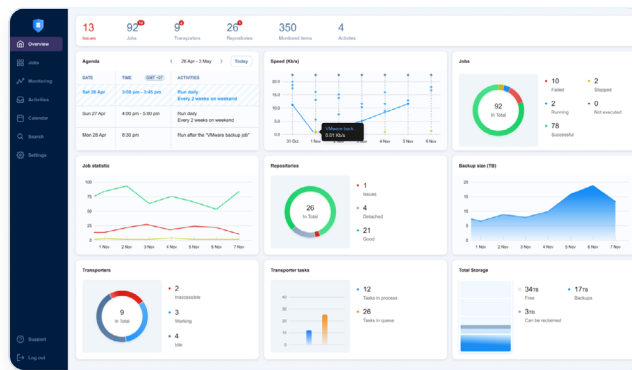


Comprehensive Backup and Recovery for NAS File Shares

The NAS Backup functionality in NAKIVO Backup & Replication delivers an array of powerful backup, full and granular restore, and ransomware protection capabilities to protect SMB/NFS shares on NAS devices and file servers running Windows or Linux. Designed to minimize data loss and downtime, the solution ensures data availability across file storage environments in any data-loss event.



SINGLE PANE OF GLASS

for backup, full and instant granular restore, and ransomware protection.

DEPLOY ANYWHERE

on NAS, Windows, Linux, or as a pre-configured Nutanix/VMware VA or AMI.

STORE ANYWHERE

on local, cloud, S3-compatible storage, other NFS/SMB shares, deduplication appliances and tape.

SAVE ON COSTS

starting at **\$29** per workload/year (subscription) or **\$149** per terabyte (perpetual).

FAST, RELIABLE, AND SECURE FILE SHARE BACKUP

NAKIVO NAS Backup provides a set of features to ensure a complete, up-to-date copy of your unstructured file data is ready for recovery when needed.

Incremental backup: Create fast incremental file share backups using NAKIVO's proprietary change tracking technology to optimize storage and speed up backup processes.

Granular backup: Browse, search and select specific folders within a file share for backup, rather than backing up the entire share.

Backup copy: Create backup copies and send them offsite cloud and other S3-compatible storage) or to other supported destinations.

Backup to Cloud: Directly back up unstructured NAS data to public clouds, including Amazon S3, Wasabi, Backblaze B2, and Azure Blob Storage.

Backup to S3-compatible storage: Send file share backups to object storage platforms that use the S3 API.

Deduplication appliance integration: Back up to HPE StoreOnce, Dell EMC Data Domain, and NEC HYDRastor appliances with support for native deduplication protocols.

Backup copy to Tape: Create and send backup copies of your file share data to physical tape libraries and AWS VTL for secure and cost-effective archiving.

Flexible retention: Retain up to 4,000 recovery points per backup job and rotate them daily, weekly, monthly or yearly for point-in-time recovery should data loss or corruption occur.

Federated Repository: Combines various "member" repositories into a single, scalable repository to ensure backups are automatically shifted to available repositories in case of storage failures or capacity issues.

BENEFITS

2X

faster NAS backups with change tracking, Network acceleration and more

49%

lower TCO than other vendors for the same functionality or better

4.8 STARS

average rating on top IT communities for saving time and money

5 MIN

to fully deploy and configure the solution in your environment

4,000

recovery points per backup to meet strict RPO requirements

GARTNER PEER INSIGHTS

NAKIVO Earns Recognition in Gartner® Peer Insights™ Voice of the Customer Report for Enterprise Backup and Recovery Solutions

4.8



Overall rating

98%*



Willingness to recommend

EFFICIENT FILE SHARE RECOVERY

NAKIVO NAS Backup allows you to recover entire shares or specific files and folders to meet RTO/RPO objectives in any data-loss event with little to no downtime.

Full file share recovery: Recover the contents of entire NFS/SMB shares from backups to any locations.

Granular recovery: Quickly recover the files and folders you need from your file share backups to the selected destination in seconds without performing a full recovery.

Multiple recovery options. Recover data to a custom location on SMB or NFS shares, send via email or download to a browser.

Seamless navigation: Quickly locate specific files and folders within backups using the search box, or browse through the navigation panel to find the exact files you need for recovery.

RANSOMWARE PROTECTION FOR NAS FILE SHARE

NAKIVO NAS Backup allows you to protect NAS data backups against ransomware and other security risks with robust built-in measures, ensuring data remains secure even before an attack occurs.

Backup data tiering: Store file share backup copies across multiple locations —onsite, offsite, and in the cloud— to ensure data is readily available for recovery in the event of an attack.

Immutable local backups: Enable immutability for NAS file share backups stored in Linux-based local repositories to prevent accidental deletions, modifications or even encryption by ransomware.

Immutable cloud backups: Create immutable file share backups in public cloud platforms (Amazon S3, Wasabi, Azure Blob, and Backblaze B2) as well as other S3-compatible storage platforms.

Deduplication appliance immutability: Enable immutability for file share backups residing on NEC HYDRastor storage systems.

Air-gapped backups: Keep backup copies offline on tape and other detachable storage to ensure secure and isolated recovery options.

Multi-staged encryption: Protect backups with AES-256 encryption at every stage — at the source, during transit, and at rest in the repository.

Robust security controls: Prevent unauthorized access to file share backups with role-based access control (RBAC) and two-factor authentication (2FA).

APPLY THE 3-2-1-1 BACKUP STRATEGY WITH NAKIVO



3 copies of your data

Keep at least **three** copies on local storage, cloud, tape, etc.



Stored on 2 devices

Store on **two** different media (tape or the cloud).



With 1 device off-site

Keep **one** copy offsite or in the cloud.



And 1 copy of immutable/air-gapped

Make **one** backup copy immutable or air-gapped.

COMPLIANCE WITH CYBERSECURITY REGULATIONS AND STANDARDS

NAKIVO Backup & Replication can help reinforce your cyber resiliency strategies by enabling proactive data protection, security and recovery.



NIS2 DIRECTIVE



NIST CSF 2.0



GDPR



HIPAA

STREAMLINED BACKUP MANAGEMENT

Ensure your NAS data protection processes are efficient and effective with NAKIVO Backup & Replication.

Flexible Deployment: Deploy as a virtual appliance/AMI, install on Linux or Windows OS, or a NAS to create an all-in-one backup appliance.

Web interface: Use an intuitive web-based management console to access the backup solution anytime and from any device.

Overview dashboard: Monitor the status of all data protection activities, solution components, and issues in one centralized dashboard.

Calendar dashboard: Manage current and future data protection workflows, schedule jobs and prevent overlap through the calendar dashboard.

Network acceleration: Speed up data transfer over busy networks with advanced compression and traffic reduction techniques.

Job chaining: Link backup and backup copy jobs to create seamless workflows. For example, a successful file share backup to local storage can trigger a Backup Copy job to transfer the new backups to a public cloud.

API integration: Integrate NAKIVO Backup & Replication with monitoring, automation, and orchestration solutions via HTTP API to enhance the flexibility, efficiency, and reliability of your backup and recovery operations.

Minimal footprint: Save resources with a small solution footprint, requiring only 2 CPUs and 4GB RAM for a full solution deployment.

BAAS AND DRAAS OFFERINGS

NAKIVO Backup & Replication enables MSPs to offer reliable backup and disaster recovery services across diverse IT environments, all while streamlining operations and delivering significant value.

MSP Console: Deliver full BaaS/DRaaS services and centrally manage environments with standalone instances as remote tenants alongside local tenants.

Multi-Tenancy: Create up to 100 isolated tenants within one instance and manage them from a single pane of glass.

Tenant overview dashboard: Get a real-time view of all existing tenants' environments, including jobs, repositories, nodes, inventory, and allocated resources — all at a glance.

Self-Service: Offload data protection and recovery tasks to tenants using the Self-Service Portal to save time and management overhead.

Tenant Resource Allocation: Allocate data protection infrastructure resources, including hosts, clusters, VMs, Transporters, backup repositories, etc.) to your tenants based on their individual needs.

Direct Connect: Access the remote environments of your tenants via a single port connection without having to set up a VPN first.

TRUSTED BY GLOBAL BRANDS



WHAT CUSTOMERS SAY ABOUT NAKIVO

50% lower costs

With NAKIVO, the licensing costs for the end-users that we support are about half as expensive as our prior product.

Michael Marchuk, Senior Technical Director at American Datacenters.

7X faster backups

The solution is faster than other products I have used and supports many different configurations.

Praful Soni, Senior IT Manager at Transpek

99% faster recovery

With granular recovery, we can restore files in just a few minutes, while previously it would have taken us hours to restore the entire VM that held it.

Krister Laag, CIO at Stendahls

TOP RATED SOLUTION ON BIGGEST REVIEW PLATFORMS



System Requirements

Supported File Share Types

- NFS and SMB shares on NAS, Windows, and Linux

Full solution deployment requirements

- **Server:** 2 CPU cores, 4 GB RAM
- **NAS:** Refer to [System Requirements](#)

Pricing for NAKIVO NAS Backup

Two license types to fit any budget

- **Perpetual licensing:** \$149 per Terabyte (TB) — each 1 TB of source data to be backed up is a licensed unit.
- **Subscription licensing:** \$29 per workload per year.

Deployment Options

Virtual Appliance

- Pre-configured VMware
- Pre-configured Nutanix Acropolis

Windows

- Windows Server
- Windows 11
- Windows 10
- Windows 8

NAS

- QNAP QTS
- QNAP QuTS Hero
- QNAP QuTScloud
- Synology DSM
- ASUSTOR ADM
- TrueNAS CORE
- Netgear ReadyNAS OS
- WD MyCloud OS

Linux

- Ubuntu Server
- Ubuntu Server LTS
- Red Hat Enterprise Linux
- SUSE Linux Enterprise 15
- SUSE Linux Enterprise 12
- CentOS Linux
- CentOS Stream
- Debian
- AlmaLinux
- Oracle Linux
- Rocky Linux

For more information: Refer to [Deployment Requirements](#).

START PROTECTING YOUR NAS DATA TODAY

[DOWNLOAD FREE TRIAL](#)[BOOK FREE DEMO](#)