What's New in NAKIVO Backup for VMware

Table of Contents

INTRODUCTION

NAKIVO Backup & Replication delivers all-in-one backup, instant restore, ransomware protection, and disaster recovery capabilities to safeguard VMware environments against the effects of data loss and cyber threats.

LATEST FEATURES AND ENHANCEMENTS

The IT threat landscape is in constant change, creating frequent shifts in data protection needs. To help organizations adapt their backup and disaster recovery strategies, NAKIVO consistently releases updates that introduce new data protection features and enhance existing capabilities.

Since January 2023, we have rolled out eight new versions of NAKIVO Backup & Replication with various backup and anti-ransomware tools to protect critical data in VMware environments. The following is an overview of the latest additions up to version 11.0.4.

VMware vSphere Support Updates

NAKIVO continues to lead with early support for the latest versions of VMware vSphere, helping customers maintain uninterrupted protection through every upgrade.

We were among the first backup vendors to deliver full support for vSphere 8.0 GA, followed by support for subsequent VMware releases, including vSphere 8.0 U2, vSphere 8.0U2b, vSphere 8.0U2c and vSphere 8.0U3.

Now, with the latest v11.0.4, we've extended compatibility support to include VMware vSphere 9, ensuring continuous backup and recovery support for environments running VMware's latest release.

Source-Side Backup Encryption

NAKIVO Backup & Replication enables you to encrypt backups at the source side before they are transferred over the network to their storage destination.

Encrypted backups can be stored in local folders, public cloud platforms (Amazon S3, Wasabi, Azure Blob, Backblaze B2), S3-compatible storage targets, SMB/NFS network shares, tape, and deduplication appliances. A password is required to decrypt the backup data, and the feature also supports integration with AWS KMS as a failsafe device in case you lose the decryption keys.

Federated Repository

The Federated Repository is an easily scalable and flexible type of backup repository that addresses bottlenecks in performance and complexity in large environments with big datasets.

A Federated Repository acts like an expandable storage pool composed of multiple standalone repositories, called "members". You can expand a Federated Repository quickly and easily by adding new members to hold more data. No complex configurations are required to add or remove members, as the process takes only a few clicks. In a Federated Repository, backup and recovery operations continue without interruption even if one of the member repositories fails or runs out of space, as long as another usable member is available.

Backup from NetApp Storage Snapshots

NAKIVO has added NetApp FAS and NetApp AFF storage arrays to the list of supported storage devices for the Backup for Storage Snapshots feature. Backing up VMware VMs directly from storage snapshots instead of regular VM snapshots reduces the impact of VM backup operations on resources and performance in your production environment.

Tenant Overview Dashboard

We've expanded the MSP Console with the Tenant Overview Dashboard, which provides a high-level overview of all managed tenants in one place.

From this dynamic dashboard, you can view real-time insights and alerts about your client data protection infrastructures, including node status, available resources, scheduled activities, and inventory information. You can sort, filter, and search through your tenant list to extract the information you need, identify pending issues, and apply bulk actions.

Immutable Storage on NEC HYDRAstor

NAKIVO Backup & Replication supports NEC HYDRAstor as a backup storage destination among other deduplication appliances.

You can now enable immutability for backups residing on your NEC HYDRAstor storage system to protect them against ransomware attacks, accidental deletions, and other forms of unwanted modification.

Granular Notifications

Granular Notifications enhances workflow tracking capabilities, giving you greater visibility into running backup and replication jobs. While a job is running, NAKIVO Backup & Replication displays descriptions of ongoing actions, such as data transfer or log truncation. The status updates take place in real time to keep you informed as the job progresses.

File System Indexing

File System Indexing builds on the existing capabilities of the Global Search function to create an index of all files and folders within your VM backups. Consequently, when you perform granular recovery to restore one or more files or folders, you can use Global Search to locate the required items quickly, saving valuable time in the process.

Alarms and Reporting for IT Monitoring

With Alarms and Reporting for IT Monitoring, you can create and configure custom alerts that are triggered when specific conditions are met.

Alarms have several uses, including proactive detection of unusual activity that could signal malicious behavior, such as when CPU usage suddenly exceeds normal levels. With the reporting functionality, you can view, export, and email various details about monitored VMware vSphere items in your infrastructure.

Backup from HPE Alletra and HPE Primera Storage Snapshots

NAKIVO has added HPE Alletra and HPE Primera to the list of supported storage devices for the Backup for Storage Snapshots feature. You can back up your VMware vSphere VMs stored on these storage devices more efficiently by utilizing storage snapshots instead of regular VM snapshots.

Real-Time Replication (Beta) for VMware

Real-Time Replication (Beta) for VMware is a powerful addition to the disaster recovery capabilities of NAKIVO Backup & Replication.

You can create real-time replicas of VMware vSphere VMs and set them to be continuously updated with data changes that occur in the source VMs. Changes in the source VM data are processed in real-time with update rates (and recovery point objectives) as low as 1 second, which ensures continuous availability of critical machines and data.

Real-Time Replication (Beta) for VMware: vSphere 9.0 Compatibility

NAKIVO has expanded the scope of Real-Time Replication (Beta) for VMware to cover vSphere 9.0, allowing you to maintain uninterrupted replication workflows as you upgrade your VMware environment.

Backup Malware Scan

The Backup Malware Scan feature is an important addition to the ransomware protection capabilities of NAKIVO Backup & Replication. Using this feature, you can scan backups for malware and ransomware before performing recovery in order to prevent infections in your infrastructure.

You can integrate the solution with Windows Defender, ESET NOD32, and Sophos to run malware scans and ensure backups can be safely used for recovery. If malware is detected during a scan, you have the choice to either fail the recovery job or use an isolated network as the recovery destination.

Direct Recovery from Tape

With Direct Recovery from Tape, you can recover full virtual machines and Amazon EC2 instances directly to your infrastructure from backups stored on tape media.

The direct restore approach improves recovery times and efficiency. In addition to VMware vSphere, supported platforms include Microsoft Hyper-V, Nutanix AHV, and Amazon EC2, in addition to physical workloads via Physical-to-Virtual Recovery.

S3-Compatible Object Storage Support

Expanding the hybrid backup storage capabilities of NAKIVO Backup & Replication, S3-Compatible Object Storage Support allows you to store backups in local and cloud-based storage targets that employ the S3 API.

You can choose from a variety of S3-compatible storage destinations that fit your organization's needs and budget. Moreover, you can enable immutability for recovery points stored in S3-compatible storage locations to protect against ransomware infections, accidental deletions, and other unwanted modifications.

Permanent VM Agent

With the addition of the Permanent VM Agent feature in NAKIVO Backup & Replication, you can deploy a persistent agent on VMware vSphere VMs to streamline guest processing without the need to provide OS credentials.

Using persistent agents, the solution communicates with target VMs over a single port, which ensures alignment with security policies that prohibit the sharing of OS credentials and other sensitive information.

NAKIVO BACKUP FOR VMWARE: MAIN CAPABILITIES

NAKIVO Backup & Replication delivers fast agentless backup, instant VM and granular recovery, and multi-layered ransomware protection to ensure that data in your VMware environment is protected and recoverable. The following is an overview of notable features and capabilities for backup, disaster recovery, ransomware protection, security and compliance, and administration:

Backup

- **Incremental backup:** Run fast and efficient incremental backups using the native VMware Changed Block Tracking technology to process only changed data blocks on each backup job run.
- **App-aware processing:** Ensure that backup data for different apps (Microsoft Exchange Server, Active Directory, SQL Server, etc.) and databases is transactionally consistent and ready for swift recovery.
- **Hybrid backup storage:** Apply the 3-2-1 backup strategy by sending backups and backup copies to local folders, NFS/SMB network shares, public cloud platforms (Amazon S3, Wasabi, Azure Blob, Backblaze B2), S3-compatible object storage targets, tape, and deduplication appliances.
- **Instant verification:** Automate the instant verification of VMware vSphere VM backups and replicas using one of two built-in methods to ensure recoverability.

Disaster Recovery

- **Instant VM recovery:** Boot full VMs directly from VMware vSphere backups to resume your operations within seconds using Flash VM Boot.
- **Instant granular recovery:** Restore individual files and application objects with all permissions to their original location or to a new machine with a few clicks.
- **Efficient replication:** Create replicas from source VMs or from existing backups to ensure availability and operational continuity in case of failures.
- **Site Recovery:** Create self-running sequences for emergency/planned failover, failback, and disaster recovery testing and launch them with a single click.
- **Cross-platform recovery:** Recover VMware vSphere VMs as Microsoft Hyper-V VMs and vice versa by exporting backups in different virtual disk formats to streamline multi-platform management.
- **Physical-to-virtual recovery:** Instantly boot Windows and Linux physical machines from backups as VMware vSphere VMs with minimal downtime, then restore the VMs to be used in your production environment.

Ransomware Protection

- **Immutable local storage:** Send backups to ransomware-proof local repositories to prevent ransomware encryption and other unwanted modifications.
- **Immutable cloud storage:** Enable immutability via S3 Object Lock for backup data stored in public cloud storage platforms (Amazon S3, Wasabi, Azure Blob, Backblaze B2) to protect against ransomware infection.
- **Air-gapped backups:** Store VMware vSphere VM backup copies offline on detachable drives, such as tape, for an additional layer of ransomware protection.

Security and Compliance

- **Two-Factor Authentication (2FA):** Add a layer of security with one-time codes generated via Google Authenticator to safeguard your data protection activities.
- **Role-Based Access Control:** Assign preset and custom roles with associated rights and permissions to prevent unauthorized access to your VMware vSphere VM backups.
- **Flexible retention:** Save up to 10,000 recovery points for each VMware vSphere VM backup and rotate them on a daily, weekly, monthly, yearly, or periodic basis.
- **Native backup to tape:** Send VMware vSphere VM backup data directly to physical and virtual tape libraries for secure long-term archival.

Administration

- **Web interface:** Manage all backup and recovery activities from an easy-to-use web interface with convenient dashboards and step-by-step wizards.
- **Calendar Dashboard:** View and manage all past, current and future jobs in a simple calendar view. Easily schedule VMware vSphere VM backup jobs and avoid scheduling overlaps.
- **Global Search:** Search for and quickly locate any file or folder you need to ensure efficient and accurate recovery.
- **Policy-Based Data Protection:** Create custom policy rules to automatically add or remove VMs in data protection jobs as your environment grows and changes.
- **Job Chaining:** Link backup and backup copy jobs to automate workflows, increase efficiency, and save time on backup administration.

- **HTTP API Integration:** Integrate NAKIVO Backup & Replication with monitoring, automation and orchestration solutions seamlessly via HTTP API.
- **Performance boosters:** Manage data transfer speeds and offload production resources with Network Acceleration, LAN-free data transfer, Backup from Storage Snapshots, and Bandwidth Throttling to shorten backup windows and minimize the impact on core operations.
- **Flexible deployment:** Install the solution in a few minutes on Windows, Linux, NAS, or as a VA or AWS AMI.
- **Self-Backup:** Back up and recover your NAKIVO Backup & Replication system configuration (jobs, inventory, logs, settings, etc.) from the same unified interface.

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