

IMPLEMENTAREA TEHNOLOGIEI DE VIRTUALIZARE A SERVERELOR PENTRU MEDIUL DE AFACERI

Adrian MIHALCEA

Departamentul Telecomunicații și Sisteme Electronice, grupa RST-191FR,
Facultatea Electronică și Telecomunicații, Universitatea Tehnică a Moldovei, Chișinău, Rep. Moldova

*Autorul corespondent: Adrian Mihalcea, adrian.mihalcea@tlc.utm.md

Îndrumător/coordonator științific: **Andrei DOROGAN**, dr., l. univ., FET, UTM

Rezumat: În lucrare este explorată o soluție de virtualizare a serverului, ce are ca scop disocierea software-ului serverului de infrastructura sa hardware. Această abordare permite crearea mai multor servere virtuale pe un server fizic, fiecare operând cu un sistem de operare independent, eliminând problemele de compatibilitate. Tehnologia de virtualizare este o componentă fundamentală pentru "cloud computing", facilitând optimizarea utilizării resurselor de găzduire web și reducând semnificativ costurile implicate. Sistemul de virtualizare permite o gestionare eficientă a resurselor informaționale, asigurând un mediu securizat pentru stocarea datelor și rularea aplicațiilor.

Cuvinte cheie: server virtual, mașină virtuală, hypervisor, sistem de operare

Introducere

Virtualizarea serverului reprezintă o aplicație prin care o organizație poate detașa software-ul serverului de hardware-ul său și poate crea mai multe servere virtuale, fiecare cu propriul sistem de operare și care rulează pe același server fizic. Fiecare server virtual este complet separat de celelalte și funcționează independent, fără existența problemelor de compatibilitate. Tehnologia de virtualizare a serverelor este fundamentală pentru cloud computing și permite implementarea diverselor modele de cloud hibrid.

Prin virtualizarea serverelor, o organizație poate eficientiza utilizarea și furnizarea serviciilor de găzduire web, reducând costurile și maximizând utilizarea resurselor de calcul, stocare și rețea pentru întreaga infrastructură. Deoarece puterea de procesare a serverele este rar utilizată în mod constant, multe resurse de server rămân neutilizate. De regulă, resursele utilizate ale unui server sunt într-un interval de 15 – 25%. Astfel, serverele pot rămâne inactive ore sau chiar zile, în timp ce volumul de muncă este distribuit la un procent mic pentru toate resursele serverului unei organizații. Serverele inactive ocupă spațiul neutilizat, consumă energie și necesită atenție și efort din partea personalului IT pentru mentenanța lor.

Virtualizarea serverului permite organizației de a consolida multiple servere virtuale (cunoscute și sub denumirea de mașini virtuale sau VM-uri) pe un singur server fizic (Figura 1), astfel încât resursele serverului să fie utilizate într-un mod mai eficient. Aceasta permite unui centru de date să funcționeze mai eficient, având nevoie de mai puține mașini fizice. Prin virtualizare, organizațiile pot gestiona eficient resursele utilizate și adapta dinamic sarcinile de lucru pe măsura necesităților.

Virtualizarea memoriei

Pe lângă virtualizarea resurselor procesorului (CPU), virtualizarea memoriei este importantă și implică partajarea memoriei fizice a sistemului și alocarea dinamică a acesteia mașinilor virtuale. Virtualizarea memoriei mașinii virtuale este asemănătoare cu suportul pentru memorie virtuală oferit de sistemele de operare moderne. Aplicațiile detectează un spațiu de adrese continuu, care nu este neapărat legat de memoria fizică subiacentă din sistem. Sistemul de operare păstrează coordonatele (mapările) numerelor de pagini virtuale cu numerele de pagini fizice stocate în tabelele de pagini. Toate procesoarele moderne includ o unitate de gestionare a memoriei (MMU) și un buffer de traducere (TLB) pentru a optimiza performanța memoriei virtuale.

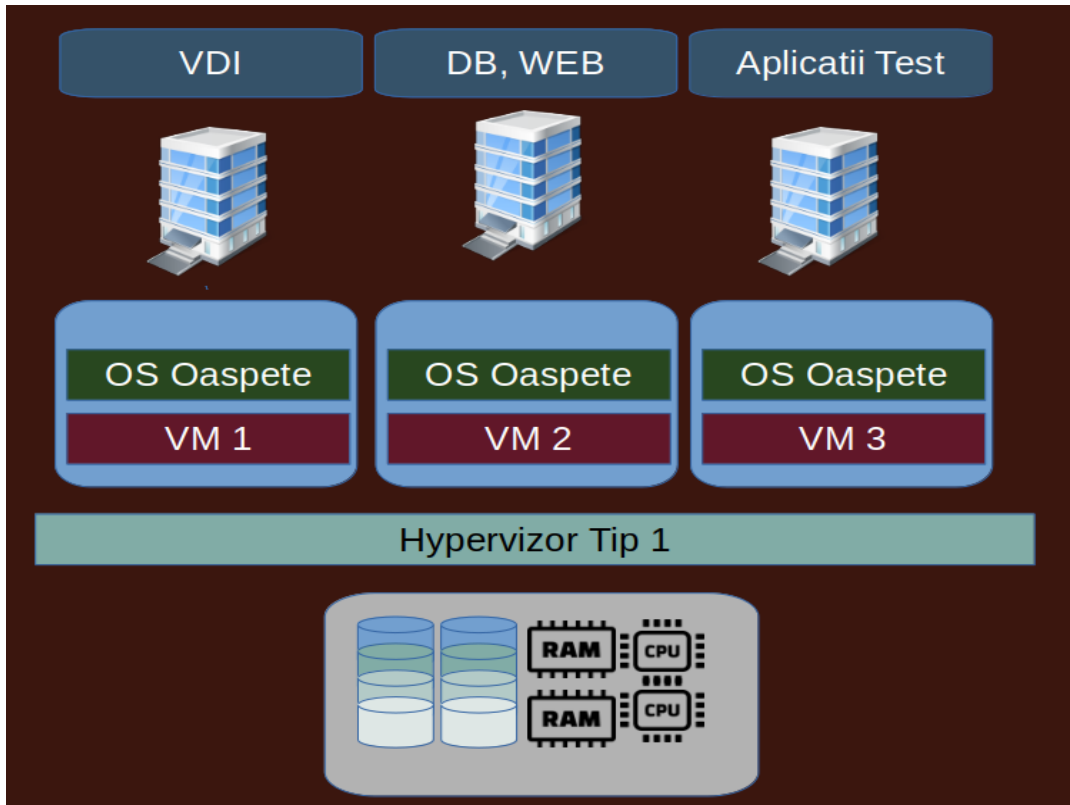


Figura 1. Virtualizarea unui server fizic în mai multe instanțe virtuale

Pentru a rula mai multe mașini virtuale pe un singur sistem, este necesar un alt nivel de virtualizare a memoriei. Cu alte cuvinte, este necesar de virtualizat MMU-ul pentru a asigura sistemul de operare (OS) instalat. Sistemul de operare continuă să controleze maparea adreselor virtuale la adresele fizice ale memoriei, însă sistemul de operare nu poate avea acces direct la memoria reală a mașinii. VMM (Managerul memoriei virtuale) este responsabil pentru maparea memoriei fizice virtualizată în memoria reală a mașinii și utilizează tabele de pagini pentru a accelera mapările.

VMM utilizează hardware-ul TLB pentru a mapa memoria virtuală direct în memoria mașinii, pentru a evita cele două niveluri de traducere pe fiecare acces. Atunci când sistemul de operare modifică memoria virtuală în maparea memoriei fizice, VMM actualizează tabelele de pagini pentru a permite o căutare directă. Virtualizarea MMU creează unele cheltuieli generale pentru toate abordările de virtualizare, dar acesta este domeniul în care virtualizarea asistată de hardware de a doua generație va oferi câștiguri în eficiența de operare.

Virtualizarea componentelor I/O

Componenta finală necesară, cu excepția CPU și virtualizării memoriei, este virtualizarea dispozitivului și virtualizarea intrărilor/ieșirilor (I/O). Aceasta implică gestionarea solicitărilor I/O de rutare între dispozitivele virtuale și hardware-ul fizic partajat.

Virtualizarea și gestionarea I/O bazate pe software, spre deosebire de cea hardware, oferă un set de opțiuni și o gestionare simplificată. Cu ajutorul rețelelor, de exemplu, NIC-urile (placa de rețea) virtuale și switch-urile creează rețele virtuale între mașinile virtuale, fără ca traficul de rețea să consume bandă în rețeaua fizică (Figura 2), Echiparea NIC permite mai multor NIC-uri fizice să apară ca unul și același, iar mașinile virtuale pot fi relocate fără probleme în diferite sisteme, păstrând în același timp adresele MAC existente. Ideea pentru virtualizarea eficientă a I/O este de a păstra aceste beneficii ale virtualizării, menținând în același timp utilizarea CPU la un nivel minim.

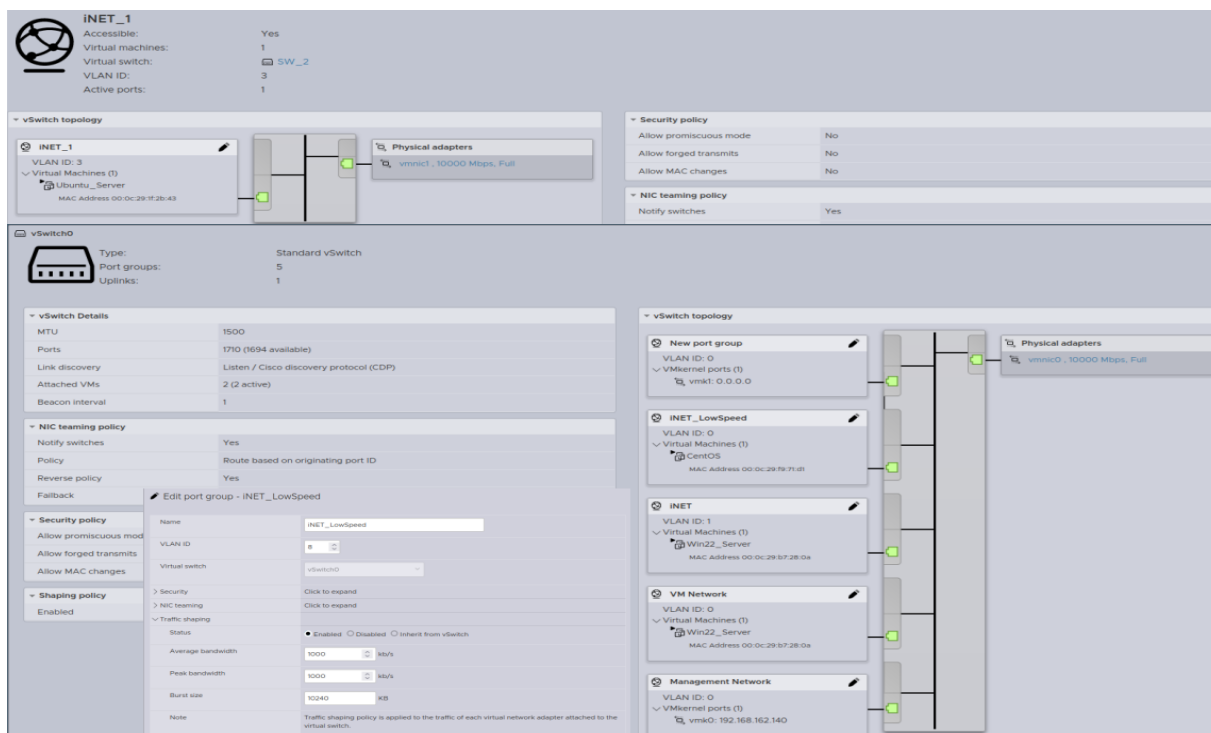


Figura 2. Conectarea serverelor virtuale la switch-uri virtuale, separarea în VLAN-uri (rețele virtuale) și gestionarea lățimii de bandă pentru fiecare VM în Hypervizorul ESXi de la VMware

Monitorizarea Serverului

Monitorizarea performanței asigură faptul ca toate VM-urile, procesoarele și alte dispozitive să funcționeze în mod optim. O simplă problemă de performanță pe o mașină virtuală VM afectează nu doar serverul fizic, ci și toate VM-urile și aplicațiile acestora. Acest aspect poate duce la pierderi esențiale pentru o companie. Gestionarea eficientă a resurselor este un alt aspect crucial al monitorizării. Unul dintre beneficiile principale ale virtualizării constă în capacitatea de a utiliza un mediu virtual pentru a valorifica resursele, care altfel pot fi subtilizate. Această oportunitate este compromisă atunci când resursele nu sunt alocate și administrate corect pe o mașină virtuală. Alocarea excesivă sau insuficientă a resurselor pentru o mașină virtuală poate duce la o utilizare inefficientă sau dezechilibrată a acestora. Prin monitorizarea atentă a utilizării resurselor în timp, poate fi determinată alocarea optimă a resurselor pentru fiecare mașină virtuală. Este esențial de monitorizat conectivitatea la rețea pentru a se asigura că mașinile virtuale funcționează corect. Suprautilizarea benzii rețelei sau traficul pe o singură interfață de rețea poate afecta semnificativ performanța tuturor mașinilor virtuale. Utilizarea resurselor de monitorizare online furnizate de către hypervisor permite prevenirea problemelor de sistem și asigură posibilitatea utilizării unui sistem independent de monitorizare (Figura 3), care va permite monitorizarea întregii infrastructurii IT distant cu expedierea alarmelor prin SMS sau Email.

Copiile de rezervă a serverului virtual

Copiile de rezervă (Backup) ale serverelor virtuale reprezintă un element indispensabil și asigură o serie de avantaje pentru utilizarea a serverului virtualizat și a tipului de backup asociat cu el. Copiile de rezervă la nivel de imagine pot fi realizate pentru datele de pe diverse tipuri de mașini, inclusiv mașini virtuale, cloud sau fizice. Funcționalitățile de recuperare includ recuperarea la nivel de imagine, recuperarea la nivel de fișier (Veeam Backup & Replication). Backup-ul se bazează pe stocarea imuabilă în cloud pentru protecția ransomware și pentru asigurarea împotriva modificării sau ștergerii. VM Backup oferă, de asemenea, funcționalități cum ar fi deduplicarea, protecția continuă a datelor și gestionarea centralizată a backup-urilor VM (Anterior Altaro VM Backup).

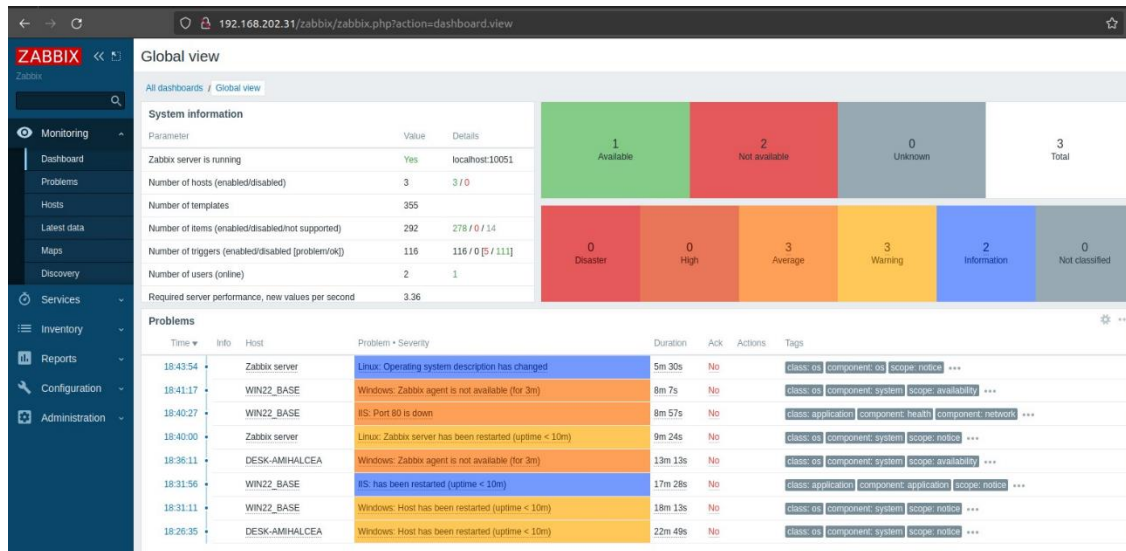


Figura 3. Monitorizarea VM-urilor, funcționalității serviciilor, dispozitivelor serverului și a întregii infrastructuri IT cu soft-ul Zabbix

Replicarea mașinilor virtuale de la gazdă la gazdă este utilizată pentru a avea o copie exactă a mașinilor virtuale, gata pentru a fi pornită în caz de defecțiune sau accident al mașinii de bază. Replicarea poate fi, de asemenea, planificată și efectuată pe mai multe destinații, permițând astfel o politică optimă de eșuări ale sistemului (Iperius Backup).

Securitatea virtualizării serverului

Virtualizarea serverului oferă diverse avantaje în ceea ce privește securitatea, unul din acestea fiind stocarea datelor într-un loc centralizat, care poate fi ușor de gestionat, fără a fi stocate pe dispozitive neautorizate sau mai puțin sigure, sau pe dispozitivele utilizatorilor finali. De asemenea, izolarea între mașinile virtuale (VM-uri) contribuie la protecția împotriva atacurilor, malware-ului, virușilor și altor vulnerabilități datorită separării și izolării lor. Aceste măsuri asigură un mediu mai sigur pentru datele și aplicațiile organizației.

Datorită controlului accesului granular al virtualizării, departamentele IT ale organizației posedă un nivel mai avansat de control asupra utilizatorilor care pot accesa datele stocate în sistem. Prin utilizarea micro-segmentării, se poate oferi acces utilizatorilor doar pentru aplicații sau resurse specifice. De asemenea, virtualizarea calculatoarelor de lucru (Desktop PC) permite personalului IT să realizeze actualizarea și să aplice patch-urile sistemelor de operare și aplicațiilor.

Hipervizorii reduc riscurile de securitate prin minimizarea suprafeței de atac în comparație cu soluțiile hardware, datorită capacităților de funcționare cu resurse reduse. Adicional, hipervizorii beneficiază de actualizări automate, ceea ce contribuie la protecția împotriva amenințărilor în evoluție.

Riscuri de securitate și soluții

Virtualizarea serverului poate implica anumite riscuri de securitate. Cel mai frecvent risc reprezintă complexitatea sporită a unui mediu virtualizat. Respectarea celor mai bune practici de securitate sau mentenanța configurațiilor și politicilor consistente pentru întregul ecosistem devine mai dificil de realizat de către departamentul IT al organizațiilor, deoarece mașinile virtuale pot fi dublate și volumul de lucru poate fi relocat cu ușurință pe diferite locații.

Creșterea numărului de mașini virtuale poate prezenta, de asemenea, un risc de securitate. Mașinile virtuale inactive consumă permanent resursele informaționale și energetice ale serverului fizic, transformându-se în ținte vulnerabile pentru atacuri, deoarece nu beneficiază de patch-uri sau actualizări corespunzătoare. Deși izolarea între mașinile virtuale (VM-uri) poate

reduce, într-o anumită măsură, riscurile de securitate, totuși nu poate contracara efectele complete unui atac distribuit de negare a serviciului (DDoS). În cazul în care un atac DDoS afectează performanța unei mașini virtuale prin inundarea cu trafic rău intenționat, celelalte VM-uri, care împart aceleași resurse ale serverului gazdă, vor fi afectate.

Pentru a reduce riscurile de securitate asociate cu virtualizarea serverului, departamentul IT al organizațiilor poate adopta unele dintre cele mai bune practici, care includ menținerea actualizării tuturor software-ului și firmware-ului pentru întregul sistem, instalarea și actualizarea software-ului antivirus și a altor soluții de securitate concepute pentru mediile de virtualizare. Este important de monitorizat și controlat accesul utilizatorilor care accesează sistemul, de criptat traficul de rețea, și de lichidat VM-urile neutilizate, de realizat copii de rezervă reglementate pentru VM-uri și servere fizice. De asemenea, este recomandabil de definit și implementat o politici de utilizare și de securitate complexe pentru VM-uri și servere gazdă.

Concluzii

Virtualizarea serverului reprezintă o tehnologie modernă care permite crearea și abstractizarea mai multor instanțe de mașini virtuale pe un singur server fizic. Virtualizarea serverului maschează resursele serverului, inclusiv numărul și identitatea serverelor fizice individuale, ale procesoarelor și ale sistemelor de operare.

Configurațiile tradiționale de hardware și software pentru calculatoare susțineau, de obicei, aplicații unice. Adesea, acest lucru forța serverele să ruleze în parte o singură sarcină de lucru, irosind în esență resursele neutilizate ale procesoarelor, capacității de memorie și altor resurse hardware. Numărul de servere hardware a crescut exponențial pe măsură ce organizațiile implementează diverse aplicații și servicii pentru întreaga organizație. Costurile corespunzătoare și cererile emergente de spațiu, energie, și conectivitate au impus limite pentru centrele de date.

Virtualizarea serverelor adaugă un nivel software adițional, numit hipervizor, la un computer, care abstractizează hardware-ul de bază. Un hipervizor organizează și gestionează resursele virtualizate ale serverului, furnizându-le în instanțe logice numite mașini virtuale (VM), fiecare dintre acestea fiind capabilă să funcționeze ca un server separat și independent. Virtualizarea poate permite unui singur server să realizeze sarcina de muncă a mai multor servere, utilizând până la 100% din hardware-ul. Acest aspect reduce numărul de servere, reduce sarcina echipamentelor centrelor de date, îmbunătățește flexibilitatea IT și reduce costul IT pentru organizație.

Referințe

- [1] <https://www.iperiusbackup.net/en/backup-esxi-and-vsphere-free-hypervisor/>
- [2] <https://www.nutanix.com/info/virtualization/server-virtualization#>
- [3] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/VMware_paravirtualization.pdf
- [4] <https://www.ninjaone.com/blog/what-is-virtual-server-backup-solutions/>
- [5] https://www.zabbix.com/documentation/6.4/en/manual/it_services
- [6] <https://docs.vmware.com/en/VMware-vSphere/index.html>