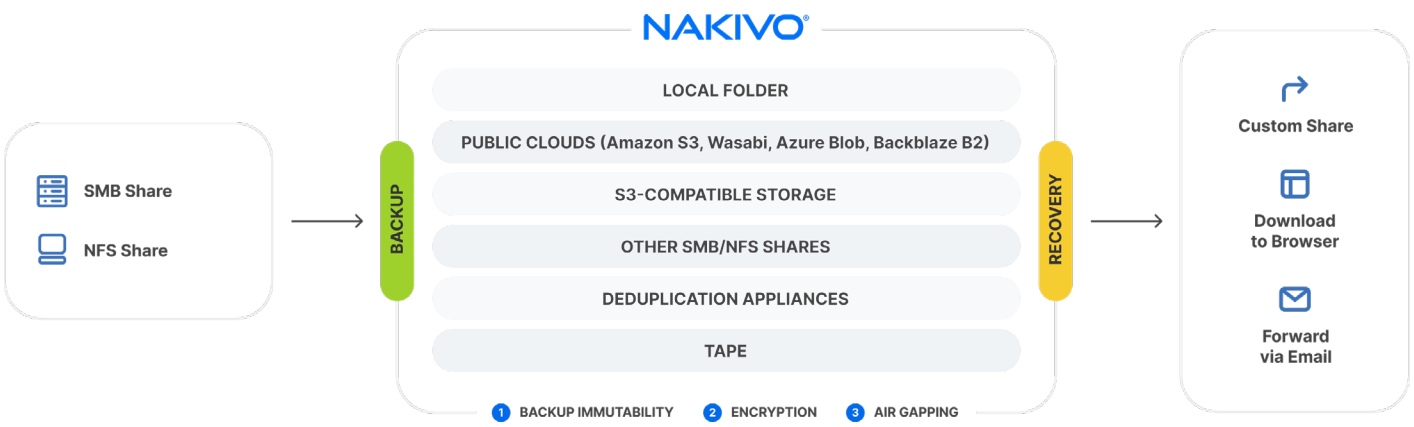
# WHAT'S NEW IN NAKIVO NAS BACKUP



# Table of Contents

## INTRODUCTION

As unstructured data in file share environments — such as Network-Attached Storage (NAS), Windows, and Linux systems — continues to grow exponentially, the challenges and costs of managing and protecting it are also increasing. While some organizations may treat NAS devices as a backup solution, they are not designed to provide true data protection. Even traditional backup tools, like NDMP, often fail to meet modern demands, leaving file shares fragmented and vulnerable to ransomware attacks and operational risks.

The NAS Backup functionality in NAKIVO Backup & Replication offers a streamlined, end-to-end solution tailored to modern data protection needs: secure, unified file share backup and recovery across NAS, Windows, and Linux systems. The solution supports **NFS 3.x, SMB 2.x, and SMB 3.x** protocols for broad compatibility with a wide range of file share environments.

The following is an overview of the latest additions to the NAKIVO NAS Backup functionality.

## DIRECT BACKUP TO CLOUD

Cloud backups offer a reliable and convenient way to protect against data loss caused by ransomware, human error, and system failures. They also enable faster and easier data recovery — requiring only an internet connection to access your files anytime, anywhere.

The latest version of NAKIVO Backup & Replication allows you to send your file share backups directly to public cloud storage platforms, including Amazon S3, Wasabi, Azure Blob, and Backblaze B2. Additionally, you can send your backups to any S3-compatible object storage platform that employs the S3 API.

## MORE BACKUP STORAGE TARGETS

You now have the flexibility to choose the storage target that best aligns with your data protection strategy and needs. NAKIVO has expanded the list of supported file share backup destinations to include:

- Local folders
- Other NFS or SMB network shares
- Cloud storage platforms
- S3-compatible storage platforms
- Deduplication appliances

## BACKUP COPY

Implementing the 3-2-1 or 3-2-1-1 rules ensures you have a clean backup copy that's safe and accessible even during a crisis.

The Backup Copy feature in NAKIVO Backup & Replication now extends to file share backups. You can create and send copies of your file share backups to the supported backup targets and to tape devices to follow the 3-2-1 backup strategy and eliminate a single point of failure.

## IMMUTABLE STORAGE

With NAKIVO Backup & Replication, you can secure NAS file share backups in immutable storage on Linux-based local repositories, public cloud, S3-compatible storage platforms, and NEC HYDRAstor storage systems.

Immutability applies a write-once-read-many (WORM) model to your recovery points, making them tamper-proof. This extra layer of security prevents ransomware encryption, accidental deletion, or unauthorized changes, ensuring that your data remains intact and ready for recovery.

## ENCRYPTED BACKUPS

NAKIVO NAS Backup offers the highest level of security for your file share backups with AES-256 encryption at every stage: at the source, during transit, and at rest.

- **Source Encryption:** Encrypt data before it leaves the source system.
- **In-Transit Encryption:** Protect data as it travels over the network.
- **At-Rest Encryption:** Secure data stored in the repository.

This comprehensive approach protects your data from unauthorized access and breaches, ensuring your backups remain secure throughout the entire lifecycle.

## NAKIVO NAS BACKUP: MAIN CAPABILITIES

### FILE SHARE BACKUP

- **Fast incremental backup** using NAKIVO's proprietary change tracking technology to speed up backup processes and optimize storage use.
- **Granular backup** to select specific folders within a file share for backup, rather than backing up the entire share.
- **Direct backup to cloud** including Amazon S3, Wasabi, Backblaze B2, Azure Blob Storage, and other S3-compatible storage platforms.
- **Backup copy** to offsite and onsite targets like public clouds, S3-compatible storage, network shares, deduplication appliances, and tape.
- **Job chaining** to automate backup workflows. Once the initial backup is successfully created, subsequent copies are triggered automatically.

### FILE SHARE RECOVERY

- **Full share recovery** to restore the contents of entire NFS/SMB shares from backups to any locations.
- **Granular recovery** to choose and restore specific files and folders from your file share backups to the selected destination rather than wait for a full restore to complete.
- **Multiple options to recover** file share data, either to a custom location on SMB or NFS shares, send via email, or download to a browser.
- **Seamless navigation** across backups to instantly locate and recover specific files and folders using the search function or the navigation panel.

## RANSOMWARE PROTECTION

- **Immutable backups** stored locally, in the cloud, or on NEC HYDRAstor storage to prevent ransomware encryption and other unwanted modifications.
- **Air-gapped backups** with copies stored offline on detachable drives, such as tape, for an additional layer of protection.

## SECURITY AND COMPLIANCE

- **Robust backup encryption** to protect backup data at every stage — at the source, during transit, and in the repository.
- **Two-factor authentication (2FA)** adds a layer of security with one-time codes generated via Google Authenticator to protect your data protection activities.
- **Role-based access control (RBAC)** with preset and custom roles to prevent unauthorized access to your file share backup data.
- **Flexible retention** with numerous recovery points to retrieve the exact data copy you need for regulatory compliance, e-discovery, or disaster recovery.
- **Native backup to tape** for secure, isolated, and long-term data archival to meet stringent regulatory requirements.

## ADMINISTRATION

- **Web-based interface** with convenient dashboards and step-by-step wizards to manage all backup and recovery activities.
- **Calendar dashboard** that provides a comprehensive overview of all data protection workflows. Schedule file share backups easily and avoid overlaps.
- **Global search** to help search and locate any file or folder you need to ensure efficient and accurate recovery.
- **Streamlined operations** with features like Job Chaining and Network Acceleration to automate and enhance backup and recovery processes.
- **Flexible deployment** options on Linux, Windows, and NAS as a backup appliance, or as a VA or AWS AMI.

By deploying NAKIVO Backup & Replication, you gain a comprehensive data protection solution that extends beyond traditional NAS backup, offering robust backup capabilities, multiple backup targets, flexible recovery options, and powerful cybersecurity capabilities.

## START PROTECTING YOUR FILE SHARES

**Download Free Trial**

Free for 15 days.
No feature limitations.

**Schedule a Demo**

Get answers on features,
pricing and more.

NAKIVO®

This publication has been prepared for general guidance and does not constitute professional advice, a public offer or an undertaking. No representations or warranties (express or implied) are given as to the accuracy or completeness of the information contained in this document, and, to the extent permitted by law, NAKIVO, Inc., its affiliates, employees, contractors and agents do not accept or assume any liability, responsibility or duty of care for any consequences of anyone acting, or refraining to act, in reliance on the information contained in this document or for any decision based on it. All third party trademarks and trade names are the property of their respective owners.

**nakivo.com | +1 408 440 5605 |** 4894 Sparks Blvd., Sparks, NV USA 89436-8202

© 2025 NAKIVO, INC. All rights reserved. In this document term "NAKIVO" refers to, and is deemed to be a trade name of NAKIVO, INC.