

Come proteggere e migrare i workload aziendali tra server fisici, hypervisor e piattaforme cloud

Introduzione

Ogni azienda ha bisogno di uno strumento di backup flessibile e versatile per proteggere tutte le piattaforme fisiche, virtuali e cloud, e per consentire, quando serve, il ripristino rapido e sicuro di qualsiasi workload sulla stessa piattaforma, su un nuovo server bare-metal, su una piattaforma hypervisor differente o sul cloud. Quella libertà di movimento può proteggere anche dagli ostacoli più comuni del mondo IT, come un fornitore di tecnologia che non soddisfa più le esigenze dell'organizzazione.

VMware, noto fornitore di hypervisor, è un esempio significativo e recente. Dopo l'acquisizione da parte di Broadcom, nel 2023, VMware ha spostato l'attenzione verso il settore enterprise, aumentando i prezzi e modificando le politiche di supporto per le piccole imprese, gli MSP e i VAR. Queste condizioni meno favorevoli hanno spinto molti clienti a cercare una nuova piattaforma hypervisor.

Per qualsiasi iniziativa di migrazione di questo tipo sono disponibili molte alternative, ma il successo e la sicurezza dipendono dalla scelta degli strumenti giusti e da un'attenta pianificazione. Per proteggersi adeguatamente, un'azienda deve avere la capacità di replicare e spostare i workload liberamente, non solo tra hypervisor, ma da

L'aumento dei prezzi e le nuove politiche di supporto hanno spinto molti clienti di VMware a cercare una nuova piattaforma hypervisor.



qualsiasi server fisico, piattaforma cloud o hypervisor ad un altro. Questa flessibilità consente a un'azienda di:

- Ridurre al minimo i rischi della migrazione abilitando il rollback dalla nuova piattaforma a quella precedente se vengono riscontrati problemi prestazionali o di affidabilità nel nuovo ambiente.
- Migliorare il profilo di conformità grazie a backup, ripristino e controlli di audit omogenei su server fisici, hypervisor e cloud.
- Migliorare la resilienza nel disaster recovery tramite la replica di applicazioni e dati nel cloud.
- Analizzare i backup nel cloud alla ricerca di malware e vulnerabilità non corrette, per risolvere gli eventuali problemi riscontrati prima delle operazioni di ripristino.
- Evitare vincoli con i fornitori, spostando liberamente i workload su nuove piattaforme secondo le esigenze, ad esempio quando un fornitore di hypervisor aumenta i prezzi di rinnovo delle licenze e del supporto.

La soluzione ottimale fornisce tutte queste funzionalità in una piattaforma di backup unificata, riducendo così i costi di licenza, formazione, integrazione e supporto.

Insidie della migrazione verso una nuova piattaforma

Prendiamo come esempio la migrazione da VMware a un nuovo hypervisor. I passaggi da compiere sono chiari: esportare la macchina virtuale (VM), convertirla nel nuovo formato di hypervisor e quindi importarla nella nuova piattaforma. Sembra semplice, ma in realtà ogni passaggio di questa transizione aggiunge potenziali ostacoli e rischi cumulativi: differenze nei formati di disco virtuale, nei modelli di emulazione del chipset, nelle versioni dell'hardware virtuale, negli stack di driver e nei livelli di virtualizzazione delle reti. I modelli di VM, gli snapshot e i volumi di storage collegati hanno funzionamenti diversi. I problemi di compatibilità potrebbero non emergere fino a quando i workload non sono nell'ambiente di produzione.

I clienti in fase di migrazione da VMware segnalano spesso gravi problemi come l'instabilità delle VM, i problemi di configurazione della rete, la lentezza delle prestazioni dopo la conversione e l'incapacità di eseguire un ripristino completo se qualcosa non funziona come previsto. Il processo di migrazione da un hypervisor a un altro rischia di trasformarsi in una serie di interruzioni operative costose e prolungate. Altri spostamenti tra piattaforme, ad esempio da un server fisico a un altro o da una VM al cloud, comportano rischi simili.

Alternative interessanti per gli utenti degli hypervisor

Per continuare con l'esempio del cliente VMware insoddisfatto che cerca una strategia di uscita, va detto che il mercato offre molti hypervisor alternativi validi, tra cui:

Microsoft Hyper-V/Azure Stack HCI

una scelta adatta alle aziende che hanno già investito nell'ecosistema Windows e Azure, che offre una perfetta integrazione con Active Directory, i servizi di sicurezza Azure e le licenze Microsoft esistenti.

Proxmox VE

una diffusa piattaforma open source con licenze trasparenti, funzionalità ad alta disponibilità e un'attiva community di utenti.

Nutanix AHV

offre virtualizzazione, archiviazione e gestione semplificate in una piattaforma unificata, con un modello di abbonamento prevedibile.

Scale Computing HC3

una piattaforma iperconvergente ottimizzata per ambienti all'edge come il retail, la produzione e gli ambienti multisito distribuiti, che privilegia la semplicità.

Altri ambienti VM tra cui Citrix XenServer, Red Hat Virtualization e Linux KVM.

Tuttavia, è il processo di migrazione da VMware a una di queste alternative (e di migrazione di qualsiasi workload verso una nuova piattaforma fisica, virtuale o cloud) a implicare rischi che le aziende devono prevedere e affrontare prima di intraprendere il percorso.

Contenere i rischi della migrazione con strumenti adatti a proteggere i dati

Prima di intraprendere un percorso di migrazione della piattaforma, le aziende devono valutare quali siano gli strumenti più adatti su cui investire per contenere i potenziali rischi. Ad esempio, una soluzione di backup indipendente dalla piattaforma può facilitare il passaggio da VMware a Hyper-V, Proxmox, Nutanix o Scale Computing, oppure verso alternative non basate su hypervisor, come i server fisici e le piattaforme cloud. Un'autentica soluzione di backup any-to-any, in grado di acquisire un workload da qualsiasi origine e di ripristinarlo su qualsiasi destinazione (da qualsiasi piattaforma fisica, cloud o VM a qualsiasi altra piattaforma fisica, cloud o VM) può trasformare una conversione potenzialmente insidiosa in un percorso fluido e senza ostacoli. Considerati i potenziali rischi citati nell'esempio su VMware, la soluzione deve anche prevedere la capacità di ripristinare rapidamente i workload sulla piattaforma originale in caso di problemi di prestazioni, compatibilità o operativi.

In alcuni casi, gestire in parallelo il vecchio e il nuovo ambiente ibrido per alcuni mesi può aiutare a mitigare i rischi della migrazione. Per farlo, sarà necessario adottare misure di protezione contro la perdita di dati dovuta a una serie di possibili cause (inclusi ransomware, errori degli utenti e guasti hardware) per garantire che l'azienda continui a rispettare gli obblighi di conformità e conservazione legale dei dati. Un vantaggio aggiuntivo di queste protezioni è la libertà dai vincoli con i fornitori. Se, nel lungo termine, la nuova soluzione hypervisor non funziona come previsto, sarà possibile avviare una migrazione sicura a un'altra alternativa.

Acronis rende fluida e senza rischi la transizione dalle vecchie piattaforme

Alle aziende pronte a intraprendere questo percorso, ad esempio da VMware a un hypervisor alternativo, Acronis fornisce strumenti che rendono il processo semplice, affidabile, senza rischi e reversibile. Con le funzionalità di migrazione della piattaforma Acronis Cyber Protect e l'assistenza opzionale di Acronis Professional Services, le aziende possono beneficiare di:

- Opzioni di migrazione in grado di ridurre i tempi di transizione fino al 60%: migrazione diretta senza agente, migrazione in blocco con esecuzione e monitoraggio orchestrati e migrazione incrementale con sincronizzazione continua, per ridurre al minimo le interruzioni aziendali.

- Nessuna perdita di dati, una garanzia che assicura la protezione completa prima, durante e dopo la migrazione.
- Piattaforma unificata per la migrazione, il backup e la protezione continua del nuovo ambiente.
- Convalida della Cyber Security per gestire la postura di sicurezza durante tutto il processo di migrazione.
- Assicurazione di qualità tramite la convalida dell'integrità dei dati successiva alla migrazione.
- Strategia di migrazione progettata da consulenti esperti e su misura per l'ambiente esclusivo dell'azienda.

Acronis Cyber Protect offre la Cyber Protection integrata che combina protezione dei dati, Cyber Security e gestione degli endpoint in un'unica piattaforma. Con un team di servizi offerti da professionisti dedicati alla migrazione da VMware, Acronis offre un'implementazione più veloce del 60%, una garanzia contro la perdita di dati e una strategia di migrazione su misura.



Avvia il percorso di migrazione

1
2
3

Attiva Acronis Cyber Protect per garantire una protezione completa.

Pianifica una consulenza sulla migrazione con gli esperti di Acronis Professional Services.

Esegui la migrazione con l'assistenza degli esperti, riducendo al minimo i rischi e le interruzioni operative.

Proteggere il nuovo ambiente dopo la migrazione

La stessa piattaforma Acronis che consente una migrazione sicura da un ambiente obsoleto offre anche capacità avanzate di backup e ripristino per il nuovo ambiente, come mostra la tabella seguente.

Backup sicuro e affidabile per i principali hypervisor alternativi a VMware

Hypervisor	Principali funzionalità di backup di Acronis
Microsoft Hyper-V	Ripristino di macchine virtuali Hyper-V su qualsiasi sistema (anche su hardware nuovo, bare-metal e differente) con pochi clic. RTO rapidi grazie all'esecuzione dei backup Hyper-V come macchine virtuali.
Nutanix	Protezione efficiente, a basso impatto e senza agente per macchine virtuali Windows e Linux, con perfetta integrazione di Prism; elimina la necessità di agenti guest e riduce il carico gestionale, garantendo al contempo backup omogenei e affidabili con la convalida Nutanix Ready. Opzioni di archiviazione flessibili su, tra gli altri, Acronis Cloud, Nutanix Objects/Files e cloud pubblici di terze parti. Riduzione dei costi di storage con backup incrementali e deduplica. Analisi dei backup alla ricerca di malware, per identificare i file malevoli e prevenire la reinfezione durante il ripristino. Funzionalità di scalabilità per aggiungere o rimuovere workload protetti mano a mano che l'azienda cresce o si riorganizza. Crittografia avanzata, controllo degli accessi basato sui ruoli e immutabilità per supportare la conformità normativa e proteggere i dati dall'uso improprio. Protezione a livello di file e di immagine completa, per acquisire intere macchine virtuali Nutanix AHV; selezione facoltativa di singoli file o cartelle per backup mirati e di dimensioni ridotte; ripristino rapido di sistemi completi o di singoli elementi.
Proxmox	Backup efficiente, a basso impatto e senza agente per VM Proxmox e container LXC. Ripristino a livello di file e ripristini completi del sistema, per una protezione dei dati rapida e granulare. Opzioni di archiviazione flessibili, inclusi dischi locali, dispositivi NAS, Acronis Cloud e cloud pubblici compatibili con S3. Backup incrementali e recupero granulare per ridurre gli intervalli di backup e i tempi di ripristino. Immutabilità, scansione anti-malware e crittografia FIPS 140-2 per garantire archivi sicuri e conformi. Criteri di protezione che possono essere applicati in automatico alle nuove VM e container, per eliminare le lacune e garantire il backup automatico di ogni ambiente di test o produzione. Backup di VM e container unificati in un'unica policy.
Citrix XenServer	Protezione dei workload XenServer con backup completo dell'immagine del disco. Evita la reinstallazione del sistema operativo e delle applicazioni in caso di guasto della VM. Opzioni di archiviazione flessibili per i backup delle VM XenServer su un massimo di cinque destinazioni, inclusi dischi locali, NAS, SAN, nastro e Acronis Cloud.
Red Hat Virtualization (RHV)	Capacità di ripristinare le VM RHV in pochi minuti sulla stessa VM o su un'altra. Ripristino istantaneo di documenti, file, cartelle o intere VM direttamente dal backup. Backup dell'immagine del disco delle VM RHV, per eseguire il ripristino bare-metal su nuovo hardware.
Linux KVM	Backup di Linux KVM con backup dell'immagine del disco degli host Linux e backup con agente delle macchine virtuali. Gestione della protezione di tutti gli host KVM locali e remoti da una singola posizione, tramite un'unica console web di gestione.