

Comment les entreprises peuvent-elles assurer la protection et la migration des ressources sur et entre les serveurs physiques, les hyperviseurs et les plates-formes cloud.

Introduction

Chaque entreprise a besoin d'un outil de sauvegarde suffisamment flexible pour assurer la protection de toutes ses plates-formes physiques, virtuelles et cloud, et pour permettre une restauration rapide et sécurisée de toute ressource sur la même plate-forme, sur un nouveau serveur sur système nu, sur une plate-forme d'hyperviseur différente ou sur le cloud selon les besoins. Cette liberté de mouvement peut offrir une protection contre les défis informatiques courants, par exemple, un fournisseur technologique qui ne répond plus aux besoins de l'organisation.

Récemment, le fournisseur d'hyperviseur VMware en donne un exemple frappant. Après son acquisition par Broadcom en 2023, VMware a recentré son attention sur le secteur des grandes entreprises, augmentant ses prix et modifiant ses stratégies de support pour les petites entreprises, les MSP et les RVA. Ces nouvelles conditions défavorables ont incité de nombreux clients à rechercher une nouvelle plate-forme d'hyperviseur.

Pour un tel effort de migration, les alternatives sont nombreuses, mais y parvenir en toute sécurité nécessite un plan soigneux et les bons outils. Pour se protéger correctement, une entreprise doit pouvoir répliquer et déplacer ses ressources librement — non seulement d'un hyperviseur à un autre, mais aussi depuis n'importe quel serveur physique, hyperviseur ou plate-forme cloud à cloud.

Les augmentations de prix et les nouvelles stratégies de support ont incité de nombreux clients de VMware à rechercher une nouvelle plate-forme d'hyperviseur.



Cette flexibilité permet à une entreprise de :

- Limiter le risque de migration en permettant de revenir à l'ancienne plate-forme en cas de problèmes de performances ou de fiabilité dans le nouvel environnement.
- Améliorer son degré de conformité avec des contrôles cohérents de sauvegarde, d'opération de restauration et d'audit sur les serveurs physiques, hyperviseurs et clouds.
- Améliorer sa capacité de reprise d'activité après sinistre grâce à la réplication des applications et des données vers le cloud.
- Analyser les sauvegardes dans le cloud pour détecter les malwares et les vulnérabilités non corrigées, puis atténuer ces problèmes avant les opérations de restauration.
- Éviter l'enfermement propriétaire, en déplaçant librement les ressources vers de nouvelles plates-formes selon les besoins, par exemple, lorsqu'un fournisseur d'hyperviseur augmente ses prix de renouvellement et de support.

Pour être optimale, la solution unifie ces capacités sur une seule plate-forme de sauvegarde, réduisant ainsi les coûts de licence, de formation, d'intégration et de support informatique.

Les écueils à éviter lors de la migration vers une nouvelle plate-forme

Considérez l'exemple de la migration de VMware vers un nouvel hyperviseur. Les étapes sont claires : exportation de la machine virtuelle (VM), conversion au nouveau format d'hyperviseur et importation sur la nouvelle plate-forme. Mais chaque étape de cette transition induit des défis potentiels et un cumul des risques, y compris des différences concernant les formats de disque virtuel, les modèles d'émulation de chipset, les versions de matériel virtuel, les piles de pilotes et les couches de virtualisation en réseau. Les modèles de VM, les instantanés et les volumes de stockage attachés se comportent différemment. Les problèmes de compatibilité peuvent ne pas apparaître avant le passage des ressources en production.

Les clients qui quittent VMware signalent régulièrement de sérieux problèmes d'instabilité des machines virtuelles, des problèmes de configuration réseau, des performances lentes après conversion et l'incapacité à revenir en arrière si quelque chose tourne mal. Le processus de migration d'un hyperviseur à un autre comporte un réel risque d'interruption d'activité coûteuse et prolongée. D'autres déplacements entre plates-formes, par exemple d'un serveur physique à un autre ou d'une machine virtuelle au cloud, comportent des risques similaires.

De nombreuses alternatives attrayantes existent pour les utilisateurs d'hyperviseurs

Au client VMware mécontent qui recherche une stratégie de sortie, il existe sur le marché de nombreuses alternatives d'hyperviseurs dignes d'intérêt, notamment :

Microsoft Hyper-V / Azure Stack HCI

une solution confortable pour les entreprises déjà investies dans l'écosystème Windows et Azure, offrant une intégration étroite avec Active Directory, les services de sécurité Azure et la licence Microsoft existante.

Proxmox VE

une plate-forme open source populaire avec une licence transparente, des fonctionnalités à haute disponibilité et une communauté d'utilisateurs active.

Nutanix AHV

qui facilite la virtualisation, le stockage et la gestion sur une plate-forme unifiée avec un modèle d'abonnement prévisible.

Scale Computing HC3

une plate-forme hyperconvergée optimisée pour les environnements de périphérie comme le retail, la fabrication et les environnements multisites distribués, l'accent étant mis sur la simplicité.

Autres environnements de machines virtuelles notamment Citrix XenServer, Red Hat Virtualization et Linux KVM.

Mais le processus de migration de VMware vers l'une de ces alternatives — et la migration de toute ressource vers une nouvelle plate-forme physique, virtuelle ou cloud — comporte des risques que les entreprises devraient anticiper et traiter en amont.

Atténuer le risque de migration avec les bons outils de protection des données.

Avant toute migration de plate-forme, les entreprises devraient envisager d'investir dans les bons outils pour limiter les risques potentiels. Par exemple, une solution de sauvegarde indépendante de la plate-forme peut sécuriser la migration depuis VMware vers Hyper-V, Proxmox, Nutanix ou FCA Computing, ou vers d'autres alternatives hors hyperviseur, comme les serveurs physiques et les plates-formes cloud. Une véritable solution de sauvegarde any-to-any, capable d'ingérer une ressource de n'importe quelle source et de la restaurer dans n'importe quelle destination — d'une plate-forme physique, machine virtuelle ou cloud vers une autre plate-forme physique, machine virtuelle ou cloud — peut aider à éviter les problèmes pour une transition en douceur. Étant donné les nombreux obstacles potentiels évoqués dans l'exemple de VMware, la solution doit également permettre un retour rapide des ressources sur la plate-forme d'origine en cas de problème de performances, de compatibilité ou de fonctionnement.

Dans certains cas, conserver un environnement hybride, ancien et nouveau, pendant plusieurs mois peut aider à contenir le risque de migration. Cela suppose de déployer des protections contre la perte de données quelles qu'en soient les causes (y compris le ransomware, les erreurs d'utilisateur et la défaillance matérielle) pour garantir que l'entreprise continue d'honorer ses obligations de conformité et de rétention légale des données. Un avantage supplémentaire de ces protections est la liberté vis-à-vis du fournisseur. Si l'hyperviseur ne fonctionne pas à long terme, une migration sécurisée vers une autre alternative demeurera possible à l'avenir.

Acronis peut rendre la transition depuis les anciennes plates-formes fluide et sans risque

Pour les entreprises prêtes à effectuer une telle transition, par exemple de VMware vers un nouvel hyperviseur, Acronis dispose des outils pour rendre le processus simple, fiable, sans risque et réversible. Avec les capacités de migration de la plate-forme Acronis Cyber Protect et l'aide optionnelle des équipes Acronis Professional Services, les entreprises peuvent bénéficier de ce qui suit :

- Options de migration qui peuvent réduire le temps de transition jusqu'à 60 %, y compris la migration directe sans agent, la migration de masse avec exécution orchestrée et surveillance, et la migration incrémentielle via une synchronisation continue pour minimiser la perturbation des activités.
- La garantie de zéro perte de données qui assure une protection complète avant, pendant et après la migration.

- Une plate-forme unifiée pour la migration, la sauvegarde et la protection continue du nouvel environnement.
- La validation de la cybersécurité pour maintenir la posture de sécurité tout au long du processus de migration.
- L'assurance qualité via la validation post-migration de l'intégrité des données.
- Une stratégie de migration personnalisée élaborée par des consultants experts pour l'environnement spécifique de l'entreprise.

Acronis Cyber Protect offre une cyberprotection nativement intégrée, combinant protection des données, cybersécurité et gestion des terminaux sur une seule plate-forme. Avec une équipe de services professionnels dédiée à la migration VMware, Acronis propose une implémentation 60 % plus rapide, une garantie contre la perte de données et une stratégie de migration personnalisée.



Pour débuter le parcours de migration

- 1 [Abonnez-vous](#) à Acronis Cyber Protect afin de bénéficier d'une protection complète.
- 2 [Planifiez une consultation de migration](#) avec les experts de de l'équipe Acronis Professional Services.
- 3 Faites-vous accompagner par des experts, pour minimiser les risques et les perturbations.

Protéger le nouvel environnement après la migration.

La même plate-forme Acronis qui permet une migration sécurisée depuis un ancien environnement peut également offrir des capacités avancées de sauvegarde et de restauration pour le nouveau, comme indiqué dans le tableau :

Sauvegarde sécurisée et fiable pour les meilleures alternatives aux hyperviseurs VMware.

Hyperviseurs	Principales fonctionnalités de sauvegarde Acronis
Microsoft Hyper-V	La restauration des machines virtuelles Hyper-V sur n'importe quel système, y compris sur un système nu, nouveau ou différent, en quelques clics. Des RTO rapides en exécutant les sauvegardes Hyper-V comme des machines virtuelles.
Nutanix	Une protection sans agent, efficace et à faible impact pour les machines virtuelles Windows et Linux avec une intégration complète à Prism, éliminant le besoin d'agents clients et limitant la surcharge tout en garantissant des sauvegardes cohérentes et fiables avec la validation Nutanix Ready. Des options de stockage flexibles, y compris Acronis Cloud, Nutanix Objects / Files et les clouds publics de tiers. Des sauvegardes incrémentielles et la déduplication pour réduire les coûts de stockage. L'analyse des sauvegardes pour détecter les malwares afin de prévenir la réinfection lors de la restauration. Des fonctionnalités évolutives pour ajouter ou supprimer des ressources protégées à mesure que l'entreprise se développe ou se réorganise. Le chiffrement avancé, le contrôle d'accès basé sur les rôles et l'immuabilité pour soutenir la conformité réglementaire et protéger les données contre les abus. La protection d'image et de fichiers pour capturer l'intégralité des machines virtuelles Nutanix AHV, sélectionner certains fichiers ou dossiers pour des sauvegardes ciblées et plus légères et effectuer des restaurations rapides de systèmes complets ou d'éléments individuels.
Proxmox	La sauvegarde sans agent, efficace et à faible impact pour les machines virtuelles Proxmox et les conteneurs LXC. La récupération de fichiers et des restaurations système complètes pour une protection des données rapide et granulaire. Des options de stockage flexibles, y compris sur disques locaux, terminaux NAS, dans le Cloud Acronis et les clouds publics compatibles S3. Des sauvegardes incrémentielles et une restauration granulaire pour réduire les créneaux de sauvegarde et les temps de récupération. L'immuabilité, l'analyse anti-malware et le chiffrement FIPS 140-2 pour garantir la sécurité et la conformité des archives. Des stratégies de protection pouvant être appliquées automatiquement aux nouvelles machines virtuelles et conteneurs, éliminant les lacunes et garantissant que chaque environnement de test ou de production est automatiquement sauvegardé. L'unification de la sauvegarde des machines virtuelles et des conteneurs en une seule stratégie.
Citrix XenServer	La protection des ressources XenServer avec sauvegarde d'images disques complète. L'élimination de la réinstallation du système d'exploitation et des applications en cas de défaillance d'une machine virtuelle. Des options de stockage flexibles pour les sauvegardes de machines virtuelles XenServer dans cinq emplacements maximum, y compris les disques locaux, NAS, SAN, bandes et le Cloud Acronis.
Red Hat Virtualization (RHV)	La capacité à restaurer les machines virtuelles RHV en quelques minutes sur la même machine virtuelle ou une autre. La restauration instantanée de documents, fichiers, dossiers ou de machines virtuelles entières depuis la sauvegarde directement. La sauvegarde d'images disques des machines virtuelles RHV permettant une restauration sur système nu vers un nouveau matériel.
Linux KVM	La sauvegarde des KVM Linux par création d'images disques des hôtes Linux et la sauvegarde avec agent des machines virtuelles. La gestion de la protection de tous les hôtes KVM locaux et distants depuis un seul emplacement via une seule console web de gestion.