ISSN 1846-6168
UDK 004.056

METODE TELEMETRIJE PRIMJENJENE NA PRIMJERU SUSTAVA OPORAVKA **PODATAKA U SLUČAJU KATASTROFE**

THE METHODS OF TELEMETRY APPLIED ON EXAMPLE OF DISASTER RECOVERY

Miroslav Zorić, Igor Petrović

Stručni članak

Sažetak: *Cilj ovog rada je prikazati važnost postupka planiranja, dimenzioniranja, izvedbe i testiranja sustava koji se zasniva na telemetriji, informatičkoj opremi i virtualizaciji radne okoline, a sve prema zahtjevima krajnjeg korisnika. Takav sustav naziva se Sustav oporavka podataka u slučaju katastrofe (eng. Disaster Recovery). On sadrži primarnu i sekundarnu lokaciju, a glavni cilj mu je osigurati dostupnost podataka u slučaju prirodne katastrofe (potres, požar, poplava, isl.). Na primarnoj lokaciji nalazi se produkcija, dok se na sekundarnoj lokaciji nalaze kopirani podaci čitave primarne lokacije dobiveni metodama baziranim na telemetrijskim sustavima. U slučaju da primarna lokacija postane iz nekog razloga nedostupna podaci se oporavljaju sa sekundarne lokacije, te omogućuju neometan daljnji rad sustava.*

Ključne riječi: *podaci, oporavak, sigurnost, telemetrija, virtualizacija*

Professional paper

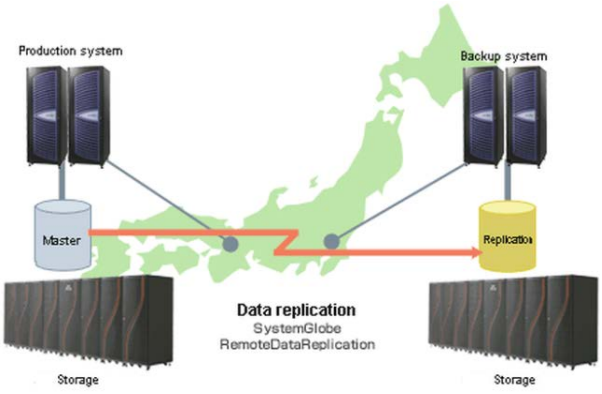
Abstract: *The main goal of this paper is to show importance of planing, dimensionig, developing and testing of a system which is based on telemetry, IT equipment and virtualization of work environment, and everything with complying the user demands. This kind of system is called Disaster Recovery. It contains of a prmary and a secondary location, and main goal is to insure data availability in case of natural disaster (earthquake, fire, flood, etc.). The production is available at a primary location, while a copy of entire primary location is available on a secondary location and is gained using methods based on telemtry systems. In cases when a primary location becomes from some reason unavailable the data is recovered from a secondary location, and enables unobstructed further work of the system.*

Key words: *data, recovery, security, telemetry, virtualization*

1. UVOD

Izrada Sustava oporavka podataka u slučaju katastrofe (eng. *Disaster Recovery*) usko je povezana sa zahtjevima korisnika koji žele višestruko zaštititi svoje poslovne podatke, opisano u [1]. U ustanovama poput banaka, osiguravajućih društava, farmaceutskih tvrtki i državnih tijela podaci su neprocjenjive vrijednosti, stoga ih je potrebno čuvati. Kada bi takve ustanove izgubile svoje podatke, koje su godinama prikupljali, nastala bi katastrofalna i nenadoknadiva šteta, kao u [2] i [3]. Zbog toga se takvi podaci višestruko štite. Razlozi gubitka podataka prirodne katastrofe (poplava, požar, potres), ljudski faktor, i slično. Opasnosti se svode na minimum kopiranjem podataka na više lokacija, te mogućnost pristupa podacima u kratkom vremenskom roku u slučaju katastrofe. Takve sustave treba pomno osmisliti, dimenzionirati i prilagoditi zahtjevima korisnika, a što je multidisciplinarni informatički zadatak, dostupno u [4]. U ovom radu prikazan je jedan takav telemetrijski sustav, te su prikazani rezultati testiranja. Sustav je srednje veličine s obzirom na zahtjeve korisnika i njegov cjenovni rang, kao u [5]. Rezultati mjerenja u probnom radu ukazuju na razinu brzine, sigurnosti i pouzdanosti izvedenog sustava. Više mogućnosti dostupni su u [6] i [7].

2. SUSTAVI ZA OPORAVAK PODATAKA U **SLUČAJU KATASTROFE**



Slika 1. Općeniti prikaz Sustava za oporavak podataka u slučaju katastrofe [8]

Sustavi za oporavak podataka u slučaju katastrofe baziraju se na prijenosu sigurnosnih kopija podataka bez utjecaja na rad glavnog sustava. Općeniti prikaz takvog sustava prikazan je na Slici 1. Sustav se gradi kao telemetrijska centralna stanica za spremanje podataka iz dislociranih pojedinačnih stanica. Garantira se mogućnost pohrane, analize i čuvanja podataka, ali ujedno i točnost tih podataka. Oporavljanje od katastrofe (DR) čine proces, mjere i procedure koje su u svezi s pripremanjem oporavljanja (vraćanja u pretkatastrofno stanje) ili nastavak postojanja tehnološke infrastrukture od kritične važnosti nekoj organizaciji ili sustavu nakon što se zbila prirodna katastrofa ili katastrofa koju je izazvao čovjek.

Kod planiranja Sustava za oporavak podataka u slučaju katastrofe, kao primjerice u [9] i [10], postoje dvije karakteristike na temelju kojih se odlučuje o samoj izvedbi sigurnosnog kopiranja podataka. Prva karakteristika je RPO (eng. *Recovery Point Objective*), odnosno maksimalan prihvatljiv gubitak podataka, obično izražen u satima. Druga karakteristika je RTO (eng. *Recovery Time Objective*), odnosno maksimalana prihvatljiva nedostupnost servisa/podataka (eng. *downtime*), obično izražen u satima. RPO i RTO su za svakog korisnika različiti i zato ih treba pažljivo odrediti te prema njima napraviti Disaster Recovery plan.

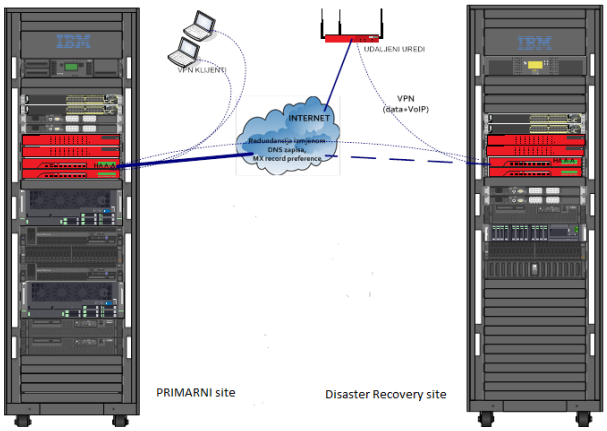
Pri nadogradnjama postojećih IT sustava sa Sustavom za oporavak podataka u slučaju katastrofe potrebno je posebnu pozornost obratiti na analizu postojećeg stanja IT sustava. Funkcionalnost postojećeg sustava ne smije biti narušena nadogradnjom. Planiranje nadogradnje izvodi se opremom koja mora biti prilagođena postojećoj opremi. Stoga se u nekim slučajevima mora odustati od standardnih rješenja i kombinacija opreme, te za svaki pojedinačni slučaj odabrati optimalno rješenje.

3. SUSTAVI ZA OPORAVAK PODATAKA U SLUČAJU KATASTROFE

Za korisnika je nakon analize postojećeg stanja izabrano optimalno rješenje Sustava za oporavak podataka u slučaju katastrofe. Prvo se provodi plan implementacije sustava s definiranim vremenskim rokovima te se dodatno korisniku objašnjava način funkcioniranja svakog komada opreme i svih aplikacija koje su potrebne za realizaciju projekta. Na temelju tog plana korisnik dostavljaju se potrebni podaci postojećeg sustava da bi se uspješno provela implementacija Sustava za oporavak podataka u slučaju katastrofe.

Za izvedeni sustav analiziran u ovom radu izabrani su na primarnoj lokaciji dva IBM UPS uređaja, dva ESXi hosta na IBM x3650 serverima za posluživanje virtualnih servera kojima upravlja VMware virtualni centar za management, jedan IBM Storwize V7000 za pohranu podataka, dva SonicWall NSA 3500 fizička Firewall-a, te dva nova Cisco switcha 2960.

Na Data Recovery strani se nalaze dva ESXi hosta realizirana pomoću Fujitsu RX servera, prebačena sa primarnog sitea za posluživanje virtualnih servera kojima upravlja VMware virtual centar za management. Na te servere je potrebno dodati procesorske snage, te RAM memorije približne snage kao novi serveri na primarnoj strani, a na njih dodati jedan IBM Storwize V7000. Kroz IBM Storewize V7000 se virtualizira, dostupno u [11], postojeći Netapp FAS 2020 storage koji se izmješta s primarne lokacije. Također, na DR lokaciji postavlja se i dva SonicWall NSA 3500 fizička Firewall-a, te dva Cisco switcha 2960 koji su se nalazili na primarnoj strani. Tu se seli i Tape Library IBM TS3100, uređaj koji je zadužen za snimanje podataka s diskovnog podsustava na trake. Kasnije se te trake pohranjuju u sef ili neku sigurnu lokaciju. Takav način pohrane donosi dodatnu prednost u slučaju nestanka primarnog i DR site-a, ali što statistički gotovo nije moguće. Tada bi korisniku ostali podaci na trakama koji se mogu raspakirati i presnimiti na neki drugi hardver, te osigurali korisniku nesmetan rad. Opisana konfiguracija je prikazana na Slici 2.



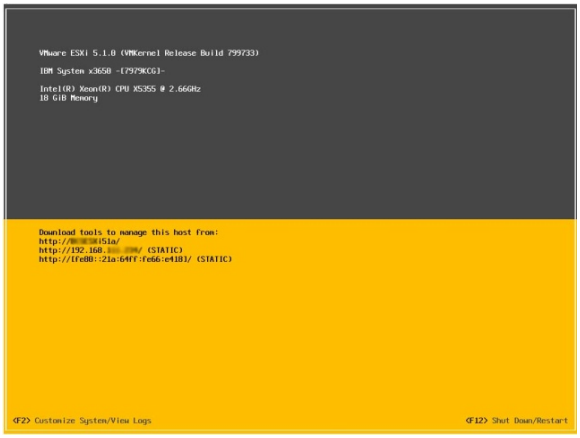
Slika 2. Shematski prikaz rješenja Sustava za oporavak podataka u slučaju katastrofe

Virtualizacija u užem smislu omogućava rad više logičkih ili aplikacijskih procesa na jednom fizičkom uređaju dijeleći na siguran i pouzdan način hardverske resurse između raznih virtualnih okruženja koja na njemu postoje. Danas virtualizacija obuhvaća pojmove kao što su virtualizacija poslužitelja (servera), virtualizacija desktopa, virtualizacija aplikacija, te u najširem smislu virtualizacija poslovanja (eng. *Cloud Computing*). Neke od prednosti u poslovanju koje donose tehnologije virtualizacije su uštede na nabavci i održavanju IT opreme, velika ušteda električne energije, oslobađanje kapaciteta postojeće IT opreme, ubrzana implementacija novih IT rješenja ili proširenja postojećih, jednostavnije upravljanje konfiguracijama te razvojnim, testnim i produkcijskim okruženjima.

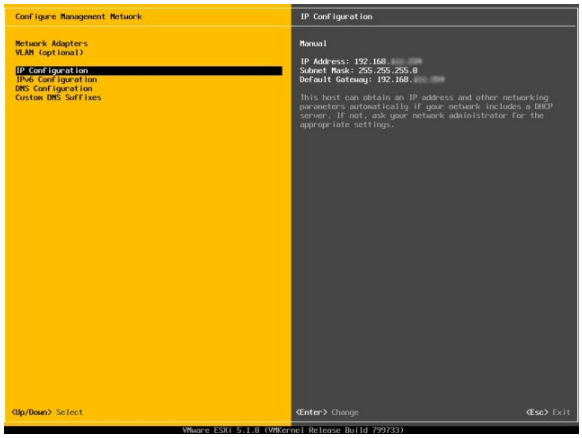
Uz navedena poboljšanja učinkovitosti upravljanja IT infrastrukturom, virtualizacija omogućava jednostavnije planiranje i provođenje upravljanja kontinuitetom poslovanja (eng. *Business Continuity*), te oporavka od ispada (eng. *Disaster Recovery*) i jednostavniju implementaciju visokodostupnih (eng. *High Availability*) sustava. VMware je jedan od najboljih programa današnjice za virtualizaciju servera, VMware ESXi predstavlja operativni sustav koji se instalira i vezan je direktno na fizički server. Operativni sustav prikazan je Slici 3. i Slici 4.

Programska podrška za navedenu opremu omogućava povezivanje ovakve konfiguracije u Sustav za oporavak

podataka u slučaju katastrofe. Rezultati mjerenja u probnom radu dani su za opisanu konfiguraciju sustava.



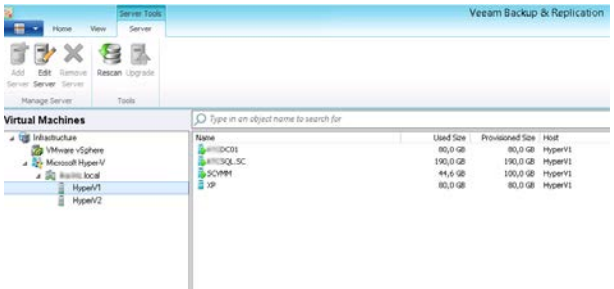
Slika 3. Izgled ESXi sučelja



Slika 4. Izgled ESXi IP

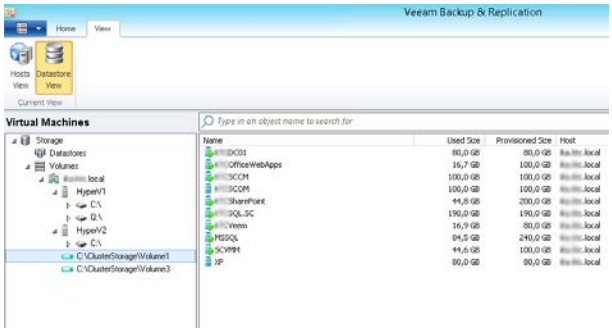
4. REZULTATI PROBNOG RADA SUSTAVA

Mjerenja na izvedenom sustavu u probnom radu vrše se na virtualnim serverima koji su izvedeni samo za tu svrhu, te su vrlo slični produkcijskim virtualnim serverima. Tako se može pretpostaviti da će rezultati probnog rada odgovarati rezultatima sustava u radu na produkcijskim serverima. Ovaj način probnog rada izabran je da se ne bi dovelo u opasnost postojeće produkcijskim virtualnim serverima na koje se ovaj sustav nadograđuje. Sustav će uz pomoć IT opreme automatski kopirati sve podatke, a u slučaju potrebe u najkraćem roku učiniti ih dostupnima uz minimalan ljudski napor. Dio podataka u rezultatima skriven je zbog zaštite korisnika.



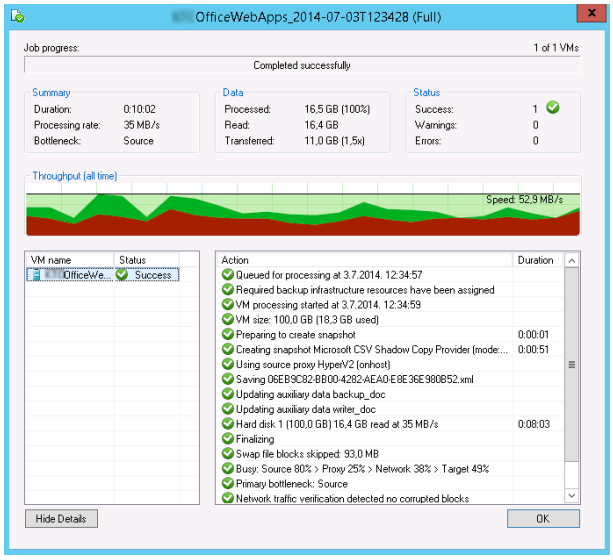
Slika 5. Dio Veeam Backup & Replication konzole

Na Slici 5. je prikazan izgled Veeam Backup & Replication konzole. S lijeve strane vide se hostovi, dok su s desne strane virtualni serveri na prvom hostu. Uz imena virtualnih servera vidi se podatak vezan za količinu prostora koju pojedini server zauzima na diskovnom sustavu, te na kojem od hostova se nalazi pojedini virtualni server.

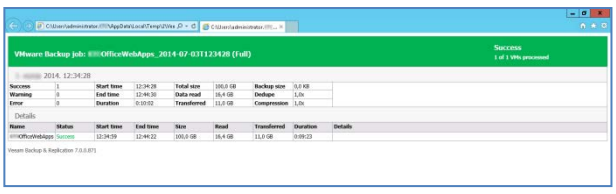


Slika 6. Prikaz Storage konfiguracije

Na Slici 6. prikazana je konfiguracija IBM Storwize-a V7000, odnosno kako Veeam vidi Storwize i hostove s Virtualnim serverima. Plavi okvir na slici pokazuje mjesto na Storwize-u gdje se nalaze virtualni serveri drugog hosta, dok su serveri vidljivi s desne strane. Naime, ti isti virtualni serveri su najmanje tri puta kopirani unutar *Volume1*, a zbog RAID polja na Storwize-u koje dodatno nastoji osigurati podatke. Ako na Storwize-u dođe do uništavanja jednog od Hard Diskova ti podaci neće biti izgubljeni jer se njihova kopija nalazi na barem još dva diska unutar Storwize-a.



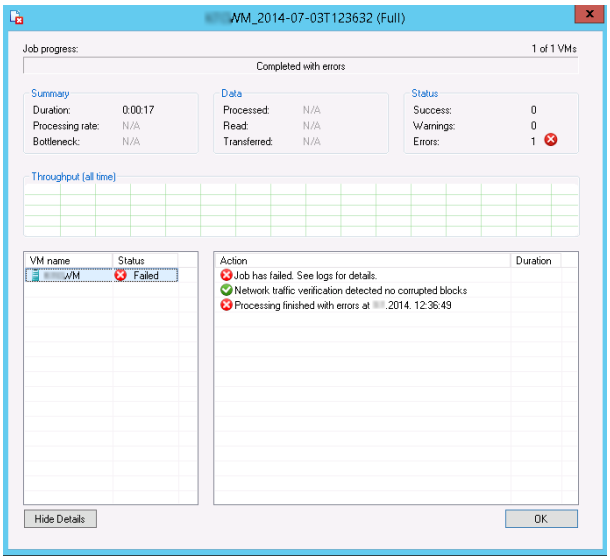
Slika 7. Detaljni prikaz uspješnog backupa



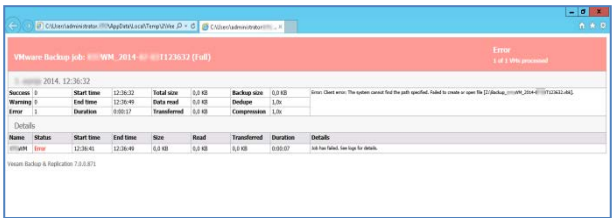
Slika 8. Izvještaj o uspješno provedenom backupu

Na Slici 7. i Slici 8. prikazani su detalji uspješnog backupa jednog virtualnog servera. Na njima je jasno

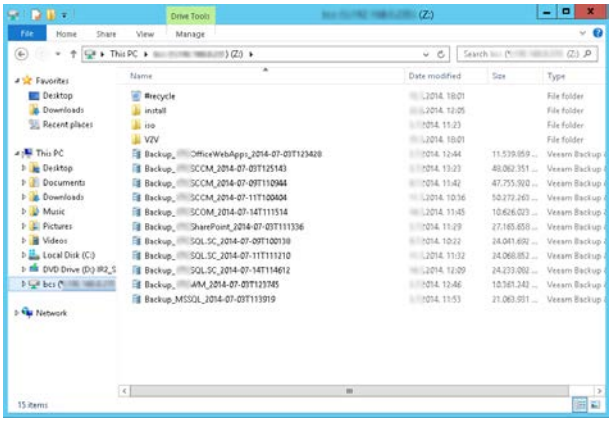
vidljivo koliko je ovom sustavu bilo potrebno vremena da prenese podatke, kolikom brzinom ih je prenosio, te u konačnici kolika količina podataka je kopirana. Na slikama je izvještaj koji možemo automatizmom generirati i uputiti administratorima sustava putem e-mail poruka. Dakle, sustav i u slučaju izvještavanja ima bitnu ulogu. Ovim načinom informacije o statusu replikacija dostupne su bez potrebe da administratori budu logirani na sustav. To je korisno u slučajevima kada se primjerice backup radi nekoliko puta u danu i noći, a administrator ne može biti logiran na sustav cijelo to vrijeme. Međutim e-mail poruke na mobilnom uređaju su mu stalno dostupne i mora reagirati samo u slučaju kada sustav pošalje izvještaj u kojem ga upozorava na neuspješno izvršen backup pojedinog virtualnog servera.



Slika 9. Primjer neuspjelog backupa virtualnog servera



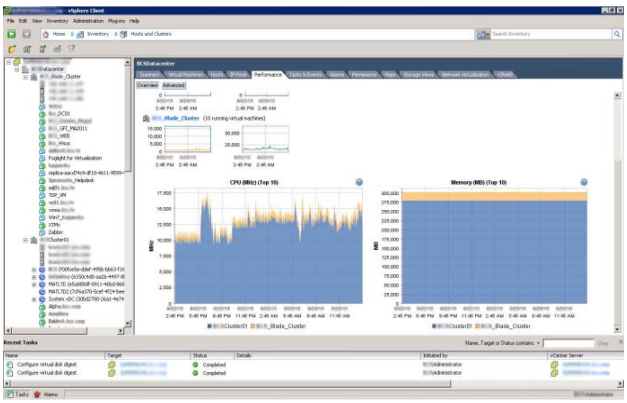
Slika 10. Izvještaj o neuspješno izvedenom backupu



Slika 11. Izgled virtualnih servera nakon backup-a

Slika 9. i Slika 10. prikazuju primjer neuspjelog backup-a jednog virtualnog servera. Sustav je u ovom slučaju parcijalno zakazao, administratoru je uspješno poslana e- mail poruka o neuspješnom backup-u. Dakle, sustav dojave i izvještavanja je u ovom sustavu ipak radio ispravno. Administrator sustava po primitku e-mail poruke mora reagirati u najkraćem roku kako bi otkrio uzrok neuspješnog backup-a.

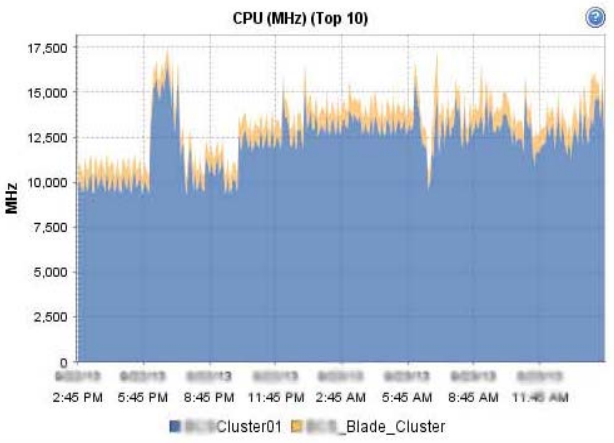
Slika 11. potvrđuje da ovaj sustav na DR lokaciji uspješno pohranjuje backup verzije pojedinih virtualnih servera na diskovni podsustav u slučaju da dođe do nedostupnosti primarne lokacije. Ove datoteke spašavaju testirani sustav jer se njihovim pokretanjem u VMware Virtual Centru na DR lokaciji testirani sustav vraća u stanje funkcionalnosti.



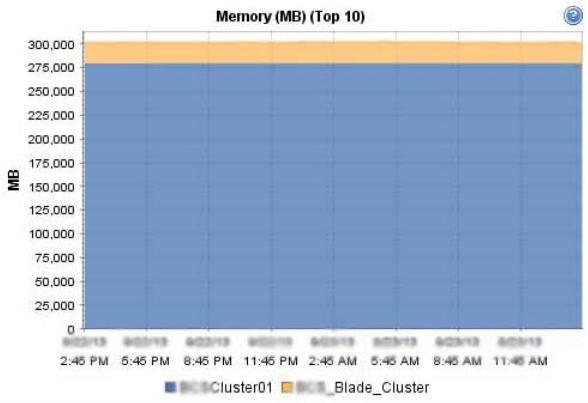
Slika 12. Izgled krajnjeg rezultata sa mjerenjima sustava u probnom radu

Slika 12. prikazuje VMware Virtual Centar na kojem je vidljivo da su dostupni Hostovi i virtualni serveri s primarne i DR lokacije, što dokazuje da telemetrijski sustav funkcionira na željeni način i da se virtualni serveri uredno kopiraju na DR lokaciju.

Slika 13. i Slika 14. prikazuju potrošnju procesorske snage i RAM memorije na primarnoj lokaciji (žuta boja) i DR lokaciji (plava boja). Vidljivo je da primarna lokacija troši više resursa, što se događa jer su trenutno na nju spojena sva klijent računala koja izvršavaju određene operacije u aplikacijama, a se nalaze na virtualnim serverima. Dakle, razlika resursa se troši na prikaz željenih podataka, njihovu izmjenu, te ponovno snimanje na diskovni podsustav.



Slika 13. Izgled primarne i DR strane nakon backup-a, detalj 1



Slika 14. Izgled primarne i DR strane nakon backup-a, detalj 2

Slika 15. Izgled primarne i DR strane nakon backup-a, detalj 3

Na Slici 15. vidi se oznaka *Cluster* koja označava cijelu primarnu lokaciju, te odmah ispod njezine Hostove i virtualne servere. Oznaka *Cluster01* označava DR lokaciju, te odmah ispod njezine Hostove i virtualne servere koji su kopirani s primarne lokacije no trenutno su ugašeni jer primarna lokacija funkcionira uredno.

5. ZAKLJUČAK

U cilju zadovoljavanja korisničkih zahtjeva izgrađen je telemetrijski sustav Disaster Recovery koji omogućuje brz i pouzdan backup podataka, te korisniku omogućuje oporavak u slučaju katastrofe na primarnoj lokaciji. Kopiranje podataka bazirano na metodama telemetrije i podizanje DR lokacije u slučaju katastrofe odvija se u unaprijed zadanim vremenskim okvirima. Probno kopiranje svakog pojedinog virtualnog servera obavljeno je nekoliko puta kako bi bilo sigurano da ne postoje varijacije u vremenskom periodu.

Za daljnji rad administratoru je važan samo pristup internetu kako bi se mogao spojiti na VPN tunel, što mu uveliko olakšava posao. Kada sustav radi stabilno potrebno je redovito kontrolirati automatski generirane izvještaje o uspješnosti kopiranja posjedinog virtualnog servera. Temeljem rezultata može se konstatirati da je izgrađeni sustav potpuno funkcionalan i pouzdan, te je zadovoljio sve očekivanja i unaprijed zadane ciljeve korisnika.

5. LITERATURA

[1] Philip, G.; Hodge, R.: Disaster area architecture: telecommunications support to disaster response and recovery, IEEE Military Communications Conference, San Diego CA, November 1995, 833-837 vol. 2

[2] Zhang, G.; Yang, Y.; Mao, X.: Disaster recovery evaluation PROC model framework based on information flow, Proceedings on Computer Science and Network Technology Conference, Harbin, December 2011, 1841-1845

[3] Alhazmi, O. H.; Malaiya, Y. K.: Evaluating disaster recovery plans using the cloud, Proceedings on Reliability and Maintainability Symposium, Orlando FL, January 2013, 1-6

[4] Han, H.; Li, L.; Zhu, D.: Research and Implementation on Remote Disaster Recovery System, Proceedings on Computer Science & Service System Conference, Nanjing, August 2012, 875-879

[5] Alhazmi, O. H.; Malaiya, Y. K.: Assesing Disaster Recovery Alternatives: On-Site, Colocation or Cloud, Proceedings on IEEE Software Reliability Engineering Workshops Symposium, Dallas TX, November 2012, 19-20

[6] Ping, Y.; Bo, K.; Jinping, L.; Mengxia, L.: Remote disaster recovery system architecture based on database replication technology, Proceedings on Computer and Communication Technologies in Agriculture Engineering, Chengdu, June 2010, 254-257 vol. 1

[7] Yu, G.; Dongsheng, W.; Chuanyi, L.: DR-Cloud: Multi-cloud based disaster recovery service, Tsinghua Science and Technology, Vol. 19, No. 1 (2014) 13-23

[8] http://www.redbooks.ibm.com/redbooks/pdfs/sg247938.pdf (Dostupno 20. 10. 2014.)

[9] Fallara, P.: Disaster recovery planning, Journal of Potentials, Vol. 22, No. 5 (2004) 42-44

[10] Wu, R.; Li, R.; Fei, Y.; Yue, G.; Wen, J.: Research on Remote Heterogeneous Disaster Recovery Technology in Grid Computing Security, Proceedings on Semantics, Knowledge and Grid, Guilin, November 2006, 75

[11] Xu, Y.; Yu, H.; Zheng, W.: A Consistent Backup Mechanism for Disaster Recovery that Using Container Based Virtualization, Proceedings on ChinaGrid Annual Conference, Beijing, September 2012, 95-100

Kontakt autora:

Miroslav Zorić, bivši student
Visoka tehnička škola u Bjelovaru
Trg Eugena Kvaternika 4, 43 000 Bjelovar
043 / 241 – 201; zoricmi@yahoo.com

dr. sc. Igor Petrović
Visoka tehnička škola u Bjelovaru
Trg Eugena Kvaternika 4, 43 000 Bjelovar
043 / 241 – 201; ipetrovic@vtsbj.hr