IMPLEMENTACIJA MICROSOFT SQL SERVER BAZE PODATAKA PREKO HYPER-V TEHNOLOGIJE

Miloš Mravik*,
Marko Šarac,
Saša Adamović

Univerzitet Singidunum,
Beograd, Srbija

Rezime:

Porast broja korisnika i uređaja koji pristupa Internetu doveo je do toga da praćenje i upravljanje IT infrastrukturom postane problematično. U radu je detaljno opisana pravilna implementacija Microsoft SQL baze podataka na klijentskoj i serverskoj strani. Radom je obuhvaćen i bezbednosni aspekt zaštite informacija implementiranog rešenja. Implementacija je vršena po pravilima dobre prakse sa fokusom na pouzdanost sistema. Kompanije koje poseduju velike i komplikovane sisteme ne smeju da dozvole da ih kompjuterska infrastruktura sputava u ostvarivanju sopstvenih ciljeva. Razvoj hardverske infrastrukture omogućio je neograničen broj softverskih mogućnosti koje su uvidele svetlost dana, a za koji je potrebna odgovarajuća IT implementacija. Rad se bavi analizom pravilne implementacije u modernom virtuelnom okruženju.

Ključne reči:

Microsoft SQL Server, Hyper-V, Virtualizacija.

1. UVOD

Upotreba Microsoft SQL Server baze podataka je veoma dominantan način skladištenja velikih količina podataka generisanih sa klijentske strane. Sprega između klijenata i baze podataka ostvarena je preko aplikacije čija je uloga da manipuliše sa podacima u bazi podataka.

Jedan od najvećih i često diskutovanih problema vezanih za baze podataka predstavlja njihova zaštita. Glavni problem zaštite javlja se u vidu nedozvoljenog pristupa delovima baze, korisnicima koji nemaju privilegije. [1]

U radu je opisan jedan od načina sigurne konekcije između klijentskog i serverskog dela baze podataka. Preporuka Microsoft-a je da se radi kompatibilnosti svih servisa i njegovih mogućnosti koriste Microsoft tehnologije, iz tog razloga testiranje je prikazano i implementirano samo uz pomoć Microsoft tehnologija.

Odgovorno lice:
Miloš Mravik

e-pošta:
mmravik@singidunum.ac.rs

DOI: 10.15308/Sinteza-2019-208-214

2. KONCEPT VIRTUALIZACIJE SAVREMENIH RAČUNARA

Polazeći od navoda u apstraktu rada virtualizacija podataka nije u potpunosti nova tehnologija u IKT okruženju. Svakako, potrebno je napomenuti tipove virtualizacije i načine implementacije:

- Hardverska virtualizacije
- Softverska virtualizacija
- Mrežna virtualizacija
- Virtualizacija podataka

Ako se osvrnemo na popularnost gore navedenih tipova virtualizacije, najpopularniji i najrasprostranjeniji vid virtualizacije jeste hardverska virtualizacija. Ovaj tip virtualizacije predstavlja kreiranje velikog broja virtualnih mašina na jednom fizičkom računaru. Sve to je moguće uz pomoć softvera hipervizor (engl. *hypervisor*).

Takođe, osvrnućemo se na još jedan tip veoma popularne tehnologije a to je mrežna virtualizacija. Ovaj pristup virtualizaciji predstavlja kombinovanje realnih mrežnih adaptera u cilju pravljenja više različitih virtualnih mrežnih adaptera. Svaka virtualna mašina može da poseduje svoj jedinstveni mrežni adapter koji će da se nalazi u mreži koja je definisana samo za tu virtualnu mašinu i na taj način fizički razdvajamo mrežu baze i mrežu klijenta koji pristupa istoj. [2]

3. IMPLEMENTACIJA MICROSOFT SQL SERVER BAZE PODATAKA

Implementacija serverske strane zahteva dodatnu osposobljenost administratora sistema. Koraci koji su potrebni za uspešnu implementaciju Microsoft SQL Server baze podataka su:

- Omogućavanje virtualizacije na hostu na kome će biti instalirane virtualne mašine;
- Kreiranje virtualnih mašina (definisanje virtualnog hardvera);
- Instalacija Windows Server 2019 sistema;
- Instalacija Microsoft SQL Server baze (u ovom radu je prikazana simulacija sa upotrebom *Express* verzije baze);
- Instalacija Microsoft SQL Server MS-a;

Podešavanje hosta na kome će biti smeštene i pokrenute virtuelne mašine, kao i instalacija dodatnog softvera gore već pomenutog softvera ne zahteva dodatne IT veštine za administratora sistema.

Važno pitanje posle svih instalacija je - da li je implementirana instanca SQL servera u potpunosti zaštićena za bezbedno skladištenje podataka?

Po pitanju bezbednosti u bazama podataka, administratori sistema imaju ozbiljan i važan zadatak prilikom instalacije baze podataka i dodeljivanju privilegija korisnicima. Naime, u toj situaciji nije dovoljna samo konfiguracija sistema za upravljanje bazom podataka , već je podjednako važna konfiguracija host-a na kome su pokrenute virtuelne mašine. [3]

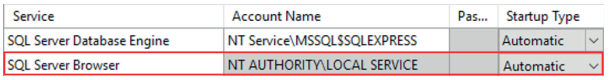
4. KONFIGURACIJA SERVERA ZA SKLADIŠTENJE PODATAKA

Nakon instalacije Microsoft SQL Server baze podataka prvenstveno je potrebno da se sam host zaštiti uz pomoć *firewall*-a, a to obično podrazumeva zatvaranje slobodnih portova koje ne koristi nijedan servis u datom trenutku i koji nisu dinamički dodeljeni nekom servisu ili aplikaciji.

Svaka aplikacija koja koristi neki servis koji nije direktno ugrađen u nju samu, mora da upotrebljava jedan od portova koji je unapred definisan. Zatvaranjem portova na *firewall*-u ublažava mogućnost prisluškivanja portova i opserviranja saobraćaja između aplikacije i baze podataka. Omogućavanje pristupa bazi podataka od strane korisnika koji se ne nalaze u lokalnoj mrežim sadrži dva koraka:

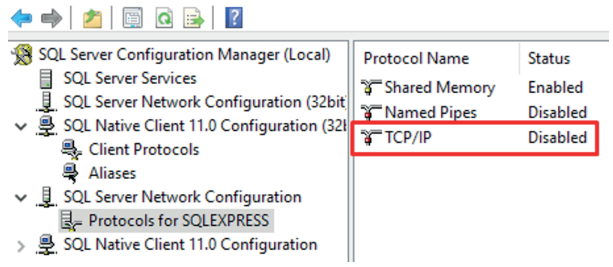
- Omogućavanje servisa SQL Server Browser;
- Omogućavanje TCP/IP protokola za pristup željenoj bazi;

Prilikom instalacije baze podataka, na administratoru sistema je da odluči koji sve to servisi treba da budu aktivni nakon startovanja samog računara. Ovo je prvi korak u kome administrator sistema ima mogućnost definisanja automatskog startovanja servisa SQL Server Browser.



Slika 1. Prikaz SQL Server Browser servisa

Drugi korak u omogućavanju pristupa bazi podataka na osnovu javne instance je omogućavanje TCP/IP protokola.

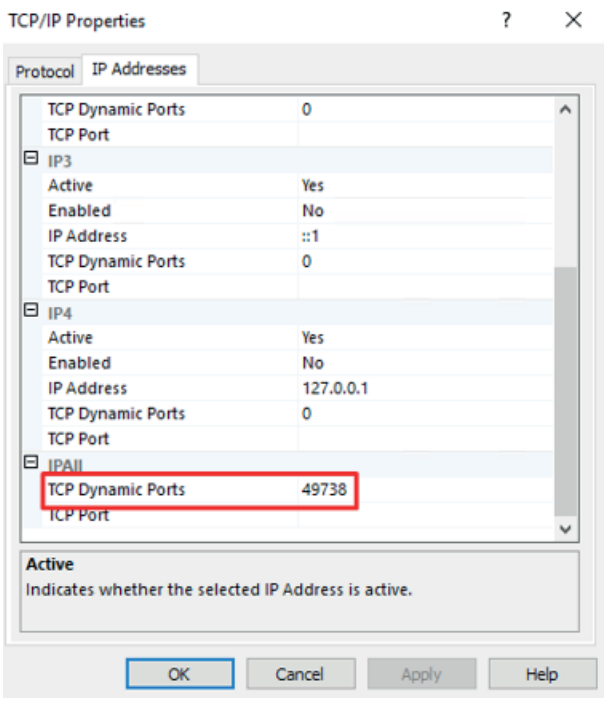


Slika 2. Prikaz omogućavanja TCP/IP protokola

Omogućavanjem TCP/IP protokola dolazimo do prvog velikog problema koji se tiče sigurnosti baze podataka. [4] Međutim, ukoliko je u ovom koraku *firewall* u potpunosti isključen dolazimo do toga da korisnik koji poseduje i zna jednu od dole navedene tri stavke može da pristup nesmetano bazi podataka, a to su:

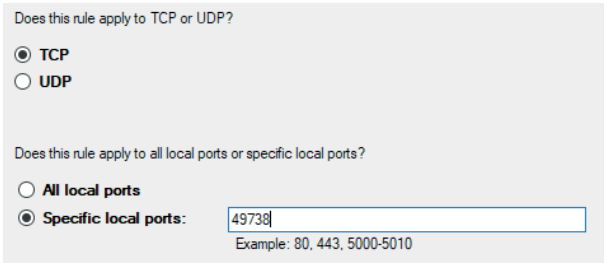
- Ime računara i ime instance baze podataka (MS-SQL-SERVER\SQLEXPRESS) – SQLEXPRESS predstavlja ime instance na osnovu koga korisnik odabire kojoj bazi podataka želi da pristupi u datom trenutku
- Lokalnu IP adresu i ime instance baze podataka (10.8.8.2\SQLEXPRESS) – Ukoliko se baza podataka nalazi u lokalnoj mreži u kojoj se nalazi i sam korisnik, korisnik će biti u mogućnosti da pristupi bazu na osnovu saznanja IP adrese.
- Javnu IP adresu i ime instance baze podataka (154.76.22.167:49738\SQLEXPRESS) – Ukoliko korisnik dođe do saznanja o javnoj IP adresi same baze i portu uz pomoć koga sama baza funkcioniše, biće u mogućnosti da pristupi svim podacima u bazi.

Da bismo izbegli gore pomenute probleme potrebno je pravilno definisati pravila na *firewall*-u virtualne mašine na kojoj se nalazi Microsoft SQL Server Express. Prvenstveno je potrebno da saznamo na kom portu radi baza podataka, prikazano na slici ispod:



Slika 3. Prikaz osnovnog porta komunikacije baze

Otvaranje porta na *firewall*-u je prikazano na slici ispod:



Slika 4. Prikaz otvaranja porta na firewall-u

U ovom delu rada nećemo se baviti samo definisanjem aktivnih i neaktivnih portova. Ukoliko su portovi dobro konfigurisani to nam ne omogućava potpunu sigurnost i sigurnost baze podataka. Drugi problem koji se javlja je vezan za korisnike i grupe korisnika sa korisničkim privilegijama za pristup bazi podataka. Pri instalaciji Microsoft SQL Servera, administrator sistema je imao mogućnost da izabere dve vrste pristupa bazi podataka:

- Windows authentication mode (pristup bazi podataka sa pristupnim parametrima sa kojima je sam korisnik ulogovan na računar sa koga želi

da pristupi bazi. Svakako, ovaj deo može da uključuje lokalni i domenski nalog, uključujući i Security group-e)

- Mixed Mode (SQL Server authentication and Windows authentication) – Ovaj režim omogućava pored gore pomenutog pristupa i definisanje novih korisnika direktno u bazi podataka.

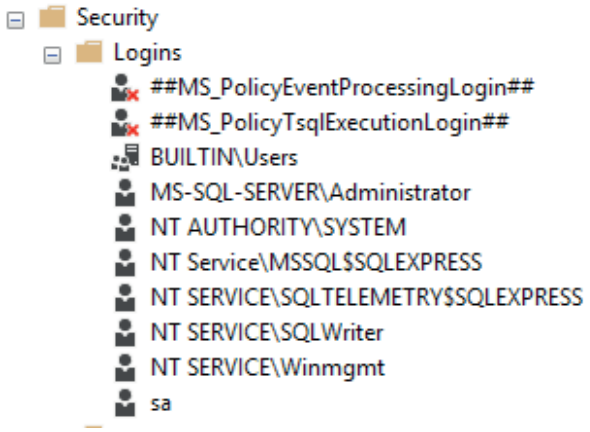
Administratorima sistema se preporučuje da izaberu vrstu Mixed Mode jer je iz više razloga sigurniji, o tome će biti više diskusije u nastavku rada. [5]

Podrazumevana podešavanja Microsoft SQL Server baze podataka definišu četiri osnovne baze i nekoliko podrazumevanih korisnika za pristup.

Četiri osnovne baze su:

- Master
- Model
- Msdb
- Tempdb

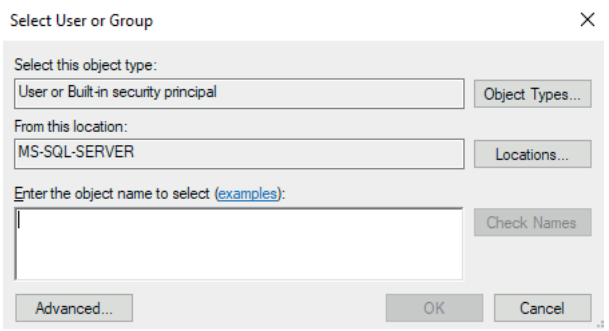
Podrazumevani korisnici baze su sledeći:



Slika 5. Prikaz osnovnih korisnika za pristup bazi

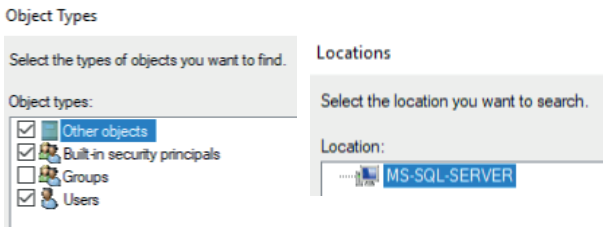
Svakako, najbitniji korisnici baze sa najvišim privilegijama su „sa“ i „Administrator“. Korisnik „sa“ predstavlja System Administratora, tj. administratora SQL Server authentication procesa prijave. Korisnik „Administrator“ predstavlja lokalnog administratora samog servera, tj. administratora Windows authentication procesa prijave.

Podrazumevani korisnici baze često nisu dovoljni za siguran pristup bazi. To znači da je naredni zadatak administratora sistema da definiše nove korisnike ili grupe korisnika koji će imati različite privilegije nad bazom.



Slika 6. Prikaz dodavanja novog korisnika u bazu

Naravno, na administratorima sistema ostaje da izaberu tip i lokaciju željenog naloga ili grupe korisnika kojima želi da dodeli privilegije za pristup nad bazom podataka.

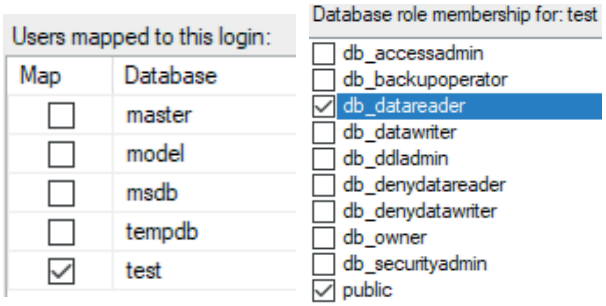


Slika 7. Prikaz odabira tipa objekta korisnika

Slika 8. Prikaz odabira tipa lokacije korisnika

Prilikom dodavanja novog korisnika za pristup bazi potrebno je prvenstveno izabrati način pristupa bazi (Windows authentication mode ili Mixed mode). Preporuka je svakako enforce-ovati password policy-u i password expiration iz razloga što ćemo na ovaj način da tražimo od korisnika da blagovremeno menja pristupne parametre za pristup bazi. Sledeći, najbitniji korak je definisanje uloga samog korisnika nad bazom. Potrebno je obratiti pažnju na ovaj deo i definisati da isključivo administratori sistema mogu da budu okarakterisani kao „sysadmin“ nalozi. Za sve ostale naloge sa manjim nivoom privilegija potrebno je definisati samo ulogu „public“ koja predstavlja način pristupa samoj bazi. Na kraju definisanja privilegija samog korisnika dolazimo do toga da moramo da izvršimo mapiranje samih baza i definisanja tačno određenih pravila koja će novokreirani korisnik moći da izvršava nad samom bazom. Pod terminom mapiranja smatramo dozvolu pristupa samoj bazi koju sve mapirali. Naime, preporuka je da se četiri osnovne baze mapiraju isključivo za administratorske naloge. Što se tiče uloga nad mapiranim bazama taj deo

zavisi od željenog nivoa privilegija novokreiranog korisnika. Obratiti pažnju na to da li sam korisnik ima mogućnost i pisanja i čitanja podataka iz baze.



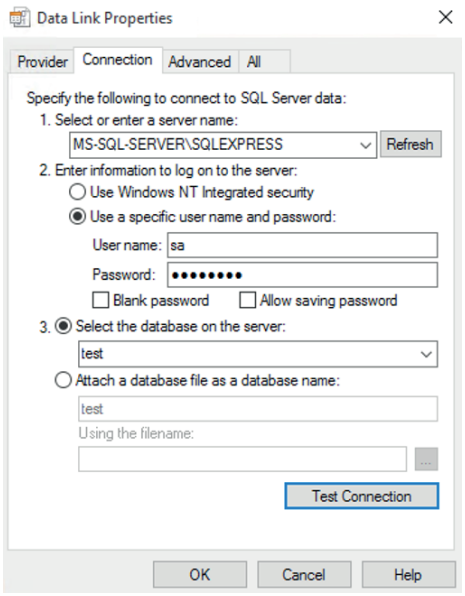
Slika 9. Prikaz mapiranja baza podataka

Slika 10. Prikaz dodeljivanja uloga korisnicima nad bazom

Na ovaj način smo definisali da novokreirani korisnik ima mogućnost samo čitanja nad bazom „test".

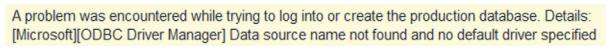
5. KONFIGURACIJA KLIJENTA ZA PRISTUP MICROSOFT SQL SERVER BAZI PODATAKA

U ovom delu rada će biti detaljno objašnjena konfiguracija klijentskog dela aplikacije. Za primer je uzeta virtualna mašina sa instaliranim Microsoft Windows 10 Professional sistemom. Potrebno je napomenuti da konfiguracija klijentskog dela ne zavisi od verzije Microsoft Windows sistema. [6] Prvi i osnovni korak koji je potrebno definisati i prikazati na korisnikom delu jeste testiranje konekcije nakon definisanja *firewall*-a na klijentskoj strani. Naime, kao test je uzet fajl sa ekstenzijom „*.udl*" koji se veoma često koristi za testiranje konekcije između klijentskom i serverskog dela neke aplikacije. Prikaz testirane konekcije je prikazan na slici ispod:



Slika 11. Prikaz testiranja konekcije između korisnika i baze upotrebom .udl fajla

Poslednja, ali ne i najmanje bitna stavka prilikom konfiguracije klijentskog dela jeste konfiguracija ODBC drajvera.



Slika 12. Prikaz zahteva za definisanjem ODBC drajvera

Instalacija ODBC drajvera ima za ulogu da omogući konekciju između Database Management System-a (DBMS) i baze koristeći SQL kao standard za pristupanje podacima. Nakon instalacije drajvera komunikacija između klijenta i servera postaje u potpunosti dozvoljena i veoma sigurna. [7]

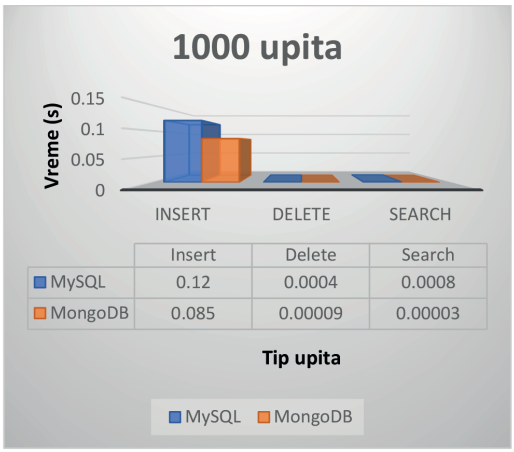
6. ALTERNATIVE MICROSOFT SQL SERVER-A

Porast broja informacija na internetu dovela je do toga da su baze podataka postale toliko kompleksne da se broj servera za skladištenje informacija na globalnom nivou povećao do broja od čitavih 75 miliona. Ovu tvrdnju najbolje objašnjava broj servera koje poseduje Microsoft, a to je 1 milion, odmah iza Microsoft-a nalazi se Google koji poseduje čitavih 900,000 serverskih mašina. Koliko su baze podataka postale kompleksne najbolje

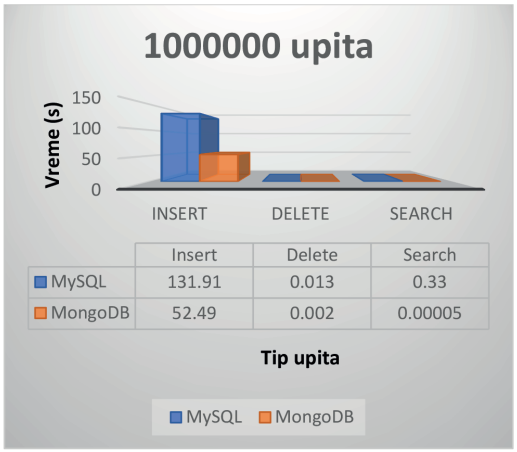
govori činjenica da Google poseduje najveći broj informacija na internetu (engl. *index of internet*), a to je samo 0,004% svih podataka na internetu.

Kada pričamo o alternativama Microsoft SQL Server-a one su mnogobrojne. Svakako, u zavisnosti od tipa podataka koji će biti skladišteni u bazi potrebno je veoma pažljivo izabrati softver za upravljanje bazom. U ovom radu smo naveli tri alternative Microsoft SQL Server-a za koje smatramo da su veliki konkurent Microsoft-ovom rešenju. Prva alternativa jeste MongoDB koja predstavlja ne-relacionu, distribuiranu bazu otvorenog koda. Glava odlika ovog tipa baze predstavlja horizontalna skalabilnost, visoka propusnost i izvršavanje na pristupačnom hardveru. Potrebno je navesti da MongoDB predstavlja jednu od najpoznatijih dokument-orijentisanih baza podataka (NoSQL). Činjenica koja MongoDB čini velikim konkurentom Microsoft-ovog rešenja jeste ta što su drajveri za povezivanje MongoDB baze podataka i klijentskih aplikacija razvijeni za sve veće programske jezike. Ova činjenica svakako omogućava lakšu upotrebu baze podataka i opredeljivanje za MongoDB rešenje. Drugo, ali ništa lošije rešenje predstavlja MySQL. MySQL predstavlja najpopularniji softver za upravljanje bazama podataka na svetu. Važno je napomenuti da je MySQL pod GPL licencom koja omogućava krajnjim korisnicima u potpunosti besplatan softver otvorenog koda. Ovo rešenje predstavlja spregu između SQL i NoSQL baza podataka i čini ih međusobno funkcionalnijim i stabilnijim.

Na slikama ispod su prikazani testovi sa upitima koji su izvršavani nad identičnim podacima sa dve različite baze podataka (SQL i MySQL). Akcenat je stavljen na brzinu dobijanja rezultata iz izvršenih upita.



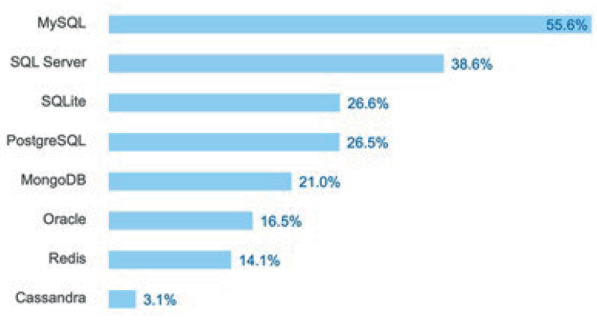
Ilustracija 1. Prikaz razlike u brzini izvršavanja hiljadu upita



Ilustracija 2. Prikaz razlike u brzini izvršavanja milion upita

Na ilustracijama iznad prikazano je vreme izvršavanja istog broja upita nad podacima u dve različite baze, Microsoft SQL i MongoDB. Iz priloženih rezultata može se konstatovati da je vreme izvršavanja upita nad podacima u MongoDB bazi podataka drastično brže. U zavisnosti od tipa upita koji se izvršavaju nad podacima dolazimo do toga da je razlika u brzini čak preko 6000 puta brža. To nam govori da će se milion upita nad MongoDB bazom podataka koji su tipa „*search*" izvršiti čitavih 6677,72 puta brže. Ova činjenica nam govori da je MongoDB baza podataka svakako bolje rešenje za aplikacije čija uloga je pretraživanje velikog broja podataka od strane krajnjih korisnika.

Na ilustraciji ispod je prikazana zastupljenost različitih tipova podataka na tržištu.



Ilustracija 3. Prikaz zastupljenosti različitih tipova podataka na tržištu

7. ZAKLJUČAK

U ovom radu prikazan je pravilna i pre svega bezbedna upotrebu virtualizacije u modernim informacionim datacentar okruženjima. U analiziranom primeru na virtuelnoj mašini je implementiran Microsoft SQL Server koji predstavlja ujedno i studiju slučaja kojom je pokazana pravilna konfiguracije više različitih parametara kako bi se ublažila ranjivost kompletnog sistema do krajnjih granica koje su limitirane i ponekad zavise od ljudskog faktora i administratora sistema.

Praksa je nametnula potrebu za sprovođenjem strogih bezbednosnih politika koje se tiču upravljanja i manipulisanjem podataka u domenu administracije sistema, jer jedino na ovaj način je moguće dostići zadovoljavajuću bezbednost celokupnog sistema.

Ovaj rad je nastao kao rezultat rada i potrebe u sopstvenom radnom okruženju, gde su prikazani stečeno iskustvo i dobri primeri iz prakse, kao i moguće loše strane.

U susret novim izazovima, bezbednost i zaštita informacija su sastavni deo svih tehnoloških rešenja u upotrebi danas, iz tog razloga diskusija na ovu temu će biti nastavljena u budućem radu.

LITERATURA

[1] M. Milosavljević i S. Adamović, Kriptologija 2, Beograd: Univerzitet Singidunum, 2017.

[2] G. Santana, Data Center Virtualization Fundamentals, San Francisco: Cisco Technologies, 2013.

[3] D. Prashanta Kumar i D. Ganesh Chandra, Design and Use of Virtualization Technology in Cloud Computing, Hershey: IGI Global, 2017.

[4] M. Veinović, G. Šimić i A. Jevremović, Baze podataka, Beograd: Univerzitet Singidunum, 2013.

[5] M. Veinović, M. Šarac, A. Jevremović i G. Šimić, Zaštita u računarskim mrežama, Beograd: Univerzitet Singidunum, 2014.

[6] M. Šarac, Infromacione tehnologije i računarske mreže, fizičko i virtualno okruženje datacentra, Beograd: Univerzitet Singidunum, 2008.

[7] M. Veinović i S. Adamović, Kriptologija 1, Beograd: Univerzitet Singidunum, 2018.