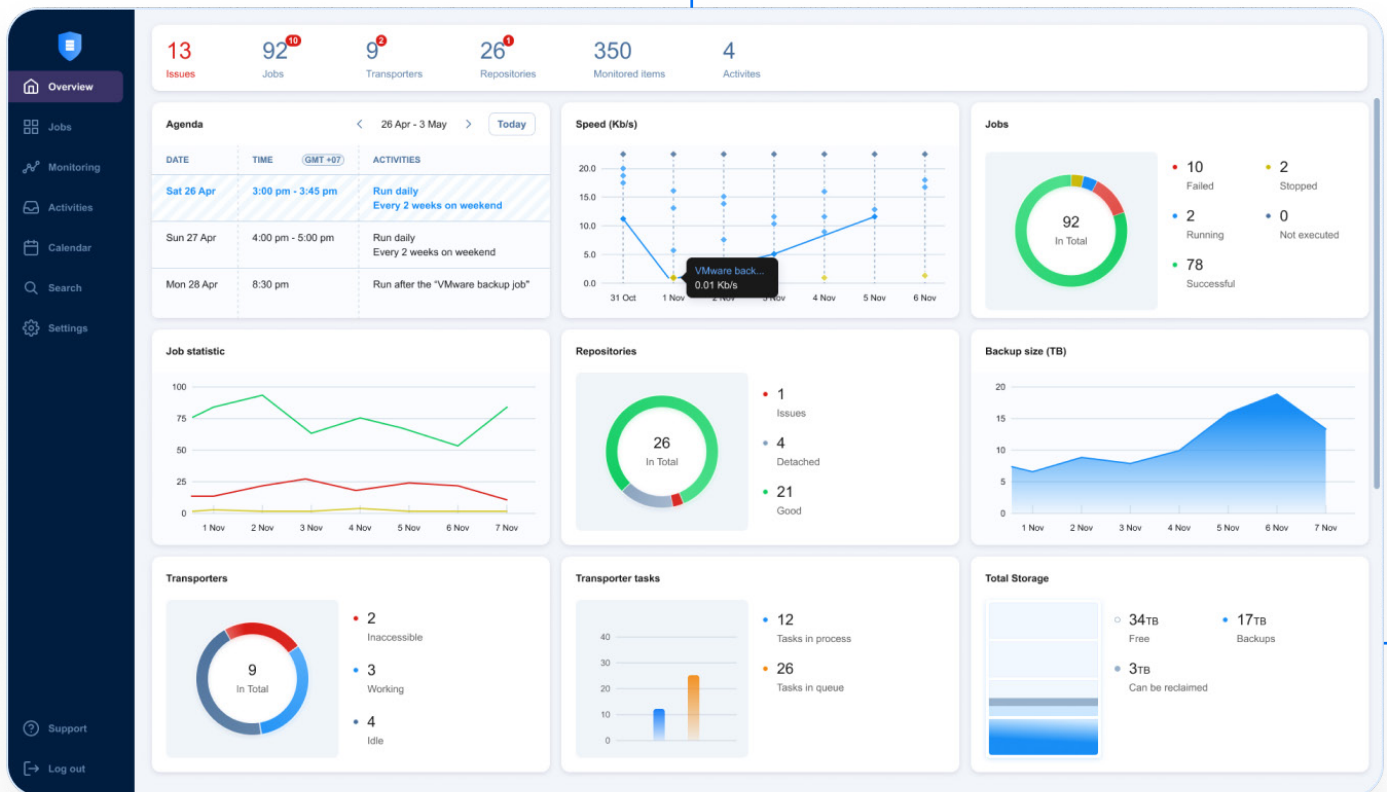


# Novità di NAKIVO Backup & Replication



# Sommario

Introduzione.....	3
Protezione per ambienti virtuali.....	3
Backup per Proxmox VE.....	3
Backup veloce ed efficiente.....	3
Destinazioni di storage flessibili.....	3
Protezione dai ransomware e sicurezza.....	3
Ripristino completo e granulare istantaneo.....	4
Replica per Proxmox VE.....	4
Replica in tempo reale per VMware.....	4
Supporto per l'ultima versione di VMware.....	4
Backup e ripristino per ambienti fisici.....	4
Backup granulare per macchine fisiche.....	4
Backup NAS.....	4
Storage ibrido e immutabile.....	4
Copia di backup automatizzata.....	5
Ripristino bare metal.....	5
Backup per Microsoft 365.....	5
Storage ibrido e immutabile.....	5
Copia di backup automatizzata.....	5
Supporto per In-Place Archive Mailbox, Litigation Hold e In-Place Hold.....	5
Fornitori di servizi gestiti (MSP).....	5
Console MSP.....	6
Dashboard panoramica tenant.....	6
Connessione diretta.....	6
Connessione diretta per MSP.....	6
Monitoraggio IT.....	6
Integrazione dispositivi di storage aziendali.....	6
Storage immutabile su NEC HYDRAsTOR.....	7
Backup dallo snapshot di storage.....	7
Storage sul cloud.....	7
S3-compatible object storage.....	7
Ripristino diretto delle VM da storage su nastro.....	7
Database.....	7
Miglioramenti ai componenti principali della soluzione.....	7
Crittografia dei backup.....	8
Federated Repository.....	8
Notifiche granulari.....	8
Scansione dei backup per rilevare i malware.....	8
Indicizzazione dei file system.....	8
Trasporto universale.....	9
Supporto Debian.....	9
Supporto Debian.....	9
Impostazioni semplificate di conservazione dei backup.....	9
Agente persistente.....	9
Priorità del lavoro.....	9
Unire i lavori.....	9
Interfaccia multilingue.....	9
Prova tutte le funzioni.....	9
PRONTO PER INIZIARE?.....	9

## Introduzione

Spinti dalla necessità di una protezione dei dati su misura, dal gennaio 2024 abbiamo rilasciato 8 nuove versioni di NAKIVO Backup & Replication, ciascuna delle quali presenta funzionalità e miglioramenti molto richiesti.

Dalle piattaforme virtualizzate e fisiche ai MSP (Managed Service Provider), dal ripristino di emergenza alla protezione dai ransomware, continuiamo a garantire ai nostri clienti un'esperienza di protezione dei dati personalizzata ed efficiente.

Di seguito è riportato un elenco delle principali nuove funzioni e miglioramenti aggiunti a NAKIVO Backup & Replication fino alla versione 11.2.

## Protezione per ambienti virtuali

NAKIVO Backup & Replication è progettato appositamente per gli ambienti virtuali e offre una protezione dei dati VM veloce e affidabile su misura per varie piattaforme di virtualizzazione, tra cui [VMware vSphere](#), [VMware Cloud Director](#), [Microsoft Hyper-V](#), [Nutanix AHV](#) e [Proxmox VE](#).

## Backup per Proxmox VE

NAKIVO Backup & Replication è in grado di eseguire backup e replica senza agente delle macchine virtuali Proxmox VE e dei modelli VM (fino all'ultimo aggiornamento v9.0), consentendo di ridurre la complessità e l'utilizzo delle risorse, ottenendo al contempo un maggiore controllo e flessibilità.

## Backup rapidi ed efficienti

È possibile eseguire il backup delle VM Proxmox VE direttamente a livello di host senza dover installare o gestire agenti OS aggiuntivi su ciascuna VM. La funzionalità consente di creare backup incrementali a livello di blocco utilizzando il tracciamento delle modifiche nativo per trasferire solo i blocchi di dati modificati dall'ultima sessione di backup. La funzione di verifica istantanea esegue controlli automatici sullo stato dei dati di backup di Proxmox VE e invia report basati su screenshot per confermare che i backup di Proxmox VE siano funzionanti e recuperabili.

## Destinazioni di storage flessibili

È possibile archiviare i backup di Proxmox VE in un'ampia gamma di destinazioni di storage, tra cui:

- [Cloud pubblici](#) e [S3-compatibile storage](#)
- [Appliance di deduplicazione](#)
- Condivisione CIFS/NFS
- Nastro adesivo.

Inoltre, è possibile utilizzare la [funzionalità copia di backup](#) per copiare i backup di Proxmox VE offsite e conservare più copie nel cloud o in qualsiasi altra ubicazione, seguendo la strategia di backup 3-2-1 per migliorare la disponibilità e garantire il ripristino di emergenza in caso di disastri.

## Protezione dai ransomware e sicurezza

È possibile proteggere il backup Proxmox VE da ransomware, accessi non autorizzati e manomissione dei dati con:

- [Crittografia dei backup](#) alla fonte, durante il trasferimento e a riposo nel repository
- [Backup immutabili](#) in archivi locali e cloud per proteggere i dati dalla crittografia ransomware o dalla cancellazione accidentale
- Backup con protezione air-gap su nastro e altri supporti scollegati per la protezione offline

## Ripristino completo e granulare istantaneo

NAKIVO Backup & Replication offre anche opzioni di ripristino completo e granulare istantaneo. È possibile scegliere di ripristinare intere VM Proxmox VE con tutti i loro dati o ripristinare istantaneamente singoli file e oggetti applicativi nella loro ubicazione originale o in una ubicazione diversa. Utilizza la funzione Avvio flash delle VM per avviare le VM Proxmox VE direttamente dai backup per un ripristino istantaneo.

## Replica per Proxmox VE

Con NAKIVO Backup & Replication, puoi garantire alta disponibilità e continuità operativa in caso di guasti o interruzioni. È possibile creare e mantenere repliche identiche delle macchine virtuali Proxmox VE di origine su un host di destinazione in un sito remoto. In caso di guasti o interruzioni, è sufficiente eseguire il failover sulla replica per ridurre al minimo i tempi di inattività e mantenere la disponibilità del servizio.

## Replica in tempo reale per VMware

La funzionalità di replica in tempo reale di NAKIVO Backup & Replication consente di creare repliche delle macchine virtuali VMware vSphere e di mantenerle aggiornate con le macchine virtuali di origine man mano che vengono apportate modifiche. Le repliche vengono aggiornate ogni secondo in tempo reale, consentendo tempi di inattività e perdite di dati prossimi allo zero in caso di guasto.

Inoltre, è possibile impostare azioni di failover per la replica in tempo reale nei lavori di ripristino dell'ambiente, in modo da passare automaticamente alle repliche in tempo reale con un solo clic durante un'interruzione. È inoltre possibile testare in anticipo il processo di failover per convalidare i piani di DR e garantire la prontezza al ripristino senza influire sull'ambiente di produzione.

## Supporto per l'ultima versione di VMware

Garantire ai clienti l'accesso alle ultime innovazioni nella tecnologia dei carichi di lavoro distribuiti è una priorità assoluta per NAKIVO. In linea con questo,

abbiamo aggiunto il supporto per le ultime versioni di VMware vSphere al momento del rilascio, incluso vSphere 9.

## Backup e ripristino per ambienti fisici

Estendendo la protezione alle infrastrutture fisiche, NAKIVO ha introdotto funzionalità di backup per [Windows](#) e [Linux](#) e stazione di lavoro per garantire la protezione dei dati in diversi ambienti IT.

## Backup granulare per le macchine fisiche

NAKIVO Backup & Replication è in grado di eseguire il backup di volumi e cartelle specifici su macchine Windows e Linux senza eseguire il backup dell'intera macchina. È possibile archiviare backup granulari di macchine fisiche su:

- Storage locale
- Condivisione file SMB e NFS
- Cloud pubblici (Amazon S3, Wasabi, BLOB di Azure, Backblaze B2)
- Piattaforme di storage oggetti compatibili con S3
- Nastro
- Appliance di deduplicazione

Per proteggersi dagli attacchi ransomware, è possibile utilizzare una combinazione di storage immutabile, backup con protezione air-gap e crittografia dei backup.

È possibile eseguire un ripristino granulare per ripristinare i dati necessari dai backup per macchine fisiche, risparmiando tempo e risorse nel processo.

## Backup per NAS

NAKIVO backup NAS consente di creare backup rapidi ed efficienti di dati non strutturati in condivisioni di rete NFS e SMB ospitate su dispositivi NAS e macchine Windows e Linux. Ecco le novità di NAKIVO backup NAS.

## Storage ibrido e immutabile

Ora è possibile inviare backup di condivisioni file a una gamma più ampia di destinazioni di archiviazione, tra cui:

- Piattaforme di storage sul cloud pubbliche (Amazon S3, Wasabi, Archiviazione BLOB di Azure, Backblaze B2)
- Piattaforme di storage compatibili con S3
- Cartelle locali
- Altre condivisioni NFS e SMB
- Appliance di deduplicazione

Quando si utilizza un repository di backup locale o basato su cloud come destinazione di archiviazione, è possibile abilitare l'immutabilità per proteggere i backup da attacchi ransomware e modifiche indesiderate.

### Copia di backup automatica

NAKIVO ha ampliato l'ambito delle funzioni di copia di backup e di concatenamento dei lavori per includere NAKIVO NAS Backup. Ora è possibile automatizzare la creazione e lo spostamento delle copie di backup tra le destinazioni di backup supportate sopra elencate, con l'aggiunta del nastro, per aumentare la resilienza del backup.

### Ripristino bare-metal

Il [ripristino bare metal](#) migliora la funzionalità di ripristino fisico esistente, fornendo un ripristino flessibile e veloce dei server fisici. È possibile ripristinare un intero server o una stazione di lavoro da un backup su hardware identico senza dover ricostruire i sistemi operativi o riconfigurare le impostazioni delle applicazioni.

Questa funzionalità offre un approccio rapido ed efficiente per ripristinare le macchine fisiche all'ultimo stato corretto conosciuto, consentendo di ripristinare da incidenti o ripristinare modifiche/cancellazioni indesiderate effettuate in precedenza.

### Backup per Microsoft 365

NAKIVO Backup per Microsoft 365 è una potente soluzione progettata per fornire backup e ripristino rapidi di [OneDrive for Business](#), [SharePoint Online](#), [Exchange Online](#) e [Microsoft Teams](#). Ecco le novità di NAKIVO Backup per Microsoft 365.

### Archiviazione ibrida e immutabile

Questa importante espansione segna una nuova pietra miliare per NAKIVO Backup per Microsoft 365, aggiungendo nuove destinazioni di storage, supporto

per backup a prova di ransomware e suddivisione in livelli dei backup. Oltre alle cartelle locali, ora è possibile inviare backup dei dati di Microsoft 365 alle seguenti destinazioni di archiviazione:

- [Piattaforme di storage sul cloud pubbliche](#) (Amazon S3, Wasabi, BLOB di Azure, Backblaze B2)
- Altro [piattaforme di storage compatibili con S3](#)
- Condivisione NFS e SMB
- [Appliance di deduplicazione](#)

Per proteggersi dagli attacchi ransomware e da altre modifiche indesiderate, è possibile abilitare l'immutabilità per i backup per Microsoft 365 archiviati in destinazioni di storage locale e sul cloud.

### Copia di backup automatica

Inoltre, ora è possibile utilizzare la [funzione Copia di backup](#) per creare copie aggiuntive dei backup di Microsoft 365 o migrare senza problemi i backup tra le destinazioni di storage sopra indicate, con l'aggiunta del nastro. Utilizzo [Concatenamento dei lavori](#) è possibile automatizzare il trasferimento delle copie di backup tra le destinazioni di storage (da nastro a cloud, da cloud a cartella locale, da condivisione di rete a nastro, ecc.).

### Supporto per l'archivio sul posto delle cassette postali, blocco per controversia legale e blocco sul posto

NAKIVO ha aggiunto il supporto per ulteriori elementi della cassetta postale Exchange Online:

- Casette postali per l'archivio sul posto
- Elementi soggetti al blocco per controversia legale
- Elementi in blocco sul posto

Ora è possibile eseguire il backup delle cartelle della cassetta postale necessarie e ripristinare l'intera cartella o file specifici nell'account utente originale o in un account utente diverso.

### Fornitori di servizi gestiti (MSP)

[Multi-tenancy](#) consente agli MSP di gestire e personalizzare in modo efficiente la protezione dei dati per più clienti da un'unica Piattaforma. Da allora,

abbiamo continuato a fornire funzioni e capacità specializzate che consentono ai fornitori di servizi di soddisfare meglio le esigenze dei propri clienti e di migliorare. Ecco le ultime funzionalità MSP introdotte in NAKIVO Backup & Replication:

## Console MSP

NAKIVO ha introdotto la [Console MSP per la gestione centralizzata di tutti i clienti](#), consentendo ai fornitori di servizi di semplificare le operazioni, migliorare l'efficienza e fornire servizi di protezione dei dati affidabili ai propri clienti.

Gli MSP possono aggiungere clienti con implementazioni autonome di NAKIVO Backup & Replication come tenant remoti nella loro distribuzione multi-tenant della soluzione. Ciò consente loro di gestire e effettuare il monitoraggio delle attività di protezione dei dati di tutti gli utenti, sia remoti che locali, da un pannello di controllo MSP unificato.

## Dashboard di panoramica dei tenant

Abbiamo integrato la Console MSP con una nuova dashboard che offre una panoramica di alto livello di tutti i tenant gestiti in un unico posto. Il Dashboard di panoramica degli inquilini fornisce informazioni e avvisi in tempo reale sulle infrastrutture di protezione dei dati dei clienti, compreso lo stato dei nodi, le risorse disponibili, le attività pianificate e le informazioni sull'inventario. Potete ordinare, filtrare e cercare nell'elenco dei tenant per estrarre le informazioni di cui avete bisogno, identificare i problemi in sospeso e applicare azioni in blocco.

Questo dashboard dinamico ti aiuta a risparmiare tempo nelle attività di routine relative alla gestione degli inquilini, a risolvere in modo efficiente problemi e colli di bottiglia e a ottimizzare l'allocazione delle risorse e delle licenze.

## Connessione diretta

La Connessione diretta consente agli MSP di accedere alle risorse remote dei propri clienti tramite un'unica connessione diretta alla porta, senza necessità di una connessione VPN. La funzione supporta VMware vSphere, Microsoft Hyper-V, Proxmox VE, macchine fisiche, host VMware ESXi e Transporter basati su NAS.

## Connessione diretta per gli MSP

Con la Connessione diretta per MSP, è possibile stabilire una connessione sicura agli ambienti dei tenant senza la necessità di porte aperte sul lato tenant. La funzione fornisce il supporto per le seguenti piattaforme per la gestione remota e la protezione dei dati:

- VMware vSphere
- Microsoft Hyper-V
- Proxmox VE
- Macchine fisiche Windows
- Macchine fisiche Linux

La Connessione diretta per MSP supporta anche i flussi di lavoro del ripristino dell'ambiente per consentire il ripristino rapido dei carichi di lavoro dei tenant in caso di disastri.

## Monitoraggio IT

Tenere traccia dell'utilizzo delle risorse nell'infrastruttura VMware è fondamentale per ottimizzare le prestazioni delle VM e prevenire i colli di bottiglia. Il [funzionalità di monitoraggio NAKIVO per VMware](#) funzionalità consente di:

- Monitorate l'utilizzo della CPU, della RAM e del disco dei vostri host VMware vSphere e delle VM, nonché degli archivi dati.
- Crea e configura avvisi personalizzati attivati da varie metriche per host, VM e archivio dati.
- Ricevi diversi tipi di report sugli elementi vSphere monitorati nella tua infrastruttura, direttamente nella tua casella di posta elettronica.

## Integrazione dei dispositivi di storage aziendali

L'approccio completo di NAKIVO consente di creare una strategia di archiviazione dei backup ibrida e multi-cloud versatile, integrando perfettamente dispositivi onsite, cloud e di deduplicazione e soluzioni di archiviazione su nastro. Ecco le novità relative alle funzionalità di storage di NAKIVO Backup & Replication.

## Storage immutabile su NEC HYDRAsstor

NAKIVO Backup & Replication supporta [NEC HYDRAsstor](#) come destinazione di storage per i backup tra le altre appliance di deduplicazione.

Ora è possibile abilitare l'immutabilità per i backup residenti sul sistema di archiviazione NEC HYDRAsstor per proteggerli da attacchi ransomware, cancellazioni accidentali e altre forme di modifiche indesiderate.

## Backup dagli snapshot di storage

NAKIVO Backup & Replication integra perfettamente i dispositivi di storage aziendali dei principali vendor per eseguire backup e repliche direttamente dagli snapshot di storage.

È possibile eseguire il backup e la replica delle macchine virtuali VMware vSphere ospitate su [HPE 3PAR storage appliances](#), [HPE Nimble storage appliances](#), [HPE Primera storage appliances](#) and [HPE Alletra storage appliances](#), oltre che su array di storage NetApp FAS e NetApp AFF, direttamente da snapshot di storage anziché da normali snapshot di VM, per risparmiare tempo e ridurre il carico sull'infrastruttura.

## Storage sul cloud

Con l'ascesa del cloud ibrido (che combina infrastrutture cloud private e pubbliche), le aziende potrebbero trovarsi ad affrontare nuove sfide nella gestione dei costi del cloud.

Le versioni precedenti di NAKIVO Backup & Replication supportavano opzioni di storage sul cloud, come [Amazon S3](#), [Wasabi](#), [BLOB di Azure](#) e [Backblaze B2](#), che offrivano uno spazio di archiviazione sicuro per le esigenze di backup e ripristino con un'opzione di immutabilità per proteggere i backup dalle infezioni ransomware.

## Storage di oggetti compatibile con S3

NAKIVO Backup & Replication ha introdotto il supporto per [object storage compatibile con S3](#) per i backup, offrendo agli utenti un'ulteriore opzione per l'archiviazione dei propri dati di backup. Consente di archiviare i backup in uno spazio di storage compatibile

con l'API S3 e di scegliere tra una varietà di piattaforme convenienti che soddisfano le vostre esigenze.

Inoltre, i backup archiviati in uno storage compatibile con S3 possono essere configurati come immutabili, fornendo protezione contro gli attacchi ransomware e la cancellazione accidentale.

## Ripristino diretto delle VM dall'storage su nastro

Sebbene la maggior parte delle aziende si affidi a backup su disco o su cloud, i backup su nastro sono ancora ampiamente utilizzati per l'archiviazione dei dati di backup e la conservazione a lungo termine. NAKIVO supporta da tempo l'archiviazione [backup dei dati su librerie su nastro LTO](#) e unità autonome, nonché su AWS Virtual Tape Library (VTL).

Con il nuovo [ripristino diretto della VM dal nastro](#), la funzione consente ai clienti di eseguire ripristini rapidi senza la necessità di un repository di staging. Possono ripristinare VM complete, istanze di EC2 e macchine fisiche come VM VMware direttamente dai backup archiviati su supporti nastro alla propria infrastruttura.

## Banche dati

NAKIVO Backup & Replication supporta da tempo [il backup e il ripristino dei database Oracle](#) tramite la funzionalità nativa RMAN.

La funzionalità esistente supporta il backup tramite RMAN per Oracle Database su Windows. Le nostre ultime versioni hanno esteso questo supporto per includere Oracle RMAN sui sistemi Linux. I clienti possono proteggere i propri Oracle Database con un sistema integrato e automatizzato di backup e ripristino su piattaforme Windows e Linux, il tutto da una console unificata.

## Miglioramenti alle componenti principali della soluzione

NAKIVO è attivo nel miglioramento dei componenti e delle funzionalità della soluzione per semplificare e ottimizzare le attività di protezione dei dati per i nostri clienti. Ciascuno di questi miglioramenti

contribuisce a rendere più affidabile ed efficiente la protezione dei dati. La sezione seguente evidenzia i principali miglioramenti apportati a NAKIVO Backup & Replication:

### **Crittografia dei backup**

La funzione di crittografia dei backup consente di crittografare i backup sul lato sorgente prima che vengano trasmessi in rete alla loro destinazione di archiviazione. I backup crittografati possono essere archiviati in cartelle locali, piattaforme cloud pubbliche, storage compatibile con S3, condivisioni di rete SMB/ NFS, nastri e appliance di deduplicazione. La crittografia è supportata per tutti gli ambienti e le piattaforme supportati da NAKIVO Backup & Replication. È anche possibile effettuare la crittografia [Backup automatico](#) che contengono le configurazioni del sistema di protezione dei dati. Per effettuare la crittografia e la decrittografia dei dati è obbligatoria una password; la funzione supporta anche l'integrazione con AWS KMS come meccanismo per garantire la protezione in caso di smarrimento della password.

### **Repository federato**

Il Federated Repository è un tipo di repository di backup facilmente scalabile e flessibile che risolve i colli di bottiglia in termini di prestazioni e complessità in ambienti di grandi dimensioni con dataset di grandi dimensioni.

Un repository federato funziona come un pool di storage espandibile composto da più repository autonomi, denominati "membri". È possibile espandere rapidamente e facilmente un repository federato aggiungendo nuovi membri per conservare più dati. Non sono necessarie configurazioni complesse per aggiungere o rimuovere membri: il processo richiede solo pochi clic. In un repository federato, le operazioni di backup e ripristino continuano senza interruzioni anche se uno dei repository membri si guasta o ha lo spazio esaurito, purché sia disponibile un altro membro utilizzabile.

### **Notifiche granulari**

Le notifiche granulari sono un miglioramento delle funzionalità di monitoraggio del flusso di lavoro che offrono una maggiore visibilità sui lavori di backup e replica in esecuzione. Durante l'esecuzione di un processo, NAKIVO Backup & Replication visualizza le descrizioni delle azioni in corso, come il trasferimento dei dati o il troncamento dei registri. Gli aggiornamenti di stato avvengono in tempo reale per tenerti informato sull'avanzamento del lavoro.

### **Autenticazione e-mail sicura OAuth 2.0**

Questo miglioramento aggiunge il supporto integrato OAuth 2.0 per comunicazioni e-mail sicure e conformi su tutte le piattaforme di posta elettronica moderne. Grazie all'integrazione nativa con Google Gmail OAuth 2.0 e Microsoft 365 OAuth, NAKIVO elimina la necessità dell'autenticazione SMTP di base legacy e allinea le Notifiche per e-mail agli attuali requisiti di sicurezza cloud.

### **Scansione dei backup per rilevare eventuali malware**

[Esegui la scansione dei backup per rilevare i malware](#) e ransomware prima del ripristino per prevenire infezioni nella tua infrastruttura. Integra la soluzione con Windows Defender, ESET NOD32 e Sophos per eseguire una scansione antimalware e garantire che i backup possano essere utilizzati in modo sicuro per il ripristino. Se viene rilevato un malware, scegliere di interrompere il ripristino o di ripristinare su una rete isolata.

### **Indicizzazione del file system**

Crea un indice di tutti i file e le cartelle presenti nei backup delle macchine virtuali VMware e Hyper-V e trova facilmente un file o una cartella specifici per risparmiare tempo durante i ripristini granulari. Per ripristinare un file o una cartella, basta utilizzare la Ricerca globale per trovarlo nell'indice.

## Transporter universale

Utilizza un unico trasportatore universale per gestire server fisici, VM, dispositivi a nastro e Oracle Database tramite RMAN residenti sullo stesso host.

## Supporto Debian

Installa la soluzione direttamente sui sistemi operativi Debian e/o proteggi le tue macchine fisiche basate su sistema operativo Debian. Crea un backup incrementale coerente con le applicazioni per macchine fisiche che eseguono Debian 10.1 e fino a Debian 11.6.

## Impostazioni semplificate di conservazione dei backup

Configura le pianificazioni dei lavori e le impostazioni di conservazione in un unico passaggio e in un'unica schermata. Specificare le impostazioni di conservazione per ogni pianificazione all'interno di un lavoro di backup o replica e impostare le date di scadenza per i punti di ripristino per un controllo più granulare.

## Agente persistente

Implementare un [Agente persistente](#) sulle VM per l'elaborazione degli ospiti. Accedi alle tue VM senza inserire credenziali per semplificare l'amministrazione ed evitare problemi di sicurezza.

## Priorità del lavoro

Imposta il livello di priorità nella coda affinché i lavori di backup critici vengano elaborati per primi e assicurati che vengano completati in tempo. Assegnare livelli di

priorità da 1 a 5, dove 1 è il più alto, per garantire che i lavori ad alta priorità ottengano le risorse necessarie non appena disponibili.

## Unisci lavori

Unisci i lavori di protezione dei dati dello stesso tipo in un unico lavoro per semplificare la gestione dei backup e dedicare meno tempo alle attività di routine. Mantieni i tuoi flussi di lavoro ordinati aggregando i lavori di backup, copia di backup o replica in un unico lavoro.

## Interfaccia multilingue

Oltre all'inglese, l'interfaccia web di NAKIVO Backup & Replication supporta lo spagnolo, il francese, il tedesco, l'italiano, il polacco e il cinese.

È possibile navigare e gestire la soluzione nella lingua preferita, tra cui:

- Gestisci backup, copie di backup, replica e ripristino.
- Generare rapporti sulla protezione dei dati.
- Configurare le impostazioni e i controlli di sicurezza.

## Prova tutte le funzioni

Ottieni accesso immediato alla suite completa di funzionalità di NAKIVO Backup & Replication per 15 giorni con un solo clic, indipendentemente dall'edizione della tua soluzione.

## Pronto per iniziare?

[SCARICA LA PROVA GRATUITA](#)[PRENOTA UNA DEMO GRATUITA](#)