Backup and Recovery for unsupported ONTAP versions after a SnapMirror relationship has been deleted.

21 February 2025

This NetApp Backup and Recovery release includes the following updates.

High performance indexing

NetApp Backup and Recovery introduces an updated indexing feature that makes the indexing of data on the source system more efficient. The new indexing feature includes updates to the UI, improved performance of the Search & Restore method of restoring data, upgrades to global search capabilities, and better scalability.

Here's a breakdown of the improvements:

- **Folder consolidation**: The updated version groups folders together using names that include specific identifiers, making the indexing process smoother.
- **Parquet file compaction**: The updated version reduces the number of files used for indexing each volume, simplifying the process and removing the need for an extra database.
- **Scale-out with more sessions**: The new version adds more sessions to handle indexing tasks, speeding up the process.
- **Support for multiple index containers**: The new version uses multiple containers to better manage and distribute indexing tasks.
- **Split index workflow**: The new version divides the indexing process into two parts, enhancing efficiency.
- **Improved concurrency**: The new version makes it possible to delete or move directories at the same time, speeding up the indexing process.

Who benefits from this feature?

The new indexing feature is available to all new customers.

How do you enable indexing?

Before you can use the Search & Restore method of restoring data, you need to enable "Indexing" on each source system from which you're planning to restore volumes or files. This allows the Indexed Catalog to track every volume and every backup file, making your searches quick and efficient.

Enable indexing on the source working environment by selecting the "Enable Indexing" option when you are performing a Search & Restore.

For more information, see the documentation how to restore ONTAP data using Search & Restore.

Supported scale

The new indexing feature supports the following:

- Global search efficiency in less than 3 minutes

- Up to 5 billion files
- Up to 5000 volumes per cluster
- Up to 100K snapshots per volume
- Maximum time for baseline indexing is less than 7 days. The actual time will vary depending on your environment.

Global search performance improvements

This release also includes enhancements to global search performance. You will now see progress indicators and more detailed search results, including the count of files and the time taken for the search. Dedicated containers for search and indexing ensure that global searches are completed in under five minutes.

Note these considerations related to global search:

- The new index is not performed on snapshots labeled as hourly.
- The new indexing feature works only on snapshots on FlexVols, and not for snapshots on FlexGroups.

13 February 2025

This NetApp Backup and Recovery release includes the following updates.

NetApp Backup and Recovery Preview Release

This Preview release of NetApp Backup and Recovery provides an updated user interface that enables you to manage Microsoft SQL Server workloads using a 3-2-1 protection strategy, familiar in NetApp Backup and Recovery. With this new version, you can back up these workloads to primary storage, replicate them to secondary storage, and back them up to cloud object storage.

This documentation is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

This version of NetApp Backup and Recovery Preview 2025 includes the following updates.

- A redesigned user interface that provides a more intuitive experience for managing your backup and recovery tasks.
- The Preview version enables you to back up and restore Microsoft SQL Server databases. (Support for other workloads will be added in future releases.)
- This version integrates SnapCenter capabilities, enabling you to manage and protect your SnapCenter resources with a 3-2-1 data protection strategy from the NetApp Backup and Recovery user interface.
- This version enables you to import SnapCenter workloads into NetApp Backup and Recovery.

22 November 2024

This NetApp Backup and Recovery release includes the following updates.

SnapLock Compliance and SnapLock Enterprise protection modes

NetApp Backup and Recovery now can back up both FlexVol and FlexGroup on-premises volumes that are configured using either SnapLock Compliance or SnapLock Enterprise protection modes. Your clusters must be running ONTAP 9.14 or greater for this support. Backing up FlexVol volumes using SnapLock Enterprise

mode has been supported since ONTAP version 9.11.1. Earlier ONTAP releases provide no support for backing up SnapLock protection volumes.

See the complete list of supported volumes in the Learn about NetApp Backup and Recovery.

Indexing for Search & Restore process on Volumes page

Before you can use Search & Restore, you need to enable "Indexing" on each source system from which you'll want to restore volume data. This enables the Indexed Catalog to track the backup files for every volume. The Volumes page now shows the indexing status:

- Indexed: Volumes have been indexed.
- In-progress
- Not Indexed
- Indexing paused
- Error
- Not Enabled

27 September 2024

This NetApp Backup and Recovery release includes the following updates.

Podman support on RHEL 8 or 9 with Browse and Restore

NetApp Backup and Recovery now supports file and folder restores on Red Hat Enterprise Linux (RHEL) versions 8 and 9 using the Podman engine. This applies to the NetApp Backup and Recovery Browse and Restore method.

Console agent version 3.9.40 supports certain versions of Red Hat Enterprise Linux versions 8 and 9 for any manual installation of the Console agent software on a RHEL 8 or 9 host, regardless of the location in addition to the operating systems mentioned in the host requirements. These newer RHEL versions require the Podman engine instead of the Docker engine. Previously, NetApp Backup and Recovery had two limitations when using the Podman engine. These limitations have been removed.

Learn more about restoring ONTAP data from backup files.

Faster catalog indexing improves Search and Restore

This release includes an improved catalog index that completes the baseline indexing much faster. Faster indexing enables you to use the Search and Restore feature more quickly.

Learn more about restoring ONTAP data from backup files.

Known limitations with NetApp Backup and Recovery for ONTAP volumes

Platforms, devices, or features that do not work or do not work well with this version are listed here. Read these limitations carefully.

- NetApp Backup and Recovery can back up Cloud Volumes ONTAP to an object store in the AWS China regions (including Beijing and Ningxia); however, you might need to manually modify Identity and access

policies first.

For details about creating a Console agent in AWS, refer to Installing a Console agent in AWS.

For additional details, refer to the blog post NetApp Backup and Recovery Feature Blog May 2023.

- NetApp Backup and Recovery does not support Microsoft Azure China regions.

  For details about creating a Console agent in Azure, refer to Installing a Console agent in Azure.

- NetApp Backup and Recovery does not support backups of FlexCache volumes.

Replication limitations for ONTAP volumes

- You can select only one FlexGroup volume at a time for replication. You'll need to activate backups separately for each FlexGroup volume.

  There is no limitation for FlexVol volumes - you can select all FlexVol volumes in your system and assign the same backup policies.

- The following functionality is supported in NetApp Replication, but not when using the replication feature of NetApp Backup and Recovery:
  - There is no support for a cascade configuration where replication occurs from volume A to volume B and from volume B to volume C. Support includes replication from volume A to volume B.
  - There is no support for replicating data to and from FSx for ONTAP systems.
  - There is no support for creating a one-time replication of a volume.
- When creating replications from on-premises ONTAP systems, if the ONTAP version on the target Cloud Volumes ONTAP system is 9.8, 9.9, or 9.11, only mirror-vault policies are allowed.
- NetApp Backup & Recovery does not support converting a FlexVol volume with an active cloud backup relationship to a FlexGroup volume while maintaining cloud backup functionality.

Backup-to-object limitations for ONTAP volumes

- When backing up data, NetApp Backup and Recovery will not maintain NetApp Volume Encryption (NVE). This means that encrypted data on the NVE volume will be decrypted while the data is being transferred to the destination and the encryption will not be maintained.

  For an explanation about these encryption types, refer to Configure NetApp Volume Encryption overview.

- If long-term retention snapshots are enabled on a SnapMirror destination volume using the schedule in the SnapMirror policy, snapshots are created directly on the destination volume. In this case, you should not back up those volumes using NetApp Backup and Recovery because those snapshots will not be moved to object storage.
- When backing up data, NetApp Backup and Recovery will not maintain NetApp Volume Encryption (NVE). This means that encrypted data on the NVE volume will be decrypted while the data is being transferred to the destination and the encryption will not be maintained.

  For an explanation about these encryption types, refer to Configure NetApp Volume Encryption overview.

- If long-term retention snapshots are enabled on a SnapMirror destination volume using the schedule in the

SnapMirror policy, snapshots are created directly on the destination volume. In this case, you should not back up those volumes using NetApp Backup and Recovery because those snapshots will not be moved to object storage.

- When you create or edit a backup policy when no volumes are assigned to the policy, the number of retained backups can be a maximum of 1018. After you assign volumes to the policy, you can edit the policy to create up to 4000 backups.
- When backing up data protection (DP) volumes:
  - Relationships with the SnapMirror labels `app_consistent` and `all_source_snapshot` won't be backed up to cloud.
  - If you create local copies of Snapshots on the SnapMirror destination volume (irrespective of the SnapMirror labels used) these Snapshots will not be moved to the cloud as backups. At this time you'll need to create a Snapshot policy with the desired labels to the source DP volume in order for NetApp Backup and Recovery to back them up.
- FlexGroup volume backups can't be moved to archival storage.
- FlexGroup volume backups can use DataLock and Ransomware protection if the cluster is running ONTAP 9.13.1 or greater.
- SVM-DR volume backup is supported with the following restrictions:
  - Backups are supported from the ONTAP secondary only.
  - The Snapshot policy applied to the volume must be one of the policies recognized by NetApp Backup and Recovery, including daily, weekly, monthly, etc. The default "sm_created" policy (used for **Mirror All Snapshots**) is not recognized and the DP volume will not be shown in the list of volumes that can be backed up.
  - SVM-DR and volume backup and recovery work fully independently when the backup is taken from either the source or destination. The only restriction is that SVM-DR does not replicate the SnapMirror cloud relationship. In the DR scenario when the SVM goes online in the secondary location, you must manually update the SnapMirror cloud relationship.
- MetroCluster support:
  - When you use ONTAP 9.12.1 GA or greater, backup is supported when connected to the primary system. The entire backup configuration is transferred to the secondary system so that backups to the cloud continue automatically after switchover. You don't need to set up backup on the secondary system (in fact, you are restricted from doing so).
  - When you use ONTAP 9.12.0 and earlier, backup is supported only from the ONTAP secondary system.
  - Beginning with ONTAP 9.18.1, FlexGroup volume backups are supported in MetroCluster configurations.
- Ad-hoc volume backup using the **Backup Now** button isn't supported on data protection volumes.
- SM-BC configurations are not supported.
- ONTAP doesn't support fan-out of SnapMirror relationships from a single volume to multiple object stores; therefore, this configuration is not supported by NetApp Backup and Recovery.
- WORM/Compliance mode on an object store is supported on Amazon S3, Azure, and StorageGRID at this time. This is known as the DataLock feature, and it must be managed by using NetApp Backup and Recovery settings, not by using the cloud provider interface.

Restore limitations for ONTAP volumes

These limitations apply to both the Search & Restore and the Browse & Restore methods of restoring files and folders; unless called out specifically.

- Browse & Restore can restore up to 100 individual files at a time.
- Search & Restore can restore 1 file at a time.
- When using ONTAP 9.13.0 or greater, Browse & Restore and Search & Restore can restore a folder along with all files and sub-folders within it.

  When using a version of ONTAP greater than 9.11.1 but before 9.13.0, the restore operation can restore only the selected folder and the files in that folder - no sub-folders, or files in sub-folders, are restored.

  When using a version of ONTAP before 9.11.1, folder restore is not supported.
- Directory/folder restore is supported for data that resides in archival storage only when the cluster is running ONTAP 9.13.1 and greater.
- Directory/folder restore is supported for data that is protected using DataLock only when the cluster is running ONTAP 9.13.1 and greater.
- Directory/folder restore is not currently supported from replications and/or local snapshots.
- Restoring from FlexGroup volumes to FlexVol volumes, or FlexVol volumes to FlexGroup volumes is not supported.
- The file being restored must be using the same language as the language on the destination volume. You will receive an error message if the languages are not the same.
- The *High* restore priority is not supported when restoring data from Azure archival storage to StorageGRID systems.
- If you back up a DP volume and then decide to break the SnapMirror relationship to that volume, you cannot restore files to that volume unless you also delete the SnapMirror relationship or reverse the SnapMirror direction.
- Quick restore limitations:
  - The destination location must be a Cloud Volumes ONTAP system using ONTAP 9.13.0 or greater.
  - It is not supported with backups located in archived storage.
  - FlexGroup volumes are supported only if the source system from which the cloud backup was created was running ONTAP 9.12.1 or greater.
  - SnapLock volumes are supported only if the source system from which the cloud backup was created was running ONTAP 9.11.0 or greater.

Known limitations with NetApp Backup and Recovery for Microsoft SQL Server workloads

Platforms, devices, or features that do not work or do not work well with this version are listed here. Read these limitations carefully.

Clone lifecycle support

- Cloning from object storage is not supported.

- Bulk clone operations are not supported for on-demand clones.
- Choosing I-groups is not supported.
- Choosing QOS (maximum throughput) options is not supported.

Standard deployment mode only

This NetApp Backup and Recovery version works only in standard deployment mode, not restricted or private modes.

Windows cluster name restriction

The Windows cluster name cannot contain an underscore (_) character.

SnapCenter migration issues

The migration of resources from SnapCenter into NetApp Backup and Recovery has the following limitations.

For details about how SnapCenter policies migrate to NetApp Backup and Recovery policies, see Policies in SnapCenter compared to those in NetApp Backup and Recovery.

Resource group limitations

If all the resources in a resource group are protected and one of those resources is also protected outside of the resource group, the migration from SnapCenter is blocked.

Workaround: Protect the resource either in a resource group or by itself, but not in both.

Resources with multiple policies using the same schedule tier not supported

You cannot have assign multiple policies that use the same schedule tier (for example, hourly, daily, weekly, etc.) to a resource. NetApp Backup and Recovery will not import those resources from SnapCenter.

Workaround: Attach only one policy using the same schedule tier to a resource.

Hourly policies must begin at the start of the hour

If you have a SnapCenter policy that repeats hourly but does not use intervals at the start of the hour, NetApp Backup and Recovery will not import the resource. For example, policies with schedules of 1:30, 2:30, 3:30, etc. are not supported, while policies with schedules of 1:00, 2:00, 3:00, etc. are supported.

Workaround: Use a policy that repeats in 1-hour intervals starting at the top of the hour.

Both daily and monthly policies attached to one resource not supported

If a SnapCenter policy repeats both in day and month intervals, NetApp Backup and Recovery will not import the policy.

For example, you cannot attach a daily policy (with less than or equal to 7 days or greater than 7 days) to a resource and also attach a monthly policy to the same resource.

Workaround: Use a policy that uses a daily or a monthly interval, but not both.

On demand backup policies not migrated

NetApp Backup and Recovery does not import on demand backup policies from SnapCenter.

Log-only backup policies not migrated

NetApp Backup and Recovery does not import log-only backup policies from SnapCenter. If a SnapCenter policy includes log-only backups, NetApp Backup and Recovery will not import the resource.

Workaround: Use a policy in SnapCenter that uses more than just log-only backups.

Host mapping

SnapCenter does not have map storage clusters or SVMs for the resources to hosts, but NetApp Backup and Recovery does. The on-premises ONTAP cluster or SVM will not be mapped to a host in NetApp Backup and Recovery preview versions. Additionally, NetApp Console does not support SVMs.

Workaround: Before importing resources from SnapCenter, create a system in NetApp Backup and Recovery for all the on-premises ONTAP storage systems that are registered in on-premises SnapCenter. Then, import the resources for that cluster from SnapCenter into NetApp Backup and Recovery.

Schedules not in 15-minute intervals

If you have a SnapCenter policy schedule that starts at a certain time and repeats in intervals other than 15-minute intervals, NetApp Backup and Recovery will not import the schedule.

Workaround: Use SnapCenter to adjust the policy so that it repeats in 15-minute intervals.

Limited support for virtualization management software

When you protect KVM workloads, NetApp Backup and Recovery does not support discovery of KVM workloads when virtualization management software such as Apache CloudStack or Red Hat OpenShift Virtualization is in use.

Known limitations with NetApp Backup and Recovery for VMware workloads

Platforms, devices, or features that do not work or do not work well with this version are listed here. Read these limitations carefully.

The following actions are not supported in the preview version of VMware workloads in NetApp Backup and Recovery:

- Mount
- Unmount
- Attach VMDK
- Detach VMDK
- vVol support
- NVMe support
- Email integration

- Edit policy
- Edit protection group
- Role-based access control (RBAC) support

Known limitations with NetApp Backup and Recovery for Hyper-V workloads

Platforms, devices, or features that do not work or do not work well with this version are listed here. Read these limitations carefully.

Unsupported actions

The following actions are not supported in the private preview version of Hyper-V workloads in NetApp Backup and Recovery:

- Create resource groups using VMs from multiple Hyper-V hosts
- Restore VMs to an alternate location
- Spanning disks (across multiple CIFS shares)
- Protect VMs over SAN
- You cannot restore VMs or VM data between systems with different CPU vendors (Intel to AMD or vice versa), regardless of the "Processor compatibility" setting in Hyper-V. This setting only supports compatibility between different generations of the same vendor (e.g., Intel to Intel or AMD to AMD).

In the January 19 2026 release, you cannot upgrade the NetApp plugins for Hyper-V or Windows using the **Upgrade** option in the Actions menu. Instead, remove each Hyper-V host and add it again to update the plugins.

Known limitations with NetApp Backup and Recovery for KVM workloads

Platforms, devices, or features that do not work or do not work well with this version are listed here. Read these limitations carefully.

The following actions and configurations are not supported in the private preview version of KVM workloads in NetApp Backup and Recovery:

Unsupported actions

The following actions are not supported in the private preview release:

- Clone, mount, or unmount VMs
- Restore VMs to an alternate location
- Protect VMs stored on SAN
- Protect applications
- Edit protection groups

- Create protection groups using VMs from multiple KVM hosts
- Create user-defined backups (only backups initiated from the NetApp Console are supported)

Unsupported configurations

The following configurations are not supported:

- Role-based access control (RBAC)
- Disks directly attached to the KVM host
- Disks spanned across multiple NFS mount points or shares
- RAW disk format
- Storage pool types other than NetFS (only NetFS is supported)

Troubleshooting notes

Make note of the following when using the private preview of KVM workloads with NetApp Backup and Recovery:

- To ensure that KVM workload restores complete successfully, make sure that the **Enable VM-consistent snapshot** setting is active in the protection policy you use for KVM backups.
- You cannot back up a storage pool with KVM hosts managed by Apache CloudStack unless you add all managed hosts to NetApp Backup and Recovery. As a workaround, add every CloudStack-managed KVM host to NetApp Backup and Recovery.
- You cannot back up a stopped VM that belongs to a protection group. As a workaround, remove the stopped VM from the protection group before starting the backup.

Known limitations with NetApp Backup and Recovery for Oracle Database workloads

Platforms, devices, or features that do not work or do not work well with this version are listed here. Read these limitations carefully.

The following action is not supported in the private preview version of Oracle Database workloads in NetApp Backup and Recovery:

- Offline backup

Oracle Database is supported only as a standalone deployment using NFS, SAN, or ASM SAN in the private preview version of Oracle Database workloads.

Copyright information

Trademark information