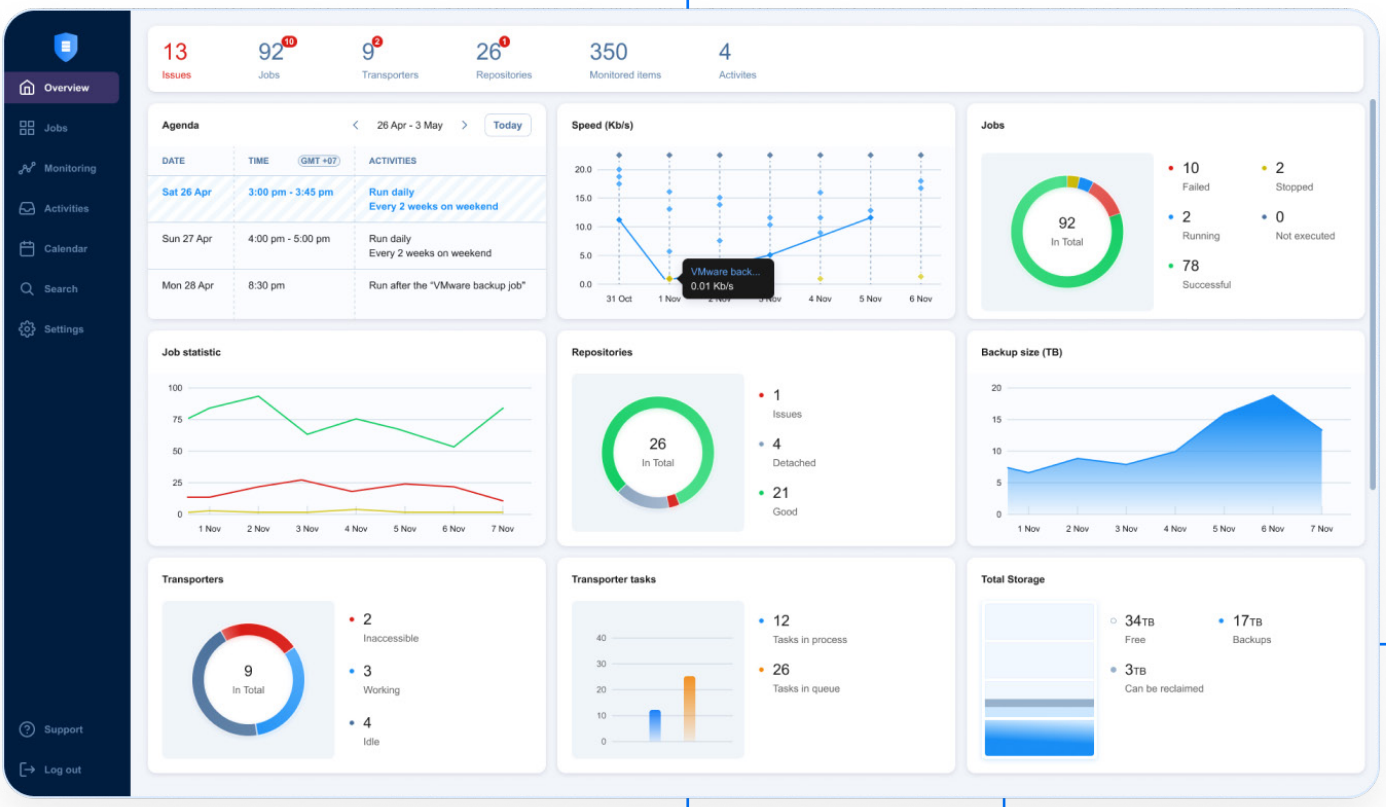
Novità in NAKIVO Backup & Replication



Sommario

Introduzione

Spinti dall'esigenza di una protezione dei dati su misura, da gennaio 2023 abbiamo rilasciato 4 nuove versioni di NAKIVO Backup & Replication, ognuna con funzioni e progressi molto richiesti.

Da piattaforme virtuali e fisiche a provider di servizi gestiti (MSP), ripristino di emergenza e protezione dai ransomware, continuiamo a garantire ai nostri clienti un'esperienza di protezione dei dati personalizzata ed efficiente.

Di seguito sono elencate le principali funzioni e i miglioramenti aggiunti a NAKIVO Backup & Replication fino alla versione 11.1.

Protezione per ambienti virtuali

NAKIVO Backup & Replication è costruito appositamente per gli ambienti virtuali, offrendo una protezione dei dati VM veloce e affidabile, adatta a varie piattaforme di virtualizzazione, tra cui VMware vSphere, VMware Cloud Director, Microsoft Hyper-V e Proxmox VE.

Backup per Proxmox VE

NAKIVO Backup & Replication è in grado di eseguire il backup e la replica agentless delle VM e dei modelli di VM di Proxmox VE, consentendo di ridurre la complessità e l'utilizzo delle risorse e di ottenere un maggiore controllo e flessibilità.

È possibile eseguire il backup delle VM Proxmox VE direttamente a livello di host senza dover installare o gestire agenti OS aggiuntivi su ogni VM. La funzionalità consente di creare backup incrementali a livello di blocco utilizzando la tecnologia nativa di tracciamento delle modifiche per trasferire solo i blocchi di dati modificati dall'ultima sessione di backup.

È possibile inviare i backup di Backup di Intervallo VE a un'ampia gamma di destinazioni di storage, tra cui cloud e storage compatibile con S3, appliance di deduplicazione Condivisione CIFS, condivisione NFS o Nastri. Inoltre, con la funzionalità Backup Copy, tutte le copie di backup di Proxmox VE possono essere copiate offsite, direttamente nel cloud o in qualsiasi altra ubicazione. L'archiviazione di copie multiple di dati in ubicazioni diverse segue rigorosamente la strategia di backup 3-2-1 per aumentare la disponibilità e garantire il ripristino in caso di disastro.

È possibile abilitare la crittografia e l'immutabilità. Immutabile per i backup archiviati nei repository locali e nel cloud o creare backup con protezione air-gap su nastro per proteggersi dalle violazioni dei dati, dai ransomware e da altre modifiche indesiderate.

NAKIVO Backup & Replication offre anche opzioni di ripristino granulare completo e istantaneo. È possibile scegliere di ripristinare intere VM di Proxmox VE con tutti i loro dati o di ripristinare istantaneamente singoli file e oggetti delle applicazioni nella loro ubicazione originale o in una diversa. Grazie alla funzione Avvio flash delle VM, è possibile avviare le VM direttamente dai backup per un ripristino istantaneo. La funzione di verifica istantanea consente di eseguire controlli automatici sullo stato di salute dei dati di backup di Proxmox VE e di garantirne la ripristinabilità.

Replica per VMware in tempo reale

Questa funzionalità di ripristino di emergenza consente di creare repliche delle VMware vSphere e di aggiornarle con le VM di origine man mano che vengono apportate modifiche. Le repliche vengono aggiornate in tempo reale con una frequenza di ogni secondo, consentendo tempi di inattività delle applicazioni prossimi allo zero e perdite di dati prossime allo zero in caso di disastro.

Grazie alla funzionalità Ripristino dell'ambiente, è possibile impostare sequenze automatiche di ripristino di emergenza con azioni annidate, che possono essere avviate con un solo clic. L'impostazione di Real-Time Replication per VMware è semplice e completamente automatizzata.

Supporto per l'ultima versione di VMware

Garantire ai clienti l'accesso agli ultimi progressi nella tecnologia dei cargas de trabajo distribuiti è una priorità assoluta per NAKIVO. In linea con ciò, abbiamo aggiunto il supporto per le versioni più recenti di VMware vSphere al momento del rilascio, incluso vSphere 9.

Backup e ripristino per gli ambienti fisici

Estendendo la protezione alle infrastrutture fisiche, NAKIVO ha introdotto le funzionalità di backup di macchine fisiche per Windows e Linux Server e workstation Windows e Linux per garantire la protezione dei dati in diversi ambienti IT.

Backup granulare per le macchine fisiche

NAKIVO Backup & Replication può 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 per macchine fisiche:

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

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

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

Backup per NAS

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

Storage ibrido e immutabile

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

- Piattaforme di storage sul cloud pubblico (Amazon S3, Wasabi, 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 storage, è possibile abilitare l'immutabilità per proteggere i backup da attacchi ransomware e modifiche indesiderate.

Copia di backup automatizzata

NAKIVO ha ampliato la portata delle funzioni di copia di backup e concatenamento dei lavori includendo NAKIVO NAS Backup. È ora 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 dei backup.

Ripristino bare-metal

Il ripristino bare metal migliora la funzionalità di ripristino fisico esistente, offrendo un ripristino flessibile e veloce dei server fisici. È possibile ripristinare un intero server o una workstation da un backup su un hardware identico senza ricostruire i sistemi operativi o riconfigurare le impostazioni delle applicazioni.

Questa funzionalità offre un approccio rapido ed efficiente al ripristino delle macchine fisiche all'ultimo stato conosciuto, consentendo di ripristinare gli incidenti o di eseguire il rollback di modifiche/cancellazioni indesiderate effettuate in precedenza.

Backup per Microsoft 365

NAKIVO Backup per Microsoft 365 è una potente soluzione progettata per fornire un backup e un ripristino rapidi di OneDrive for Business, SharePoint Online, Exchange Online e Microsoft Teams dati. Ecco quali sono le novità di NAKIVO Backup per Microsoft 365.

Storage ibrido 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 automatica in livelli. Oltre alle cartelle locali, è ora possibile inviare i backup dei dati di Microsoft 365 alle seguenti destinazioni di storage:

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

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

Copia di backup automatizzata

Inoltre, è ora possibile utilizzare la funzione copia di backup per creare copie aggiuntive di backup per Microsoft 365 o per migrare i backup tra le destinazioni di storage di cui sopra, con l'aggiunta del nastro. Utilizzo di 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 cassette postali, blocco per controversie legali e blocco sul posto

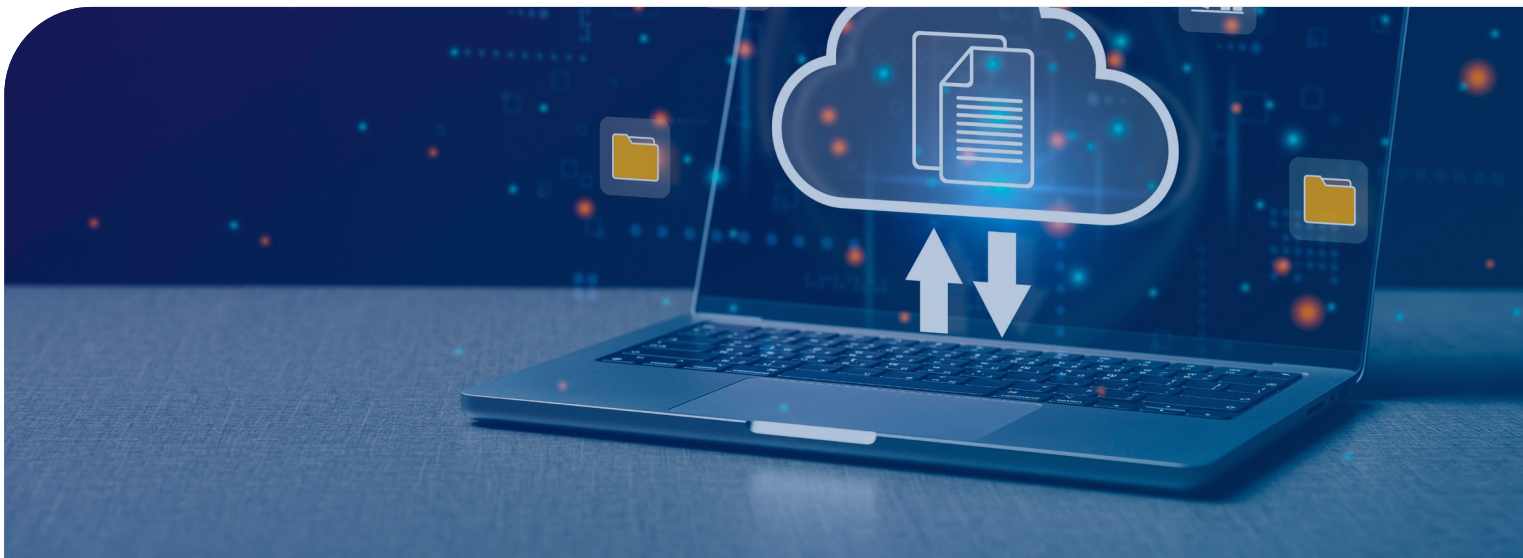
NAKIVO ha aggiunto il supporto per altri elementi della cassetta postale di Exchange Online:

- Cassette postali dell'archivio sul posto
- Elementi di blocco per controversia legale
- Elementi del 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 altro account utente.

Fornitori di servizi gestiti (MSP)

Multi-Tenancy consente ai fornitori di servizi gestiti 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 permettono ai fornitori di servizi di soddisfare meglio le esigenze dei loro clienti e di migliorare. Ecco le ultime funzioni MSP introdotte in NAKIVO Backup & Replication:



Console MSP

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

Gli MSP possono aggiungere clienti con implementazioni di NAKIVO Backup & Replication standalone come tenant remoti nella loro implementazione multi-tenant della soluzione. Ciò consente loro di gestire e monitorare le attività di protezione dei dati di tutti i tenant, sia remoti che locali, con facilità da una dashboard MSP unificata.

Dashboard di panoramica dei tenant

Abbiamo integrato la Console MSP con una nuova dashboard che fornisce una panoramica di alto livello di tutti i tenant gestiti in un'unica posizione. Il Dashboard di panoramica del tenant offre approfondimenti e avvisi in tempo reale sulle infrastrutture di protezione dei dati dei clienti, tra cui 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.

Questa dashboard dinamica vi guida a risparmiare tempo sulle attività di routine di gestione dei tenant, a risolvere problemi e colli di bottiglia in modo efficiente e a ottimizzare l'allocazione delle risorse e delle licenze.

Connessione diretta

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

Connessione diretta per gli MSP

Con Connessione diretta per gli MSP, è possibile stabilire una connessione sicura agli ambienti dei tenant senza la necessità di porte aperte da parte di questi ultimi. La funzione supporta le seguenti piattaforme per la gestione e la protezione dei dati in remoto:

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

Connetti per gli MSP supporta anche i flussi di lavoro di Ripristino di emergenza per consentire un rapido ripristino dei carichi di lavoro dei tenant in scenari di emergenza.

Monitoraggio IT

Tenere traccia dell'utilizzo delle risorse nell'Infrastruttura VM è fondamentale per ottimizzare le prestazioni delle VM e prevenire i colli di bottiglia. Il NAKIVO Monitoraggio per VMware consente di:

- Monitoraggio dell'utilizzo di CPU, RAM e disco dei VMware vSphere host e VM e degli archivi dati.
- Creare e configurare avvisi personalizzati attivati da varie metriche per host, VM e archivi dati.
- Ricevete diversi tipi di report sugli elementi monitorati di vSphere nella vostra infrastruttura, direttamente nella vostra casella di posta.

Integrazione dei Dispositivi di storage aziendale

L'approccio completo di NAKIVO consente di creare una strategia versatile di storage di backup ibrido e multi-cloud, integrando perfettamente appliance di deduplicazione e soluzioni di storage sul cloud, onsite e cloud. Ecco le novità nelle funzionalità di storage di NAKIVO Backup & Replication.

Storage immutabile su NEC HYDRAstor

NAKIVO Backup & Replication supporta NEC HYDRAstor come destinazione di backup tra le altre appliance di deduplicazione.

È ora possibile abilitare l'immutabilità per i backup che risiedono sullo storage di NEC HYDRAstor 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 effettuare backup e repliche direttamente dagli snapshot di storage.

È possibile eseguire il backup e la replica per VMware vSphere hostato su HPE 3PAR, HPE Nimble, HPE Primera e HPE Alletra Storage appliance oltre agli array di storage NetApp FAS e NetApp AFF, direttamente da snapshot di storage invece che da normali snapshot di VM, per risparmiare tempo e ridurre il carico dell'infrastruttura.

Storage sul cloud

Con l'affermarsi del cloud ibrido (che mescola infrastrutture cloud private e pubbliche), le aziende possono 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 ad esempio Amazon S3, Wasabi, BLOB di Azure e Backblaze B2 che offriva uno storage di backup immutabile per le esigenze di backup e ripristino con un'opzione di immutabilità per proteggere i backup dalle infezioni da ransomware.

Storage di oggetti compatibile con S3

NAKIVO Backup & Replication ha introdotto il supporto per storage a oggetti compatibile con S3 per i repository di backup, offrendo agli utenti un'ulteriore opzione per l'archiviazione dei dati di backup. Consente di archiviare i backup in storage compatibili con l'API S3 e di scegliere tra una serie di piattaforme economiche adatte alle proprie esigenze.

Inoltre, i backup in storage compatibile con S3 possono essere configurati come immutabili, offrendo protezione dagli attacchi ransomware e dalla cancellazione accidentale.

Ripristino diretto da storage su nastro per VM

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

Con il nuovo ripristino diretto della VM da nastro i clienti possono eseguire ripristini rapidi senza la necessità di un repository di staging. Possono ripristinare VM complete, istanze di EC2 e macchine fisiche come VMware direttamente dai backup archiviati su nastro nella loro infrastruttura.

Banche dati

NAKIVO Backup & Replication supporta da molto tempo backup per Oracle Database e il suo ripristino tramite la funzionalità nativa di RMAN.

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

Miglioramenti dei componenti della soluzione principale

NAKIVO è costantemente impegnata a migliorare i componenti e le capacità della soluzione per semplificare e ottimizzare le attività di protezione dei dati per i nostri clienti. Ognuno di questi miglioramenti contribuisce a rendere la protezione dei dati più affidabile ed efficiente. La sezione seguente evidenzia i principali miglioramenti apportati a NAKIVO Backup & Replication:

Crittografia dei backup

La funzione Crittografia dei backup consente di crittografare i backup all'origine prima che vengano trasmessi in rete alla destinazione di storage. I backup crittografati possono essere archiviati in cartelle locali, piattaforme di 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 supportate da NAKIVO Backup & Replication. È anche possibile crittografare i backup automatici che contengono le configurazioni del sistema di protezione dei dati. Per crittografare e decrittografare i dati è obbligatoria una password e la funzione supporta anche l'integrazione con AWS KMS come meccanismo per garantire la protezione dalla perdita della password.

Repository federato

Il Federated Repository è un tipo di repository di backup federato 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 agisce come un pool di storage espandibile composto da più repository indipendenti, chiamati "membri". È possibile espandere un Repository federato in modo rapido e semplice, aggiungendo nuovi membri per contenere più dati. Non sono obbligatorie configurazioni complesse per aggiungere o rimuovere membri: il processo richiede solo pochi clic. In un Repository di backup federato, le operazioni di backup e ripristino continuano senza interruzioni anche se uno dei repository membri si guasta o esaurisce lo spazio, purché sia disponibile un altro membro utilizzabile.

Notifiche granulari

Granular Notifications è un miglioramento delle funzionalità di tracciamento dei flussi di lavoro, che offre una maggiore visibilità sui lavori di backup e replica in corso. Durante l'esecuzione di un lavoro, 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 tenervi informati sull'avanzamento del lavoro.

Scansione dei backup per rilevare eventuali malware

La scansione dei backup per rilevare i malware e ransomware prima del ripristino per prevenire le infezioni nella vostra Infrastruttura. Integrare la soluzione con Windows Defender, ESET NOD32 e Sophos per eseguire una scansione dei backup per rilevare i malware e garantire che i backup possano essere utilizzati in modo sicuro per il ripristino. Se viene rilevato un malware, scegliere di non eseguire il ripristino o di ripristinare in una rete isolata.

Indicizzazione del file system

Create un indice di tutti i file e le cartelle dei backup di VMware e Hyper-V e trovate facilmente un file o una cartella specifica per risparmiare tempo durante i ripristini granulari. Per ripristinare un file o una cartella, è sufficiente utilizzare la Ricerca globale per trovarlo nell'indice.

Transporter universale

Utilizzate un unico transporter universale per gestire server fisici, macchine fisiche, dispositivi a nastro e Oracle Database tramite RMAN che risiede sullo stesso host.

Supporto per Debian

Installate la soluzione direttamente sui sistemi operativi Debian e/o proteggete le vostre macchine fisiche basate su OS Debian. Crea backup coerenti con le

applicazioni e incrementali di macchine fisiche con Debian 10.1 e fino a Debian 11.6.

Impostazioni semplificate di conservazione del backup

Configurate le pianificazioni dei lavori e le impostazioni di conservazione in un unico passaggio e in un'unica visualizzazione. Specificate le impostazioni di conservazione per ogni pianifica all'interno di un lavoro di backup o di replica e impostate le date di scadenza dei punti di ripristino per un controllo più granulare.

Agente persistente

Implementazione di un agente Agente persistente sulle VM per l'elaborazione dei guest. Accedete alle VM senza inserire credenziali per semplificare l'amministrazione ed evitare problemi di sicurezza.

Priorità del lavoro

Impostare il livello di priorità nella coda per i lavori di backup critici da elaborare per primi e garantire che vengano completati in tempo. Assegnate livelli di priorità da 1 a 5, di cui uno è il più alto, per garantire che i lavori ad alta priorità ricevano le risorse necessarie per la soluzione non appena disponibili.

Unire i lavori

Gestisci 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. Mantenete i 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

Ottenete l'accesso immediato alla serie completa di funzioni di NAKIVO Backup & Replication per 15 giorni con un solo clic, indipendentemente dalla vostra edizione della soluzione.

Pronto per iniziare?

PROVA GRATUITAMENTE

OTTIENI UNA DEMO GRATUITA

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