

Como as empresas podem proteger e realizar a migração de workloads entre servidores físicos, hipervisores e plataformas de nuvem.

Introdução

Todo negócio precisa de uma ferramenta de backup que seja flexível o suficiente para oferecer proteção a todas as suas plataformas físicas, virtuais e de nuvem, e para permitir a recuperação rápida e segura de qualquer workload para a mesma plataforma, para um novo servidor bare metal, para uma plataforma de hipervisor diferente ou para a nuvem conforme necessário. Essa liberdade de movimento pode oferecer proteção contra desafios comuns de TI, por exemplo, um fornecedor de tecnologia que não atende mais às necessidades da organização.

O fornecedor de hipervisor VMware fornece um exemplo recente e dramático. Após sua aquisição pela Broadcom em 2023, a VMware mudou seu foco para o setor de grandes empresas, aumentando seus preços e alterando suas políticas de suporte para pequenas empresas, MSPs e VARs. Esses novos termos desfavoráveis incentivaram muitos clientes finais a buscar uma nova plataforma de hipervisor.

Em qualquer esforço de migração, as alternativas são muitas, mas chegar lá com segurança requer um planejamento cuidadoso e as ferramentas certas. Para se proteger adequadamente, uma empresa precisa da capacidade de replicar e mover seus workloads livremente — não apenas de um hipervisor para outro, mas de qualquer servidor físico, hipervisor ou plataforma de nuvem para outra. Essa flexibilidade permite que uma empresa:

Aumentos de preços e alterações nas políticas de suporte incentivaram muitos clientes finais da VMware a buscar uma nova plataforma de hipervisor.



- Minimize o risco de migração habilitando a opção de reverter da nova plataforma para a antiga em caso de problemas de desempenho ou confiabilidade no novo ambiente.
- Melhore sua postura de conformidade com backup consistente, operações de recuperação e controles de auditoria em servidores físicos, hipervisores e nuvens.
- Aprimore sua postura de recuperação de desastres por meio da replicação de aplicativos e dados para a nuvem.
- Escaneie backups na nuvem em busca de malware e vulnerabilidades não corrigidas, e mitigue esses problemas antes das operações de recuperação.
- Evite o lock-in de fornecedores, movendo workloads livremente para novas plataformas conforme necessário, por exemplo, quando um fornecedor de hipervisor aumenta seus preços de renovação e suporte.

A solução ideal oferece essas capacidades em uma plataforma de backup unificada, reduzindo assim os custos de licenciamento, treinamento, integração e suporte de TI.

Armadilhas de migração no caminho para uma nova plataforma

Considere o exemplo de migração do VMware para um novo hipervisor. Os passos são claros: Exportar a máquina virtual (VM), convertê-la para o novo formato de hipervisor e importá-la para a nova plataforma. Mas cada etapa nessa transição adiciona desafios potenciais e risco cumulativo, incluindo diferentes formatos de disco virtual, modelos de emulação de chipset, versões de hardware virtual, pilhas de drivers e camadas de virtualização de rede. Modelos de VM, instantâneos e volumes de armazenamento anexados se comportam de maneira diferente. Problemas de compatibilidade podem não surgir até que workloads estejam sob carga de produção.

Clientes que estão se afastando da VMware frequentemente relatam sérios problemas de instabilidade de VM, problemas de configuração de rede, desempenho lento após a conversão e a incapacidade de reverter completamente se algo der errado. O processo de migração de um hipervisor para outro traz um risco real de se transformar em um incidente de tempo de inatividade caro e prolongado. Outras mudanças entre plataformas, como de um servidor físico para outro ou de uma VM para a nuvem, apresentam riscos semelhantes.

Usuários de hipervisor têm muitas alternativas atraentes

Continuando com o exemplo do cliente final insatisfeito da VMware que busca uma estratégia de saída, o mercado oferece muitas alternativas de hipervisor dignas, incluindo:

Microsoft Hyper-V / Azure Stack HCI

uma escolha confortável para empresas já investidas no ecossistema Windows e Azure, oferecendo integração estreita com Active Directory, serviços de segurança do Azure e licenciamento Microsoft existente.

Proxmox VE

uma plataforma popular de código aberto com licenciamento transparente, recursos de alta disponibilidade e uma comunidade de usuários ativa.

Nutanix AHV

que oferece virtualização simplificada, gerenciamento de armazenamento e gerenciamento sob uma plataforma unificada com um modelo de assinatura previsível.

Scale Computing HC3

uma plataforma hiperconvergente otimizada para ambientes de borda, como varejo, fabricação e ambientes distribuídos de múltiplos sites, com foco na simplicidade.

Outros ambientes de máquinas virtuais incluindo Citrix XenServer, Red Hat Virtualization e Linux KVM.

Mas o processo de migração da VMware para qualquer uma dessas alternativas — e, de fato, de migração de qualquer workload para uma nova plataforma física, virtual ou de nuvem — envolve riscos que as empresas devem antecipar e abordar antes de embarcar nessa jornada.

Mitigando o risco de migração com as ferramentas de proteção de dados certas.

Antes de embarcar em uma jornada de migração de plataforma, as empresas devem considerar investir nas ferramentas certas para ajudar a mitigar os riscos potenciais. Por exemplo, uma solução de backup agnóstica de plataforma pode atuar como um canal seguro do VMware para o Hyper-V, Proxmox, Nutanix ou Scale Computing, ou para alternativas sem hipervisor, como servidores físicos e plataformas de nuvem. Uma solução de backup verdadeiramente qualquer-para-qualquer, que possa ingerir uma workload de qualquer fonte e restaurá-la para qualquer destino — de qualquer plataforma física, VM ou nuvem para qualquer outra plataforma física, VM ou nuvem — pode transformar uma saída perigosa em um caminho suave. Dadas as muitas possíveis falhas citadas no exemplo da VMware acima, também deve incluir a capacidade de reverter rapidamente as workloads para a plataforma original em caso de problema de desempenho, compatibilidade ou operacional.

Em alguns casos, manter um ambiente híbrido antigo e novo por alguns meses pode ajudar a mitigar o risco de migração. Isso requer a implantação de proteção contra perda de dados por várias causas possíveis (incluindo ransomware, erros de usuário e falha de hardware) para garantir que a empresa continue a cumprir suas obrigações de conformidade e retenção legal de dados. Um benefício adicional dessas proteções é a liberdade de bloqueio de fornecedor. Se a nova solução de hipervisor não funcionar a longo prazo, uma migração segura para outra alternativa também é possível no futuro.

A Acronis pode tornar a transição de plataformas antigas suave e sem riscos

Para empresas prontas para fazer essa transição, por exemplo, do VMware para um hipervisor alternativo, a Acronis tem as ferramentas para tornar o processo simples, confiável, sem riscos e reversível. Com as capacidades de migração da Acronis Cyber Protect e a ajuda opcional dos Serviços Profissionais da Acronis, as empresas podem desfrutar de:

- Opções de migração que podem reduzir o tempo de transição em até 60%, incluindo migração direta sem agente, migração em massa com execução e monitoramento orquestrados, e migração incremental via sincronização contínua para minimizar a interrupção dos negócios.
- Uma garantia de zero perda de dados que assegura

proteção completa antes, durante e após a migração.

- Uma plataforma unificada para migração, backup e proteção contínua do novo ambiente.
- Validação de cibersegurança para manter a postura de segurança durante todo o processo de migração.
- Garantia de qualidade por meio de validação pós-migração da integridade dos dados.
- Uma estratégia de migração personalizada, desenvolvida por consultores especializados para o ambiente único do cliente final.

Acronis Cyber Protect oferece proteção cibernética nativamente integrada, combinando proteção de dados, cibersegurança e gerenciamento de endpoint em uma única plataforma. Com uma equipe de serviços profissionais dedicada à migração VMware, a Acronis oferece uma implementação 60% mais rápida, garantia contra perda de dados e uma estratégia de migração personalizada.



Para iniciar a jornada de migração

- 1 [Inscreva-se](#) para que o Acronis Cyber Protect garanta proteção completa.
- 2 [Agende uma consulta sobre migração](#) com especialistas dos Serviços Profissionais da Acronis.
- 3 Migre com orientação especializada, minimizando riscos e interrupções.

Protegendo o novo ambiente após a migração.

A mesma plataforma Acronis que permite uma migração segura de um ambiente antigo também pode oferecer capacidades avançadas de backup e recuperação para o novo, conforme destacado na tabela:

Backup seguro e confiável para principais alternativas de hipervisor ao VMware.

Hipervisor	Principais recursos do Backup da Acronis
Microsoft Hyper-V	Recuperação de VMs do Hyper-V para qualquer sistema — incluindo novo, bare metal ou hardware diferente — com apenas alguns cliques. RTOs rápidos executando backups do Hyper-V como VMs.
Nutanix	Proteção eficiente, de baixo impacto e sem agente para VMs Windows e Linux com total integração ao Prism, eliminando a necessidade de agentes convidados e reduzindo a sobrecarga, enquanto garante backups consistentes e confiáveis com a Validação Nutanix Ready. Opções de armazenamento flexíveis, incluindo Acronis Cloud, Nutanix Objects / Files e nuvens públicas de terceiros. Backups incrementais e deduplicação para reduzir custos de armazenamento. Verificação de backup para malware que identifica arquivos nocivos para prevenir reinfecção durante a recuperação. Recursos de escalabilidade para adicionar ou remover workloads protegidos à medida que o negócio cresce ou se reorganiza. Criptografia avançada, controle de acesso baseado em funções e imutabilidade para suportar conformidade regulatória e manter os dados seguros contra uso indevido. Proteção completa em imagem e em nível de arquivo para capturar máquinas virtuais Nutanix AHV inteiras, selecionar opcionalmente certos arquivos ou pastas para backups menores e direcionados, e garantir restaurações rápidas de sistemas completos ou itens individuais.
Proxmox	Backup eficiente, de baixo impacto e sem agente para VMs Proxmox e contêineres LXC. Recuperação em nível de arquivo e restaurações completas de sistema para proteção de dados rápida e granular. Opções de armazenamento flexíveis, incluindo discos locais, dispositivos NAS, Acronis Cloud e nuvens públicas compatíveis com S3. Backups incrementais e recuperação granular para reduzir janelas de backup e tempos de recuperação. A imutabilidade, a varredura antimalware e a criptografia FIPS 140-2 mantêm os arquivos seguros e em conformidade. Políticas de proteção que podem ser aplicadas automaticamente a novas VMs e contêineres, eliminando lacunas e garantindo que todo ambiente de teste ou produção seja automaticamente protegido. Unifique o backup de VMs e contêineres em uma única política.
Citrix XenServer	Proteção de workloads XenServer com backup completo em imagem de disco. Eliminação da reinstalação do sistema operacional e de aplicativos no caso de falha de uma VM. Opções flexíveis de armazenamento para backups de VMs XenServer em até cinco locais, incluindo discos locais, NAS, SAN, fita e a nuvem da Acronis.
Red Hat Virtualization (RHV)	Capacidade de restaurar VMs RHV em minutos para a mesma ou outra VM. Recuperação instantânea de documentos, arquivos, pastas ou VMs inteiras diretamente do backup. Backup em imagem de VMs RHV que permite restauração bare metal para novo hardware.
Linux KVM	Backup de KVMs Linux com backup em imagem de hosts Linux e backup baseado em agente de máquinas virtuais. Gestão de proteção de todos os hosts KVM locais e remotos a partir de um único local com uma management console baseada na web.