

Migration von Workloads: Wie Unternehmen sicher zwischen physischen Servern, Hypervisoren und Cloud-Plattformen wechseln

Einleitung

Jedes Unternehmen benötigt ein Backup-Tool, das flexibel genug ist, um alle vorhandenen physischen, virtuellen und Cloud-Plattformen zu schützen. Es muss eine schnelle und sichere Wiederherstellung aller Workloads ermöglichen – je nach Bedarf auf derselben Plattform, auf einem fabrikneuen Server, auf einer anderen Hypervisor-Plattform oder in der Cloud. Diese hohe Flexibilität kann Schutz vor häufigen IT-Problemen bieten, beispielsweise wenn ein Technologieanbieter nicht mehr den Anforderungen des Unternehmens entspricht.

Ein aktuelles und eindrucksvolles Beispiel hierfür lieferte der Hypervisor-Anbieter VMware. Nach der Übernahme durch Broadcom im Jahr 2023 verlagerte das Unternehmen seinen Geschäftsfokus auf Großunternehmen, erhöhte seine Preise und änderte seine Support-Richtlinien für kleinere Unternehmen, MSPs und VARs. Die neuen, ungünstigeren Konditionen veranlassten viele Kund:innen, sich nach einer neuen Hypervisor-Plattform umzusehen.

Für solche Migrationsvorhaben gibt es zwar viele Alternativen, doch um sicher ans Ziel zu gelangen, sind eine sorgfältige Planung und die richtigen Tools unerlässlich. Damit ein Unternehmen angemessen geschützt ist, muss es seine Workloads frei replizieren und verschieben können – nicht nur von einem Hypervisor zu einem anderen, sondern auch von jedem physischen Server, Hypervisor oder jeder Cloud-Plattform zu einer alternativen Lösung. Diese Flexibilität bietet Unternehmen folgende Vorteile:

www.acronis.com

Preiserhöhungen und geänderte Support-Richtlinien haben viele VMware-Kund:innen dazu bewogen, nach einer neuen Hypervisor-Plattform zu suchen.



- Geringeres Risiko bei der Migration: Bei Leistungs- oder Zuverlässigkeitsproblemen in der neuen Plattform ist ein Rollback auf die alte Plattform jederzeit möglich.
- Verbesserung der Einhaltung von Vorschriften durch konsistente Backups, Wiederherstellungen und Audit-Kontrollen für physische Server, Hypervisoren und Clouds.
- Verbesserung der Disaster Recovery-Fähigkeiten durch Replikation von Anwendungen und Daten in die Cloud.
- Überprüfung von Backups in der Cloud auf Malware und ungepatchte Schwachstellen sowie Behebung dieser Probleme vor der Datenwiederherstellung.
- Vermeidung von Anbieterabhängigkeit durch die freie Übertragbarkeit von Workloads auf neue Plattformen (z. B. wenn ein Hypervisor-Anbieter seine Preise für Verlängerung und Support erhöht).

Die optimale Lösung bietet all diese Funktionen in einer einzigen, einheitlichen Backup-Plattform. Dadurch lassen sich die Kosten für IT-Lizenzen, Schulungen, Integrationen und Support senken.

Herausforderungen bei der Migration auf eine neue Plattform

Ein Beispiel hierfür ist die Migration von VMware zu einem

neuen Hypervisor. Die einzelnen Schritte sind klar definiert: Zunächst wird die virtuelle Maschine (VM) exportiert, dann in das Format des neuen Hypervisors konvertiert und schließlich in die neue Plattform importiert. Doch jeder dieser Schritte birgt potenzielle Herausforderungen und kumulative Risiken. Dazu zählen unterschiedliche Formate virtueller Laufwerke, Chipsatz-Emulationsmodelle, virtuelle Hardwareversionen, Gerätetreiber und Netzwerkvirtualisierungsebenen. Hinzu kommt, dass sich VM-Vorlagen, Snapshots und angeschlossene Speicher-Volumes unterschiedlich verhalten. Kompatibilitätsprobleme zeigen sich möglicherweise erst, wenn die Workloads in der Produktivumgebung ausgeführt werden.

Kund:innen, die von VMware zu einer anderen Lösung migrieren, berichten regelmäßig von schwerwiegenden Problemen wie VM-Instabilität, Netzwerkkonfigurationsproblemen, Leistungseinbußen nach der Migration und der Tatsache, dass bei Problemen keine vollständige Rückkehr zum alten System möglich ist. Ein Migrationsprozess von einem Hypervisor zu einem anderen birgt das sehr reale Risiko eines langwierigen und kostspieligen Ausfalls. Ähnliche Risiken bestehen auch bei anderen Plattformwechseln, beispielsweise von einem physischen Server zu einem anderen oder von einer VM in die Cloud.

Es gibt viele gute Hypervisor-Alternativen zu VMware

Bleiben wir beim Beispiel der unzufriedenen VMware-Kund:innen, die nach einer Alternative suchen. Der Markt bietet schließlich viele gute Hypervisor-Alternativen, zum Beispiel:

Microsoft Hyper-V / Azure Stack HCI

Dies ist eine komfortable Lösung für Unternehmen, die bereits in das Windows- und Azure-Ökosystem investiert haben. Sie ermöglicht eine enge Integration mit Active Directory, den Azure-Sicherheitsdiensten und bestehenden Microsoft-Lizenzen.

Proxmox VE

Diese beliebte Open-Source-Plattform zeichnet sich durch eine transparente Lizenzierung, eine hohe Verfügbarkeit sowie eine aktive Benutzer-Community aus.

Nutanix AHV

Diese Lösung bietet eine vereinfachte Virtualisierung, Speicherung und Verwaltung über eine einheitliche Plattform. Sie basiert auf einem vorhersehbaren Abonnementmodell.

Scale Computing HC3

Diese hyperkonvergente Plattform ist für Edge-Umgebungen, wie sie beispielsweise im Einzelhandel und in der Fertigung zu finden sind, sowie für verteilte Umgebungen mit mehreren Standorten optimiert. Der Schwerpunkt liegt dabei auf Benutzerfreundlichkeit.

Weitere VM-Umgebungensind beispielsweise Citrix XenServer, Red Hat Virtualization und Linux KVM.

Der Migrationsprozess von VMware zu einer dieser Alternativen ist jedoch mit Risiken verbunden. Unternehmen sollten diese daher vor Beginn der Migration kennen und entsprechende Maßnahmen ergreifen. Dies gilt grundsätzlich für alle Migrationsprozesse von Workloads zu einer neuen physischen, virtuellen oder Cloud-Plattform.

Mit den richtigen Data Protection-Tools lassen sich Migrationsrisiken minimieren

Um potenzielle Risiken so gering wie möglich zu halten, sollten Unternehmen vor einer Plattformmigration in die richtigen Tools investieren. Eine plattformunabhängige Backup-Lösung kann beispielsweise einen sicheren Wechsel von VMware zu Hyper-V, Proxmox, Nutanix, Scale Computing oder zu hypervisorunabhängigen Alternativen wie physischen Servern und Cloud-Plattformen ermöglichen. Eine echte Any-to-Any-Backup-Lösung, die Workloads aus beliebigen Quellen verarbeiten und an beliebigen Zielorten wiederherstellen kann (d. h. von allen physischen, VM- oder Cloud-Plattformen auf alle anderen physischen, VM- oder Cloud-Plattformen), kann eine potenziell riskante Migration zu einem sicheren und zuverlässigen Vorgang machen. Die Lösung muss auch die Möglichkeit bieten, Workloads im Falle von Leistungs-, Kompatibilitäts- oder Betriebsproblemen schnell auf die ursprüngliche Plattform zurückzusetzen. So lassen sich die im obigen VMware-Beispiel genannten Migrationsrisiken vermeiden.

In einigen Fällen kann es auch sinnvoll sein, eine hybride Alt-und-Neu-Umgebung über einen gewissen Zeitraum hinweg aufrechtzuerhalten, um Migrationsrisiken abzusichern. Dies erfordert den Einsatz von Schutzmaßnahmen gegen Datenverlust, der verschiedene Ursachen haben kann (z. B. Ransomware-Angriffe, Benutzer- oder Hardware-Fehler), um sicherzustellen, dass das Unternehmen seinen Compliance- und gesetzlichen Aufbewahrungspflichten weiterhin nachkommt. Ein zusätzlicher Vorteil dieser Schutzmaßnahmen ist, dass Unternehmen sich nicht von einem Anbieter abhängig machen. Sollte sich die neue Hypervisor-Lösung langfristig nicht bewähren, ist ein sicherer Wechsel zu einer anderen Lösung jederzeit möglich.

Acronis ermöglicht eine einfache und risikofreie Migration von einer Plattform zur anderen

Unternehmen, die einen Plattformwechsel – etwa von VMware zu einem alternativen Hypervisor – planen, erhalten von Acronis die nötigen Tools, um diesen Prozess einfach, zuverlässig, risikofrei und umkehrbar zu gestalten. Die Migrationsfunktionen der Acronis Cyber Protect-Plattform in Kombination mit der optionalen Unterstützung durch Acronis Professional Services bieten Unternehmen folgende Vorteile:

- Verschiedene Migrationsoptionen, die die Migrationszeit um bis zu 60 % verkürzen können, darunter direkte agentenlose Migration, Massenmigration mit koordinierter Ausführung und Überwachung sowie inkrementelle Migration durch kontinuierliche Synchronisierung, um

Betriebsunterbrechungen so kurz wie möglich zu halten.

- 100-prozentiger Schutz vor Datenverlust vor, während und nach der Migration.
- Eine einzige, einheitliche Plattform für Migrationen, Backups und den kontinuierlichen Schutz der neuen Umgebung.
- Validierung der Cybersicherheit zur Aufrechterhaltung der IT-Sicherheit während des gesamten Migrationsprozesses.
- Qualitätssicherung durch Validierung der Datenintegrität nach der Migration.
- Eine speziell für die individuellen Anforderungen Ihres Unternehmens entwickelte Migrationsstrategie, die von erfahrenen Migrationsspezialist:innen erstellt wurde.

Acronis Cyber Protect ist eine umfassende, nativ integrierte Cyber Protection-Lösung. Sie vereint die Bereiche Data Protection, Cyber Security und Endpunktverwaltung in einer einzigen Plattform. In Kombination mit dem auf VMware-Migrationen spezialisierten Team von Acronis Professional Services profitieren Sie von einer um 60 % schnelleren Implementierung, einer Schutzgarantie gegen Datenverlust und einer maßgeschneiderten Migrationsstrategie.



Wie Sie sicher migrieren

- 1** [Registrieren](#) Sie sich für Acronis Cyber Protect, um für umfassenden Schutz zu sorgen.
- 2** [Vereinbaren Sie einen Beratungstermin](#) mit dem auf Migrationen spezialisierten Team von Acronis Professional Services.
- 3** Migrieren Sie unter professioneller Anleitung, um Risiken und Störungen zu minimieren.

Schutz der neuen Umgebung nach der Migration

Die gleiche Acronis Plattform, die die sichere Migration aus der alten Umgebung ermöglicht hat, bietet auch erweiterte Backup- und Wiederherstellungsfunktionen für die neue Umgebung. Diese sind in der folgenden Tabelle aufgeführt:

Eine sichere und zuverlässige Backup-Lösung für die führenden Hypervisor-Alternativen zu VMware

Hypervisor	Wichtigste Vorteile von Acronis Backup
Microsoft Hyper-V	Hyper-V VMs können mit nur wenigen Klicks auf jedem System wiederhergestellt werden – einschließlich neuer, fabrikneuer oder abweichender Hardware. Kurze RTOs durch das Ausführen von Hyper-V-Backups als VMs.
Nutanix	Effizienter, ressourcenschonender und agentenloser Schutz für Windows- und Linux-VMs mit vollständiger Prism-Integration. Dadurch werden Gastagenten überflüssig und der Aufwand reduziert sich. Gleichzeitig sind konsistente und zuverlässige Backups mit „Nutanix Ready“-Validierung gewährleistet. Es stehen flexible Storage-Optionen zur Verfügung, darunter Acronis Cloud, Nutanix Objects/Files und Public Clouds von Drittanbietern. Durch inkrementelle Backups und Deduplizierung lassen sich die Storage-Kosten senken. Backups werden auf Malware gescannt, um schädliche Dateien zu identifizieren und eine erneute Infektion während der Wiederherstellung zu verhindern. Möglichkeit zur Skalierung, um bei Wachstum oder Umstrukturierung des Unternehmens geschützte Workloads hinzufügen oder entfernen zu können. Sichere Verschlüsselung, rollenbasierte Zugriffskontrolle und Unveränderlichkeit zur Unterstützung der Einhaltung gesetzlicher Vorschriften und zum Schutz der Daten vor Missbrauch. Sicherung kompletter Nutanix AHV VMs mit vollständigen Image-Backups. Es ist auch möglich, nur bestimmte Dateien oder Ordner für kleinere, gezielte Backups auszuwählen. Dadurch ist eine schnelle Wiederherstellung vollständiger Systeme oder einzelner Objekte gewährleistet.
Proxmox	Effizientes, ressourcenschonendes und agentenloses Backup für Proxmox VMs und LXC-Container. Wiederherstellung auf Dateiebene sowie vollständige Systemwiederherstellung für eine schnelle und granulare Datensicherung. Flexible Storage-Optionen, einschließlich lokaler Laufwerke, NAS-Geräte, der Acronis Cloud sowie S3-kompatibler Public Clouds. Inkrementelle Backups und granulare Wiederherstellung, um die Backup- und Wiederherstellungszeiten zu verkürzen. Funktionalitäten wie Unveränderlichkeit, Malware-Scanning und FIPS 140-2-Verschlüsselung sorgen für sichere und Compliance-konforme Backup-Archive. Schutzrichtlinien können automatisch auf neue VMs und Container angewendet werden. Dadurch werden Sicherheitslücken geschlossen und sichergestellt, dass jede Test- oder Produktivumgebung automatisch gesichert wird. Eine einheitliche Backup-Richtlinie für VMs und Container.
Citrix XenServer	XenServer-Workloads werden durch vollständige Laufwerk-Image-Backups geschützt. Wenn die VM ausfällt, ist keine Neuinstallation des Betriebssystems und der Programme erforderlich. Flexible Storage-Optionen für XenServer VM-Backups an bis zu fünf Speicherorten: lokale Laufwerke, NAS-Geräte, SANs, Bandlaufwerke und die Acronis Cloud.
Red Hat Virtualization (RHV)	RHV VMs können innerhalb weniger Minuten auf derselben oder einer anderen VM wiederhergestellt werden. Dokumente, Dateien, Ordner oder ganze VMs lassen sich umgehend aus dem Backup wiederherstellen. Laufwerk-Image-Backups von RHV VMs ermöglichen eine Wiederherstellung auf fabrikneuer Hardware.
Linux KVM	Backup von Linux KVMs mit Laufwerk-Image-Backup von Linux Hosts und agentenbasiertem Backup von VMs. Der Schutz aller lokalen und Remote-KVM-Hosts wird zentral über eine einzige webbasierte Management-Konsole verwaltet.