# Was ist neu in NAKIVO Backup zum VMware

# Inhaltsübersicht

# EINFÜHRUNG

NAKIVO Backup & Replikation bietet All-in-One-Funktionen für Backup, sofortige Wiederherstellung, Schutz vor Ransomware und Disaster Recovery, um VMware-Umgebungen vor den Auswirkungen von Datenverlusten und Cyber-Bedrohungen zu schützen.

# NEUESTE FUNKTIONEN UND ERWEITERUNGEN

Die IT-Bedrohungslandschaft ist einem ständigen Wandel unterworfen, wodurch sich die Anforderungen an die Datensicherheit häufig ändern. Um Unternehmen bei der Anpassung ihrer Strategien zum Backup und zur Wiederherstellung von Daten zu unterstützen, gibt NAKIVO regelmäßig Updates heraus, die neue Funktionen zum Schutz von Daten einführen und bestehende Funktionen verbessern.

Seit Januar 2023 haben wir acht neue Versionen von NAKIVO Backup & Replikation mit verschiedenen Backup- und Anti-Ransomware-Tools zum Schutz kritischer Daten in VMware-Umgebungen auf den Markt gebracht. Nachfolgend finden Sie einen Überblick über die neuesten Ergänzungen bis zur Version 11.0.4.

## VMware vSphere-Support-Updates

NAKIVO ist weiterhin führend mit dem frühzeitigen Support für die neuesten Versionen von VMware vSphere und hilft seinen Kunden, bei jedem Upgrade einen unterbrechungsfreien Schutz zu gewährleisten.

Wir gehörten zu den ersten Anbietern von Backups, die vollen Support für vSphere 8.0 GA lieferten, gefolgt von Support für nachfolgende VMware-Versionen, einschließlich vSphere 8.0 U2, vSphere 8.0U2b, vSphere 8.0U2c und vSphere 8.0U3.

Mit der neuesten Version 11.0.4 haben wir den Kompatibilitätssupport auf VMware vSphere 9 ausgeweitet, um einen kontinuierlichen Support für Backup und Wiederherstellung von Umgebungen mit der neuesten VMware-Version sicherzustellen.

## Source-Side-Backup-Verschlüsselung

Mit NAKIVO Backup & Replikation können Sie Backups auf der Quellseite verschlüsseln, bevor sie über das Netzwerk zu ihrem Ziel im Speicher übertragen werden.

Verschlüsselte Backups können in lokalen Ordnern gespeichert werden, öffentlichen Cloud-Plattformen (Amazon S3, Wasabi, Azure Blob, Backblaze B2) gespeichert werden, S3-kompatiblen Speicherzielen SMB/NFS-Netzwerkfreigaben, Bänder und Deduplizierungs-Geräte. Für die Entschlüsselung der Backup-Daten ist ein Passwort erforderlich, und die Funktion unterstützt auch die Integration mit AWS KMS als ausfallsicheres Gerät, falls Sie die Entschlüsselungsschlüssel verlieren.

## Föderiertes Repository

Das Federated Repositorys ist ein leicht skalierbares und flexibles Backup-Repository, das Engpässe bei Leistung und Komplexität in großen Umgebungen mit großen Datensätzen beseitigt.

Ein Federated Repository funktioniert wie ein erweiterbarer Speicherpool, der aus mehreren eigenständigen Repositories, den so genannten "Mitgliedern", besteht. Sie können ein Federated Repository schnell und einfach erweitern, indem Sie neue Mitglieder hinzufügen, um mehr Daten zu speichern. Zum Hinzufügen oder Entfernen von Mitgliedern sind keine komplexen Konfigurationen erforderlich, da der Vorgang nur wenige Klicks erfordert. In einem Federated Repository werden die Backup- und Wiederherstellungsvorgänge ohne Unterbrechung fortgesetzt, selbst wenn eines der Repositorys ausfällt oder keinen Speicherplatz mehr hat, solange ein anderes nutzbares Mitglied verfügbar ist.

## Backup von NetApp-Speicher-Snapshots

NAKIVO hat NetApp FAS und NetApp AFF Storage Arrays in die Liste der unterstützten Geräte für das Backup von Speicher-Snapshots Funktion aufgenommen. Das Backup von VMware-VMs direkt von Speicher-Snapshots anstelle

von regulären VM-Snapshots reduziert die Auswirkungen von VM-Backups auf Ressourcen und Leistung in Ihrer Produktionsumgebung.

## Übersichts-Dashboard für Mandanten

Wir haben die MSP-Konsole um das Übersicht-Dashboard für Mandanten erweitert, das einen umfassenden Überblick über alle verwalteten Mandanten an einem Ort bietet.

Von diesem dynamischen Dashboard aus können Sie in Echtzeit Einblicke und Warnungen zu Ihren Client-Datenschutzinfrastrukturen erhalten, einschließlich Knoten-Status, verfügbare Ressourcen, geplante Aktivitäten und Inventar-Informationen. Sie können Ihre Mandantenliste sortieren, filtern und durchsuchen, um die benötigten Informationen zu extrahieren, ausstehende Probleme zu identifizieren und Massenaktionen anzuwenden.

## Unveränderlicher Speicher auf NEC HYDRAstor

NAKIVO Backup & Replikation unterstützt NEC HYDRAstor als Ziel zum Backup-Speicher neben anderen Deduplizierungs-Appliances.

Sie können jetzt die Unveränderlichkeit für Backups auf Ihrem NEC HYDRAstor Speichersystem aktivieren, um sie vor Ransomware-Angriffen, versehentlichem Löschen und anderen Formen der unerwünschten Veränderung zu schützen.

## Granulare Benachrichtigungen

Granulare Benachrichtigungen verbessern die Funktionen zur Verfolgung des Workflows und verschaffen Ihnen einen besseren Überblick über zum Backup und zur Replikation ausgeführte Aufträge. Während ein Auftrag ausgeführt wird, zeigt NAKIVO Backup & Replikation Beschreibungen laufender Aktionen an, z. B. Datenübertragung oder Log-Trunkierung. Die Status-Updates erfolgen in Echtzeit, um Sie über den Fortgang des Auftrags auf dem Laufenden zu halten.

## Dateisystem-Indizierung

Dateisystem-Indizierung baut auf den bestehenden Möglichkeiten der Globalen Suche Funktion auf, um einen Index aller Dateien und Ordner innerhalb Ihrer VM-Backups zu erstellen. Wenn Sie also eine granulare Wiederherstellung durchführen, um eine oder mehrere Dateien oder Ordner wiederherzustellen, können Sie die Globale Suche nutzen, um die benötigten Elemente schnell zu finden und dabei wertvolle Zeit zu sparen.

## Alarme und Berichte für die IT-Überwachung

Mit Alarmen und Berichten für IT Monitoring können Sie benutzerdefinierte Alarme erstellen und konfigurieren, die ausgelöst werden, wenn bestimmte Bedingungen erfüllt sind.

Alarme haben mehrere Verwendungszwecke, darunter die proaktive Erkennung ungewöhnlicher Aktivitäten, die auf bösartiges Verhalten hindeuten könnten, z. B. wenn die CPU-Auslastung plötzlich das normale Maß überschreitet. Mit der Berichtsfunktionalität können Sie verschiedene Details zu überwachten VMware vSphere Elementen in Ihrer Infrastruktur ansehen, exportieren und per E-Mail versenden.

## Sicherung von HPE Alletra und HPE Primera Speicher-Snapshots

NAKIVO hat HPE Alletra und HPE Primera in die Liste der unterstützten Geräte für die Funktion Backup von Speicher-Snapshots aufgenommen. Sie können Ihre VMware vSphere VMs, die auf diesen Speichergeräten gespeichert sind, effizienter sichern, indem Sie Speicher-Snappschüsse anstelle von regulären VM-Snappschüssen verwenden.

## Replikation in Echtzeit (Beta) für VMware

Echtzeit-Replikation (Beta) für VMware ist eine leistungsstarke Ergänzung zu den Disaster Recovery-Funktionen von NAKIVO Backup & Replikation.

Sie können Replikate von VMware vSphere-VMs in Echtzeit erstellen und sie so einstellen, dass sie kontinuierlich mit Datenänderungen aktualisiert werden, die in den Quell-VMs auftreten. Änderungen der VM-Quelldaten werden in Echtzeit mit Aktualisierungsraten (und Zielen der Wiederherstellungspunkte) von nur 1 Sekunde verarbeitet, was eine kontinuierliche Verfügbarkeit kritischer Maschinen und Daten gewährleistet.

**Echtzeit-Replikation (Beta) für VMware: vSphere 9.0-Kompatibilität**

NAKIVO hat den Anwendungsbereich von Echtzeit-Replikation (Beta) für VMware auf vSphere 9.0 ausgeweitet, so dass Sie beim Upgrade Ihrer VMware-Umgebung unterbrechungsfreie Replikations-Workflows aufrechterhalten können.

## Malware-Scan für Backups

Die Backup-Malware-Scan Funktion ist eine wichtige Ergänzung der Funktionen zum Schutz vor Ransomware in NAKIVO Backup & Replikation. Mit dieser Funktion können Sie Backups vor der Wiederherstellung auf Malware und Ransomware scannen, um Infektionen in Ihrer Infrastruktur zu verhindern.

Sie können die Lösung mit Windows Defender, ESET NOD32 und Sophos integrieren, um Malware-Scans durchzuführen und sicherzustellen, dass Backups sicher zur Wiederherstellung verwendet werden können. Wenn bei einem Scan Malware entdeckt wird, haben Sie die Wahl, den Auftrag zur Wiederherstellung fehlschlagen zu lassen oder ein isoliertes Netzwerk als Ziel für die Wiederherstellung zu verwenden.

## Direkte Wiederherstellung von Band

Mit Direkte Wiederherstellung von Bändern können Sie vollständige virtuelle Maschinen und Amazon EC2-Instanzen direkt von auf Bändern gespeicherten Backups zu Ihrer Infrastruktur wiederherstellen.

Der Ansatz der direkten Wiederherstellung verbessert die Zeiten der Wiederherstellung und die Effizienz. Neben VMware vSphere werden auch Plattformen wie Microsoft Hyper-V, Nutanix AHV und Amazon EC2 unterstützt, zusätzlich zu physischen Workloads über Physical-to-Virtuell Recovery.

## Unterstützung für S3-kompatible Objektspeicher

Der Support für S3-kompatiblen Objektspeicher erweitert die hybriden Backup-Speichermöglichkeiten von NAKIVO Backup & Replikation und ermöglicht es Ihnen, Backups in lokalen und Cloud-basierten Speicherzielen zu speichern, die die S3-API verwenden.

Sie können aus einer Vielzahl von S3-kompatiblen Speicherzielen wählen, die den Anforderungen und dem Budget Ihres Unternehmens entsprechen. Darüber hinaus können Sie die Unveränderlichkeit für Wiederherstellungspunkte aktivieren, die an S3-kompatiblen Speicherstandorten gespeichert sind, um sich vor Ransomware-Infektionen, versehentlichen Löschungen und anderen unerwünschten Änderungen zu schützen.

## Permanenter VM-Agent

Mit der zusätzlichen Funktion Dauerhafter Agent in NAKIVO Backup & Replikation können Sie einen dauerhaften Agenten auf VMware vSphere VMs bereitstellen, um die Gastverarbeitung zu optimieren, ohne Anmeldeinformationen für das Betriebssystem bereitstellen zu müssen.

Durch die Verwendung von dauerhaften Agenten kommuniziert die Lösung mit den Ziel-VMs über einen einzigen Port, was die Einhaltung von Sicherheitsrichtlinien gewährleistet, die das Teilen von Anmeldeinformationen des Betriebssystems und anderen sensiblen Informationen verbieten.

# NAKIVO BACKUP FÜR VMWARE: DIE WICHTIGSTEN FUNKTIONEN

NAKIVO Backup & Replikation bietet schnelle agentenlose Backups, sofortige Wiederherstellung von VMs und granulare Wiederherstellung sowie mehrschichtigen Schutz vor Ransomware, um sicherzustellen, dass die Daten in Ihrer VMware-Umgebung geschützt und wiederherstellbar sind. Im Folgenden finden Sie einen Überblick über die wichtigsten Funktionen und Möglichkeiten zum Backup, Disaster Recovery, Schutz vor Ransomware, Sicherheit und Compliance sowie zur Verwaltung:

## Backup

- **Inkrementelles Backup:** Führen Sie schnelle und effiziente inkrementelle Backups mit der nativen VMware-Verfolgung geänderter Blöcke Technologie, um bei jedem Auftrag zum Backup nur geänderte Datenblöcke zu verarbeiten.
- **App-Aware-Verarbeitung:** Sicherstellen, dass die Backup-Daten für verschiedene Anwendungen (Microsoft Exchange Server, Active Directory, SQL Server usw.) und Datenbanken transaktionsbezogen konsistent und für eine schnelle Wiederherstellung bereit sind.
- **Hybrider Speicher zum Backup:** Anwenden der 3-2-1-Sicherungsstrategie durch Senden von Backups und Sicherungskopien an lokale Ordner, NFS/SMB-Netzwerkfreigaben, öffentliche Cloud-Plattformen (Amazon S3, Wasabi, Azure Blob, Backblaze B2), S3-kompatible Objektspeicherziele, Bänder und Deduplizierungsgeräte.
- **Sofortige Verifizierung:** Automatisieren Sie die Sofortige Verifizierung von VMware vSphere-VM-Backups und -Replikaten mit einer von zwei integrierten Methoden, um die Wiederherstellbarkeit zu gewährleisten.

## Katastrophenwiederherstellung

- **Sofortige Wiederherstellung von VMs:** Booten Sie komplette VMs direkt von VMware vSphere-Backups, um Ihren Betrieb innerhalb von Sekunden wieder aufzunehmen. Flash-VM-Boot.
- **Sofortige granulare Wiederherstellung:** Wiederherstellung einzelner Dateien und Anwendungsobjekte mit allen Berechtigungen an ihrem ursprünglichen Standort oder auf einem neuen Rechner mit wenigen Klicks wiederherstellen.
- **Effiziente Replikation:** Erstellen Sie Replikate von Quell-VMs oder von bestehenden Backups, um Verfügbarkeit und Betriebskontinuität bei Ausfällen zu gewährleisten.
- **Standortwiederherstellung:** erstellen selbstablaufende Sequenzen für das Testen von Failover, Failback und Disaster Recovery in Notfällen/geplanten Situationen und starten Sie sie mit einem einzigen Klick.
- **Plattformübergreifende Wiederherstellung:** Wiederherstellen von VMware vSphere VMs als Microsoft Hyper-V VMs und vice versa von Export von Backups zum Backup in verschiedenen Formaten virtueller Festplatten, um das Management mehrerer Plattformen zu optimieren.
- **Physisch-zu-virtuelle Wiederherstellung:** Sofortiges Booten von Windows und Linux physische Maschinen von Backups als VMware vSphere-VMs mit minimaler Ausfallzeit booten und dann die VMs für die Verwendung in Ihrer Produktionsumgebung wiederherstellen.

## Schutz vor Ransomware

- **Unveränderlicher lokaler Speicher:** Senden Sie Backups zum Ransomware-sicheren lokale Repositorys, um Verschlüsselung durch Ransomware und andere unerwünschte Änderungen zu verhindern.
- **Unveränderlicher Cloud-Speicher:** Aktivieren Sie Unveränderlichkeit über S3 Object Lock für Backup-Daten, die in öffentlichen Cloud-Speicher-Plattformen (Amazon S3, Wasabi, Azure Blob, Backblaze B2) gespeichert sind, zum Schutz vor Ransomware-Infektionen.

- **Air-gapped Backups:** Speichern Sie VMware vSphere-VM-Backup-Kopien offline auf abnehmbaren Laufwerken, z. B. auf Bändern, um einen zusätzlichen Schutz vor Ransomware zu gewährleisten.

## Sicherheit und Compliance

- **Zwei-Faktor-Authentifizierung (2FA):** Fügen Sie eine zusätzliche Sicherheitsebene hinzu mit einmaligen Codes die über Google Authenticator generiert werden, um Ihre Aktivitäten zum Schutz Ihrer Daten zu schützen.
- **Rollenbasierte Zugriffskontrolle:** Zuweisung von voreingestellte und benutzerdefinierte Rollen mit zugehörigen Rechten und Berechtigungen zu, um unberechtigten Zugriff auf Ihre VMware vSphere VM Backups zu verhindern.
- **Flexible Aufbewahrung:** Speichern Sie bis zu 10.000 Wiederherstellungspunkte für jedes VMware vSphere VM-Backup und rotieren Sie diese täglich, wöchentlich, monatlich, jährlich oder periodisch.
- **Native Sicherung auf Band:** Senden Sie VMware vSphere VM-Backup-Daten direkt an physische und virtuelle Bandbibliotheken zur sicheren Langzeitarchivierung.

## Verwaltung

- **Web-Oberfläche:** Verwalten Sie alle Aktivitäten zum Backup und zur Wiederherstellung über eine benutzerfreundliche Weboberfläche mit praktischen Dashboards und Schritt-für-Schritt-Assistenten.
- **Kalender-Dashboard:** Ansehen und Verwalten aller vergangenen, aktuellen und zukünftigen Aufträge in einem einfachen Kalenderansicht. Planen Sie mühelos Aufträge zum Backup von VMware vSphere VM und vermeiden Sie Überschneidungen bei der Planung.
- **Globale Suche:** Dateien und Ordner schnell und effizient finden, um eine präzise Wiederherstellung zu ermöglichen.
- **Richtlinienbasierter Datenschutz:** Erstellen Sie benutzerdefinierte Regeln zum automatischen Hinzufügen oder Entfernen von VMs in Aufträgen zur Datensicherung, wenn Ihre Umgebung wächst und sich verändert.
- **Auftrag-Chaining:** Verknüpfen Sie Aufträge zum Backup und Backupkopie-Auftrag, um Arbeitsabläufe zu automatisierenzu automatisieren, die Effizienz zu steigern und Zeit bei der Verwaltung von Backups zu sparen.
- **HTTP-API-Integration:** Integrieren Sie NAKIVO Backup & Replikation nahtlos in Überwachungs-, Automatisierungs- und Orchestrierungslösungen über HTTP-API.
- **Steigerung der Leistung:** Verwalten Sie die Datenübertragungsgeschwindigkeiten und entlasten Sie die Produktionsressourcen mit Netzwerkbeschleunigung, LAN-freie DatenübertragungBackup von Speicher-Snapshots, und Bandbreitendrosselung um die Zeitfenster zum Backup zu verkürzen und die Auswirkungen auf den Kernbetrieb zu minimieren.
- **Flexible Bereitstellung:** Installieren Sie die Lösung in wenigen Minuten auf Windows, Linux, NAS oder als VA oder AWS AMI.
- **Self-Backup:** Sichern und Wiederherstellen Ihrer NAKIVO Backup & Replikation Systemkonfiguration (Aufträge, Inventar, Protokolle, Einstellungen usw.) von der gleichen, einheitlichen Oberfläche aus.





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