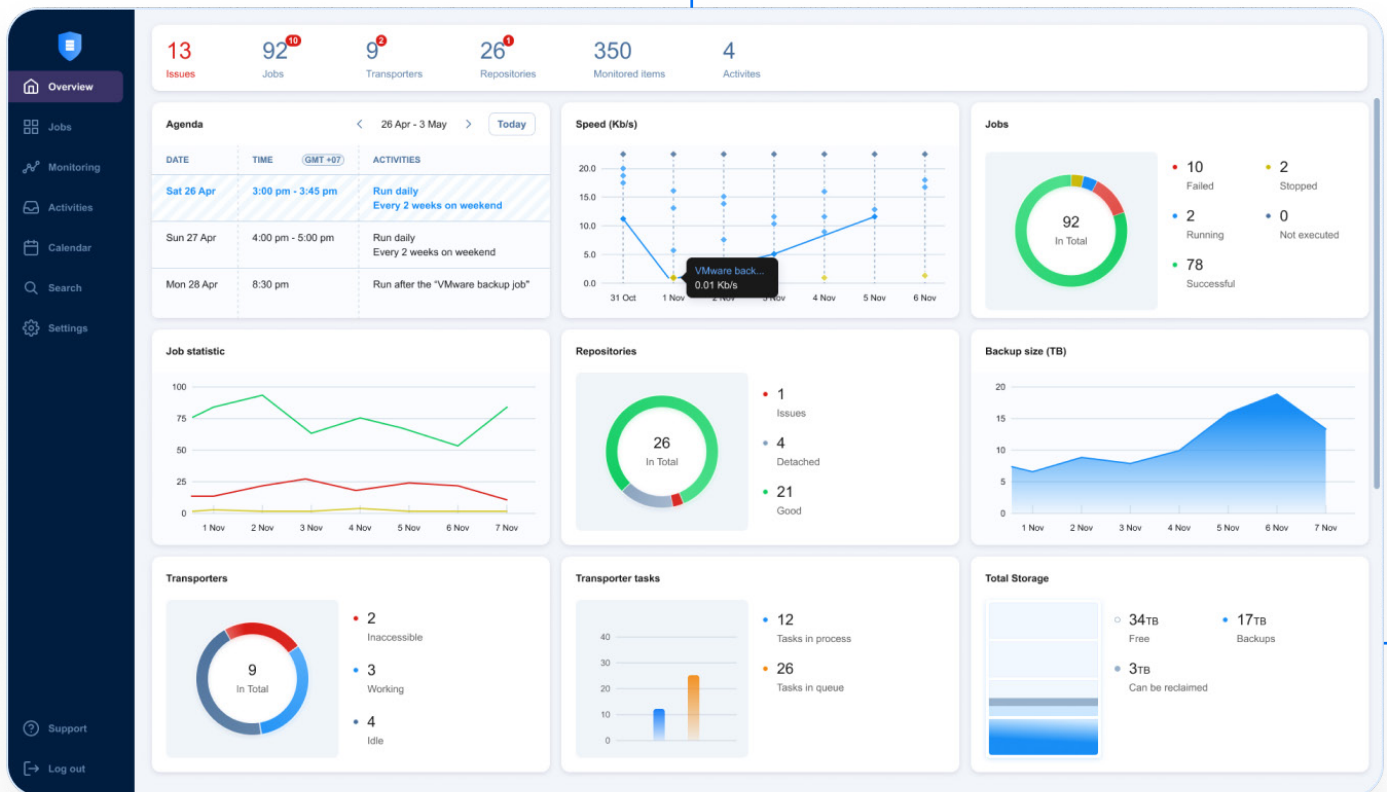


Was gibt es Neues in NAKIVO Backup & Replication



Inhaltsübersicht

Einführung.....	3
Schutz für virtuelle Umgebungen.....	3
Backup für Proxmox VE.....	3
Schnelle und effiziente Sicherung von Backups.....	3
Flexible Speicherziele.....	3
Schutz vor Ransomware und Sicherheit.....	3
Sofortige vollständige und granulare Wiederherstellung.....	4
Replikation für Proxmox VE.....	4
Echtzeit-Replikation für VMware.....	4
Support für die neueste VMware-Version.....	4
Sicherung und Wiederherstellung für physische Umgebungen.....	4
Granulares Backup für physische Maschinen.....	4
NAS-Backup.....	4
Hybrider und unveränderlicher Speicher.....	4
Automatisierte Backupkopie.....	5
Bare-Metal-Wiederherstellung.....	5
Backup für Microsoft 365.....	5
Hybrider und unveränderlicher Speicher.....	5
Automatisierte Backupkopie.....	5
Support für In-Place-Archiv von Postfächern, Rechtsstreit-Sperre und In-Place-Aufbewahrung.....	5
Managed Services Provider (MSPs).....	6
MSP-Konsole.....	6
Übersicht-Dashboard für Mandanten.....	6
Direktverbindung.....	6
Direktverbindung für MSPs.....	6
IT Monitoring.....	6
Integration von Enterprise-Speichergeräten.....	6
Unveränderlicher Speicher auf NEC HYDRAsstor.....	6
Backup von Speicher-Snapshots.....	7
Cloud-Speicher.....	7
S3-kompatibler Objektspeicher.....	7
Direktwiederherstellung aus Bandspeicher für VM-Systeme.....	7
Datenbanken.....	7
Verbesserungen der Kernkomponenten der Lösung.....	7
Sicherung verschlüsseln.....	7
Verbundene Repositories.....	8
Granulare Benachrichtigungen.....	8
Backup-Malware-Scan.....	8
Dateisystem-Indizierung.....	8
Universal Transporter.....	8
Debian-Unterstützung.....	8
Debian-Unterstützung.....	8
Vereinfachte Aufbewahrungseinstellungen für Backups.....	8
Dauerhafter Agent.....	9
Auftragspriorität.....	9
Aufträge zusammenführen.....	9
Mehrsprachige Benutzeroberfläche.....	9
Alle Funktionen ausprobieren.....	9
SIND SIE BEREIT, LOSZULEGEN?.....	9

Einführung

Angetrieben von der Notwendigkeit einer maßgeschneiderten Datensicherheit haben wir seit Januar 2024 acht neue Versionen von NAKIVO Backup & Replication freigegeben, die jeweils mit begehrten Funktionen und Verbesserungen ausgestattet sind.

Von virtualisierten und physischen Plattformen über Managed Services Provider (MSPs) bis hin zu Disaster Recovery und Schutz vor Ransomware sorgen wir weiterhin dafür, dass unsere Kunden eine maßgeschneiderte und effiziente Datensicherheit erhalten.

Im Folgenden finden Sie eine Liste der wichtigsten neuen Funktionen und Verbesserungen, die bis zur Version 11.2 zu NAKIVO Backup & Replication hinzugefügt wurden.

Schutz für virtuelle Umgebungen

NAKIVO Backup & Replication wurde speziell für virtuelle Umgebungen entwickelt und bietet schnellen und zuverlässigen VM-Datenschutz, der auf verschiedene Virtualisierungsplattformen zugeschnitten ist, darunter [VMware vSphere](#), [VMware Cloud Director](#), [Microsoft Hyper-V](#), [Nutanix AHV](#) und [Proxmox VE](#).

Backup für Proxmox VE

NAKIVO Backup & Replication kann agentenlose Backups und Replikationen von Proxmox VE-VMs und VM-Vorlagen (bis zum neuesten Update v9.0) durchführen, wodurch Sie die Komplexität und den Ressourcenverbrauch reduzieren und gleichzeitig mehr Kontrolle und Flexibilität erzielen können.

Schnelles und effizientes Backup

Sie können Proxmox VE-VMs direkt auf Host-Ebene sichern, ohne zusätzliche Betriebssystem-Agenten auf jeder VM installieren oder verwalten zu müssen. Mit dieser Funktionalität können Sie inkrementelle Backups auf Blockebene erstellen, indem Sie die Native Änderungsverfolgung nutzen, um nur die Datenblöcke zu übertragen, die seit der letzten Backup-Sitzung geändert wurden. Die Funktion „Sofortige Verifizierung“ führt automatisierte Zustandsprüfungen Ihrer Proxmox VE-Backup-Daten durch und sendet Screenshot-basierte Berichte, um zu bestätigen, dass die Proxmox VE-Backups funktionsfähig und wiederherstellbar sind.

Flexible Speicherziele

Sie können Ihre Proxmox VE-Backups in einem breiten Bereich von Speichergeräten speichern, darunter:

- [Öffentliche Clouds](#) und [S3-kompatibler Speicher](#)
- [Deduplizierungs-Appliances](#)
- CIFS/NFS-Freigabe
- Band.

Zusätzlich können Sie die [Funktionalität „Backupkopie“](#), um Proxmox VE-Backups außerhalb des Standorts zu kopieren und mehrere Kopien in der Cloud oder an einem anderen Standort aufzubewahren. Dabei befolgen Sie die 3-2-1-Backup-Strategie, um die Verfügbarkeit zu verbessern und die Wiederherstellung in Katastrophenfällen sicherzustellen.

Schutz vor Ransomware und Sicherheit

Sie können Ihr Proxmox VE-Backup vor Ransomware, unbefugtem Zugriff und Manipulationen der Daten schützen, indem Sie Folgendes verwenden:

- [Sicherung verschlüsse](#) In an der Quelle, während der Übertragung und im Repository
- [Unveränderliche Backups](#) in lokalen und Cloud-Repositories zum Schutz der Daten vor Verschlüsselung durch Ransomware oder versehentlichem Löschen
- Air-gapped Backups auf Band und anderen getrennten Medien für den Offline-Schutz

Sofortige vollständige und detaillierte Wiederherstellung

NAKIVO Backup & Replication bietet außerdem Optionen zur vollständigen und sofortigen Wiederherstellung. Sie können wählen, ob Sie ganze Proxmox VE-VMs mit all ihren Daten wiederherstellen oder einzelne Dateien und Anwendungsobjekte sofort an ihrem ursprünglichen oder einem anderen Standort wiederherstellen möchten. Verwenden Sie die Flash-VM-Boot-Funktion, um Proxmox VE-VMs direkt aus Backups zu starten und so eine sofortige Wiederherstellung zu ermöglichen.

Replikation für Proxmox VE

Mit NAKIVO Backup & Replication können Sie bei Ausfällen oder Störungen eine hohe Verfügbarkeit und Geschäftskontinuität sicherstellen. Sie können identische Replikate Ihrer Quelle-Proxmox-VE-VMs auf einem Ziel-Host an einem entfernten Standort erstellen und verwalten. Bei Ausfällen oder Störungen können Sie einfach einen Failover auf Ihr Replikat durchführen, um Ausfallzeiten zu minimieren und die Verfügbarkeit des Dienstes aufrechtzuerhalten.

Real-Time Replication für VMware

Mit dieser Echtzeit-Replikationsfunktionalität in NAKIVO Backup & Replication können Sie Replikate Ihrer VMware vSphere-VMs erstellen und diese bei Änderungen mit den Quell-VMs synchronisieren. Replikate werden in Echtzeit bis zu einmal pro Sekunde aktualisiert, wodurch nahezu null Ausfallzeiten und Datenverlust im Katastrophenfall entstehen.

Darüber hinaus können Sie Failover-Aktionen für die Echtzeitreplikation in Standortwiederherstellungs-Aufträgen einrichten, um während eines Ausfalls mit einem einzigen Klick automatisch auf Echtzeit-Replikate umzuschalten. Sie können den Failover-Prozess auch vorab testen, um Ihre DR-Pläne zu validieren und die Bereitschaft für die Wiederherstellung sicherzustellen, ohne die Produktionsumgebung zu beeinträchtigen.

Support für die neueste VMware-Version

NAKIVO legt größten Wert darauf, dass Kunden Zugang zu den neuesten Entwicklungen im Bereich der verteilten Workload-Technologie haben. In diesem Zusammenhang haben wir den Support für die neuesten VMware vSphere-Versionen beim Freigeben hinzugefügt, einschließlich vSphere 9.

Sicherung und Wiederherstellung für physische Umgebungen

NAKIVO hat den Schutz auf die physische Infrastruktur ausgeweitet und Backup-Funktionen für [Windows](#) und [Linux](#)-Server und -Arbeitsstationen ein, um die Datensicherheit in unterschiedlichen IT-Landschaften zu gewährleisten.

Granulares Backup für physische Maschinen

NAKIVO Backup & Replication kann bestimmte Volumes und Ordner auf Windows- und Linux-Rechnern sichern, ohne den gesamten Rechner zum Backup zu nehmen. Sie können detaillierte Backups physischer Maschinen speichern auf:

- Lokaler Speicher
- SMB- und NFS-Dateifreigaben
- Öffentliche Clouds (Amazon S3, Wasabi, Azure Blob, Backblaze B2)
- S3-kompatible Plattformen für Objektspeicher
- Band
- Deduplizierungs-Appliances

Zum Schutz vor Ransomware-Angriffen können Sie eine Kombination aus unveränderlichem Speicher, air-gapped Backups und Sicherung verschlüsseln verwenden.

Sie können eine granulare Wiederherstellung durchführen, um die benötigten Daten aus den Backups Ihrer physischen Maschinen wiederherzustellen und dabei Zeit und Ressourcen zu sparen.

NAS-Backup

Mit NAKIVO NAS-Backup können Sie schnelle und effiziente Backups von unstrukturierten Daten in NFS- und SMB-Netzwerkfreigaben erstellen, die auf NAS-Geräten sowie Windows- und Linux-Rechnern gehostet werden. Hier sind die Neuerungen im NAKIVO NAS-Backup.

Hybrider und unveränderlicher Speicher

Sie können nun Backups von Dateifreigaben an eine größere Auswahl an Speicherzielen senden, darunter:

- Öffentliche Cloud-Speicher-Plattformen (Amazon S3, Wasabi, Azure Blob, Backblaze B2)
- S3-kompatible Speicherplattformen
- Lokale Ordner
- Andere NFS- und SMB-Freigaben
- Deduplizierungs-Appliances

Wenn Sie ein lokales oder cloudbasiertes Backup-Repository als Speicherziel verwenden, können Sie die Unveränderbarkeit aktivieren, um Backups vor Ransomware-Angriffen und unerwünschten Änderungen zu schützen.

Automatische Backupkopie

NAKIVO hat den Umfang der Funktionen „Backupkopie“ und „Auftrag-Chaining“ um NAKIVO NAS-Backup erweitert. Sie können nun die Erstellung und Verschiebung von Backupkopien über die oben aufgeführten unterstützten Sicherungsziele hinweg automatisieren, wobei zusätzlich Bandlaufwerke hinzugefügt wurden, um die Resilienz der Backups zu erhöhen.

Bare-Metal-Wiederherstellung

Die [Bare-Metal-Wiederherstellung](#) erweitert die bestehende physische Wiederherstellungsfunktion und ermöglicht Ihnen eine flexible und schnelle physische Serverwiederherstellung. Sie können einen gesamten Server oder eine gesamte Arbeitsstation aus einem Backup auf identischer Hardware wiederherstellen, ohne die Betriebssysteme neu zu installieren oder die Anwendungseinstellungen neu zu konfigurieren.

Diese Funktionalität bietet einen schnellen und effizienten Ansatz, um physische Maschinen auf den letzten bekannten fehlerfreien Zustand zurückzusetzen, sodass Sie nach Zwischenfällen die Wiederherstellung durchführen oder zuvor vorgenommene unerwünschte Änderungen/Löschungen rückgängig machen können.

Sicherung für Microsoft 365

NAKIVO Backup für Microsoft 365 ist eine leistungsstarke Lösung für die schnelle Sicherung und Wiederherstellung von [OneDrive for Business](#), [SharePoint Online](#), [Exchange Online](#) und [Microsoft Teams](#) Daten. Hier sind die Neuerungen in NAKIVO Backup für Microsoft 365.

Hybrider und unveränderlicher Speicher

Diese bedeutende Erweiterung stellt einen neuen Meilenstein für NAKIVO Backup für Microsoft 365 dar und

umfasst neue Speicherziele, Support für ransomware-sichere Backups und automatisiertes Tiering für Backups. Zusätzlich zu lokalen Ordnern können Sie nun Backups von Microsoft 365-Daten an die folgenden Speicherziele senden:

- [Öffentliche Cloud-Speicher-Plattformen](#) (Amazon S3, Wasabi, Azure Blob, Backblaze B2)
- Sonstige [S3-kompatible Speicherplattformen](#)
- NFS- und SMB-Freigaben
- [Deduplizierungs-Appliances](#)

Zum Schutz vor Ransomware-Angriffen und anderen unerwünschten Änderungen können Sie die Unveränderbarkeit für Microsoft 365-Backups aktivieren, die in lokalen und Cloud-Speicherzielen gespeichert sind.

Automatische Backupkopie

Darüber hinaus können Sie jetzt die [Backupkopie](#) Funktion verwenden, um zusätzliche Kopien von Microsoft 365-Backups zu erstellen oder Backups nahtlos zwischen den oben genannten Speicherzielen zu migrieren, wobei nun auch Bandlaufwerke hinzugefügt wurden. Verwendung [Auftrag-Chaining](#) können Sie die Übertragung von Backupkopien zwischen Speicherzielen (Band zu Cloud, Cloud zu lokalem Ordner, Netzwerkfreigabe zu Band usw.) automatisieren.

Support für In-Place-Archiv-Postfächer, Rechtsstreit-Sperre und In-Place-Aufbewahrungspflicht

NAKIVO hat den Support für weitere Exchange Online-Postfach-Elemente hinzugefügt:

- In-Place-Archiv-Postfächer
- Rechtsstreit-Sperre für Elemente
- Vor-Ort -Elemente

Sie können nun die benötigten Postfach-Ordner sichern und den gesamten Ordner oder bestimmte Dateien auf dem ursprünglichen oder einem anderen Benutzerkonto wiederherstellen.

Managed Services Provider (MSPs)

[Multi-Tenancy](#) ermöglicht es Managed Services Providern, die Datensicherheit für mehrere Kunden effizient von einer einzigen Plattform aus zu verwalten und anzupassen. Seitdem bieten wir weiterhin spezielle Funktionen und Fähigkeiten, mit denen Dienstleister besser auf die Bedürfnisse ihrer Kunden eingehen und sich verbessern können. Hier finden Sie die neuesten Funktionen für MSP, die in NAKIVO Backup & Replication eingeführt wurden:

MSP-Konsole

NAKIVO hat die [MSP-Konsole für das zentrale Management aller Kunden](#), die es Dienstleistern ermöglicht, ihre Abläufe zu optimieren, die Effizienz zu steigern und ihren Kunden robuste Dienste für die Datensicherheit anzubieten.

MSPs können Kunden mit eigenständigen NAKIVO Backup & Replication Bereitstellungen als Remote-Mandanten in ihre mandantenfähige Bereitstellung der Lösung aufnehmen. Dadurch können sie die Aktivitäten zur Datensicherheit aller Mandanten, sowohl remote als auch lokal, einfach über ein einheitliches MSP-Dashboard verwalten und überwachen.

Übersichts-Dashboard für Mandanten

Wir haben die MSP-Konsole um ein neues Dashboard erweitert, das einen umfassenden Überblick über alle verwalteten Mandanten an einem Ort bietet. Das Übersicht-Dashboard für Mandanten bietet Ihnen Echtzeit-Einblicke und Warnmeldungen zu Ihren Infrastrukturen für Datensicherheit, einschließlich Knoten-Status, verfügbaren Ressourcen, geplanten Aktivitäten und Informationen zum Inventar. Sie können Ihre Liste der Mandanten sortieren, filtern und durchsuchen, um die benötigten Informationen zu extrahieren, offene Probleme zu identifizieren und Massenaktionen anzuwenden.

Dieses dynamische Dashboard hilft Ihnen, Zeit bei routinemäßigen Aufgaben des Mandanten-Managements zu sparen, Probleme und Engpässe effizient zu lösen und die Zuweisung von Ressourcen und Lizenzen zu optimieren.

Direktverbindung

Mit einer Direktverbindung können MSPs über eine einzige direkte Portverbindung auf die Remote-Ressourcen ihrer Kunden zugreifen, ohne dass eine VPN-Verbindung erforderlich ist. Die Funktion unterstützt VMware vSphere, Microsoft Hyper-V, Proxmox VE, Physische Maschinen, VMware Free ESXi-Hosts und NAS-basierte Transporter.

Direct Connect für MSPs

Mit der Direktverbindung für MSPs können Sie eine sichere Verbindung zu Mandantenumgebungen herstellen, ohne dass auf Seiten des Mandanten offene Ports erforderlich sind. Die Funktion bietet Support für die folgenden Plattformen für Fernmanagement und Datensicherheit:

- VMware vSphere
- Microsoft Hyper-V-VM
- Proxmox VE
- Physische Windows-Maschinen
- Physische Linux-Maschinen

Die Direktverbindung für MSPs unterstützt auch Workflows für Standortwiederherstellung, um eine schnelle Wiederherstellung von Workloads der Mandanten in Katastrophenszenarien zu ermöglichen.

IT-Überwachung

Das Behalten der Ressourcennutzung in der VMware-Infrastruktur ist entscheidend für die Optimierung der VM-Leistung und die Vermeidung von Engpässen. Die [NAKIVO Überwachung für VMware](#) bietet Ihnen folgende Funktionalitäten:

- Überwachen Sie die CPU-, RAM- und Festplattenauslastung Ihrer VMware vSphere-Hosts und -VMs sowie Ihrer Datenspeicher.
- Erstellen und konfigurieren Sie benutzerdefinierte Warnmeldungen, die von verschiedenen Metriken für Hosts, VMs und Datenspeicher ausgelöst werden.
- Erhalten Sie verschiedene Arten von Berichten zu den überwachten vSphere-Elementen in Ihrer Infrastruktur direkt in Ihren Posteingang.

Integration von Unternehmensspeichergeräten

Der umfassende Ansatz von NAKIVO ermöglicht Ihnen die Erstellung einer vielseitigen hybriden und Multi-Cloud-Backup-Speicherstrategie, die Geräte vor Ort, in der Cloud und für die Deduplizierung sowie Bandspeicherlösungen nahtlos integriert. Hier finden Sie die Neuerungen bei den Speicherfunktionen von NAKIVO Backup & Replication.

Unveränderlicher Speicher auf NEC HYDRAsstor

NAKIVO Backup & Replication unterstützt [NEC HYDRAsstor](#) als Ziel zum Backup-Speicher neben anderen Deduplizierungs-Appliances.

Sie können nun die Unveränderlichkeit für Backups auf Ihrem NEC HYDRAsstor-Speichersystem aktivieren, um sie vor Ransomware-Angriffen, versehentlichem Löschen und anderen Formen unerwünschter Änderungen zu schützen.

Backup von Speichersnapshots

NAKIVO Backup & Replication integriert nahtlos die Speichergeräte führender Anbieter für Backups und Replikate direkt von Speicher-Snapshots.

Sie können VMware vSphere-VMs, die auf folgenden Plattformen gehostet werden, sichern und replizieren [HPE 3PAR-, HPE Nimble-, HPE Primera- und HPE Alletra Speicher-Appliances](#) sowie auf NetApp FAS- und NetApp AFF-Speicher-Arrays direkt aus Speicher-Schnappschüssen statt aus regulären VM-Schnappschüssen sichern und replizieren, um Zeit zu sparen und die Infrastrukturbelastung zu reduzieren.

Cloud-Speicher

Mit dem Aufkommen der Hybrid Cloud (eine Mischung aus privaten und öffentlichen Cloud-Infrastrukturen) könnten Unternehmen beim Verwalten ihrer Cloud-Kosten vor neuen Herausforderungen stehen.

Frühere Versionen von NAKIVO Backup & Replication unterstützten Optionen für Cloud-Speicher, wie z. B. [Amazon S3](#), [Wasabi](#), [Azure Blob](#) und [Backblaze B2](#) die einen sicheren Speicher zum Backup und zur Wiederherstellung mit einer Unveränderlichkeitsoption zum Schutz von Backups vor Ransomware-Infektionen bieten.

S3-kompatible Objektspeicherung

NAKIVO Backup & Replication bietet jetzt Support für [S3-kompatiblen Objektspeichern](#) Repositories für Backups eingeführt, die den Anwendern eine zusätzliche Option für die Speicherung ihrer Backup-Daten bieten. Damit können Sie Backups in einem mit der S3-API kompatiblen Speicher ablegen und aus einer Vielzahl kostengünstiger Plattformen wählen, die Ihren Anforderungen entsprechen.

Darüber hinaus können Backups, die in S3-kompatiblen Speichern abgelegt sind, als unveränderlich konfiguriert werden, wodurch sie vor Ransomware-Angriffen und versehentlichem Löschen geschützt sind.

Direktwiederherstellung aus Band-Speicher

Obwohl die meisten Unternehmen auf Festplatten- oder Cloud-Backups setzen, werden Band-Backups nach wie vor häufig für die Archivierung von Backup-Daten und den Langzeitspeicher verwendet. NAKIVO unterstützt seit langem die Speicherung [Backups auf LTO-Bandbibliotheken](#) und eigenständigen Laufwerken sowie AWS Virtual Tape Library (VTL).

Mit der neuen [direkte VM-Wiederherstellung von Band](#) Kunden können schnelle Wiederherstellungen durchführen, ohne dass ein Staging-Repository erforderlich ist. Sie können vollständige VMs, EC2-Instanzen und physische Maschinen als VMware-VMs direkt aus ihren auf Bandmedien gespeicherten Backups in ihre Infrastruktur wiederherstellen.

Datenbanken

NAKIVO Backup & Replication unterstützt seit langem [Oracle-Datenbank Backup und Wiederherstellung](#) über die native Funktionalität von RMAN.

Die vorhandene Funktionalität unterstützt das Backup über RMAN für Oracle-Datenbanken unter Windows. Unsere neuesten Versionen haben diesen Support für Oracle RMAN auf Linux-Systemen ausgeweitet. Kunden können ihre Oracle-Datenbanken mit einem integrierten, automatisierten System für Backup und Wiederherstellung sowohl auf Windows- als auch auf Linux-Plattformen schützen – alles über eine einheitliche Konsole.

Verbesserungen der Kernkomponenten der Lösung

NAKIVO arbeitet kontinuierlich daran, die Komponenten und Funktionen der Lösung zu verbessern, um die Aktivitäten zur Datensicherheit für unsere Kunden zu vereinfachen und zu optimieren. Jede dieser Verbesserungen trägt zu einer zuverlässigeren und effizienteren Datensicherheit bei. Der folgende Abschnitt hebt die wichtigsten Verbesserungen in NAKIVO Backup & Replication hervor:

Backupverschlüsselung

Mit der Funktion „Sicherung verschlüsseln“ können Sie Backups auf der Quelle verschlüsseln, bevor sie über das Netzwerk an ihren Speicher übertragen werden. Verschlüsselte Backups können in lokalen Ordnern, öffentlichen Cloud-Plattformen, S3-kompatiblen Speichern, SMB/NFS-Netzwerkfreigaben, Bändern und Deduplizierungs-Geräten gespeichert werden. Die Verschlüsselung wird für alle von NAKIVO Backup & Replication unterstützten Umgebungen und Plattformen unterstützt. Sie können auch [Self-Backups](#), die die Konfigurationen des Systems für die Datensicherheit enthalten. Für die Verschlüsselung und Entschlüsselung der Daten ist ein Passwort erforderlich. Die Funktion unterstützt auch die Integration mit AWS KMS als Mechanismus zum Schutz vor Passwortverlust.

Föderiertes Repository

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

Ein Verbund-Repository fungiert wie ein erweiterbarer Speicherpool, der aus mehreren eigenständigen Repositories besteht, die als „Mitglieder“ bezeichnet werden. Sie können ein Verbund-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 – der Vorgang ist mit wenigen Klicks erledigt. In einem Verbund-Repository werden Sicherungs- und Wiederherstellungsvorgänge ohne Unterbrechung fortgesetzt, selbst wenn eines der Mitglieds-Repositories ausfällt oder kein Speicherplatz mehr verfügbar ist, solange ein anderes nutzbares Mitglied verfügbar ist.

Detaillierte Benachrichtigungen

Granular Notifications ist eine Erweiterung der Workflow-Tracking-Funktionen, die Ihnen einen besseren Überblick über laufende Backup- und Replikationsaufträge verschafft. Während ein Auftrag ausgeführt wird, zeigt NAKIVO Backup & Replication Beschreibungen laufender Aktionen an, z. B. Datenübertragung oder Log-Trunkierung. Die Statusaktualisierungen erfolgen in Echtzeit, damit Sie über den Fortschritt des Auftrags auf dem Laufenden bleiben.

OAuth 2.0 Sicherheit der E-Mail-Authentifizierung

Diese Erweiterung bietet integriertes OAuth 2.0-Support für sichere, konforme E-Mail-Kommunikation über moderne E-Mail-Plattformen hinweg. Dank der nativen Integration für Google Gmail OAuth 2.0 und Microsoft 365 OAuth macht NAKIVO die veraltete SMTP-Basisauthentifizierung überflüssig und passt E-Mail-Benachrichtigungen an die aktuellen Anforderungen an die Cloud-Sicherheit an.

Malware-Scan für Backups

[Sichern Sie Backups auf Malware](#) und Ransomware, bevor Sie die Wiederherstellung durchführen, um

Infektionen in Ihrer Infrastruktur zu verhindern. Integrieren Sie die Lösung in Windows Defender, ESET NOD32 und Sophos, um einen Malware-Scan durchzuführen und sicherzustellen, dass Backups sicher für die Wiederherstellung verwendet werden können. Wenn Malware erkannt wird, wählen Sie, ob die Wiederherstellung fehlschlagen oder in einem isolierten Netzwerk erfolgen soll.

Dateisystem-Indizierung

Erstellen Sie einen Index aller Dateien und Ordner in Ihren VMware- und Hyper-V-VM-Backups und finden Sie ganz einfach eine bestimmte Datei oder einen bestimmten Ordner, um bei granularen Wiederherstellungen Zeit zu sparen. Um eine Datei oder einen Ordner wiederherzustellen, verwenden Sie einfach die Globale Suche, um sie im Index zu finden.

Universaltransporter

Verwenden Sie einen einzigen universellen Transporter, um physische Server, Virtuelle Maschinen, Bandgeräte und Oracle-Datenbanken über RMAN zu verwalten, die sich auf demselben Host befinden.

Debian-Support

Installieren Sie die Lösung direkt auf Debian-Betriebssystemen und/oder schützen Sie Ihre physischen Maschinen, die auf Debian-Betriebssystemen basieren. Erstellen Sie App-Aware Backups inkrementeller Art von physischen Maschinen, auf denen Debian 10.1 bis Debian 11.6 läuft.

Vereinfachte Aufbewahrungseinstellungen für Backups

Konfigurieren Sie Zeitpläne für Aufträge und Aufbewahrungseinstellungen in einem Schritt und in einer einzigen Ansicht. Legen Sie Aufbewahrungseinstellungen für jeden Plan innerhalb eines Backup- oder Replikationsauftrags fest und legen Sie Ablaufdaten für Wiederherstellungspunkte fest, um eine detailliertere Kontrolle zu ermöglichen.

Dauerhafter Agent

Bereitstellen Sie einen [dauerhafte Agenten](#) auf virtuellen Maschinen für die Gastverarbeitung bereit. Greifen Sie auf Ihre VMs zu, ohne Anmeldeinformationen eingeben zu müssen, um die Verwaltung zu optimieren und Probleme der Sicherheit zu vermeiden.

Auftragspriorität

Legen Sie die Prioritätsstufe in der Warteschlange für kritische Backup-Aufträge fest, damit diese zuerst verarbeitet werden und rechtzeitig abgeschlossen sind. Weisen Sie Prioritätsstufen von 1 bis 5 zu, wobei 1 die höchste Stufe ist, um sicherzustellen, dass Aufträge mit hoher Priorität die erforderlichen Lösungsressourcen erhalten, sobald diese verfügbar sind.

Aufträge zusammenführen

Führen Sie Backupaufträge desselben Typs zu einem einzigen Auftrag zusammen, um das Management der Datensicherheit zu optimieren und weniger Zeit für Routineaufgaben aufzuwenden. Halten Sie Ihre

Arbeitsabläufe übersichtlich, indem Sie Backup-, Backupkopie- oder Replikationsaufträge in einem einzigen Auftrag zusammenfassen.

Mehrsprachige Benutzeroberfläche

Die NAKIVO Backup & Replication-Weboberfläche unterstützt neben Englisch auch Spanisch, Französisch, Deutsch, Italienisch, Polnisch und Chinesisch.

Sie können die Lösung in Ihrer bevorzugten Sprache navigieren und verwalten, darunter:

- Verwalten Sie Backups, Backupkopien, Replikationen und Wiederherstellungen.
- Datensicherheitsberichte erstellen.
- Konfigurieren Sie Einstellungen und Kontrollen zur Sicherheit.

Alle Funktionen ausprobieren

Mit einem einzigen Klick erhalten Sie 15 Tage lang sofortigen Zugriff auf alle Funktionen von NAKIVO Backup & Replication, unabhängig von Ihrer Ausgabe der Lösung.

Sind Sie bereit, loszulegen?

[KOSTENLOSE TESTVERSION](#)[KOSTENLOSE DEMO BUCHEN](#)