

Cómo pueden las empresas proteger y migrar cargas de trabajo entre servidores físicos, hipervisores y plataformas en la nube

Introducción

Todas las empresas necesitan una herramienta de copia de seguridad lo suficientemente flexible como para proteger todas sus plataformas físicas, virtuales y en la nube, y que permita una recuperación rápida y segura de cualquier carga de trabajo: ya sea en la misma plataforma, en un nuevo servidor desde cero, en un hipervisor diferente o en la nube, según sea necesario. Ese alto nivel de flexibilidad ofrece protección frente a desafíos habituales de TI, como cuando un proveedor tecnológico deja de satisfacer las necesidades de una organización.

El proveedor de hipervisores VMware ofrece un ejemplo reciente y significativo. Tras su adquisición por Broadcom en 2023, VMware centró su estrategia en el sector de grandes empresas, incrementó sus precios y modificó sus políticas de soporte para pequeñas empresas, proveedores de servicios gestionados (MSP) y distribuidores de valor añadido (VAR). Estas nuevas condiciones desfavorables llevaron a muchos clientes a buscar una plataforma de hipervisor alternativa.

En cualquier proceso de migración a nuevas plataformas, las opciones disponibles son numerosas, pero llegar a ellas de forma segura requiere una planificación cuidadosa y las herramientas adecuadas. Para protegerse como es debido, una empresa necesita poder replicar y mover sus cargas de trabajo con total libertad, no solo de un hipervisor a otro,

Los aumentos de precios y los cambios en las políticas de soporte han llevado a muchos clientes de VMware a buscar una nueva plataforma de hipervisor.



sino de cualquier servidor físico, hipervisor o plataforma en la nube a otra. Esta flexibilidad permite a una empresa:

- Minimizar el riesgo de migración, al permitir la reversión desde la nueva plataforma a la anterior en caso de que se produzcan problemas de rendimiento o de fiabilidad en el nuevo entorno.
- Mejorar su nivel de cumplimiento normativo, gracias a las funciones de copia de seguridad, recuperación y controles de auditoría coherentes en servidores físicos, hipervisores y nubes.
- Reforzar su estrategia de recuperación ante desastres mediante la replicación de aplicaciones y datos en la nube.
- Analizar las copias de seguridad en la nube para detectar malware y vulnerabilidades que no se hayan corregido mediante parches, y mitigar esos problemas antes de iniciar cualquier proceso de recuperación.
- Evitar depender de un solo proveedor, lo que permitiría mover las cargas de trabajo con total libertad a nuevas plataformas cuando sea necesario, por ejemplo, cuando un proveedor de hipervisores incrementa sus precios de renovación y soporte.

La solución óptima ofrece estas funciones en una plataforma de copia de seguridad unificada, lo que reduce los costes de licencias, formación, integración y soporte de TI.

Obstáculos al migrar cargas de trabajo hacia una nueva plataforma

Pongamos como ejemplo la migración de VMware a un nuevo hipervisor. Los pasos son sencillos: exportar la máquina virtual (VM), convertirla al formato del nuevo hipervisor e importarla en la nueva plataforma. Sin embargo, cada fase de esta transición introduce posibles desafíos y un riesgo acumulado: diferencias en los formatos de disco virtual, modelos de emulación de chipset, versiones de hardware virtual, pilas de controladores y capas de virtualización de red. Las plantillas de VM, las instantáneas y los volúmenes de almacenamiento adjuntos también se comportan de forma distinta. Los problemas de compatibilidad pueden no aparecer hasta que las cargas de trabajo están bajo carga de producción.

Los clientes que dejan atrás VMware para pasarse a nuevas plataformas suelen señalar algunos problemas serios: inestabilidad de las VM, errores de configuración de red, bajo rendimiento tras la conversión y la imposibilidad de revertir las cargas de trabajo completamente si algo falla. El proceso de migrar de un hipervisor a otro conlleva un riesgo real de convertirse en un incidente costoso y prolongado de tiempo de inactividad. Otros movimientos entre plataformas, como por ejemplo de un servidor físico a otro o de una máquina virtual a la nube, presentan riesgos similares.

Los usuarios de hipervisores cuentan con varias alternativas interesantes

Siguiendo con el ejemplo del cliente descontento de VMware que busca una estrategia de salida, el mercado ofrece múltiples hipervisores de gran calidad, entre ellos:

Microsoft Hyper-V / Azure Stack HCI

Una opción muy adecuada para empresas ya integradas en el ecosistema de Windows y Azure, que ofrece una estrecha integración con Active Directory, los servicios de seguridad de Azure y los modelos de licencia existentes de Microsoft.

Proxmox VE

Una plataforma de código abierto muy popular, con licencias transparentes, funciones de alta disponibilidad y una comunidad de usuarios activa.

Nutanix AHV

Ofrece virtualización, administración y almacenamiento simplificados bajo una plataforma unificada, con un modelo de suscripción previsible.

Scale Computing HC3

Una plataforma hiperconvergente optimizada para entornos perimetrales, como los que se utilizan en el comercio minorista, en el sector de la fabricación y en empresas con entornos multisitio, con un enfoque claro en la simplicidad.

Hay más entornos de virtualización disponibles en el mercado, como Citrix XenServer, Red Hat Virtualization y Linux KVM.

No obstante, el proceso de migrar desde VMware a cualquiera de estas alternativas —y, en realidad, de migrar cualquier carga de trabajo a una nueva plataforma física, virtual o de la nube— conlleva riesgos que las empresas deben anticipar y abordar antes de iniciar la transición.

Cómo mitigar el riesgo de migración con las herramientas adecuadas de protección de datos

Antes de iniciar una migración entre plataformas, las empresas deberían plantearse invertir en las herramientas adecuadas para ayudar a mitigar los posibles riesgos. Por ejemplo, una solución de copia de seguridad independiente de la plataforma puede actuar como un canal seguro desde VMware hacia Hyper-V, Proxmox, Nutanix o Scale Computing, o hacia alternativas sin hipervisor, como servidores físicos y plataformas en la nube. Una solución de copia de seguridad altamente flexible, capaz de importar una carga de trabajo desde cualquier origen y restaurarla en cualquier destino —de cualquier plataforma física, virtual o en la nube a cualquier otra plataforma física, virtual o en la nube— puede transformar una migración arriesgada en un proceso fluido. Dado el número de posibles contratiempos mencionados en el ejemplo de VMware, esta solución también debe incluir la posibilidad de revertir rápidamente las cargas de trabajo a la plataforma original en caso de que surja cualquier problema de rendimiento, compatibilidad o funcionamiento.

En algunos casos, mantener un entorno híbrido entre la plataforma antigua y la nueva durante varios meses puede ayudar a reducir el riesgo de migración. Esto exige desplegar medidas de protección frente a la pérdida de datos por diversas causas (incluidos el ransomware, los posibles errores de usuario y los fallos de hardware) para garantizar que la empresa sigue cumpliendo sus obligaciones de retención legal y cumplimiento normativo. Una ventaja adicional de estas medidas de protección es la libertad frente a la dependencia de un proveedor. Si la nueva solución de hipervisor no resulta adecuada a largo plazo, también será posible migrar de forma segura a otra alternativa en el futuro.

Acronis puede hacer que la transición desde plataformas antiguas sea fluida y sin riesgos

Para las empresas preparadas para dar este paso, por ejemplo, desde VMware hacia un hipervisor alternativo, Acronis dispone de las herramientas necesarias para que el proceso resulte sencillo, fiable, sin riesgos y reversible. Con las funciones de migración de la plataforma Acronis Cyber Protect y, si se desea, el apoyo de Acronis Professional Services, las empresas pueden disfrutar de las siguientes ventajas:

- Opciones de migración que pueden reducir el tiempo de transición hasta un 60 %, incluidas la migración directa sin agente, la migración masiva con ejecución y supervisión orquestadas, y la migración incremental mediante

sincronización continua para minimizar las interrupciones operativas.

- La garantía de que no se perderá ningún dato, gracias a medidas de protección integrales antes, durante y después de la migración.
- Una plataforma unificada para la migración, las copias de seguridad y la protección continua del nuevo entorno.
- Validación de ciberseguridad para mantener el estado de la seguridad durante todo el proceso de migración.
- Control de calidad mediante la validación posterior a la migración, que confirma la integridad de los datos.
- Una estrategia de migración personalizada, diseñada por consultores expertos para el entorno específico de cada empresa.

Acronis Cyber Protect ofrece ciberprotección integrada de forma nativa, que unifica la protección de datos, la ciberseguridad y la administración de endpoints en una sola plataforma. Con un equipo de servicios profesionales especializado en migraciones desde VMware, Acronis proporciona una implementación un 60 % más rápida, una garantía frente a la pérdida de datos y una estrategia de migración adaptada a cada organización.



Para iniciar el proceso de migración

- 1 [Regístrese](#) en Acronis Cyber Protect para garantizar una protección completa.
- 2 [Programe una consulta de migración](#) con los expertos de Acronis Professional Services.
- 3 Realice la migración con la ayuda de expertos para minimizar posibles riesgos e interrupciones.

Protección del nuevo entorno tras la migración

La misma plataforma de Acronis que permite realizar una migración segura desde un entorno anterior también ofrece funciones avanzadas de copia de seguridad y recuperación para el nuevo entorno, como se muestra en la siguiente tabla:

Copias de seguridad seguras y fiables para los principales hipervisores alternativos a VMware

Hipervisor	Funciones clave de la copia de seguridad de Acronis
Microsoft Hyper-V	Recuperación de máquinas virtuales de Hyper-V en cualquier sistema, incluido hardware nuevo, diferente o sin sistema operativo, con solo unos pocos clics. Objetivos de tiempo de recuperación (RTO) muy rápidos gracias a la posibilidad de ejecutar las copias de seguridad de Hyper-V como máquinas virtuales.
Nutanix	Protección eficaz, de bajo impacto y sin agente para máquinas virtuales Windows y Linux, con integración completa con Prism, lo que elimina la necesidad de agentes invitados y reduce la carga del sistema, a la vez que garantiza copias de seguridad coherentes y fiables gracias a la validación Nutanix Ready. Opciones de almacenamiento flexibles, que incluyen la nube de Acronis, Nutanix Objects/Files y nubes públicas de terceros. Copias de seguridad incrementales y deduplicación para reducir los costes de almacenamiento. Análisis de copias de seguridad en busca de malware, capaz de identificar archivos dañinos y evitar reinfecciones durante la recuperación. Funciones de escalabilidad que permiten añadir o retirar cargas de trabajo protegidas a medida que la empresa crece o se reorganiza. Cifrado avanzado, control de acceso basado en roles e inmutabilidad, para facilitar el cumplimiento normativo y proteger los datos frente a usos indebidos. Protección a nivel de imagen completa y a nivel de archivo, que permite capturar máquinas virtuales de Nutanix AHV completas, seleccionar archivos o carpetas concretos para copias de seguridad más pequeñas y específicas, y garantizar procesos de restauración rápida tanto de sistemas completos como de archivos individuales.
Proxmox	Copias de seguridad sin agente, eficaces y de bajo impacto para máquinas virtuales Proxmox y contenedores LXC. Recuperación a nivel de archivo y restauración completa del sistema, lo que permite una protección de datos rápida y granular. Opciones de almacenamiento flexibles, incluidos discos locales, dispositivos NAS, la nube de Acronis y nubes públicas compatibles con S3. Copias de seguridad incrementales y recuperación granular para reducir las ventanas de copia de seguridad y los tiempos de recuperación. Inmutabilidad, análisis antimalware y cifrado FIPS 140-2 para mantener los archivos de copia de seguridad seguros y en cumplimiento con las normativas. Directivas de protección que se pueden aplicar automáticamente a nuevas máquinas virtuales y contenedores, lo que elimina brechas de seguridad y garantiza que cualquier entorno de pruebas o producción quede protegido mediante copias de seguridad desde el primer momento. Copia de seguridad unificada de máquinas virtuales y contenedores bajo una misma directiva.
Citrix XenServer	Protección de cargas de trabajo XenServer mediante copias de seguridad de imagen completa del disco. Eliminación de la reinstalación del sistema operativo y de las aplicaciones en caso de fallo de una máquina virtual. Opciones de almacenamiento flexibles para las copias de seguridad de máquinas virtuales XenServer en hasta cinco ubicaciones, incluidos discos locales, dispositivos NAS, SAN, cintas y la nube de Acronis.
Red Hat Virtualization (RHV)	Capacidad para restaurar máquinas virtuales RHV en cuestión de minutos, ya sea en la misma máquina virtual o en otra distinta. Recuperación instantánea de documentos, archivos, carpetas o máquinas virtuales completas directamente desde la copia de seguridad. Copia de seguridad de imagen completa del disco de máquinas virtuales RHV, que permite restauraciones desde cero en hardware nuevo.
Linux KVM	Copias de seguridad de KVM en Linux, de imagen completa del disco de los hosts Linux y basadas en agente para las máquinas virtuales. Gestión centralizada de la protección de todos los hosts KVM locales y remotos desde una sola ubicación mediante una consola de administración basada en la web.