Sponsorizzato da

VEEAM
Modern Data Protection

I cinque punti fondamentali di una Moderna Protezione dei dati

David Davis
vExpert

La maggior parte dei dirigenti aziendali (inclusi CFO e molti CIO) dà per "scontata" la protezione dei dati aziendali. Poiché il software di backup è stato acquistato e gli stipendi del team IT vengono pagati, presumono che i dati d'importanza critica e le applicazioni che li gestiscono siano protetti. Purtroppo, in molti casi la realtà è ben diversa.

La protezione delle applicazioni e dei dati aziendali è tanto importante quanto lo era dieci anni fa. Tuttavia, oggi è più complessa rispetto al passato. Con l'introduzione della virtualizzazione, del cloud computing e di tante altre applicazioni, la tecnologia per la protezione dei dati utilizzata da molte aziende è ormai antiquata e inadeguata. Ciò comporta inutili rischi per l'azienda e inutili complicazioni per gli amministratori IT.

Ciò che apprenderete in questo documento è che la protezione dei dati è cambiata e che è ora disponibile del software per una moderna protezione dei dati, che vi consente di proteggere i dati e le applicazioni d'importanza critica della vostra azienda in modo più affidabile ed efficiente.

Non date per scontata la protezione dei dati. Continuate a leggere per scoprire i cinque punti fondamentali della moderna protezione dei dati:

1. Usare un software per la protezione dei dati appositamente progettato per la virtualizzazione

Esistono centinaia di strumenti per la protezione dei dati, ma solo pochi di essi sono adatti alla virtualizzazione. Gli strumenti tradizionali per la protezione dei dati considerano solitamente qualsiasi server allo stesso modo, ovvero come un server fisico. Ritenendo, erroneamente, che tutti i server siano uguali, il backup o ripristino delle applicazioni e dei dati sono costellati di terribili inefficienze. Per esempio, anche quando sono stati modificati solo una piccola parte di blocchi, vengono eseguiti lunghi backup a livello filesystem.

Gli strumenti per la protezione dei dati progettati per la virtualizzazione sono in grado di parlare direttamente all'infrastruttura virtuale. Attraverso questo tipo di comunicazione, gli strumenti per la protezione dei dati ottengono:

- Conoscenza delle macchine virtuali (VM) e degli host su cui sono eseguiti
- Conoscenza dello storage virtuale per comprendere ciò che deve essere incluso nel backup
- Capacità di creare degli snapshot delle VM ed eseguirne il backup senza alcuna interruzione
- Capacità di eseguire il backup solo dei blocchi del disco della VM che sono cambiati, per ridurre drasticamente i tempi di backup e la quantità di dati di backup (il cosiddetto “Changed Block Tracking”)

Questa interazione consente inoltre di accedere ad ulteriori funzionalità che solitamente non ci si aspetta di trovare nel proprio ambiente virtuale, né tanto meno nel software di backup, tra cui:

- Creazione di ambienti di laboratorio virtuale, dove i backup possono essere testati o utilizzati automaticamente per ripristinare in modo selettivo i dati delle applicazioni
- Virtualizzazione del processo di ripristino, per rendere disponibili più rapidamente le VM malfunzionanti.

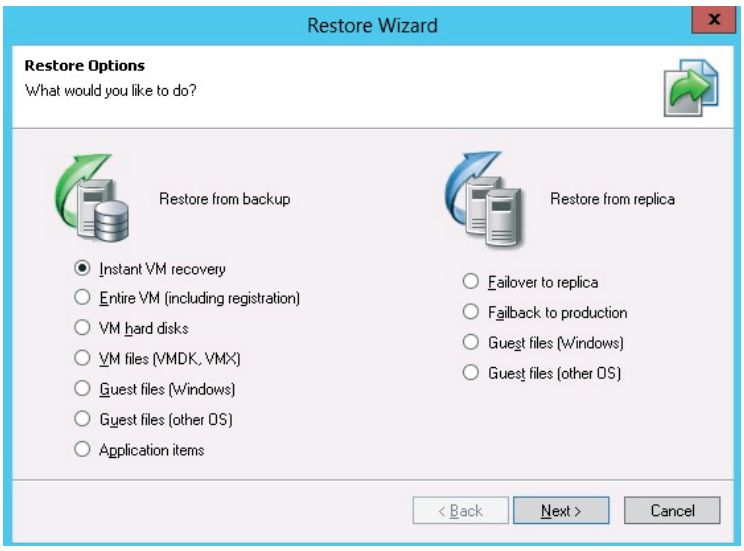


Figura 1. Sono disponibili numerose opzioni di ripristino per le macchine virtuali.

Sì, alcuni strumenti tradizionali per la protezione dei dati sono stati adattati, con il passare del tempo, per riconoscere l'infrastruttura virtuale, ma nessuno di questi strumenti è stato progettato appositamente per la virtualizzazione. Via via che un numero sempre maggiore di server viene virtualizzato, la mossa più intelligente consiste nello scegliere uno strumento per la protezione dei dati che sia progettato per la virtualizzazione e, proprio per questo, che possa offrire il massimo della flessibilità, della funzionalità e dell'efficienza.

2. Scegliere una soluzione per la protezione dei dati priva di agenti

Gli strumenti tradizionali per la protezione dei dati prevedono l'installazione di uno o più agenti su ciascuna VM da proteggere. Tuttavia, gli agenti introducono degli svantaggi, tra cui:

- Richiedono l'installazione di un nuovo componente software su ciascuna VM. Se una VM non contiene gli agenti, non è protetta ed è esposta alla perdita dei dati.
- Possono creare conflitti con le altre applicazioni.
- Sono difficili da gestire ed è difficile capire quali siano le VM con gli agenti installati.
- Utilizzano la CPU e la memoria su ogni VM.

In altre parole, gli agenti non sono efficienti sotto tutti i punti di vista.

Alcune aziende di software per la protezione dei dati sostengono di offrire una soluzione "agentless" perché sono in grado di eseguire un backup senza agenti. Tuttavia, molti di questi vendor richiedono degli agenti per i ripristini a livello di file, per il corretto backup delle applicazioni, oppure per ripristinare i dati delle applicazioni. Il mio consiglio è di assicurarsi che il proprio strumento per la protezione dei dati sia in grado di affrontare tutti questi scenari di backup e ripristino senza ricorrere ad alcun agente.

Gli strumenti per la protezione dei dati appositamente progettati per la virtualizzazione sono in grado di interagire direttamente col sistema host o virtuale per la gestione dell'infrastruttura (vCenter Server o SCVMM), trovare i nomi e le posizioni dei dischi virtuali e quindi eseguire il backup delle VM, il tutto senza agenti.

Ciò significa che non è necessario installare e mantenere agenti su ciascuna VM da proteggere, che le VM opereranno in modo più efficiente, e che sfrutterete al massimo la vostra infrastruttura virtuale.

Non sono necessari agenti anche quando si tratta di ripristinare una VM o i file all'interno di una VM. Come potete vedere nella figura 1, esistono vari tipi di ripristini, nessuno dei quali richiede un agente.

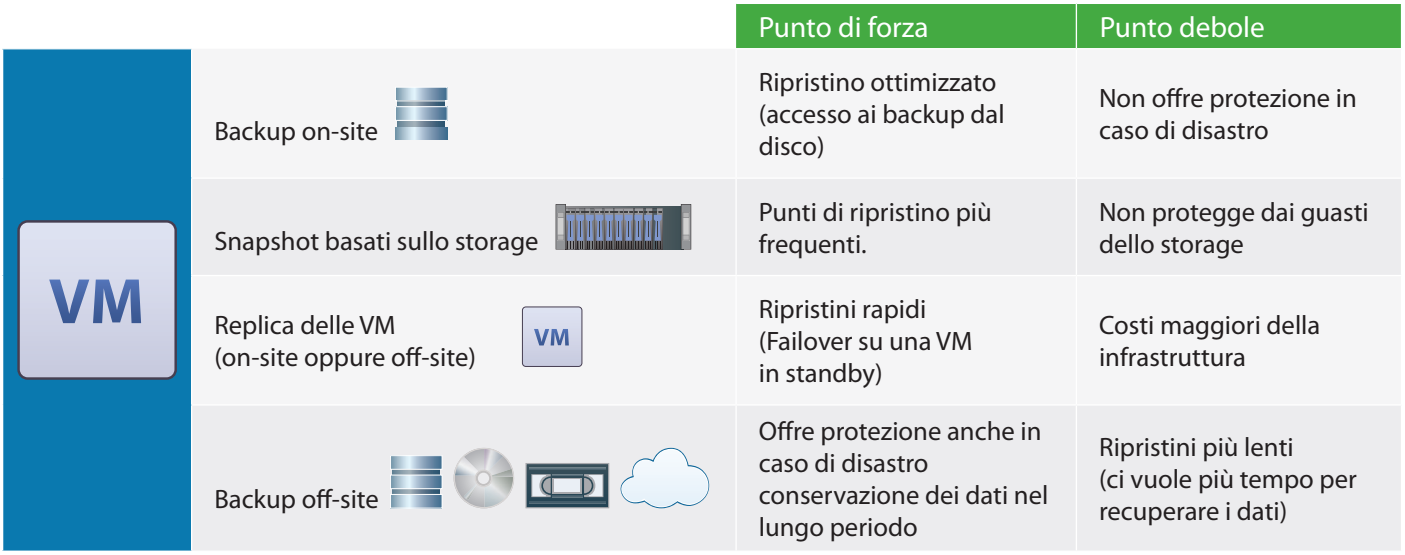
3. Adottare un approccio multilivello per la protezione dei dati

Il backup dei dati su nastro (con la conservazione dei nastri presso una struttura esterna) è ormai un ricordo del passato. I data center moderni utilizzano un approccio multilivello per la protezione dei dati.

Questo approccio può comprendere:

- Backup locale su disco
- Snapshot basati sullo storage
- Replica delle VM (on-site oppure off-site)
- Archiviazione su nastro o cloud storage

L'obiettivo è proteggere le applicazioni e i dati nella maggior parte di modalità possibili, rendendo i ripristini quanto più rapidi e semplici.



	Punto di forza	Punto debole
Backup on-site	Ripristino ottimizzato (accesso ai backup dal disco)	Non offre protezione in caso di disastro
Snapshot basati sullo storage	Punti di ripristino più frequenti.	Non protegge dai guasti dello storage
Replica delle VM (on-site oppure off-site)	Ripristini rapidi (Failover su una VM in standby)	Costi maggiori della infrastruttura
Backup off-site	Offre protezione anche in caso di disastro conservazione dei dati nel lungo periodo	Ripristini più lenti (ci vuole più tempo per recuperare i dati)

Figura 2. Un approccio multilivello alla protezione dei dati sfrutta le tecnologie più nuove e in evoluzione, per ottenere i migliori obiettivi RTO e RPO in tutti gli scenari di ripristino.

I vantaggi dell'approccio multilivello alla protezione dei dati comprendono:

- Accesso immediato ai backup per il ripristino istantaneo di intere VM, di singoli file o di dati delle applicazioni
- Ripristino comprovato, attraverso il caricamento di backup locali in qualsiasi momento, per la verifica automatica dei backup e le prove di disaster recovery
- Frequenti punti di ripristino e capacità di rispettare tutti gli obiettivi RPO (Recovery Point Objective)
- Automatizzazione dei backup off-site e della replica delle VM ai fini del disaster recovery (DR)
- Archiviazione a lungo termine su nastro oppure nel cloud, per garantire un livello finale di protezione dei dati, che offra tranquillità e conformità ai requisiti di auditing

4. Ridurre i dati dei backup con la deduplica

È noto che il costo della protezione dei dati varia notevolmente, a seconda del numero e delle dimensioni delle VM da proteggere. Per ottimizzare gli investimenti nella protezione dei dati è necessario sfruttare le tecnologie che riducono la dimensione dei backup. La protezione dei dati tradizionale si limita semplicemente ad eseguire il backup dei dati così come sono o, nel migliore dei casi, facendone una banale compressione.

Uno dei modi più comuni per ridurre la dimensione dei backup è ricorrere alla deduplica. Gli strumenti moderni per la protezione dei dati eseguono automaticamente la deduplica E la compressione. La deduplica identifica i blocchi di dati identici nelle VM sorgente e memorizza ogni blocco soltanto una volta. Poiché i backup basati su immagine utilizzati nella virtualizzazione catturano l'intera VM, incluso il Guest OS, e poiché l'OS è spesso il medesimo tra le VM, ciò dà solitamente origine a moltissime duplicazioni. La deduplica consente di ridurre drasticamente le dimensioni del repository di backup, il tempo necessario per eseguire il backup delle VM, la quantità di dati di backup replicati off-site e la quantità di dati inviati al nastro o al cloud storage.

Cercate sempre di proteggere la vostra infrastruttura virtuale con uno strumento che offra la funzionalità di deduplica. Altre funzionalità desiderabili per risparmiare spazio includono:

- **Backup "sempre incrementali"**: esecuzione di un backup full iniziale, dopodiché esecuzione di backup incrementali per sempre. Via via che vengono eseguiti i backup incrementali, il backup full è aggiornato con le modifiche, per creare un backup completo della VM, sempre pronto da ripristinare.
- **Supporto al thin-provisioning dell'hypervisor**: lo strumento di backup deve comprendere che l'hypervisor può creare dischi virtuali thin-provisioned. Lo strumento di backup deve essere in grado di supportare i dischi thin-provisioned e mantenere il thin-provisioning per l'intera durata delle operazioni di backup, ripristino e replica.
- **Esclusione dei dati non necessari**: gli strumenti moderni per la protezione dei dati devono riconoscere che le VM sono costituite da file speciali, come i file di configurazione, file di swap, snapshot, e il disco virtuale. Non è necessario eseguire il backup di tutti questi file. È necessario essere in grado di specificare quali di questi file debbano esser esclusi dal backup per risparmiare tempo, banda di rete, e spazio nel repository di backup.

5. Scegliere una sola soluzione per più hypervisor

Il rilascio di Windows Server 2012 Hyper-V, con le sue funzionalità avanzate ad un prezzo estremamente accessibile, ha fatto felici molte aziende. Tuttavia, molte aziende continuano a voler eseguire le loro applicazioni di primo livello su VMware vSphere. Utilizzando entrambi gli hypervisor all'interno del data centre, le aziende possono ridurre notevolmente la spesa per il software di virtualizzazione. Indipendentemente dal fatto che utilizziate o meno più hypervisor nel data center, il consiglio è di tenere aperte quante più opzioni possibili.

Scegliendo uno strumento per la protezione dei dati in grado di proteggere sia VMware vSphere, sia Microsoft Hyper-V, state scegliendo lo strumento necessario per un'infrastruttura multi-hypervisor / tiered-hypervisor.

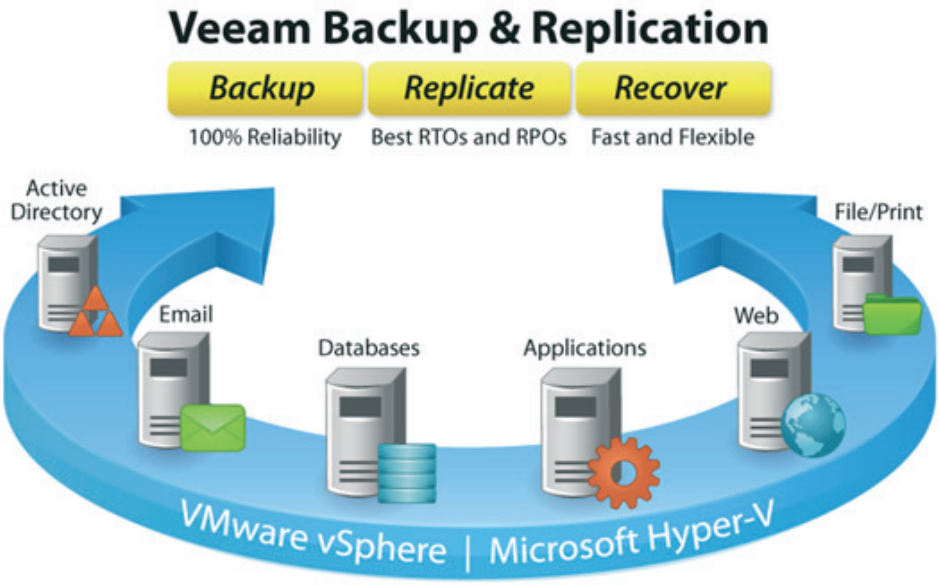


Figura 3. Veeam Backup & Replication offre una moderna protezione dei dati per VMware ed Hyper-V.

Sintesi

La gestione di un data center ricorda l'attività di un giocoliere. La costante introduzione di nuove applicazioni, nuove applicazioni e nuovi problemi rischia di far dimenticare i capisaldi fondamentali di un data center, tra cui la protezione dei dati. In molti casi i data center preferiscono "il diavolo che conoscono" e continuano a utilizzare le stesse applicazioni tradizionali di backup utilizzate negli ultimi 10 anni. Il problema di questo approccio è che lascia un numerose inefficienze agli amministratori IT, crea più malfuzionamenti e perdite di dati per gli utenti finali , ed espone i dati dell'azienda a potenziali pericoli. La protezione dei dati moderna è pienamente consapevole del layer di virtualizzazione, non prevede l'uso di agenti, utilizza un approccio multilivello, include funzionalità che riducono le dimensioni del repository di backup e protegge le VM sulle piattaforme di virtualizzazione più diffuse. Raccomando di valutare al più presto questi strumenti per una moderna protezione dei dati, da utilizzare nel vostro data center.

Informazioni sull'autore

David Davis è l'autore della celebre libreria di video formativi su VMware vSphere disponibile attraverso TrainSignal.com. Davis ha scritto centinaia di articoli online sulla virtualizzazione, oltre ad essere un VMware vExpert, VCP, VCAP-DCA e CCIE #9369, con oltre 18 anni di esperienza nel settore dell'IT aziendale. Il suo sito web personale è VMwareVideos.com.

Informazioni su Veeam Software

Veeam® Software sviluppa soluzioni innovative per i backup VMware, i backup Hyper-V e la gestione della virtualizzazione. Veeam Backup & Replication™ è la soluzione n. 1 per il backup delle VM. Veeam ONE™ è una soluzione completa per il monitoraggio in tempo reale, l'ottimizzazione delle risorse, la documentazione e la reportistica relative all'amministrazione di VMware e Hyper-V. Veeam estende il monitoraggio approfondito di VMware a Microsoft System Center con Veeam Management Pack™ (MP) e ad HP Operations Manager con Veeam Smart Plug-In™ (SPI). Veeam offre inoltre strumenti gratuiti per la virtualizzazione. Per maggiori informazioni visitare www.veeam.com.

VEEAM

vmware PARTNER TECHNOLOGY ALLIANCE

Microsoft Partner
Gold Application Development
Gold Management and Virtualization

Modern Data Protection
Built for Virtualization

Potente | Facile da utilizzare | Economico

Veeam Backup & Replication

Il #1 per il backup delle macchine virtuali VMware e Hyper-V

La virtualizzazione cambia tutto, specialmente il backup. Se la vostra azienda utilizza una macchina virtuale con **Microsoft Hyper-V** o **VMware**, è arrivato il momento di passare alla soluzione di protezione dati creata appositamente: Veeam **Backup & Replication**.

A differenza dei backup tradizionali, affetti dal **problema delle "3C"** (capacità mancanti, complessità e costi), Veeam è:

- **Potente:** ripristina una macchina virtuale (VM) completa o un singolo file, e-mail o record di database in 2 minuti
- **Facile da utilizzare:** semplicemente… funziona!
- **Economico:** nessuna licenza o assistenza per agenti, funziona con lo storage esistente e comprende deduplicazione, replica della VM, ripristino di Microsoft Exchange e molte altre funzionalità.

Unisciti alle 58.000 organizzazioni che hanno già modernizzato la protezione dati con Veeam. **Scarica Veeam Backup & Replication ora!**

BEST OF vmworld 2010 GOLD AWARD NEW TECHNOLOGY

BEST OF vmworld 2011 GOLD AWARD NEW TECHNOLOGY

InfoWorld.com ★2013 AWARDS★ TECHNOLOGY OF THE YEAR

Windows IT Pro 2012 Community Choice GOLD

Windows IT Pro 2012 Community Choice SILVER

WINNER 2011 VIRTUALIZATION REVIEW

Per maggiori informazioni, visita **http://vee.am/backupit**