

UTICAJ VIRTUALIZACIJE NA PERFORMANSE PRI ZAŠTITI PODATAKA U BAZAMA PODATAKA SA KRIPTOGRAFSKIM ALGORITMIMA

Saša Adamović

Univezitet Singidunum

E-mail: sadamovic@singidunum.ac.rs

Mladen Veinović

Univezitet Singidunum

E-mail: mveinovic@singidunum.ac.rs

Marko Šarac

Univezitet Singidunum

E-mail: msarac@singidunum.ac.rs

Sažetak: U ovom radu analiziran je uticaj virtualnog okruženja na performanse pri zaštiti podataka i informacija u bazama podataka sa AES algoritmom. Analiza obuhvata standardna bezbednosna rešenja zasnovana na komercijalno dostupnim kriptografskim algoritmima. Urađena je komparativna analiza između procesa zaštite realizovanog na virtualnoj platformi i procesa zaštite realizovanog u standardnom fizičkom okruženju. Prednost virtuelnog okruženja je optimalnije raspolaganje i iskorišćenje fizičkih resursa (procesorska snaga, ram, virtualni mrežni adapter), s obzirom na navedene prednosti očekuje se poboljšanje performansi baze podataka. Primenjenim (predočenim) rešenjima podaci su zaštićeni u bazi podataka, kao i podaci koji se nalaze u virtuelnom komunikacionom kanalu između aplikativnog servera i servera baze podataka.

Ključne reči: Virtualizacija, virtualna mašina, analiza performansi, algoritmi za šifrovanje, AES, zaštita podataka, mysql, apache, aplikativni server

Abstract: In this paper i will study influence of virtual environment of data encryption in database. Analysis is focused on changing of time component of the cryptographic algorithm on Windows operating system during implementation of cryptographic module in purpose of data security on physical and virtual environment. Results for encryption are given as diagrams. Results have shown that virtual environment has many advantages over physical environment.

Obvious advantages are faster encryption and on the security aspect achieving much greater system encapsulation.

Key words: Physical and virtual environment, datacenter, virtual, AES, Hyper-V, algorithm, apache, database performance, security.

1. UVOD

U profesionalnim sistemima, zaštita baza podataka je postala visok prioritet u svetu. Cilj svake organizacije je da štiti bezbednosno osetljive podatke u bazama podataka u kojima se nalaze informacije o klijentima i njihovim poslovanjima kao i raznovrsna tehnička dokumentacija. Pri kreiranju strategije za zaštitu baze podataka od značaja je više faktora. Jedan od njih je Virtualizacija. Virtualizacija je koncept i skup zrelih proizvoda koji su danas na dohvata ruke (rešenja Hiper-V, Vmware, Xen, itd.), koji uspešno rešava brojne probleme u

datacentru, i koji će u godinama koje slede iz temelja izmeniti arhitekturu datacentra, operativnih sistema, modela licenciranja softvera i najzad samog koncepta IT servisa.

2. VIRTUALIZACIJA

Savremena virtuelizacija dozvoljava pokretanje više instanci operativnih sistema na jednom računaru. Ovi operativni sistemi dele resurse zajedničkog hardvera. Kontrola nad hardverom je prepuštena softveru pod nazivom virtuelna mašina, koja se bavi pristupima procesoru, memoriji, ulazno-izlaznim operacijama, hard diskovima i mrežnim hardverom. Virtuelizacija je tako, na sebi svojstven način, pomirila dve krajnosti u pogledu organizacije IT sistema – centralizovan sistem naspram decentralizovanog. Umesto da se nabavljaju novi računari sa savremenim perifernim uređajima, korišćenjem virtuelizacije u upotrebu se stavlja centralni hardver na sloju ispod virtuelnih mašina i na taj način se obavlja centralizacija čitavog sistema. Osnovna korist od ovoga jeste to što takva celina sada može mnogo lakše da se održava. Potrebno je samo na jednom računaru instalirati sigurnosne zakrpe, nove verzije aplikacija ili dodatne alatke i svi korisnici sistema preko virtuelnih mašina imaju iste uslove za rad.

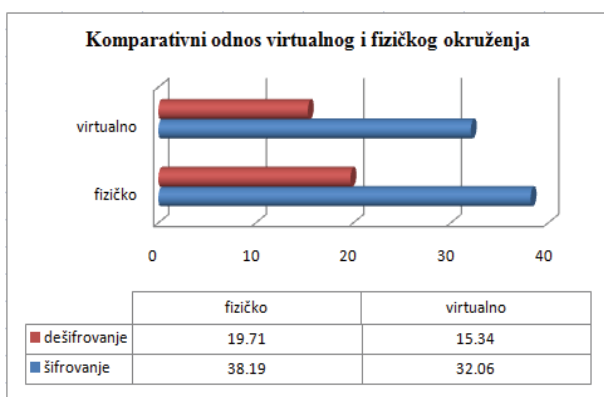
U ovom radu predstavljeni su i testirani koncepti virtualizacije vodećeg proizvođača procesora Intel-a.

2.1 PREDNOSTI VIRTUALNOG U ODNOSU NA FIZIČKO OKRUŽENJE

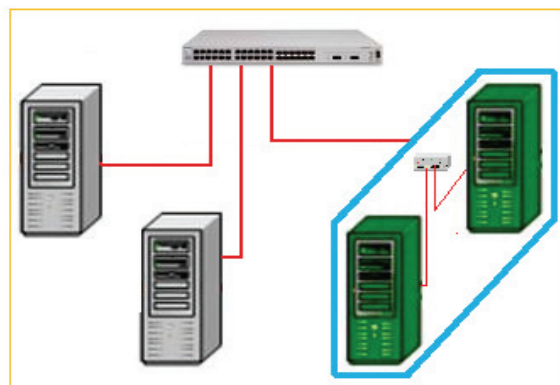
U poslednje vreme baze podataka napreduju jako brzo tako da je od suštinske važnosti održavati korak sa novim trendovima u svetu koji postaju sve više virtualizovani na svakom nivou. Korišćenjem virtualizacije moguće je podići efikasnost korišćenja IT resursa na 60-80% (približno kao u mainframe okruženju). Pri tome je broj fizičkih servera, kako pokazuju slučajevi mnogih od preko 20.000 korisnika, moguće smanjiti za 8-30 puta. Virtuelizacija je trenutno najuzbudljiviji segment na polju poslovne inteligencije a virtuelizacija će olakšati analitike niske latencije na mnogo jači način nego što to čine tradicionalni pristupi. Virutelizacija baza podataka će omogućiti real-time poslovnu inteligenciju kroz politički vođenu memorijsku mrežu koja omogućava infrastrukture na svim nivoima.

Za potrebe ovog rada realizovano je jedno fizičko okruženje koje se sastoji od dva servera. Na jednom serveru se nalazi aplikativni server sa instaliranim kriptografskim modulom za šifrovanje. Kriptografski modul koristi AES (256key) algoritam koji je napisan prema FIPS-ovim standardima a realizovan u PHP programskom jeziku. Podaci se šifruju na aplikativnom serveru, zatim se se kroz lokalnu mrežnu infrastrukturu u šifrovanoj formi prosleđuju serveru baze podataka.

Posle fizičkog okruženja realizovano je virtualno okruženje koje se sastoji od jednog fizičkog servera na kome se nalaze dva virtualna servera. Jedan server ima ulogu aplikativnog a drugi ulogu servera baze podataka. Na aplikativnom serveru se nalazi kriptografski modul identičan modulu iz fizičkog okruženja. Podaci šifrovani na aplikativnom serveru se šalju u šifrovanoj formi serveru baze podataka preko virtualne mrežne infrastrukture u okviru jedne fizičke mašine. Ovakva realizacija virtualizovane klijent – server arhitekture je odlična sa aspekta performansi i aspekta bezbednosti sistema za zaštitu podataka.



Slika 1 Rezultati eksperimenta



Slika 2 Ilustracija virtualnog i fizičkog okruženja

Komparativnom analizom rezultata utvrđeno je da performanse virtualizovanog okruženja imaju dobre prednost u odnosu na fizičko okruženje.

3. ZAKLJUČAK

U radu su predstavljena dva potpuno različita okruženja sa identičnim funkcionalnostima za kriptografsku zaštitu podataka i čuvanje istih. Virtualizacija je koncept i skup zrelih proizvoda koji su danas na dohvat ruke. Kompletom eksperimentalnom analizom utvrđeno je da postoje brojne prednosti virtualizovanih rešenja. Kompletan realizacija virtualizovanog okruženja je postavljena na jednom fizičkom serveru. Zbog virtualnog mrežnog adaptera dobijene su bolje performanse u odnosu na komunikaciju servera u fizičkom okruženju. Sa aspekta bezbednosti ostvarena je veća mrežna izolovanost sistema od okoline. Sama paradigma virtualizacije omogućava pravljenje bekapa i stvara hardversku nezavisnost kao i optimalnije iskorišćenje hardvera. S obzirom na sve navedene prednosti možemo da kažemo da koncept virtualizacije predstavlja jedn zreo proizvod u IT-u.

LITERATURA

- [1] Hoopes, J.: Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting
- [2] Daeman, J.: Design of Rijndael: Aes - the Advanced Encryption Standard
- [3] Companies, Inc. Microsoft Windows Server 2008: Implementation and Administration, Barrie Sosinsky
- [4] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.
- [5] A Menezes at all., "Handbook of Applied Cryptography", CRC Press, 1996.
- [6] Adamović S, Veinović M, "Analiza zaštite podataka u bazama podataka na lokalnom i serverskom nivou", rad ID=1026 objavljen u zborniku radova 16. Telekomunikacionog foruma TELFOR 2008