10 best practice per il backup di VMware vSphere

Data: 24 febbraio 2021

Veeam v11

VMware versione 7.0 U1

Hannes Kasparick

Principal Analyst,

Veeam Product Management Team

Indice

Executive summary

La virtualizzazione dei server è una prassi ampiamente diffusa in tutto il mondo. Nel 2021, VMware è ancora il leader di mercato in questo settore e molti clienti Veeam® utilizzano WMware vSphere come piattaforma di virtualizzazione preferita. Questo white paper descrive le best practice specifiche per il backup e l'availability di VMware vSphere con Veeam Backup & Replication™ v11. In questa versione abbiamo incluso alcuni suggerimenti e recensioni di membri esperti della community, al fine di offrire il punto di vista dei colleghi sul backup di VMware, per aiutarvi a sviluppare con sicurezza la migliore strategia di backup. Tuttavia, il documento non include le best practice generiche per Hyper-V e Nutanix AHV, né indicazioni specifiche per gli agenti Veeam.

Introduzione

Il backup delle macchine virtuali (VM) su vSphere rappresenta solo una piccola parte della disponibilità dei servizi. Il backup è alla base dei ripristini, è quindi essenziale avere a disposizione dei backup sempre disponibili alla velocità richiesta. La best practice più importante per i backup è la regola 3-2-1.

Ciò significa avere almeno tre copie dei dati (dati di produzione, più una prima e seconda linea di backup). Questa regola raccomanda inoltre l'archiviazione delle copie del backup su almeno due tipi di supporti indipendenti. Il concetto di "indipendente" è fondamentale. In questo caso, "supporto indipendente" significa che, tra i supporti, non c'è alcuna dipendenza dal punto di vista tecnologico. Infine, un'altra copia dovrebbe essere off-site e offline, fuori dalla portata di calamità naturali, software dannoso e persone non autorizzate. Per esempio, Veeam ha aggiunto il supporto per il blocco degli oggetti S3 in Veeam Backup & Replication v10 e i repository Linux immutabili/con protezione avanzata nella v11. Naturalmente, il nastro rimane sempre un'opzione per lo storage off-site dei backup.

Veeam Backup & Replication consente di estendere la regola 3-2-1 alla regola 3-2-1-0, che introduce un approccio più moderno. La suddivisione dell'uno in due rappresenta sia la tecnologia off-site che quella offline, così da garantire una maggiore protezione dal ransomware. Lo zero rappresenta il fatto che non dovrebbero esserci errori a livello di recuperabilità, il che è reso possibile dai test di ripristino automatizzati con i job Veeam SureBackup® e SureReplica. SureBackup esiste principalmente per identificare i problemi logici nei backup, al fine di prevenire i problemi durante le operazioni di ripristino standard. Si pensi per esempio a uno scenario in cui qualcuno ha installato degli aggiornamenti senza mai eseguire un riavvio. Dopo un riavvio, apparirebbero una schermata blu o un kernel panic.

Questo documento descrive diverse best practice di Veeam Backup & Replication e VMware vSphere che aiutano a eliminare le perdite di dati e il ransomware. Queste best practice riguardano esclusivamente Veeam e VMware; il presente documento non tratta altri hypervisor.

Queste best practice generali comprendono:

- Adottare una strategia di backup e ripristino che risponda alle esigenze del business
- Eseguire il corretto dimensionamento
- Assicurarsi che VSS funzioni sulle macchine Windows
- Disporre di sufficiente spazio di backup

Queste best practice si applicano in ogni caso, indipendentemente dal fatto che si tratti del backup di VMware, Hyper-V, Nutanix AHV, provider cloud o server fisici.

La prima cosa da fare (e la più importante), prima di pianificare o implementare qualsiasi soluzione, consiste nell'essere certi dei suoi requisiti. In un mondo ideale, l'azienda crea i requisiti e comunica all'IT quali obiettivi Recovery Point Objective (RPO) e Recovery Time Objective (RTO) sono necessari. Per esempio, serve solo il backup o anche il disaster recovery (DR)? Un RTO ridotto implica l'ulteriore configurazione della replica Veeam, di Veeam Continuous Data Protection o degli snapshot storage?

Con questa informazione è possibile dimensionare meglio l'hardware. Ciò include il numero di core della CPU, la quantità di memoria e i requisiti di ampiezza di banda per WAN, LAN e SAN. Per finire, servono un'origine e uno storage di backup sufficientemente veloci per raggiungere la velocità richiesta.

Il passo successivo è costituito dal backup stesso. L'elaborazione application-aware delle immagini di Veeam utilizza Microsoft VSS per ottenere un backup consistente a livello applicativo delle VM Windows. Questo meccanismo non utilizza la sospensione degli strumenti VMware. Per garantire che l'elaborazione application-aware delle immagini funzioni in modo affidabile, è necessario che i writer VSS delle VM funzionino correttamente.

N.1: utilizzare le versioni aggiornate di Veeam e vSphere

Le ultime versioni di Veeam Backup & Replication migliorano le prestazioni e la sicurezza insieme a VMware vSphere.

Veeam Backup & Replication v11 introduce ovunque la lettura asincrona e la scrittura senza buffer per la scrittura dei backup nel sistema di storage. La lettura asincrona migliora le letture di tutti i tipi. Nella versione 10, Veeam utilizzava già la lettura asincrona per i ripristini a livello di file di Windows, per l'Instant VM Recovery™ e per creare backup full sintetici virtuali per i job backup-to-tape.Nella versione 11, Veeam la utilizza per tutti i tipi di letture, come i job di copia del backup e backup-to-tape.

Le scritture senza buffer aiutano a migliorare le prestazioni dei backup in scrittura. Con la versione 10 abbiamo assistito a velocità di backup pari a circa 4 GByte/s su un singolo server con 56 dischi NL-SAS. Con la versione 11 abbiamo pressoché raddoppiato questa velocità, raggiungendo connessioni da 100 Gbit/s.

Il miglioramento della sicurezza rappresenta una priorità continua per VMware e Veeam. L'utilizzo dell'ultima versione dei prodotti garantisce l'implementazione dei miglioramenti a livello di sicurezza.

> *"I vostri ingegneri hanno fatto un lavoro fantastico ottimizzando il codice della v11; con 10 GiB/s in un singolo server, Veeam su Apollo 4510 rappresenta una soluzione da record. La V10 era già una delle soluzioni di protezione dei dati più veloci, tuttavia la v11 ridefinisce il concetto di prestazioni di livello enterprise. Non ho mai visto alcuna azienda raddoppiare le prestazioni da una release all'altra".*
>
> – Federico Venier, Ingegnere di HPE

La best practice: cercare i miglioramenti nelle ultime versioni di Veeam Backup & Replication e vSphere.

N.2: scegliere correttamente la modalità di backup

Veeam Backup & Replication mette a disposizione tre diverse modalità di trasporto per eseguire il backup delle VM su vSphere. A partire dalla versione 11, Veeam supporterà anche quasi tutte le modalità di backup per i proxy Linux. Per chi preferisce Linux, si tratta della prima decisione da prendere. Ciascuna modalità presenta dei pro e dei contro e non esiste una regola generale su quale sia la migliore. Saranno l'ambiente e i requisiti specifici a determinare la modalità da scegliere:

1. Modalità rete o NBD
2. Accesso diretto allo storage, incluso il backup dagli snapshot storage
3. Appliance virtuale o "Hot Add"

Le proprietà di ciascun proxy consentono di configurare le opzioni elencate qui sopra nella sezione della modalità di trasporto.

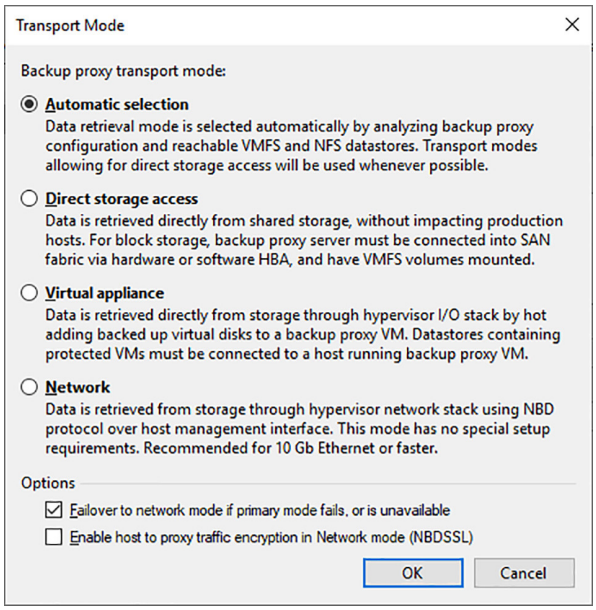


Figura 1: modalità di trasporto disponibili

La modalità di rete o NBD è il modo più semplice per eseguire backup di VMware. In questo caso, il server proxy Veeam utilizza la porta di gestione ESXi di ciascun host ESXi per trasferire i dati del backup. Ciò rende la configurazione molto semplice, poiché non richiede alcuna configurazione aggiuntiva di VM o storage, oltre a scalare in base al numero di host ESXi. Inoltre, la gestione è minima, il che rappresenta un ulteriore vantaggio. Rispetto alla modalità Hot Add, non necessita di ulteriori operazioni di mount con aggiunta a caldo, consentendo di risparmiare tempo. Non crea inoltre ulteriori snapshot storage come il backup dagli snapshot storage con sistemi di storage integrati. Il coordinamento di VM e snapshot storage richiede tempo, quindi la modalità di rete può anche essere la più veloce per i backup incrementali in ambienti con molte VM e un basso tasso di modifica dei dati.

La porta di gestione ESXi può diventare un collo di bottiglia, soprattutto se si tratta di un'interfaccia da 1 Gbit. Tuttavia, con 10 Gbit e migliori schede di interfaccia di rete questo di solito non è un problema.

Il traffico di backup della modalità di accesso diretto allo storage passa direttamente dal sistema di storage al proxy di backup Veeam. In questo caso, non è necessario che il traffico di backup passi attraverso l'hypervisor ESXi e il protocollo dipende dall'ambiente di storage. Solitamente, si tratta di FibreChannel o iSCSI. La modalità di accesso diretto allo storage presenta inoltre un vantaggio rispetto all'Hot Add come modalità di rete, poiché non c'è nessuna operazione di aggiunta a caldo, dispendiosa in termini di tempo. D'altro canto, entrambe le modalità utilizzano VMware vStorage API for Data Protection (VADP).

VADP è l'API ufficiale di VMware per il backup delle VM. Presenta di per se alcune implicazioni sulle prestazioni di backup, ed è per questo motivo che Veeam Backup & Replication non utilizza VADP in tre specifiche configurazioni. Queste tre configurazioni sono:

- Backup dagli storage snapshot
- Direct NFS (simile all'accesso diretto allo storage)
- Appliance virtuale/Hot-Add

Il segreto di Veeam, nell'evitare VADP, genera notevoli miglioramenti a livello di prestazioni di backup. Si tratta di uno dei motivi per cui l'Hot-Add è molto apprezzato. Il ricorso alla modalità Hot-Add offre tuttavia ulteriori vantaggi. Nella modalità Hot-Add, il proxy di backup Veeam è eseguito come VM aggiuntiva per i backup; carica gli snapshot delle VM nel backup e invia il traffico sulla normale rete della VM. Anche questa modalità non utilizza l'interfaccia di gestione ESXi. Ciò rende la modalità Hot-Add un'alternativa veloce nelle reti da 1 GBit, dove le modalità di backup con accesso diretto allo storage non sono possibili.

> *"La flessibilità e la vasta gamma di modalità di trasporto rende Veeam la soluzione perfetta per tutti i tipi di ambienti VMware vSphere. La modalità di rete per le PMI, l'Hot-Add per HCI e per scopi generici, l'accesso diretto allo storage e l'integrazione dello storage introducono enormi variazioni e riducono al minimo l'impatto sull'ambiente di produzione".*
>
> – Markus Kraus, Veeam Vanguard e VMware vExpert

In generale, la modalità di backup Hot-Add non è consigliata con i datastore NFS. Con NFS, si raccomanda di utilizzare l'accesso diretto allo storage, che comporta la modalità Direct NFS. Direct NFS non presenta opzioni separate nell'interfaccia utente; è solo una versione dell'accesso diretto allo storage. Il motivo di questa raccomandazione è che spesso l'Hot-Add provoca lo stun delle VM se il proxy Veeam non è eseguito sullo stesso host ESXi della VM. L'articolo KB1681 di Veeam fornisce ulteriori dettagli nella sezione relativa agli ambienti con data store NFS. Per coloro che volessero utilizzare comunque la modalità Hot-Add sui datastore NFS, il consiglio è quello di applicare le seguenti regole e impostazioni:

- Un unico proxy Hot-Add per host ESXi
- Impostare EnableSameHostHotAddMode = 1 in HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication

Nota: il backup Direct NFS esegue solo il backup delle VM senza gli snapshot esistenti. VMware raccomanda di rimuovere gli snapshot il prima possibile. Nel caso in cui sia presente uno snapshot della VM, Veeam eseguirà il failover su modalità di backup alternative.

Poiché esistono diverse opzioni per eseguire i backup, è possibile utilizzare la tabella seguente per quantificare i risultati di ciascuna modalità e decidere quale sia la migliore per il proprio scenario.

Mode	Operation	Time	Speed
Direct Storage Access	Full backup		
Direct Storage Access	Incremental backup		
Backup from Storage Snapshots	Full backup		
Backup from Storage Snapshots	Incremental backup		
Virtual Appliance	Full backup		
Virtual Appliance	Incremental backup		
Network	Full backup		
Network	Incremental backup		

La best practice: verificare quale modalità di backup sia più adatta per il proprio ambiente.

N.3: pianificare le modalità di ripristino

Dopo avere definito la modalità di backup ottimale, è importante considerare anche la modalità di ripristino. Qualunque siano i risultati dei test di ripristino, essi devono soddisfare l'obiettivo Recovery Time Objective (RTO), il che significa che potrebbe essere necessario utilizzare hardware con prestazioni più elevate. Veeam offre moltissimi scenari di ripristino per ripristinare le VM on-premises o da provider cloud, macchine fisiche, file e oggetti applicativi. A partire dalla versione 10, è possibile persino eseguire il ripristino istantaneo di qualsiasi backup a livello immagine su VMware.

Per prima cosa, è importante sapere che il ripristino di un file o di un oggetto è diverso dal ripristino di una VM o di un disco. Veeam ripristina file o oggetti (come le e-mail di Microsoft Exchange o gli oggetti di Microsoft Active Directory) tramite la rete. "Tramite la rete" significa una connessione RPC (Windows) o SSH (Linux), più delle porte data mover necessarie per trasferire i dati nelle VM. Il motivo di ciò è che Veeam è, per default, agentless per i backup delle VM . Per ridurre i requisiti a livello di porte ai fini dei backup e ripristini Windows, è possibile utilizzare il nuovo guest agent persistente Veeam nella versione 11.

Poiché il backup è basato su snapshot VM come un backup a livello di blocco, anche il ripristino di VM complete o dischi virtuali è basato su blocchi. A seconda della modalità di ripristino, il fatto che la VM sia stata sottoposta a thick o thin provisioning può fare la differenza. Le modalità di ripristino sono le stesse del backup (ovvero accesso diretto allo storage, appliance virtuale e rete). Oltre a ciò, è disponibile Instant VM Recovery abbinato a Storage VMotion o alla migrazione veloce.

L'Hot Add e la modalità di rete possono ripristinare le VM con thick e thin provisioning. Come già accennato, l'appliance virtuale o il trasporto Hot-Add offrono ottime prestazioni per il backup. Ciò vale anche per i ripristini di una VM o di un disco completi con il cosiddetto "Hot-Add". In molti scenari, è ragionevole avere almeno un proxy Hot-Add disponibile per il ripristino delle VM o dei dischi.

La modalità di rete è in genere il modo più lento per eseguire un ripristino.

La modalità di accesso diretto allo storage funziona molto bene, ma può ripristinare solo dischi sottoposti a thick provisioning. I dischi con thin provisioning verrebbero convertiti al volo in dischi thick. Poiché la modalità di accesso diretto allo storage utilizza VADP per i ripristini, non è solitamente l'opzione più veloce. Fa eccezione il ripristino con Direct NFS, in cui Veeam Backup & Replication non utilizza VADP.

Per ripristinare una VM o un disco virtuale, non è necessario trasferire completamente tutti i dati. Se le informazioni di Changed Block Tracking sullo storage di produzione sono corrette, è possibile eseguire un ripristino basato sul rilevamento dei blocchi modificati. La scelta di questa opzione può ridurre i tempi di ripristino; a tale scopo, l'opzione di rollback veloce deve essere abilitata manualmente durante il ripristino.

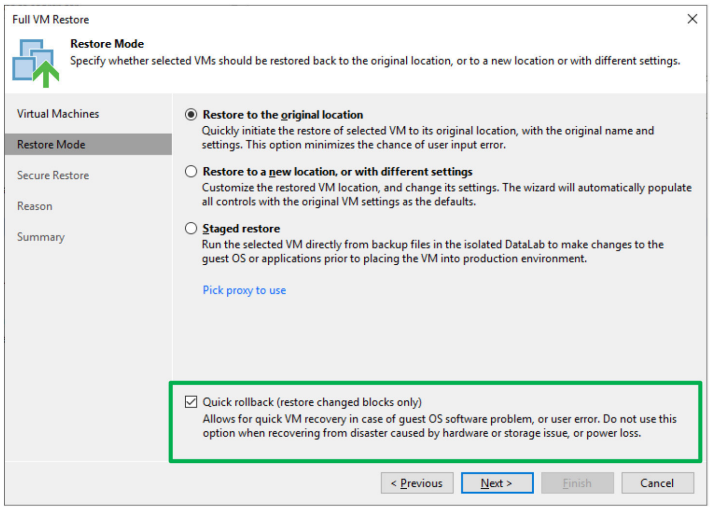


Figura 2: rollback veloce basato sulle informazioni di Changed Block Tracking

L'Instant VM Recovery è un modo alternativo per eseguire un ripristino completo della VM (ciò vale anche per il ripristino istantaneo del disco della VM al posto del ripristino completo del disco). La funzionalità Instant VM Recovery consente di avviare immediatamente una VM, direttamente dal repository di backup. Il repository di backup svolge il ruolo di datastore NFS montato su un host ESXi. Le prestazioni della funzionalità Instant VM Recovery sono migliorate notevolmente nella versione 10. Esistono due opzioni per trasferire i dati della VM dal datastore NFS del repository al datastore di produzione:

- Migrazione veloce Veeam
- VMware Storage VMotion

Poiché esistono diverse opzioni per il ripristino completo della VM, è possibile utilizzare la tabella seguente per quantificare i risultati di ciascuna modalità e decidere quale sia la migliore per il proprio scenario.

Mode	Operation	Time	Speed
Direct Storage Access	Full VM restore		
Direct Storage Access	Full VM restore CBT		
Virtual Appliance	Full VM restore		
Virtual Appliance	Full VM restore CBT		
Network	Full VM restore		
Network	Full VM restore CBT		
Instant VM recovery + Storage Vmotion	Full VM restore		
Instant VM recovery + Quick Migration	Full VM restore		

La best practice: pianificare e sottoporre a test le opzioni di ripristino in base al proprio storage e alle proprie modalità di trasporto. Se non si utilizzano i datastore NFS, è necessario installare almeno un proxy "Hot-Add" come riserva.

N.4: integrare la Continuous Data Protection di Veeam nella propria strategia di disaster recovery

Con Veeam Backup & Replication è possibile replicare le VM VMware a intervalli di secondi, senza snapshot VMware. La funzionalità si chiama Continuous Data Protection (CDP) e consente di ridurre i tempi di RPO e RTO per il disaster recovery. La funzionalità CDP si basa sulle vSphere APIs for IO Filtering (VAIO) e può essere utilizzata in modo simile alle classiche repliche di Veeam.

Durante la pianificazione della CDP, è necessario prendere in considerazione alcuni aspetti. Come sempre, è necessario allocare le risorse hardware per il trasferimento dei dati e per l'archiviazione dei dati modificati. Mentre i backup tradizionali avvengono ogni 8, 12 o 24 ore e utilizzano l'ampiezza di banda solo qualche volta al giorno, la CDP ha un continuo flusso di dati da trasferire. Le stime dell'ampiezza di banda possono essere effettuate monitorando il traffico dello storage in scrittura. Veeam applica la compressione e filtra i blocchi non necessari (ovvero trasferisce solo l'ultima versione di un blocco che è cambiato più volte nell'ambito della finestra dell'RPO). A causa di ciò, l'ampiezza di banda necessaria sarà leggermente ridotta rispetto a ciò che si vede nello storage.

Per quanto riguarda la destinazione del datastore VMware, è necessario disporre di sufficiente spazio libero e di capacità di I/O per i punti di ripristino. Tanto più basso è il tempo dell'RPO e tanto più lunga è la retention, quanto più spazio su disco è necessario. Raccomandiamo di utilizzare tempi di RPO di almeno 10 secondi. Un RPO di due secondi è possibile, tuttavia utilizza più spazio su disco e crea più I/O sul datastore di destinazione e le scritture sul datastore di destinazione non sono controllate. Nel caso in cui sul sistema di storage di destinazione vi siano anche VM di produzione, si raccomanda di utilizzare un datastore dedicato per le VM replicate.

A seconda del carico di I/O e del tempo dell'RPO, il traffico di rete della CDP potrebbe essere elevato. MTU 9000 aumenta di circa il 25% le prestazioni sulle reti a 10 Gbit/s. Si raccomanda inoltre un adattatore VMkernel dedicato, con un uplink fisico dedicato (o più uplink). Ciò garantisce che il traffico della funzionalità CDP non interferisca con altri tipi di traffico (ad es. il traffico di gestione). Non è necessario abilitare alcun servizio su questi adattatori VMkernel (vedi Figura 3). È possibile utilizzare gli switch virtuali (distribuiti) esistenti, senza alcuna necessità di configurare un vSwitch dedicato per il traffico CDP.

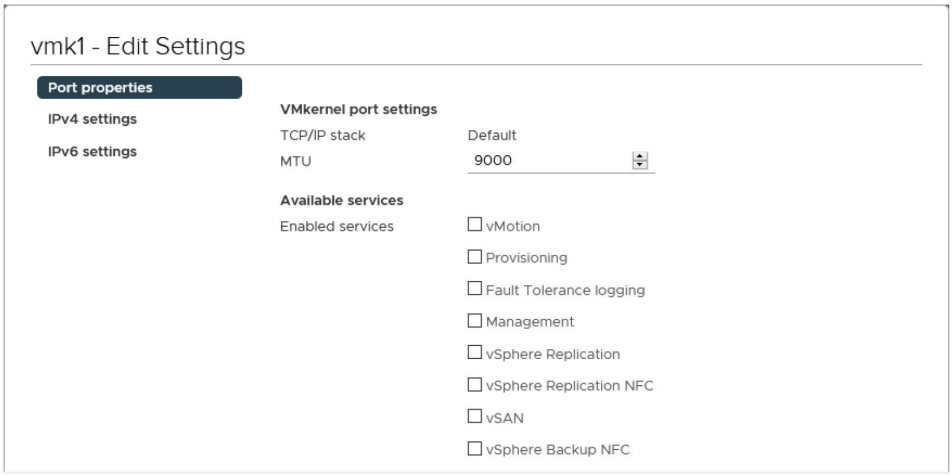


Figura 3: nessun servizio abilitato per la porta VMkernel

Le domande per la progettazione del proxy sono simili al backup:

- Pochi proxy (fisici) di grandi dimensioni
- Molti proxy (virtuali) di piccole dimensioni

Devono esserci almeno due proxy sorgente e di destinazione ai fini della ridondanza. Nel caso in cui si utilizzino dei proxy virtuali, un proxy per ESXi rappresenta il modo migliore per ottimizzare il flusso del traffico di rete. Si raccomanda inoltre di utilizzare dei proxy dedicati per sorgente e destinazione. Per la cache del proxy, si raccomandano SSD veloci per i carichi di lavoro misti.

La best practice: utilizzare Veeam Continuous Data Protection (CDP) per il disaster recovery se non si dispone di una funzionalità di replica basata sullo storage.

N.5: installare gli strumenti VMware

In molte situazioni, Veeam Backup & Replication fa affidamento sull'esistenza di strumenti VMware eseguiti nelle VM. Senza gli strumenti VMware, Veeam Backup & Replication non può trovare, per esempio, indirizzi IP o la versione del sistema operativo. Di conseguenza, l'elaborazione delle immagini application-aware non andrà a buon fine.

Ciò è dovuto al fatto che Veeam Backup & Replication non è in grado di rilevare l'indirizzo IP e, senza indirizzo IP, Veeam non può connettersi alla VM tramite la rete. Anche l'API vSphere o VIX del meccanismo di fallback per l'interazione guest non funzionano a causa della mancanza di strumenti VMware (consulta la best practice numero 10 per ulteriori informazioni su VIX). La Figura 4 lo dimostra in un esempio di test delle credenziali guest non riuscito a causa della mancanza di strumenti VMware:

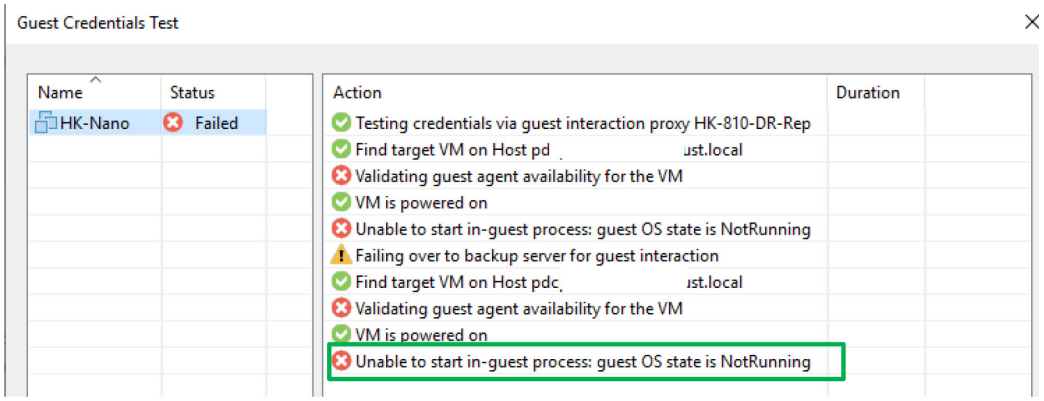


Figura 4: test dell'elaborazione application-aware non riuscito

Il secondo esempio sono i test di SureBackup. I test di heartbeat e di ping non andranno a buon fine se non sono presenti gli strumenti VMware. Per gli strumenti VMware vale la prima regola: mantenerli aggiornati.

La best practice: installare gli strumenti VMware e mantenerli aggiornati.

N.6: integrare gli snapshot basati su storage nella propria strategia di backup

Gli snapshot storage non sostituiscono i backup, tuttavia possono contribuire a ridurre al minimo la perdita di dati in molte situazioni. Veeam Backup & Replication è dotato delle integrazioni con diversi fornitori di storage in collaborazione con VMware vSphere. L'integrazione storage aggiunge ulteriori opzioni per la protezione dei dati. Un elenco dei sistemi di storage dotati di integrazione è disponibile qui.

Il primo vantaggio è che Veeam Backup & Replication può aprire snapshot storage e ripristinare file e oggetti direttamente dallo snapshot storage. In questo modo è possibile, ad esempio, pianificare gli snapshot storage ogni 15 minuti senza dover creare anche snapshot della VM. Sebbene uno snapshot ogni 15 minuti non sia un vero backup in quanto non soddisfa la regola 3-2-1, contribuisce a ridurre i tempi di RPO.

Nota: è possibile scegliere tra snapshot crash-consistent e consistenti a livello applicativo. Solo gli snapshot consistenti a livello applicativo creano uno snapshot VMware prima dello snapshot storage.

La Figura 5 mostra Veeam Explorer™ for Storage Snapshots, che segue un concetto simile. A sinistra ci sono gli snapshot storage (ovvero i LUN e gli snapshot di un solo LUN). A destra ci sono le VM di ciascuno snapshot storage. Da qui è possibile ripristinare le VM con Instant VM Recovery o ripristinare file e oggetti applicativi.

Ora immaginiamo che lo storage esegua degli snapshot di LUN o di volumi critici ogni 15 minuti e li elimini dopo quattro ore. Ciò significa che è possibile ripristinare i dati di 15 minuti fa, anziché i dati più vecchi dell'ultimo backup notturno.

"Utilizzo l'integrazione dello storage con Veeam, abbinando l'orchestrazione degli snapshot storage ai miei job di backup, nei quali utilizzo il backup dagli snapshot storage. L'abilitazione di entrambe le funzionalità in Veeam mi consente di avere a disposizione un unico pannello di gestione per la gestione dei miei storage snapshot e di allineare la retention degli snapshot storage alla programmazione dei miei backup. Ciò si è rivelato d'importanza chiave recentemente, quando ho dovuto ripristinare i nostri dati più critici che erano stati cancellati, eseguendo il ripristino completo dei dati con una perdita minima".

– Shane Williford, Systems Architect, North Kansas City School District

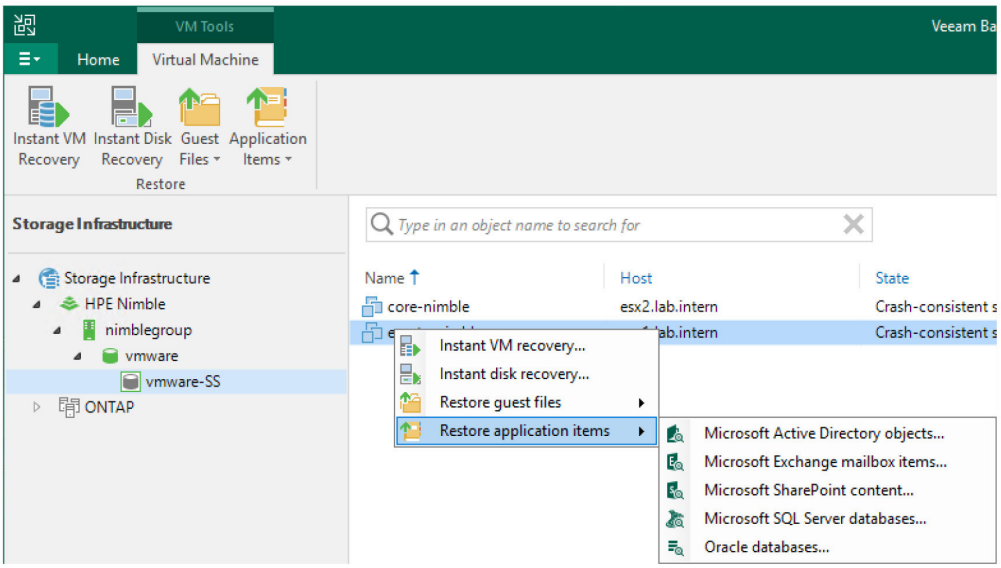


Figura 5: ripristino di oggetti da snapshot storage

Il secondo vantaggio offerto dall'integrazione dello storage consiste nella possibilità di eseguire backup dagli snapshot storage. Il backup dagli snapshot storage consente di eseguire il backup di VM altamente transazionali, come i server di database, senza il rischio di stun della VM durante il consolidamento degli snapshot VMware. Sebbene la situazione sia molto migliore con le attuali versioni di vSphere, questo è ancora il motivo principale per utilizzare gli snapshot storage.

Infine, il backup dagli storage snapshot consente a Veeam di utilizzare i propri meccanismi dei fetcher dei dati proprietari per superare in prestazioni i classici backup VADP. Ciò è particolarmente rilevante per i backup full o per qualsiasi backup con percentuali di modifica elevate.

La best practice: utilizzare l'integrazione storage se si dispone di uno storage che supporta gli snapshot per Veeam Backup & Replication.

N.7: backup di VMware vSAN

Protocolli di storage tradizionali, il che significa che non è disponibile l'accesso diretto allo storage o l'opzione di backup dagli storage snapshot.

Le modalità di backup supportate sono l'appliance virtuale/Hot-Add e la modalità di rete. La modalità di rete è l'opzione migliore, poiché non richiede il processo Hot-Add, questo può rendere più veloci i backup incrementali. Con la modalità Hot-Add, Veeam Backup & Replication esegue il backup delle VM in relazione alla prossimità dei dati della VM. Ciò significa che i backup avvengono tramite il proxy sull'host che contiene i dati più specifici della VM. Per far funzionare correttamente questo meccanismo, deve essere presente un unico proxy Hot-Add per host ESXi. L'affinità dell'host per le regole della VM proxy impedisce a VMware Distributed Resource Scheduler (DRS) di spostare tali VM su altri host ESXi.

Questo comporta finestre di backup più brevi, dato che il traffico di rete e la latenza sono minori. Se una VM si trovava su un host e il proxy su un host diverso, il traffico sulla rete è maggiore, con un conseguente aumento della latenza e una riduzione della velocità. Con la versione 10, Veeam ha introdotto il supporto per i proxy Linux che supportano la modalità Hot-Add. La versione 11 ha aggiunto il supporto per nuove modalità di backup per i proxy Linux, ad esempio:

- La modalità di rete (NBD) utilizzabile con vSAN
- Direct SAN (NFS, iSCSI e FC)
- Backup dagli storage snapshot (iSCSI, FC)

Veeam Backup & Replication è certificato come VMware Ready per vSAN all'interno della categoria di protezione dei dati.

Il VMware vSAN HCL contiene ulteriori informazioni. La compatibilità è valida anche per VSAN in VMware Cloud on AWS.

> *"Eseguiamo il backup della nostra infrastruttura vSAN con un proxy virtuale dedicato per ciascun host ESXi. A causa di ciò, ci sono molti proxy, ma sono relativamente piccoli (4 vCPU). Inoltre, la nostra configurazione cluster VSAN si trova sotto pressione a causa di data center molto distanziati tra di loro. Un proxy per ciascun host ESXi garantisce che Veeam assegni sempre il proxy "più vicino" a ciascuna VM che necessita di backup. Ciò evita traffico inutile sulle interconnessioni dei data center".*
>
> – Manuel Aigner, Porsche Informatik

La best practice: verificare quale modalità di backup è più veloce per il proprio ambiente. Un proxy Hot-Add per ESXi riduce il traffico di rete VSAN. In generale, l'Hot-Add ha un throughput più elevato, mentre la modalità di rete ha meno gestione.

N.8: sicurezza

Veeam Backup & Replication si collega a vCenter per gestire i backup e i ripristini delle VM. Dal punto di vista della sicurezza, è sempre consigliabile lavorare con i privilegi minimi richiesti. VMware vCenter offre permessi granulari per consentire i backup.

Il documento con i permessi necessari contiene una descrizione dettagliata dei permessi da configurare per le varie modalità di backup. Le diverse modalità di backup richiedono autorizzazioni diverse. Un'autorizzazione rilevante a livello di sicurezza con la modalità di backup appliance virtuale è quella "rimuovi disco". La Figura 6 mostra un ruolo dedicato, con autorizzazioni limitate adatte ai backup.

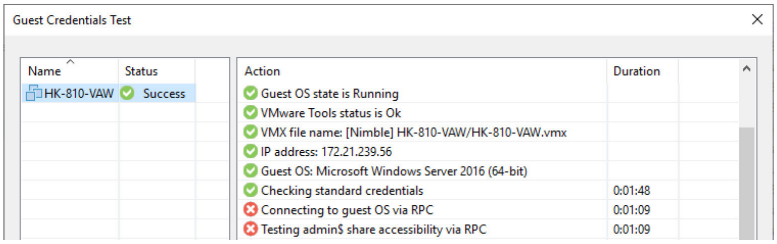


Figura 6: ruoli vSphere dedicati per Veeam Backup & Replication

Queste considerazioni sulla sicurezza possono influire sulla scelta della modalità di backup. È anche possibile limitare specifici server di backup (se ne esistono diversi) a posizioni o oggetti specifici in vCenter.

Poiché gli attacchi ai server di backup sono sempre più diffusi, l'ambiente di backup deve essere protetto maggiormente seguendo la guida alle best practice. Anche il "repository con protezione avanzata" è un'opzione da prendere in considerazione per la conservazione dei backup immutabili.

La best practice: lavorare entro i limiti del principio del privilegio minimo.

N.9: pianificare l'implementazione di Veeam Backup & Replication con Veeam ONE

Veeam Availability Suite™ contiene un potente strumento di pianificazione per le implementazioni di Veeam Backup & Replication chiamato Veeam ONE™.

Il monitor Veeam ONE mostra lo stato e i problemi attuali dell'ambiente vSphere. I problemi rilevanti legati al backup potrebbero essere, ad esempio, un'elevata latenza dello storage o snapshot della VM obsoleti, grandi, numerosi oppure orfani.

Il reporter Veeam ONE comprende il report di valutazione della configurazione delle VM che mostra eventuali problemi di backup.

I problemi tipici evidenziati dal report sono:

- Strumenti VMware non installati
- Versione hardware 4 o precedente
- Dischi di cui non è possibile eseguire il backup (ad esempio, dischi indipendenti)
- Datastore con spazio libero inferiore al 10%
- Raw device mapping nelle VM

La correzione di questi problemi prima di eseguire i backup evita ulteriori problemi di backup.

La best practice: utilizzare Veeam ONE per pianificare l'installazione di Veeam Backup & Replication.

N.10: backup application-aware tramite l'API VIX

La best practice numero 4 consiglia di installare e aggiornare sempre gli strumenti VMware. Gli strumenti VMware offrono all'amministratore Veeam la possibilità di eseguire backup application-aware per VM Windows senza una connessione di rete diretta alla VM.

La modalità preferita per eseguire un backup application-aware è collegare il proxy dell'applicazione tramite RPC o agente guest persistente alla VM. Questo è il modo più veloce. Se la segmentazione della rete o i firewall impediscono una comunicazione di rete con la VM, Veeam può utilizzare l'API VIX o, nelle versioni vSphere più recenti (la 6.5 e successive), l'API vSphere per l'interazione guest. La figura 6 mostra l'accesso tramite VIX contrassegnato in verde.

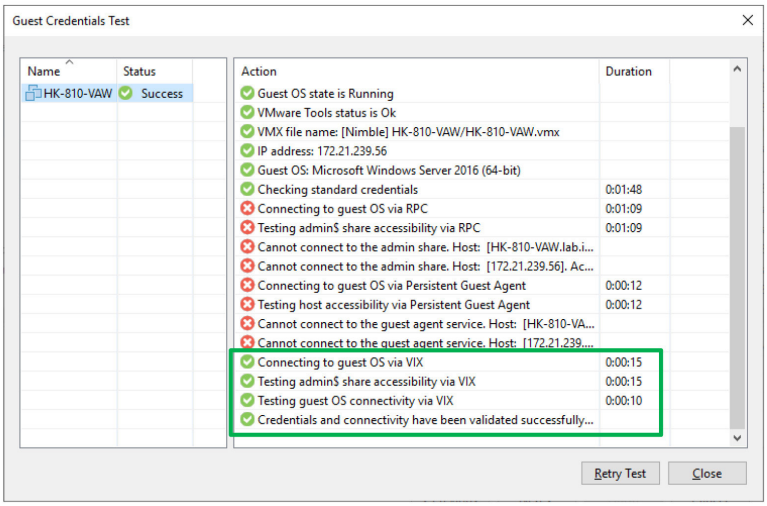


Figura 7: test delle credenziali guest tramite l'API VIX

L'API VIX o vSphere per l'interazione guest non è subito pronta all'uso. L'articolo KB 1788 di Veeam descrive i requisiti in dettaglio. Riassumendo, i requisiti sono due:

- L'account utente utilizzato da Veeam deve essere un membro del gruppo degli amministratori locali.
- Se l'account non riporta il titolo "amministratore", l'User Account Control (UAC) di Windows deve essere disabilitato.

L'API VIX o vSphere per l'interazione guest è la modalità di fallback se l'RPC non funziona. Il risultato per l'ambiente, in cui molte VM non sono raggiungibili tramite RPC, è che il backup impiegherà più tempo poiché Veeam prova sempre prima l'RPC. Per tali ambienti è possibile modificare l'ordine in "precedenza VIX" con la chiave di registro sul server di backup o il proxy di interazione guest seguente:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veeam\Veeam Backup and
Replication\ DWORD: InverseVssProtocolOrder

Value = 1

Per disabilitare (comportamento predefinito), il valore
è 0 (false)
```

È importante sapere che l'API VIX o vSphere per l'interazione guest presenta alcune limitazioni sulle operazioni di ripristino. Possono essere ripristinati solo i file e non gli elementi applicativi. Ciò significa che non è possibile ripristinare Microsoft Active Directory, Exchange o altri oggetti simili in questo modo e che per i ripristini è necessaria una connessione di rete. Il secondo aspetto è che il file è molto più lento quando si passa attraverso la rete.

A proposito di velocità, anche il servizio VeeamLogShipper che esegue il log-shipping di SQL è in grado di usare VIX come meccanismo di ripiego se non riesce a raggiungere il repository tramite la rete. Ciò potrebbe risultare troppo lento per la maggior parte degli ambienti. Detto ciò, si raccomanda di eseguire il log-shipping di SQL tramite la rete.

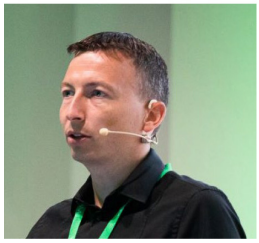
La best practice: tenere presenti le limitazioni dell'API VIX o vSphere per l'interazione guest.

Conclusioni

La combinazione di Veeam Backup & Replication e VMware vSphere è solitamente pronta all'uso, tuttavia queste best practice possono fare funzionare tutto ancor meglio e sono solitamente facilmente configurabili.

Per osservare in azione queste best practice, avvia una prova GRATUITA di 30 giorni.

Informazioni sull'autore



Hannes è un membro del Product Management Team di Veeam. In precedenza, è stato Senior Systems Engineer di Veeam per la regione CEMEA. In questo ruolo ha aiutato clienti e partner a progettare soluzioni di backup e DR efficienti ed efficaci, basate sui prodotti Veeam.

Ha gestito ambienti Linux e Windows, oltre a servizi di infrastruttura come storage, rete, firewall e VMware. Vanta più di 15 anni di esperienza nel business dell'IT.

Informazioni su Veeam

Veeam® è il leader nelle soluzioni di backup che offrono il Cloud Data Management™. Veeam offre una singola piattaforma per modernizzare il backup, accelerare il cloud ibrido e proteggere i dati. Con più di 400.000 clienti in tutto il mondo, tra cui l'82% delle aziende Fortune 500 e il 69% delle aziende Global 2.000, i punteggi di soddisfazione del cliente di Veeam sono pari a 3,5 volte la media di mercato, i più elevati del settore. L'ecosistema completamente di canale di Veeam comprende partner globali oltre a HPE, NetApp, Cisco e Lenovo come rivenditori esclusivi. Veeam ha uffici in oltre 30 Paesi. Per maggiori informazioni, visita https://www.veeam.com/it oppure segui Veeam su Twitter @veeam.