Novità in NAKIVO Backup per VMware

Sommario

INTRODUZIONE

NAKIVO Backup & Replication offre funzionalità all-in-one di backup, ripristino istantaneo, protezione dai ransomware e ripristino di emergenza per salvaguardare gli ambienti VMware dagli effetti della perdita di dati e delle minacce informatiche.

FUNZIONI E MIGLIORAMENTI PIÙ RECENTI

Il panorama delle minacce informatiche è in costante evoluzione e crea frequenti cambiamenti nelle esigenze di protezione dei dati. Per aiutare le aziende ad adattare le loro strategie di backup e ripristino di emergenza, NAKIVO rilascia costantemente aggiornamenti che introducono nuove funzioni di protezione dei dati e migliorano le funzionalità esistenti.

Da gennaio 2023, abbiamo lanciato otto nuove versioni di NAKIVO Backup & Replication con vari strumenti di backup e anti-ransomware per proteggere i dati critici negli ambienti VMware. Di seguito viene riportata una panoramica delle ultime aggiunte fino alla versione 11.0.4.

Aggiornamenti del supporto di VMware vSphere

NAKIVO continua ad essere leader con il supporto precoce per le ultime versioni di VMware vSphere, guidando i clienti a mantenere una protezione ininterrotta durante ogni upgrade.

Siamo stati tra i primi vendor di backup a fornire il supporto completo per vSphere 8.0 GA, seguito dal supporto per le successive release di VMware, tra cui vSphere 8.0 U2, vSphere 8.0U2b, vSphere 8.0U2c e vSphere 8.0U3.

Ora, con l'ultima versione v11.0.4, abbiamo esteso il supporto di compatibilità a VMware vSphere 9, garantendo un supporto continuo per il backup e il ripristino degli ambienti con l'ultima release di VMware.

Crittografia dei backup all'origine

NAKIVO Backup & Replication consente di crittografare i backup all'origine prima che vengano trasferiti in rete alla destinazione di storage.

I backup crittografati possono essere archiviati in cartelle locali, Piattaforme cloud pubbliche (Amazon S3, Wasabi, BLOB di Azure, Backblaze B2), destinazioni di storage compatibili con S3e condivisioni di rete SMB/NFS, Nastrie appliance di deduplicazione. Per decrittografare i dati di backup è obbligatoria una password e la funzione supporta anche l'integrazione con AWS KMS come dispositivo di sicurezza in caso di perdita delle chiavi di decrittografia.

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, poiché 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.

Backup dagli snapshot di storage NetApp

NAKIVO ha aggiunto gli array di storage NetApp FAS e NetApp AFF all'elenco dei dispositivi di storage supportati da Backup dallo snapshot di storage funzione. Il backup di VMware direttamente dagli snapshot di storage invece che dai normali snapshot di VM riduce l'impatto delle operazioni di backup di VM sulle risorse e sulle prestazioni dell'ambiente di produzione.

Dashboard di panoramica dei tenant

Abbiamo ampliato la Console MSP con il Dashboard di panoramica dei tenant, che offre una panoramica di alto livello di tutti i tenant gestiti in un'unica posizione.

Da questa dashboard dinamica è possibile visualizzare in tempo reale informazioni e avvisi 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.

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.

Notifiche granulari

Le notifiche granulari migliorano le funzionalità di tracciamento dei flussi di lavoro, offrendo una maggiore visibilità sui lavori di backup e replica in corso. Mentre un lavoro è in esecuzione, 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.

Indicizzazione del file system

L'Indicizzazione dei file system si basa sulle capacità esistenti di Ricerca Globale per creare un indice di tutti i file e cartelle dei backup della VM. Di conseguenza, quando si esegue il ripristino granulare per ripristinare uno o più file o cartelle, è possibile utilizzare la Ricerca globale per individuare rapidamente gli elementi obbligatori, risparmiando tempo prezioso nel processo.

Avvisi e reportistica per il monitoraggio IT

Con allarmi e reportistica per Monitoraggio ITè possibile creare e configurare avvisi personalizzati che vengono attivati quando si verificano condizioni specifiche.

Gli allarmi hanno diverse funzioni, tra cui il rilevamento proattivo di attività insolite che potrebbero segnalare un comportamento dannoso, ad esempio quando l'utilizzo della CPU supera improvvisamente i livelli normali. Grazie alla funzionalità di reporting, è possibile visualizzare, esportare ed e-mail vari dettagli sugli elementi VMware vSphere monitorati nella vostra infrastruttura.

Backup dagli snapshot di storage HPE Alletra e HPE Primera

NAKIVO ha aggiunto HPE Alletra e HPE Primera all'elenco dei dispositivi di storage supportati per la funzione Backup dallo snapshot di storage. È possibile eseguire il backup delle VMware vSphere memorizzate su questi dispositivi di storage in modo più efficiente utilizzando snapshot dello storage invece dei normali snapshot della VM.

Replica in tempo reale (Beta) per VMware

Replica in tempo reale (Beta) per VMware è una potente aggiunta alle funzionalità di ripristino di emergenza di NAKIVO Backup & Replication.

È possibile creare repliche in tempo reale di VMware vSphere e impostarle in modo che vengano continuamente aggiornate con le modifiche dei dati che avvengono nelle VM di origine. Le modifiche ai dati della VM di origine vengono

elaborate in tempo reale con velocità di aggiornamento (e obiettivi di punto di ripristino) a partire da 1 secondo, il che garantisce la disponibilità continua di macchine e dati critici.

Replica in tempo reale (Beta) per VMware: compatibilità con vSphere 9.0

NAKIVO ha esteso la portata di Replica in tempo reale (Beta) per VMware a vSphere 9.0, consentendo di mantenere ininterrotti i flussi di lavoro di replica durante l'upgrade dell'ambiente VMware.

Scansione dei backup per rilevare eventuali malware

Il Scansione dei malware del backup per rilevare i malware è un'importante aggiunta alle funzioni di protezione dai ransomware di NAKIVO Backup & Replication. Grazie a questa funzione, è possibile eseguire la scansione dei backup per rilevare i malware e i ransomware prima di eseguire il ripristino, al fine di prevenire le infezioni nella vostra infrastruttura.

È possibile integrare la soluzione con Windows Defender, ESET NOD32 e Sophos per eseguire scansioni dei malware e garantire che i backup possano essere utilizzati in modo sicuro per il ripristino. Se durante la scansione viene rilevato un malware, è possibile scegliere se fallire il lavoro di ripristino o utilizzare una rete isolata come destinazione del ripristino.

Ripristino diretto da nastro

Con Ripristino diretto da nastroè possibile ripristinare macchine virtuali complete e istanze di Amazon EC2 direttamente sulla vostra infrastruttura da backup completi archiviati su nastri.

L'approccio di ripristino diretto migliora i tempi di ripristino e l'efficienza. Oltre a VMware vSphere, le piattaforme supportate includono Microsoft Hyper-V, Nutanix AHV e Amazon EC2, oltre ai carichi di lavoro fisici tramite Physical-to-Virtual Recovery.

Supporto per lo storage di oggetti compatibile con S3

L'espansione delle capacità di archiviazione ibrida dei backup di NAKIVO Backup & Replication, il supporto per lo storage in storage compatibile con S3, consente di archiviare i backup in destinazioni di archiviazione locali e basate su cloud che utilizzano l'API S3.

È possibile scegliere da una serie di destinazioni di storage compatibili con S3 che si adattano alle esigenze e al budget dell'organizzazione. Inoltre, è possibile abilitare l'immutabilità per i punti di ripristino archiviati in ubicazioni di storage compatibili con S3 per proteggersi dalle infezioni da ransomware, dalle cancellazioni accidentali e da altre modifiche indesiderate.

Agente VM permanente

Con l'aggiunta della funzione Agente permanente per VM in NAKIVO Backup & Replication, è possibile implementare un agente persistente su VMware vSphere per ottimizzare l'elaborazione del guest senza la necessità di fornire le credenziali del sistema operativo.

Utilizzando agenti persistenti, la soluzione comunica con le VM di destinazione su un'unica porta, garantendo l'allineamento con i criteri di sicurezza che vietano la condivisione delle credenziali del sistema operativo e di altre informazioni sensibili.

BACKUP DI NAKIVO PER VMWARE: FUNZIONALITÀ PRINCIPALI

NAKIVO Backup & Replication offre un rapido backup agentless, un ripristino istantaneo per VM e granulare e una protezione dai ransomware a più livelli per garantire la protezione e la recuperabilità dei dati nell'ambiente VMware. Di seguito una panoramica delle funzioni e delle funzionalità più importanti per il backup, il ripristino di emergenza, la protezione dai ransomware, la sicurezza e la conformità e l'amministrazione:

Backup

- **Backup incrementale:** Eseguire backup incrementali rapidi ed efficienti utilizzando la funzione tracciamento nativo dei blocchi modificati di VMware per elaborare solo i blocchi di dati modificati in ogni lavoro di backup.
- **Elaborazione coerente con le applicazioni:** Assicura che i dati di backup per le diverse applicazioni (Microsoft Exchange Server, Active Directory, SQL Server, ecc.) e i database siano coerenti dal punto di vista delle transazioni e pronti per un rapido ripristino.
- **Storage di backup ibrido:** Applica la strategia di backup 3-2-1 inviando backup e copie di backup a cartelle locali, condivisioni di rete NFS/SMB, piattaforme cloud pubbliche (Amazon S3, Wasabi, BLOB di Azure, Backblaze B2), target di storage a oggetti compatibili con S3, nastro e appliance di deduplicazione.
- **Verifica istantanea:** Automatizzare la verifica istantanea dei backup e delle repliche di VMware vSphere utilizzando uno dei due metodi integrati per garantire la ripristinabilità.

Ripristino di emergenza

- **Ripristino istantaneo delle VM:** Avvio di VM complete direttamente da backup per VMware vSphere per riprendere le operazioni in pochi secondi grazie a Avvio flash delle VM.
- **Ripristino istantaneo e granulare:** Ripristino di singoli file e di oggetti applicativi con tutte le autorizzazioni e oggetti di applicazioni con tutte le autorizzazioni nella loro ubicazione originale o su un nuovo computer con pochi clic.
- **Replica efficiente:** Creare repliche da macchine virtuali da VM di origine o da backup esistenti per garantire la disponibilità e la continuità operativa in caso di guasti.
- **Ripristino dell'ambiente:** Creare sequenze autogestite per i test di failback, failover e ripristino di emergenza pianificati o di emergenza e lanciarli con un solo clic.
- **Ripristino multipiattaforma:** Ripristina le VM di VMware vSphere come VM di Microsoft Hyper-V e viceversa esportando i backup. esportando i backup in diversi formati di disco virtuale per semplificare la gestione multipiattaforma.
- **Ripristino da fisico a virtuale (P2V):** Avvio istantaneo di macchine fisiche Windows e Linux macchine fisiche Windows e Linux da backup come VMware vSphere VM. con tempi di inattività minimi, quindi ripristinare le VM da utilizzare nell'ambiente di produzione.

Protezione dai ransomware

- **Storage locale immutabile:** Invio dei backup a a prova di ransomware Repository locali a prova di ransomware per evitare la crittografia e altre modifiche indesiderate.
- **Storage immutabile sul cloud:** Abilita l'immutabilità immutabile per tramite S3 Object Lock per i dati di backup in BLOB di Azure, in piattaforme pubbliche di storage sul cloud (Amazon S3, Wasabi, BLOB di Azure, Backblaze B2) per proteggersi dalle infezioni da ransomware.
- **Backup con protezione air-gap:** Archiviare le copie di backup di VMware vSphere offline su unità scollegate, come i nastri, per un ulteriore livello di protezione dai ransomware.

Sicurezza e conformità

- **Autenticazione a due fattori (2FA):** Aggiungete un livello di sicurezza con i codici una tantum generati tramite Google Authenticator per salvaguardare le vostre attività di protezione dei dati.
- **Controllo degli accessi basato sui ruoli (RBAC):** Assegnazione di ruoli preimpostati e personalizzati con diritti e autorizzazioni associati per impedire l'accesso non autorizzato ai backup di VMware vSphere.

- **Conservazione flessibile:** Salvate fino a 10.000 punti di ripristino per ogni backup di VMware vSphere e ruotateli su base giornaliera, settimanale, mensile, annuale o periodica.
- **Backup nativo su nastro:** Invio dei dati di backup di VMware vSphere direttamente alle librerie su nastro fisiche e virtuali per un'archiviazione sicura a lungo termine.

Amministrazione

- **Interfaccia web:** Gestite tutte le attività di backup e ripristino da un'interfaccia web facile da usare, con comodi dashboard e procedure guidate passo-passo.
- **Dashboard di calendario:** Visualizza e gestisce tutti i lavori passati, attuali e futuri in un semplice calendario. semplice calendario. Pianifica facilmente i lavori di backup di VMware vSphere ed evita le sovrapposizioni di pianificazione.
- **Ricerca globale:** Cerca e individua rapidamente qualsiasi file o cartella necessaria per garantire un ripristino efficiente e accurato.
- **Protezione dei dati basata sui criteri:** Creare regole di regole di criterio personalizzate per aggiungere o rimuovere automaticamente VM nei lavori di protezione dei dati man mano che l'ambiente cresce e cambia.
- **Concatenamento dei lavori:** Collegare i lavori di backup e copia di backup per automatizzare i flussi di lavoro. automatizzare i flussi di lavoroaumentare l'efficienza e risparmiare tempo nell'amministrazione dei backup.
- **Integrazione API HTTP:** Integrazione di NAKIVO Backup & Replication con soluzioni di monitoraggio, automazione e orchestrazione senza soluzione di continuità tramite API HTTP.
- **Incremento delle prestazioni:** Gestite la velocità di trasferimento dei dati e scaricate le risorse di produzione con Accelerazione di rete, Trasferimento dei dati senza LAN, Backup dagli snapshot di storage e Limitazione della larghezza di banda per ridurre le finestre di backup e minimizzare l'impatto sulle operazioni principali.
- **Implementazione flessibile:** Installate la soluzione in pochi minuti su Windows, Linux, NAS o come AMI VA o AWS.
- **Backup automatico:** Eseguire il backup e ripristinare la configurazione del sistema NAKIVO Backup & Replication configurazione del sistema (lavori, inventario, registri, impostazioni, ecc.) da un'unica interfaccia.

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