



Le novità di NAKIVO Backup & Replication per gli MSP



Sommario

Introduzione	3
Funzioni e miglioramenti MSP	3
Console MSP	3
Dashboard di panoramica dei tenant	3
Connessione diretta MSP	3
Database esterno per multi-tenancy	3
NAKIVO Backup & Replication: Ultime aggiunte chiave	4
Backup e ripristino	4
Backup senza agenti per Proxmox VE	4
Backup su cloud per Microsoft 365	4
Backup per NAS	4
Crittografia dei backup all'origine	4
Replica in tempo reale per VMware	4
Scansione dei backup per rilevare eventuali malware	4
Ripristino bare metal	4
Ripristino diretto da nastro	4
Supporto per lo storage di oggetti compatibile con S3	4
Indicizzazione del file system	4
Backup dagli snapshot di storage NetApp e HPE	4
Storage immutabile su NEC HYDRAstor e DELL EMC	5
Backup granulare per le macchine fisiche	5
Gestione del flusso di lavoro	5
Supporto e compatibilità	5

Introduzione

Con ogni release, NAKIVO Backup & Replication introduce nuove funzioni e capacità per aiutare i Managed Service Provider (MSP) a fornire offerte BaaS e DRaaS affidabili, sicure e redditizie. Le ultime modifiche si basano su questa base con miglioramenti chiave che semplificano la gestione multi-tenant, automatizzano i flussi di lavoro DR ed espandono la copertura della piattaforma.

Di seguito è riportato un elenco delle ultime aggiunte orientate a MSP, seguito da un breve riepilogo delle modifiche notevoli introdotte nella soluzione NAKIVO fino alla versione 11.1.

Funzioni e miglioramenti MSP

Console MSP

La funzionalità di [multi-tenancy](#) consente agli MSP di gestire, monitorare e personalizzare le operazioni di protezione dei dati per più clienti in un unico luogo. La [Console MSP](#) ha portato il Multi-Tenancy a nuovi livelli di centralizzazione e amministrazione efficiente.

Da questa console, gli MSP possono connettersi ai clienti che possiedono implementazioni NAKIVO Backup & Replication standalone e aggiungerli come tenant remoti nella loro implementazione multi-tenant esistente.

Invece di destreggiarsi tra diverse interfacce per istanze standalone, gli MSP possono gestire centralmente le attività di protezione dei dati e i componenti dell'infrastruttura dei tenant remoti insieme a quelli locali esistenti, il tutto in un'unica dashboard unificata.

Dashboard di panoramica dei tenant

La nuova dashboard consente agli MSP di monitorare in tempo reale le informazioni sulle infrastrutture di protezione dei dati dei clienti. Questo include lo stato dei nodi, lo stato dei lavori, le attività pianificate, le risorse disponibili, l'inventario, gli avvisi e molto altro ancora. MSP possono filtrare, ordinare e cercare per individuare e risolvere problemi, rivedere le metriche di performance e monitorare l'utilizzo delle infrastrutture tra i tenant. Possono anche eseguire azioni in blocco direttamente dall'interfaccia della soluzione per semplificare le operazioni.

Connessione diretta MSP

Con la nuova Connessione diretta per gli MSP nella versione 11.1, NAKIVO elimina una delle principali preoccupazioni dei servizi gestiti: le porte aperte dal lato del tenant. Tipicamente, gli MSP richiedono eccezioni del firewall, configurazioni VPN e porte aperte per fornire i loro servizi. Questo aumenta la superficie di attacco e complica, e a volte ritarda, l'onboarding del cliente.

Le nuove funzionalità consentono agli MSP di accedere e gestire in sicurezza gli ambienti dei tenant senza dover modificare le regole del firewall del tenant, configurare VPN o aprire porte da parte del tenant. Le comunicazioni tra MSP Director e Client Transporter sono ora completamente crittografate per garantire la privacy e la sicurezza, nonché la conformità alle normative.

Questa release estende il supporto di Connessione diretta anche a Hyper-V e Proxmox VE, oltre che a VMware e agli ambienti fisici, consentendo agli MSP di offrire una protezione sicura su infrastrutture ibride.

Database esterno per multi-tenancy

Per impostazione predefinita, NAKIVO Backup & Replication utilizza un database integrato per memorizzare i dati di configurazione del componente centrale di gestione, il Director.

Grazie a questo miglioramento, gli MSP con implementazione multi-tenant possono semplificare la gestione e garantire la coerenza dei dati Director in ambienti multi-tenant ampi e dinamici.

NAKIVO Backup & Replication: Ultime aggiunte chiave

Backup e ripristino

Backup senza agenti per Proxmox VE

Create backup incrementali e senza agenti delle VM di Proxmox VE e ripristinate intere VM, singoli file o oggetti di applicazioni in pochi minuti. Inviate backup e copie di backup a piattaforme locali, cloud, compatibili con S3, dispositivi NAS, appliance di deduplicazione o nastri. Abilitate la crittografia e l'immutabilità per i backup archiviati in destinazioni locali e cloud per una resilienza ottimale al ransomware.

Backup su cloud per Microsoft 365

Eseguite il backup dei dati di Microsoft 365 direttamente sui principali cloud pubblici, come Amazon S3, Wasabi, BLOB di Azure, Backblaze B2 o qualsiasi altro storage compatibile con S3, per ridurre la dipendenza dall'infrastruttura on-premise. Abilita la crittografia e l'immutabilità per i backup archiviati localmente o nel cloud per proteggere dai ransomware, eliminazioni accidentali e modifiche non autorizzate. Creare copie di backup aggiuntive su diversi livelli di storage, tra cui cloud, locale, NAS e nastro, per allinearsi alla strategia di backup 3-2-1-1, eliminare un singolo punto di guasto e garantire la disponibilità dei dati. <!!Automatizza i flussi di lavoro delle copie di backup con Job Chaining per mantenere la ridondanza del backup tra diversi livelli di storage.

Backup per NAS

Eseguite il backup di condivisioni file SMB e NFS da dispositivi NAS, sistemi Windows o Linux a cloud pubblici, piattaforme compatibili con S3, NAS, appliance di deduplicazione e cartelle locali. Abilitate l'immutabilità e la crittografia dei backup archiviati localmente o nel cloud per proteggervi da ransomware, cancellazioni accidentali e modifiche non autorizzate.

Crittografia dei backup all'origine

Crittografare i backup e le copie di backup all'origine, in transito e a riposo per impedire l'accesso non autorizzato. Integrazione con AWS KMS per la gestione sicura delle chiavi e la protezione dalla perdita di password.

Replica in tempo reale per VMware

Create repliche in tempo reale delle VM con RPO di appena un secondo e fate failover automatizzato su queste repliche durante le interruzioni attraverso i workflow di ripristino dell'ambiente. Installare automaticamente il filtro I/O e il servizio journal sugli host di origine e di destinazione per eliminare l'impostazione manuale e ridurre gli errori.

Scansione dei backup per rilevare eventuali malware

Eliminate il rischio di infezioni da virus e ransomware con scansioni affidabili prima del ripristino.

Ripristino bare metal

Backup di macchine fisiche intere da backup sullo stesso hardware o su un altro identico senza reinstallare il sistema operativo/applicazioni.

Ripristino diretto da nastro

Ripristina VM (comprese le VM di Proxmox VE), istanze di EC2 di AWS e macchine fisiche come VMware vSphere direttamente nella vostra infrastruttura da backup archiviati su nastro.

Supporto per lo storage di oggetti compatibile con S3

Inviate i backup a storage di destinazione che utilizzano l'API S3 e consentono l'immutabilità per la protezione dai ransomware.

Indicizzazione del file system

Cercate facilmente file e cartelle specifiche nei vostri backup utilizzando la dashboard Ricerca globale per risparmiare tempo durante i ripristini.

Backup dagli snapshot di storage NetApp e HPE

Ottimizzate le prestazioni utilizzando snapshot di storage nativi per i backup delle VM.

Storage immutabile su NEC HYDRAstor e DELL EMC

Abilitate l'immutabilità per i backup archiviati sui sistemi di storage NEC HYDRAstor o DELL EMC per proteggervi dai ransomware, dalle cancellazioni accidentali e dalle modifiche non autorizzate.

Backup granulare per le macchine fisiche

Crea backup granulari di volumi o cartelle specifiche su macchine Windows e Linux e ripristina i dati selezionati direttamente su condivisioni SMB/NFS, e-mail o tramite download dal browser.

Gestione del flusso di lavoro

- **Interfaccia multilingue:** Gestisce le operazioni di backup e ripristino in inglese, spagnolo, francese, italiano, tedesco, polacco e cinese. Controllare i report sui lavori, gli avvisi e-mail e le schermate di verifica degli screenshot nella lingua selezionata.
- **Repository federato:** Combinare più repository di backup "membri" per creare un repository di grandi dimensioni, facilmente scalabile, in grado di gestire volumi di dati crescenti e di eliminare i colli di bottiglia dello storage. Se un repository membro si guasta o raggiunge la capacità, i backup passano automaticamente ad altri membri disponibili.
- **Priorità del lavoro:** Assegnare livelli di priorità (1-5) ai lavori in base alla loro importanza.
- **Unire i lavori:** Semplifica la gestione dei lavori di backup esistenti tramite la fusione.
- **Conservazione dei backup migliorata:** Possibilità di specificare le impostazioni di conservazione per ogni pianifica all'interno di un singolo lavoro e di impostare date di scadenza per i punti di ripristino.
- **Universal Transporter:** migliora l'efficienza del flusso di lavoro e riduce il carico di rete utilizzando un unico transporter universale per più tipi di carico di lavoro sullo stesso host.

Supporto e compatibilità

- Supporto completo per VMware vSphere 9
- Supporto per Debian

Offrire BaaS e DRaaS potenti con NAKIVO

[SCARICA LA PROVA GRATUITA](#)

Gratuita per 15 giorni. Nessuna limitazione delle funzioni.

[PIANIFICA UNA DEMO](#)

Ottenete risposte su funzioni, prezzi e casi d'uso.