

Novedades en NAKIVO Backup para VMware



Contenido

Introducción	3
Últimas funciones y mejoras	3
Actualizaciones de soporte de VMware vSphere	3
Cifrado de los backups del lado de origen	3
Federated Repositorio	3
Backup desde instantáneas del almacenamiento de NetApp	3
Tenant Overview Dashboard	4
Almacenamiento inmutable en NEC HYDRAsTOR	4
Notificaciones granulares	4
Indexación del sistema de archivos	4
Alarmas e informes para la supervisión de TI	4
Backup desde instantáneas del almacenamiento de HPE Alletra y HPE Primera	4
Replicación en tiempo real (beta) de VMware	5
Análisis de malware en los backups	5
Recuperación directa desde cintas	5
Soporte de almacenamiento de objetos compatible con S3	5
Agente de máquina virtual permanente	5
NAKIVO Backup de VMware: Capacidades principales	6
Backups	6
Recuperación ante desastres	6
Protección contra ransomware	6
Seguridad y cumplimiento	7
Administración	7

INTRODUCCIÓN

NAKIVO Backup & Replication ofrece funciones todo en uno de backup, restauración instantánea, protección contra el ransomware y recuperación ante desastres para proteger los entornos VMware contra los efectos de la pérdida de datos y las ciberamenazas.

ÚLTIMAS FUNCIONES Y MEJORAS

El panorama de las amenazas informáticas está en constante cambio, lo que genera frecuentes modificaciones en las necesidades de protección de datos. Para ayudar a las organizaciones a adaptar sus estrategias de backup y recuperación ante desastres, NAKIVO hace constantes actualizaciones que introducen nuevas funciones de protección de datos y mejoran las capacidades existentes.

Desde enero de 2023, hemos lanzado ocho nuevas versiones de NAKIVO Backup & Replication con varias herramientas de backup y antirransomware para proteger los datos críticos en entornos VMware. A continuación se describen las últimas novedades hasta la versión 11.0.4.

Actualizaciones de soporte de VMware vSphere

NAKIVO continúa a la cabeza con soporte anticipado para las últimas versiones de VMware vSphere, ayudando a los clientes a mantener una protección ininterrumpida a través de cada actualización.

Fuimos de los primeros proveedores de backups en ofrecer compatibilidad total con vSphere 8.0 GA, seguida de compatibilidad con las versiones posteriores de VMware, incluidas vSphere 8.0 U2, vSphere 8.0U2b, vSphere 8.0U2c y vSphere 8.0U3.

Ahora, con la última versión 11.0.4, hemos ampliado el soporte de compatibilidad para incluir VMware vSphere 9, garantizando un soporte continuo de backups y recuperación para los entornos que ejecutan la última versión de VMware.

Cifrado de backups en el origen

NAKIVO Backup & Replication permite cifrar los backups en el origen antes de que se transfieran por la red a su destino de almacenamiento.

Los backups cifrados pueden almacenarse en carpetas locales, [plataformas públicas en la nube](#) (Amazon S3, Wasabi, Azure Blob, Backblaze B2), [destinos de almacenamiento compatibles con S3](#) y recursos compartidos de red SMB/NFS, [cintasy appliance de deduplicación](#). Se requiere una contraseña para descifrar los datos de backups, y la función también admite la integración con AWS KMS como dispositivo a prueba de fallos en caso de que pierda las claves de descifrado.

El repositorio federado

El Repositorio Federado es un tipo de repositorio de backups fácilmente ampliable y flexible que resuelve los cuellos de botella en cuanto a rendimiento y complejidad en grandes entornos con grandes conjuntos de datos.

Un Repositorio Federado actúa como un conjunto de almacenamiento ampliable compuesto por múltiples repositorios independientes, denominados "miembros". Puede ampliar un Repositorio Federado de forma rápida y sencilla añadiendo nuevos miembros para albergar más datos. No se requieren configuraciones complejas para añadir o eliminar miembros, ya que el proceso sólo requiere unos pocos clics. En un repositorio federado, las operaciones de backup y recuperación continúan sin interrupción aunque uno de los repositorios miembro falle o se quede sin espacio, siempre que haya otro miembro utilizable disponible.

El backup desde instantáneas del almacenamiento NetApp

NAKIVO ha añadido las matrices de almacenamiento NetApp FAS y NetApp AFF a la lista de dispositivos de almacenamiento compatibles con la aplicación [Backups desde instantáneas del almacenamiento](#) de almacenamiento. Hacer backups de

máquinas virtuales de VMware directamente desde instantáneas del almacenamiento, en lugar de las instantáneas de máquinas virtuales habituales, reduce el impacto de las operaciones de backup de máquinas virtuales en los recursos y el rendimiento de su entorno de producción.

El panel de control de inquilinos

Hemos ampliado la [consola para MSP](#) con el panel de control Visión general de inquilinos, que proporciona una visión general de alto nivel de todos los inquilinos gestionados en un solo lugar.

De este panel dinámico, puede ver en tiempo real información y alertas sobre las infraestructuras de protección de datos de sus clientes, incluido el estado de los nodos, los recursos disponibles, las actividades programadas y la información de inventario. Los MSP pueden ordenar, filtrar y buscar en la lista de inquilinos para extraer los datos necesarios, identificar problemas pendientes y aplicar acciones masivas.

Almacenamiento inmutable en NEC HYDRAsTOR

NAKIVO Backup & Replication soporta [NEC HYDRAsTOR](#) como destino de almacenamiento de backups entre otros appliance de deduplicación.

Ahora puede activar la inmutabilidad de los backups que residen en su sistema de almacenamiento NEC HYDRAsTOR para protegerlos contra ataques de ransomware, borrados accidentales y otras formas de modificación no deseada.

Las notificaciones granulares

Las notificaciones granulares mejoran las capacidades de seguimiento del flujo de trabajo, lo que le proporciona una mayor visibilidad de los jobs de backup y replicación en ejecución. Mientras se ejecuta un job, NAKIVO Backup & Replication muestra descripciones de las acciones en curso, como la transferencia de datos o el truncamiento de registros. Las actualizaciones de estado se producen en tiempo real para mantenerle informado a medida que avanza el job.

Indexación del sistema de archivos.

La indexación del sistema de archivos se basa en las capacidades existentes de la [búsqueda global](#) para crear un índice de todos los archivos y carpetas de sus backups de máquina virtual. En consecuencia, cuando realice una recuperación granular para restaurar uno o varios Archivos o carpetas, puede utilizar la búsqueda global para localizar rápidamente los elementos necesarios, ahorrando un valioso tiempo en el proceso.

Alarmas e informes para IT Monitoring

Con alarmas e informes para [supervisión del entorno](#) puede crear y configurar alertas personalizadas que se activan cuando se cumplen determinadas condiciones.

Las alarmas tienen varios usos, incluida la detección proactiva de actividades inusuales que podrían indicar un comportamiento malicioso, como cuando el uso de la CPU supera repentinamente los niveles normales. Con las funciones de elaboración de informes, puede ver, exportar y enviar por correo electrónico diversos detalles sobre los elementos supervisados de VMware vSphere en su infraestructura.

Backup desde instantáneas del almacenamiento HPE Alletra y HPE Primera

NAKIVO ha añadido HPE Alletra y HPE Primera a la lista de dispositivos de almacenamiento compatibles para la función backup desde instantáneas del almacenamiento. Puede hacer backup de sus máquinas virtuales de VMware vSphere almacenadas en estos dispositivos de almacenamiento de forma más eficiente utilizando instantáneas de almacenamiento en lugar de instantáneas de máquinas virtuales normales.

Replicación en tiempo real (Beta) para VMware

[Replicación en tiempo real \(beta\) de VMware](#) es una potente adición a las capacidades de recuperación ante desastres de NAKIVO Backup & Replication.

Puede crear réplicas en tiempo real de máquinas virtuales VMware vSphere y configurarlas para que se actualicen continuamente con los cambios de datos que se produzcan en las máquinas virtuales de origen. Los cambios en los datos de la máquina virtual de origen se procesan en tiempo real con velocidades de actualización (y objetivos de punto de recuperación) tan bajas como 1 segundo, lo que garantiza la disponibilidad continua de máquinas y datos críticos.

Replicación en tiempo real (beta) de VMware: compatibilidad con vSphere 9.0

NAKIVO ha ampliado el alcance de Replicación en tiempo real (beta) de VMware para cubrir vSphere 9.0, lo que le permite mantener flujos de trabajo de replicación ininterrumpidos a medida que actualiza su entorno VMware.

Análisis de malware en los backups

El [Análisis de malware en los backups](#) es una importante función que se añade a las capacidades de protección contra el ransomware de NAKIVO Backup & Replication. Con esta función, puede analizar los backups en busca de malware y ransomware antes de hacer la recuperación para evitar infecciones en su infraestructura.

Puede integrar la solución con Windows Defender, ESET NOD32 y Sophos para ejecutar análisis de malware y garantizar que los backups puedan utilizarse de forma segura para la recuperación. Si se detecta malware durante un escaneo, puede elegir entre suspender el job de recuperación o utilizar una red aislada como destino de la recuperación.

Recuperación directa desde cinta

Con [Direct Recovery De Cinta](#) puede recuperar máquinas virtuales completas e instancias de Amazon EC2 directamente en su infraestructura a partir de backups almacenados en soportes de cinta.

El método de restauración directa mejora los tiempos de recuperación y la eficacia. Además de VMware vSphere, las plataformas compatibles incluyen Microsoft Hyper-V, Nutanix AHV y Amazon EC2, además de cargas de trabajo físicas mediante la recuperación de físico a virtual.

Soporte de almacenamiento de objetos compatible con S3

Ampliando las capacidades de almacenamiento de backups híbridos de NAKIVO Backup & Replication, el soporte de almacenamiento de objetos compatible con S3 permite hacer backups en destinos de almacenamiento locales y en la nube que emplean la API S3.

Puede elegir entre una variedad de destinos de almacenamiento compatibles con S3 que se ajusten a las necesidades y al presupuesto de su organización. Además, puede habilitar la inmutabilidad para los puntos de recuperación almacenados en ubicaciones de almacenamiento compatibles con S3 para protegerse contra infecciones de ransomware, eliminaciones accidentales y otras modificaciones no deseadas.

Agente de máquina virtual permanente

Con la incorporación de la función Permanent VM Agent en NAKIVO Backup & Replication, puede instalar un agente persistente en las máquinas virtuales de VMware vSphere para agilizar el procesamiento de invitados sin necesidad de proporcionar credenciales del sistema operativo.

Mediante el uso de agentes persistentes, la solución se comunica con las máquinas virtuales de destino a través de un único puerto, lo que garantiza el cumplimiento de las políticas de seguridad que prohíben compartir las credenciales del sistema operativo y otra información confidencial.

NAKIVO BACKUP DE VMWARE: CAPACIDADES PRINCIPALES

NAKIVO Backup & Replication ofrece copias de seguridad rápidas sin agentes, recuperación instantánea de máquinas virtuales y granular, y protección multicapa contra el ransomware para garantizar que los datos de su entorno VMware estén protegidos y sean recuperables. A continuación se ofrece un resumen de las funciones y capacidades más destacadas para hacer backups, recuperación ante desastres, protección contra el ransomware, seguridad y cumplimiento de normativas, y administración:

Recuperación

- **Backups incrementales:** Ejecuta backups incrementales rápidos y eficientes utilizando el sistema de [seguimiento de cambios nativo de VMware](#) para procesar sólo los bloques de datos modificados en cada ejecución de job de backups.
- **Procesamiento App-aware:** Garantiza que los datos de backup de las distintas aplicaciones (Microsoft Exchange Server, Active Directory, SQL Server, etc.) y bases de datos sean coherentes desde el punto de vista transaccional y estén listos para una rápida recuperación.
- **Almacenamiento híbrido de backups:** Aplicar la estrategia de copia de seguridad 3-2-1 enviando backups y copias de seguridad a carpetas locales, recursos compartidos de red NFS/SMB, plataformas de nube pública (Amazon S3, Wasabi, Azure Blob, Backblaze B2), objetivos de almacenamiento de objetos compatibles con S3, cintas y appliance de deduplicación.
- **Verificación instantánea:** Automatice la [verificación instantánea](#) de los backups y réplicas de máquinas virtuales de VMware vSphere mediante uno de los dos métodos integrados para garantizar la recuperabilidad.

Recuperación ante desastres

- **Recuperación instantánea de máquinas virtuales:** Arranque máquinas virtuales completas directamente desde backups de VMware vSphere para reanudar sus operaciones en cuestión de segundos utilizando [Inicio rápido de máquinas virtuales](#).
- **Recuperación granular instantánea:** [Restaura archivos individuales](#) y objetos de aplicación con todos los permisos a su ubicación original o a un nuevo equipo con unos pocos clics.
- **Replicación eficaz:** [Cree réplicas](#) a partir de máquinas virtuales de origen o de backups existentes para garantizar la disponibilidad y la continuidad operativa en caso de fallos.
- **Restauración del entorno:** Crear [secuencias autoejecutables](#) para pruebas de conmutación por error, conmutación por recuperación y recuperación ante desastres planificadas o de emergencia, y ejecútelas con un solo clic.
- **Recuperación entre plataformas:** Recupere máquinas virtuales de VMware vSphere como máquinas virtuales de Microsoft Hyper-V y viceversa mediante [exportando backups](#) en distintos formatos de disco virtual para agilizar la gestión multiplataforma.
- **Recuperación de físico a virtual:** Arranque instantáneo de máquinas físicas Windows y Linux [máquinas físicas a partir de backups como VM de VMware vSphere](#) con un tiempo de inactividad mínimo y, a continuación, restaure las máquinas virtuales para utilizarlas en su entorno de producción.

Protección antirransomware

- **Almacenamiento local inmutable:** Envío de backups a [a prueba de ransomware](#) a prueba de ransomware para evitar el cifrado por ransomware y otras modificaciones no deseadas.

- **Almacenamiento en la nube inmutable:** Habilite [inmutabilidad](#) mediante S3 Object Lock para hacer backups de los datos almacenados en plataformas de almacenamiento en la nube públicas (Amazon S3, Wasabi, Azure Blob, Backblaze B2) para protegerlos contra la infección por ransomware.
- **Backups aislados de la red:** Almacene copias de backup de VMware vSphere VM sin conexión en unidades desconectables, como cintas, para obtener una capa adicional de protección contra el ransomware.

Seguridad y cumplimiento

- **Autenticación de dos factores (2FA):** Añada una capa de seguridad con [códigos de un solo uso](#) generados a través de Google Authenticator para salvaguardar tus actividades de protección de datos.
- **Control de accesos basado en roles:** Asigne [roles preestablecidos y personalizados](#) con derechos y permisos asociados para evitar el acceso no autorizado a sus backups de VMware vSphere VM.
- **Retención flexible:** Guarde hasta 10 000 puntos de recuperación para cada backup de máquina virtual de VMware vSphere y rótelos de forma diaria, semanal, mensual, anual o periódica.
- **Backups nativos en cinta:** Envíe los datos de backup de VMware vSphere VM directamente a bibliotecas de cintas físicas y virtuales para archivarlos de forma segura a largo plazo.

Administración sencilla

- **Interfaz web:** De gestión de todas las actividades de backups y recuperación desde una interfaz web fácil de usar con cómodos paneles y asistentes paso a paso.
- **Panel de control Calendario:** Ver y gestionar todos los jobs pasados, actuales y futuros en un [sencilla vista de Calendario](#). Programe fácilmente los jobs de backups de máquinas virtuales de VMware vSphere y evite solapamientos en la programación.
- **Búsqueda global:** Localización rápida de archivos o carpetas para garantizar recuperaciones precisas y eficientes.
- **Protección de datos basada en políticas:** Cree [reglas de política personalizadas](#) para añadir o eliminar automáticamente máquinas virtuales en jobs de protección de datos a medida que su entorno crece y cambia.
- **Encadenamiento de jobs:** Enlaza jobs de backups y copias de backups para [automatizar los flujos de trabajo](#) aumentar la eficacia y guardar tiempo en la administración de backups.
- **Integración API HTTP:** Integre NAKIVO Backup & Replication con soluciones de supervisión, automatización y orquestación sin problemas. [a través de la API HTTP](#).
- **Potenciadores del rendimiento:** Gestione la velocidad de transferencia de datos y descargue los recursos de producción con [Aceleración de la red](#), [transferencia de datos sin LAN](#) Backups desde instantáneas del almacenamiento, y [limitación del ancho de banda](#) para acortar las ventanas de backups y minimizar el impacto en las operaciones principales.
- **Instalación flexible:** Instale la solución en pocos minutos en Windows, Linux, NAS o como VA o AWS AMI.
- **Autobackup:** Haga backups y recupere su NAKIVO Backup & Replication. [configuración del sistema](#) (jobs, inventario, logs, ajustes, etc.) desde la misma interfaz unificada.