

Cele mai bune 12 practici pentru virtualizarea controlerelor de domeniu Active Directory

Greg Shields

Microsoft MVP și VMware vExpert

Modern Data Protection
Built for Virtualization | **#1 VM Backup**

Domeniul nostru se dezvoltă spre realitatea în care fiecare sarcină de lucru din domeniul IT poate să fie acum virtualizată.

Serviciile, aplicațiile, chiar bazele de date de mare capacitate au devenit acum candidați de mașini virtuale (VM) mulțumită îmbunătățirilor aduse tehnologiei hardware și hipervizorilor. Deși toate tipurile de aplicații funcționează peste mașinile virtuale de astăzi, realizarea aceluiași lucru cu controlerele de domenii Active Directory rămâne una dintre cele mai mari provocări din domeniul IT. V-ați putea minuna singur:

„Mi-aș putea virtualiza controlerele de domeniu, iar dacă aș face acesta, ce greșeli aș putea face?”

Răspunsul scurt este: *O mulțime.*

Un controler de domeniu se deosebește de alte sarcini de lucru IT printr-o diversitate de moduri. Implementarea sa pentru replicarea multi-master trebuie să fie proiectată cu atenție pentru a evita producerea erorilor de replicare. Serviciile sale necesită o bază de date tranzacțională care nu poate face obiectul unui backup precum fișierele sau folderele obișnuite. Cel mai important, funcționalitatea sa există ca fundație pentru fiecare alt serviciu IT. Pierdeți Active Directory și veți pierde această fundație. Pierdeți obiecte din acesta, iar persoanele și computerele reprezentate de aceste obiecte sunt blocate rapid.

Chiar dacă controlerele de domeniu sunt decisive pentru operațiunile IT, acestea nu reprezintă mari consumatori ai resurselor serverului. Chiar într-un mediu de 1.000 de utilizatori, aceștia nu ar putea constata creșterea bazei de date Active Directory proprii mult mai mult de aprox. 400 mega-octeți. Utilizarea procesorului și memoriei tinde să fie, de asemenea, relativ redusă. Aceeași organizație de 1.000 de utilizatori ar putea avea nevoie numai de un server cu procesor dual de un giga-octet sau două de RAM pentru a funcționa cu performanță bună.

Cu toate acestea, problema este faptul că controlerele de domeniu Active Directory - la un minim - vin în pereche. Datorită distanțelor geografice, multe medii necesită ele însele mai mult. Nu este un lucru fără precedent ca pentru o organizație distribuită pe o suprafață mare să fie nevoie de grupuri de zece sau douăsprezece controlere de domeniu pentru a servi necesitățile de autentificare ale clienților. Pentru ceea ce este un serviciu relativ ușor, Active Directory pe un server fizic reprezintă un cost care pare ușor de îndepărtat prin intermediul virtualizării.

Cele mai bune 12 practici care nu trebuie să vă lipsească

Cele anume face ca aceste activități virtuale să comute brusc de la ușor la dificil? Răspunsul se află în complexitate. Gestionarea unui mediu VMware vSphere este la început o sarcină simplă: Instalați ESX(i), porniți mașinile virtuale, monitorizați-le performanțele, asigurați-vă că obțineți resursele de care au nevoie. Totuși, prin funcționarea respectivei infrastructuri virtuale cresc în proporție geometrică multe provocări, deoarece se mărește numărul dumneavoastră de gazde și mașini virtuale.

Mai mult hardware adaugă mai multe interdependențe. Mai multe mașini virtuale necesită mai mult hardware. Mai multe activități de afaceri generează mai multe mașini virtuale. Ca rezultat, menținerea nivelurilor celor mai ridicate de consolidare a serverului și a celei mai bune performanțe devine rapid o activitate pe care niciun om nu o poate efectua fără ajutor.

Contrar a ceea ce v-ați putea gândi, virtualizarea controlerelor de domeniu nu este o activitate în care să vă aventurați ușor. În timp ce virtualizarea aduce într-adevăr beneficii, aduce de asemenea și riscuri atunci când controlerele de domeniu nu sunt create în mod inteligent. Din fericire, industria noastră începe să accepte un set de recomandări inteligente care asigură sănătatea și securitatea controlerelor de domeniu virtualizate. Dacă luați în considerare virtualizarea pentru controlerele dumneavoastră de domeniu Active Directory, sau chiar dacă le-ați virtualizat deja, nu trebuie să omiteți aceste 12 importante cele mai bune practici.

Neglijarea recomandărilor oricăreia dintre aceste practici poate defecta întreaga dumneavoastră infrastructură de calcul.

Cea mai bună practică nr. 1:

Controlerele de domeniu necesită disponibilitate ridicată a mașinilor virtuale

Controlerele de domeniu care alimentează Active Directory reprezintă un miracol de disponibilitate ridicată. Prin valorificarea replicării multi-master, rar întâlnită în aplicațiile bazelor de date, Active Directory este prin el însuși un serviciu remarcabil de rezilient. Așa și trebuie să fie. Ca la orice parte a infrastructurii Windows care necesită servicii de autentificare ale Active Directory, aceste servicii trebuie să aibă mereu o disponibilitate ridicată.

Totuși, cu această disponibilitate ridicată, se așteaptă ca controlerele de domeniu să fie aproape întotdeauna operaționale. Active Directory însuși merge până la dezactivarea memoriilor cache pentru scrierea pe disc în cazul volumelor care găzduiesc fișierele sale de baze de date și jurnal. Această acțiune ajută la păstrarea integrității bazei de date în cazul în care serverul s-ar defecta în mod neașteptat.

Chiar și așa, prevenirea întreruperii funcționării controlerelor de domeniu trebuie să fie o prioritate. *Orice controler de domeniu virtualizat trebuie să fie găzduit într-un mediu virtual cu disponibilitate ridicată.* Gruparea în clustere a gazdelor virtuale permite ca mediul să închidă rapid o mașină virtuală pe o gazdă nouă atunci când se produc probleme, readucând rapid online respectivul controler de domeniu. Nu este o bună practică să se virtualizeze un controler de domeniu pe o gazdă care nu dispune de o infrastructură cu un grad înalt de disponibilitate la nivel de mașină virtuală.

Cea mai bună practică nr. 2:

Niciodată întreruperi, niciodată clonare, niciodată instantanee... cu excepția...

La prima vedere, virtualizarea pare să realizeze adăugarea unui interval larg de noi capacități pentru serverele virtuale. Odată virtualizat, starea unui server poate fi întreruptă, poate fi activată sau poate fi dezactivată. Discurile sale pot fi transformate în instantaneu și/sau clonate pentru protejarea conținutului acestora sau duplicarea lor în altă parte.

Aceste instantanee hipervizor, întreruperi și clonări ale capacităților sunt funcții ale platformei virtuale care constituie fundamentul pentru mașinile dumneavoastră virtuale. Acestea pot fi tactici excelente în căutarea de către administratorul virtual a unor soluții administrative pentru numeroase tipuri de servere. *Cu toate acestea, utilizarea oricăreia dintre ele în acest mod pentru un controler de domeniu nu este niciodată recomandată.*

Revenirea la un instantaneu anterior al mașinii virtuale a unui controler de domeniu derulează de fapt acel server în sens invers în timp. De asemenea, derulează în sens invers baza de date a controlerului de domeniu, ceea ce reprezintă un comportament pe care replicarea multi-master a Active Directory nu a fost niciodată proiectată să îl trateze. Coruperea bazei de date, derularea înapoi a USN și problemele de replicare sunt numai câteva dintre rezultatele neplăcute care se pot produce. Probleme similare pot apărea în cazul în care funcționarea controlerului de domenii virtualizat este întreruptă pentru o perioadă de timp prea lungă.

Clonarea discurilor controlerului de domeniu introduce o întreagă altă serie de probleme și trebuie să fie evitată întotdeauna. Atunci când un controler de domeniu detectează faptul că semnătura sa pe disc a fost schimbată, o situație care se poate produce la clonare, controlerul de domeniu se va auto-izola de la replicarea multi-master. Controlerul de domeniu poate părea că funcționează, dar alte controlere de domenii nu mai au funcția de replicare cu acesta. În timp, această situație creează o discrepanță între conținutul controlerului de domenii izolat și conținutul celorlalte controlere. Utilizatorilor cu conturile șterse ar putea totuși să le fie recunoscută în continuare autentificarea de acces. Alți utilizatori cu conturi nou create ar putea constata rezultate impredictibile. Evitați toate aceste probleme prin evitarea în întregime a clonării.

Acest ghid pentru principiul „niciodată instantanee” are o obiecție importantă. Unele soluții pentru protecția datelor sunt capabile de o funcționare complet silențioasă cu recunoașterea aplicației în timpul unui luării unui instantaneu. Această funcționare silențioasă previne problemele de corupere a datelor care se pot produce în cazul unor instantanee hipervizor neasistate. Deci, niciodată instantanee...numai dacă mașinile dumneavoastră virtuale se bucură de asistența unei astfel de soluții de protecție a datelor.

Cea mai bună practică nr. 3: Nu toate backup-urile sunt create egale

Luarea de instantanee și clonarea pentru platformele virtuale sunt activități care nu trebuie să fie încercate niciodată pentru un controler de domeniu. Altfel spus, termenii „instantaneu” și „clonă” au uneori alte semnificații în afara platformei virtuale, precum în cazul unor soluții de backup. Chiar dacă serviciul Microsoft încorporat de copiere din umbră a volumelor utilizează termeni similari pentru a descrie procesele de backup și restaurare care sunt, în fapt, idei bune pentru backup-urile controlerului de domeniu.

De aceea, a treia cea mai bună practică din această listă sugerează să vă autoeducați în ceea ce privește toate opțiunile de backup disponibile pentru controlerul de domeniu. Soluția de backup pe care o doriți este una care adună rapid datele necesare printr-o abordare bazată pe imagine, la nivel de bloc. Acționând astfel, se asigură o protecție aproape continuă a datelor în timpul expunerii întregului interval al restaurării elementului unic pe tot parcursul recuperării întregii păduri.

Nu puteți atinge acest obiectiv doar cu instrumentele native Microsoft. Instrumentele Microsoft pentru soluția de backup pentru Active Directory nu au fost create niciodată cu gândul să fie prietenoase cu utilizatorii. Restaurarea obiectelor individuale este dificilă. Restaurarea integrală a controlerelor de domeniu necesită un proces în mai mulți pași, plin de riscuri. Încercarea de recuperare a unei păduri corupte este o sarcină cu care chiar cei mai experimentați administratori IT nu au succes fără a primi ajutor.

Soluția corectă vă va permite să restaurați orice obiect, server sau pădure înapoi în orice perioadă de timp. Această perioadă de timp ar putea însemna „ieri” sau „acum 15 minute” în funcție de cerințele dumneavoastră referitor la recuperare.

Cea mai bună practică nr. 4: Evitați abaterea de la sincronizare a ceasului

Păstrarea ceasurilor sincronizate corespunzător este o sarcină care nu este foarte dificilă pe serverele fizice. Odată sincronizat, ceasul unui server fizic va rămâne la ora corectă pentru mult timp. Același lucru nu este neapărat adevărat în mediile virtuale. Datorită modelelor neregulate ale atenției pe care o mașină virtuală o obține de la hipervizorul său, abaterea de la sincronizare a ceasului este o problemă care necesită o atenție constantă.

Abaterea de la sincronizare a ceasului într-o mașină virtuală poate fi manipulată de către instrumentele instalate pe platforma virtuală, sau poate fi manipulată prin sincronizarea ceasurilor cu o sursă de timp externă. Alegeți una din soluții și utilizați-o pentru fiecare controler de domeniu virtual pe care îl implementați. Indiferent ce opțiune ați ales, acordați o atenție deosebită ceasurilor controlerelor dumneavoastră de domeniu. Dacă ceasurile acestora suferă o abatere chiar și de numai cinci minute, veți constata că controlerele dumneavoastră de domeniu nu mai răspund la cererile clienților.

Cea mai bună practică nr. 5: Nu supra-provizionați cu resurse

Când profesioniștii în prototipuri IT creează un controler de domeniu peste un server fizic, constată adesea că au utilizat o configurație standard. „Procesoare dual core și patru giga-octeți de memorie RAM” reprezintă un crez comun pe care îl veți auzi de la administratori. Acest nivel de putere de procesare și de memorie are sens atunci când controlerele de domeniu se află pe un hardware fizic. Diferența de cost dintre un giga-octet și patru giga-octeți de memorie RAM este adesea mai mică decât timpul necesar pentru inginer să corecteze cantitatea.

Mediile virtuale sunt foarte diferite. Chiar și cu angajarea în exces a resurselor integrate în hipervizoarele actuale, alocarea a prea multor resurse la o mașină virtuală reprezintă încă o risipă inutilă. Resursele gazdei sunt necesare pentru gestionarea angajării în exces, iar mașinile virtuale cu angajări inutile de mari ale resurselor pot complica activitățile de echilibrare a încărcării.

Nu vă faceți mediul virtual să lucreze mai mult decât este necesar. Utilizați instrumentele de management al performanței pentru a găsi și pentru a alocă cantitatea corectă a necesităților mașinilor virtuale și pentru a evita alocarea procesoarelor virtuale multiple ori de câte ori este posibil.

Cea mai bună practică nr. 6: Asigurați-vă că backup-urile funcționează în realitate

Nesăbuit este profesionistul IT care se concentrează prea exclusiv pe backup-uri; este înțelept profesionistul IT care recunoaște faptul că de fapt caracterul restaurabil este scopul final. Chiar dacă facem referire la această clasă de software ca la „soluții de backup”, ascundem realitatea faptului că un backup nu este utilizabil decât dacă poate fi restaurat într-un mod verificabil.

Soluția corectă pentru protejarea datelor dumneavoastră Active Directory nu va realiza numai backup și restaurare pentru datele respective, ci, de asemenea, va verifica în mod automat integritatea fiecărui backup. Doriți o soluție care efectuează o verificare a integrității pentru fiecare backup în numele dumneavoastră. Această verificare vă oferă garanția că fiecare restaurare de obiect, controler de domeniu sau pădure se va fi finaliza cu succes.

Cea mai bună practică nr. 7: Implementați regulile anti-afinitate

Mașinile virtuale se mișcă în mod constant în mediul lor virtual. Natura întotdeauna schimbătoare a utilizării resurselor serverului înseamnă că echilibrarea încărcării este o activitate care nu se termină niciodată. Dar cu toate că relocarea mașinilor virtuale este un lucru foarte bun pentru păstrarea echilibrului, aceasta introduce de asemenea posibilitatea ca două controlere de domeniu să ajungă în situația de a fi amplasate pe aceeași gazdă (colocare). Această colocare este o situație pe care doriți să o evitați.

Fiecare platformă virtuală sosește echipată cu o implementare unică a ceea ce are denumirea generică de „reguli de afinitate”. Regulile de afinitate permit unui administrator să determine care dintre mașinile virtuale trebuie întotdeauna și care nu trebuie niciodată să ajungă în situația de a fi amplasate pe aceeași gazdă ca rezultat al relocărilor pentru echilibrarea încărcării. *O regulă anti-afinitate este importantă pentru orice controler de domeniu virtualizat. Această regulă va instrui mediul virtual pentru a se asigura că niciodată controlerele de domeniu nu vor ajunge în situația de a fi amplasate pe aceeași gazdă. Separarea acestor controlere de domeniu asigură faptul că pierderea unei gazde nu va cauza întreruperea funcționării unui întreg Active Directory.*

Cea mai bună practică nr. 8: Separați traficul clienților de cel al administratorului

Clicurile pe un buton roșu pentru a opri o mașină virtuală nu diferă de butonul de pornire/oprire al unui server fizic. Apăsăți acel buton, fie fizic, fie virtual, și mașina virtuală împreună cu sarcina sa de lucru urmează să se oprească.

Operațiile de pornire/oprire, luarea de instantanee, clonarea și migrarea reprezintă activități care sunt efectuate de o consolă de management al platformei virtuale. Acestea reprezintă de asemenea acțiuni la care utilizatorii obișnuiți nu trebuie să aibă niciodată acces. Dumneavoastră blocați ușile de la centrul dumneavoastră de date, permițând accesul doar pentru un număr mic de privilegiați. Trebuie să faceți același lucru cu infrastructura dumneavoastră virtuală. *Separarea traficului de rețea al clienților de traficul utilizat pentru activitățile în mediu virtual este tot atât de importantă ca și blocarea centrului dumneavoastră de date.* Procedând astfel, se protejează butoanele importante, cele virtuale în acest caz, față de apăsarea accidentală (sau în mod răuvoitor).

Cea mai bună practică nr. 9: Acordați prioritate restaurărilor rapide ale obiectelor

Până la versiunea Windows Server 2008 R2, Active Directory nu a beneficiat de funcții pentru a trata restaurările obiectelor individuale. Chiar și cu această versiune, lucrul cu Recycle Bin nativ din Active Directory reprezintă o adevărată provocare. Sunt necesare operațiuni complexe PowerShell pentru colectarea datelor și restaurarea obiectelor șterse. Chiar și găsirea obiectului corect care trebuie restaurat este dificilă, în special când viteza este cerința cheie.

Din acest motiv, fiecare controler de domeniu, virtualizat sau nu, trebuie protejat utilizând soluții care acordă prioritate restaurărilor rapide. Virtualizarea poate asigura suport pentru acest proces. De exemplu, un controler de domeniu virtualizat poate fi restaurat într-o locație protejată în scopul restaurării datelor. După restaurare, controlerul de domeniu poate fi eliminat în siguranță fără a afecta mediul de producție.

Alegeți o soluție de backup pentru Active Directory care să restaureze obiectele pierdute cu timp și eforturi minime. Vă veți bucura de timpul câștigat la următoarea ștergere accidentală a unei unități organizatorice pline de obiecte.

Cea mai bună practică nr. 10: Monitorizați performanța de stocare

În zilele de început ale virtualizării, procesarea și memoria erau considerate două din cele mai mari obstacole în calea unei performanțe acceptabile. În acele timpuri, obținerea unei puteri de procesare suficiente pentru mașinile virtuale care aveau nevoie de ea era o prioritate pentru fiecare administrator virtual.

În zilele noastre, stocarea a devenit sursa principală a scăderii performanței. Scăderea performanței se poate produce ca urmare a conexiunilor incorect configurate sau cu un număr excesiv de abonamente. Poate proveni din suprataxarea discurilor SAN sau din concurența pentru axul de rotație a discului. *Deși controlerele de domeniu virtualizate tind să nu aibă cerințe de performanță privind stocarea de volume foarte mari, monitorizarea indicelui IOPS (operațiuni de intrare/ieșire pe secundă) asociat conexiunilor de stocare este important pentru gestionarea performanței.* Chiar dacă este posibil ca controlerele dumneavoastră de domeniu să nu necesite cele mai rapide discuri din lume, activitățile altor gazde și mașini virtuale pot crea probleme. Numai prin monitorizarea comportamentelor de stocare aceste activități cu impact pot fi depistate și rezolvate.

Cea mai bună practică nr. 11: Rămâneți puțin în planul fizic

Chiar cu beneficiile pe care virtualizarea le aduce serverelor, mediul dumneavoastră virtual în sine poate fi un unic punct de defectare. Vulnerabilitățile hipervizorului, întreruperile stocării și utilizarea în exces a resurselor sunt, toate, scenarii extreme care pot conduce la o defectare pe scară largă a mediului virtual.

Acest tip de defectare devine chiar și mai problematic atunci când întregul dumneavoastră Active Directory se află în mediul virtual care s-a defectat. Adeseori, rezolvarea defecțiunii începe prin remedierea serviciilor de director. Dacă serviciile de director nu pot fi făcute disponibile, rezolvarea problemei devine un proces semnificativ mai provocator.

Revenirea unui mediu virtual defect la starea de funcționare necesită aceeași fundație Active Directory de care au nevoie serverele dumneavoastră atunci când funcționează. *De aceea, păstrarea cel puțin a unui controler de domeniu ca server fizic va asigura păstrarea fundației dumneavoastră Active Directory, chiar în timpul celor mai grave defecțiuni ale mediului dumneavoastră virtual.*

Cea mai bună practică nr. 12:

Trebuie să aveți o soluție planificată pentru recuperarea în caz de dezastru

Pregătirea pentru tot ce este mai rău înseamnă mai mult decât un simplu plan pentru recuperarea în caz de dezastru. Această pregătire necesită, de asemenea, soluții care să permită executarea respectivului plan. *Încorporarea instrumentelor pentru realizarea de backup pentru Active Directory este doar o parte a planului. Verificarea regulată a funcționalității instrumentelor dumneavoastră și a capacității acestora de restaurare a serverelor și datelor - iată ce funcții trebuie să îndeplinească soluția dumneavoastră.*

Nu puteți atinge acest obiectiv doar cu soluțiile de backup native. Într-adevăr, soluțiile de backup native la nivel de Windows vor captura o copie a Active Directory, dar într-un mod în care restaurarea nu se poate realiza ușor după producerea dezastrului. Aceasta nu este o soluție care să funcționeze.

O soluție care funcționează este o soluție care restaurează integral controlerele de domeniu (precum și alte servere) în intervale de ordinul minutelor, nu al zilelor, restaurând rapid mediul dumneavoastră pentru a vă readuce rapid afacerea în mediul online. Căutați soluții care să poată restaura funcționalitatea mașinilor virtuale fără întârzierea mare necesară restaurării fizice a datelor acestora. La sfârșitul zilei, aveți nevoie de un Active Directory care să funcționeze. Soluția corectă va aduce rapid aceste servicii online și, în același timp, va finaliza în fundal procesul lung și lent de restaurare.

Virtualizați cu atenție controlerele de domeniu. Protejați datele acestora cu atenție crescută.

Luarea deciziei de a vă virtualiza controlerele de domeniu Active Directory poate fi un lucru inteligent pentru operațiunile centrului de date. Procedând astfel, eliberați resursele serverului pentru alte activități. De asemenea, în acest fel se adaugă funcții de disponibilitate ridicată și migrare, funcții de care beneficiază fiecare server virtual. Dar, cu toate că virtualizarea acestor controlere de domeniu vă poate face viața mai ușoară, o virtualizare incorectă va avea efectul opus. Aceste cele mai bune 12 practici ar trebui să vă ghideze către configurația corectă și designul corect.

O parte majoră a designului respectiv include găsirea soluțiilor adecvate pentru protejarea datelor din Active Directory. În calitate de fundație a întregului dumneavoastră centru de date, protejarea datelor necesită o atenție extremă. Procedați inteligent în privința modului în care vă virtualizați controlerele de domeniu. Procedați și mai inteligent în privința modului în care protejați datele acestora.

Despre autor



Greg Shields, Microsoft MVP și VMware vExpert, este un autor, orator și consultant IT independent, precum și un partener și tehnician principal la Concentrated Technology. Având 15 ani de experiență vastă în domeniul tehnologiei informațiilor, Greg beneficiază de o experiență extinsă în administrarea, ingineria și arhitectura sistemelor, fiind specializat în sisteme de operare Microsoft, aplicații la distanță, gestionarea sistemelor și tehnologiile de virtualizare.

About Veeam Software

Veeam® este o protecție modernă a datelor (Modern Data Protection™)- care furnizează soluții puternice, ușor de utilizat și accesibile ca preț, special concepute pentru virtualizare (Built for Virtualization™) și pentru cloud.

Veeam Backup & Replication™ furnizează **backup VMware**, **backup Hyper-V**, recuperare și replicare. Această soluție #1 VM Backup™ ajută organizațiile să își îmbunătățească obiectivele privind punctele de recuperare și timpii de recuperare, să economisească timp prețios, să elimine riscurile și să reducă dramatic cheltuielile de capital și cheltuielile operaționale. **Veeam Backup Management Suite™** combină Veeam Backup & Replication și **Veeam ONE™** într-o singură soluție integrată pentru a vă proteja investițiile în virtualizare, a crește productivitatea administratorului și a ajuta la reducerea riscurilor de management zilnice. **Veeam Management Pack™** (MP) extinde monitorizarea la nivel de întreprindere la VMware folosind Microsoft System Center. De asemenea, Veeam furnizează instrumente gratuite pentru comunitatea celor ce lucrează în domeniul virtualizării.

Înființată în anul 2006, Veeam are acționariat privat și este profitabilă începând din anul 2009. În prezent, Veeam are peste 19.000 de parteneri de tip ProPartner și 73.000 de clienți în întreaga lume. Sediul central al Veeam se află în Baar, Elveția, compania având birouri în întreaga lume. Pentru a afla mai multe, vizitați <http://www.veeam.com>.



Microsoft Partner
Gold Application Development
Gold Management and Virtualization

Modern Data Protection

Built for Virtualization

Powerful

Easy-to-Use

Affordable

Veeam Backup & Replication

#1 VM Backup for VMware and Hyper-V

Virtualization changes everything – especially backup. If you've virtualized on **VMware or Hyper-V**, now is the time to move up to the data protection solution Built for Virtualization: **Veeam Backup & Replication**.

Unlike traditional backup that suffers from the "3C" problem (missing capabilities, complexity and cost), Veeam is:

- **Powerful:** Dramatically improve your RPOs and RTOs
- **Easy-to-Use:** Save time and eliminate risk
- **Affordable:** Reduce TCO and increase ROI

Join the 80,000 organizations who have already modernized their data protection with Veeam. **Download Veeam Backup & Replication** today!



To learn more, visit <http://www.veeam.com/backup>