ELEKTROTEHNIŠKI VESTNIK 78(3): 118-122, 2011
EXISTING SEPARATE ENGLISH EDITION

Varnostne kopije podatkov v oblakih

Aljaž Zrnec

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Tržaška 25, 1000 Ljubljana, Slovenija
E-pošta: aljaz.zrnec@fri.uni-lj.si

Povzetek.V prispevku predstavimo koncept izdelovanja varnostnih kopij v oblaku. Predstavimo dosedanjo prakso izdelovanja varnostnih kopij, kjer se varnostne kopije podatkov hranijo na ločeni lokaciji, in možnost izdelave varnostne kopije v oblaku, kjer se osredinimo predvsem na ekonomske in performančne vidike uporabe oblačnega računalništva za izdelavo varnostnih kopij podatkov.

Ključne besede:oblačno računalništvo, oblak, pasovna širina, zunanje izvajanje, varnostna kopija, računalniški center

Backup in the Cloud

In the paper we introduce the concept of making backups in the Cloud. We present the current practice of making backup copies of data, where backups are stored in a separate location, and the possibility of making backups in the Cloud. We mainly focus on economic and performance aspects of using Cloud computing for making backup copies of data.

1 UVOD

Oblačno računalništvo [1] omogoča uporabnikom prek svetovnega spleta izrabiti navidezno neomejen bazen računskih virov in zmogljivosti za shranjevanje podatkov. V primerjavi s tradicionalnim pojmovanjem uporabe računalnikov, kjer imajo uporabniki popoln nadzor nad računalniškimi viri, imajo uporabniki oblačnega računalništva zelo malo ali nič vpogleda in nadzora nad računalniško infrastrukturo oblaka, tako da morajo za interakcijo z računskimi in podatkovnimi viri oblaka uporabljati ustrezne aplikacijske vmesnike (API - ApplicationProgrammingInterface), ki jih mora zagotoviti ponudnik oblačnega računalništva [2]. V zameno za navedene omejitve pa uporabniki oblakov pridobijo več pomembnih koristi, kot so preprosta razširljivost, zanesljivost, možnost samostojnega in dinamičnega prilagajanja potrebnih virov ter plačevanje samo za vire, ki se dejansko uporabijo.

Zaradi prednosti, ki jih ponujajo oblaki, v zadnjem času srečujemo ponudnike številnih storitev, med katerimi je še posebno zanimiva možnost izdelave varnostne kopije podatkov v oblaku. Zato bomo v prispevku v okviru drugega razdelka najprej predstavili razliko med klasično izdelavo varnostne kopije in izdelavo varnostne kopije podatkov v oblaku. V tretjem razdelku bomo podali primer izdelave varnostne kopije v podatkovni bazi Oracle, enkrat brez in drugič z uporabo oblaka. V okviru omenjenega razdelka bo podana tudi primerjava stroškov in hitrosti izdelave kopije za oba načina izvedbe. V sklepu bomo podali ugotovitve in smernice za nadaljnje delo.

2 IZDELAVA KLASIČNE VARNOSTNE KOPIJE IN KOPIJE V OBLAKU

2.1 Klasična varnostna kopija podatkov

Dobra praksa s področja obnavljanja podatkovnih baz po nesrečah narekuje hrambo varnostnih kopij podatkov, ki so za poslovanje kritični, na ločeni lokaciji, zunaj prostorov poslovnega sistema. Poslovni sistemi za to po navadi poskrbijo tako, da varnostne kopije zapisujejo na magnetne trakove in jih pošiljajo na neko oddaljeno lokacijo, kar pa je drag in kompleksen postopek, ki zahteva posebno strojno opremo, ustrezno usposobljene kadre in postopke (predpise), ki zagotavljajo, da se varnostne kopije sproti izdelujejo, da so zavarovane in da je podatke iz njih mogoče pridobiti in jih uporabiti v primeru nesreč. Tudi če je danes že nekaj vsakdanjega, da poslovni sistemi prepuščajo transport in varovanje varnostnih kopij podatkov zunanjim izvajalcem, pa še vedno sami skrbijo za zagotavljanje integritete podatkov v svojih varnostnih kopijah in za prej omenjene postopke.

2.2 Kopija v oblaku

Kot alternativa današnji klasični izdelavi varnostnih kopij podatkov je z razvojem oblačnega računalništva čedalje več ponudnikov oblačnih storitev, ki omogočajo izdelavo varnostnih kopij podatkov v oblakih (ang. cloudbackup).

Kopija v oblaku ali t. i. kopija "online" je način izdelave varnostne kopije podatkov, pri katerem se podatki iz podatkovne baze pošljejo po javnem ali zasebnem omrežju na podatkovni strežnik, ki se nahaja na oddaljeni lokaciji. Podatkovni strežnik upravlja ponudnik oblačnih storitev, ki stranki zaračunava storitev hranjenja kopije na podlagi potrebnega diskovnega prostora, pasovne širine ali števila uporabnikov te storitve.

Sistem za izdelavo varnostnih kopij v oblaku temelji na aplikaciji, ki se nahaja pri uporabniku storitve in se proži s frekvenco (dnevno, tedensko itd.), ki je

Prejet 10. november,2010
Odobren 18. februar, 2011

opredeljena v pogodbi o uporabi oblačne storitve (SLA - ServiceLevelAgreement) za izdelavo varnostne kopije podatkov. Če ima npr. stranka pogodbo za izdelavo dnevnih varnostnih kopij, potem aplikacija zbere, stisne, kriptira in pošlje podatke na podatkovni strežnik ponudnika storitve vsakih 24 ur. Za zmanjševanje uporabljene pasovne širine pri prenosu podatkov se lahko uporabi pristop inkrementalne izdelave varnostne kopije, kjer se intervalno, glede na sklenjeno pogodbo o uporabi oblačne storitve, v oblak prenašajo samo spremembe v originalni podatkovni bazi. Ker se podatki prenašajo po svetovnem spletu, je podatkovna prepustnost po navadi relativno zelo omejena. Poleg tega lahko tudi sami ponudniki oblačnih storitev omejujejo prepustnost, da preprečijo posamičnim uporabnikom nesorazmerno rabo virov v oblaku.

Glede na analize uporabe, ki smo jih izvedli s podatkovno bazo Oracle in Amazonove storitve, ki omogoča izdelavo varnostne kopije podatkov v oblaku - Amazon S3 [3], smo ugotovili, da ponudnik Amazon omejuje podatkovno prepustnost v okviru posamične seje na 2,5 do 3,5 Mb/s.

2.3 Prednosti izdelave varnostne kopije v oblaku

Najpomembnejše prednosti pošiljanja varnostne kopije podatkov po svetovnem spletu v oblak so: prilagodljivost oblaka našim potrebam glede performans, velik razpoložljiv prostor za shranjevanje in stroški, ki se obračunavajo samo glede na dejansko uporabo virov. Poleg tega lahko uporaba oblaka tudi znatno poenostavi lastno informacijsko infrastrukturo, ker ni več potrebe po lastnem upravljanju hrambe podatkov (npr.: delo z magnetnimi trakovi, pošiljanje magnetnih trakov na ločene lokacije itd.) in potrebe po posebni strojni opremi za izdelovanje varnostnih kopij. V razdelku 3.2 bodo predstavljene vse prednosti, ki jih ponuja podatkovna baza Oracle pri izdelavi varnostne kopije podatkov v oblaku.

Pomemben pomislek glede samega prenosa podatkov v oblaka oziroma iz njega je lahko omejena pasovna širina spleta, ki onemogoča hiter prenos velike količine podatkov (problem pri izdelavi popolne varnostne kopije). Ponudnik storitev Amazon omenjeni problem rešuje tako, da za uvoz ali izvoz podatkov ponuja posebno storitev, ki omogoča premik celotne varnostne kopije v oblak ali iz njega in transport s prenosnim trdim diskom. Primer: po nesreči nam ponudnik storitve (Amazon S3) s hitro pošto pošlje celotno varnostno kopijo na prenosnem disku. Tako je shranjevanje podatkov v oblaku primerljivo s klasično izdelavo varnostne kopije podatkov, še zlasti ko je ločena lokacija del poslovne strategije izdelave varnostnih kopij podatkov, ki vključuje varnostne kopije tako v poslovnem sistemu kot na ločenih lokacijah.

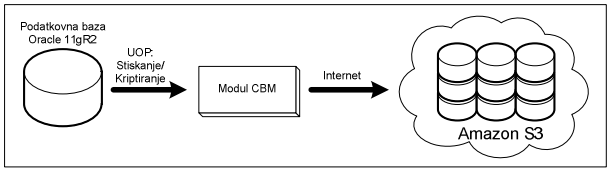
3 IZDELAVA VARNOSTNE KOPIJE V PODATKOVNI BAZI ORACLE

3.1 Testno okolje

Za analizo smo uporabili podatkovno bazo Oracle 11gR2, ki smo jo namestili na strežnik s procesorjem 2,66 GHz Xeon, trdim diskom z 10000 obr/min, 8 Gb pomnilnika in operacijskim sistemom MS Windows Server 2008 x64. Za izdelavo varnostne kopije podatkov v oblaku smo izbrali ponudnika oblačnih storitev Amazon, in sicer storitev Amazon S3.

Amazon S3 (v nadaljevanju S3) je osnovna storitev podjetja Amazon za hranjenje podatkov. Storitev omogoča prek preprostega spletnega vmesnika prenesti katerokoli količino podatkov v oblak ali iz njega ter njihovo shranjevanje. Storitev S3 odlikuje skalabilnost, kar pomeni, da je njeno delovanje neodvisno od števila uporabnikov, zanesljivost in hitrost delovanja. Pomembna je tudi cena za uporabo storitve, ki se oblikuje na podlagi pogodbe o uporabi storitve in temelji izključno na oblačnih virih, ki se dejansko uporabijo. Storitev S3 je namenjena tako hrambi klasičnih tekstovnih in numeričnih podatkov kot tudi strežbi večpredstavnih podatkov v realnem času.

V podatkovni bazi Oracle 11gR2 skrbi za izdelavo varnostnih kopij podatkov poseben modul, CloudBackup Module (v nadaljevanju CBM), ki omogoča povezovanje s storitvijo S3 in pošiljanje varnostnih kopij v oblak. Modul je združljiv z vsemi podatkovnimi bazami Oracle od različice 9iR2 naprej. Za svoje delovanje zahteva povezavo s svetovnim spletom. CBM je član družine izdelkov Oracle SecureBackup, v katero spadajo orodja za izdelavo varnostnih kopij podatkov na magnetnih trakovih ali v oblaku. Modul CBM se lahko uporabi tudi v okviru uporabe storitve AmazonElasticComputeCloud (EC2), kjer je podatkovna baza na navideznem strežniku v oblaku [4]. Prednost take uporabe so boljša prepustnost podatkov v oblaku in nižji stroški uporabe, ker odpadejo stroški za prenos podatkov v storitev S3 ali iz nje. CBM je implementiran v okviru upravitelja za obnavljanje podatkov (v nadaljevanju UOP), ki omogoča preprosto integracijo z zunanjimi knjižnicami za izdelavo varnostnih kopij. Tako lahko administratorji še naprej uporabljajo obstoječa orodja za izdelovanje varnostnih kopij. Opisane module in postopek izdelave varnostne kopije v oblaku prikazuje Slika 1.



Slika 1: Izdelava varnostne kopije podatkovne baze Oracle v oblaku

3.2 Prednosti izdelave varnostne kopije v oblaku z uporabo podatkovne baze Oracle

Izdelava varnostne kopije podatkov v oblaku ima pred klasično varnostno kopijo na magnetnem traku več prednosti:

- *Nepretrgana dosegljivost*: Varnostne kopije, ki se nahajajo v oblaku, so vedno dosegljive, podobno kot varnostne kopije na lokalnih diskih. Zato ob morebitni nesreči ni potreben transport trakov pred začetkom samega postopka obnavljanja. Administrator namesto tega lahko uporabi klasična orodja (EnterpriseManager, skripta itd.) za obnavljanje podatkovne baze po nesreči, podobno kot bi bila varnostna kopija podatkov shranjena lokalno. Tako se izpad podatkovne baze iz produkcijskega okolja skrajša z nekaj dni na nekaj ur ali celo na samo nekaj minut. Če je vseeno potreben transport podatkov iz oblaka na prenosnem disku, pa obnavljanje ne vzame več časa kot transport traku z ločene lokacije.
- *Visoka raven zanesljivosti*: Oblaki za hranjenje podatkov temeljijo na uporabi diskov, katerih zanesljivost danes presega zanesljivost magnetnih trakov. Poleg tega so v oblaku podatki tudi večkratno replicirani, s čimer ponudnik oblačne storitve zagotavlja višjo raven razpoložljivosti in skalabilnosti.
- *Neomejeno povečevanje prostora in nič vnaprejšnjih finančnih izdatkov*: Oblak zagotavlja na prvi pogled neomejeno zmogljivost za hranjenje podatkov, ne da bi za to bili potrebni vnaprejšnji finančni izdatki. To pomeni, da dinamično prilagaja velikost diskovnega prostora za hranjenje varnostnih kopij, uporabniki storitve pa plačujejo samo prostor, ki je dejansko uporabljen.
- *Nižja raven rabe magnetnih trakov in nižji stroški za hranjenje varnostnih kopij na ločenih lokacijah*: Ker oblaki zmanjšujejo ali celo odpravljajo potrebo po magnetnih trakovih, se ustrezno znižajo tudi stroški nakupa strojne in programske opreme za izdelavo varnostnih kopij na magnetnih trakovih in stroški hranjenja podatkov na ločenih lokacijah.
- *Preprosto zagotavljanje testnega in razvojnega okolja*: Varnostne kopije v oblaku so po svetovnem spletu dostopne od koderkoli. Zato je mogoče zelo hitro izdelati testno kopijo podatkovne baze za potrebe razvoja in testiranja. Na primer: varnostno kopijo, ki se hrani v Amazon S3, je z uporabo preproste skripte mogoče klonirati v navidezni računalnik – strežnik, ki ga ponuja storitev Amazon EC2.

3.3 Zagotavljanje varnosti podatkov

Varnost in zasebnost podatkov sta v javno dostopnih – deljenih okoljih, kot je oblak, zelo pomembna. Zato modul CBM pri pošiljanju podatkov v oblak uporablja posebno funkcionalnost komponente UOP, ki za zagotavljanje varnosti in zasebnosti podatkov v okviru kopije uporablja kriptiranje. Tako so podatki v varnostni kopiji dvakrat zaščiteni. En nivo zaščite pred neavtoriziranim dostopom zagotavlja že sam ponudnik oblačnih storitev, drugi nivo pa je zagotovljen s prej omenjenim kriptiranjem podatkov varnostne kopije, preden se ta pošlje v oblak. Tako se zmanjša verjetnost za krajo ali nepooblaščen dostop do podatkov pri transportu, kot tudi pri samem hranjenju podatkov v oblaku.

3.4 Stiskanje podatkov

Ker se modul CBM integrira v sistem za upravljanje podatkovne baze Oracle, lahko samostojno identificira in izloči nepotreben prostor (bloke) v podatkovni bazi, preden se varnostna kopija izdela in pošlje v oblak. Hkrati komponenta UOP ponuja številne možnosti za uporabo stiskanja podatkov, kar neposredno vpliva na hitrost izdelave varnostne kopije. Na hitrost izdelave varnostne kopije podatkov v oblaku najbolj vplivajo relativno počasne povezave v svetovnem spletu. Tako smo pri analizi vpliva stiskanja podatkov na hitrost izdelave varnostne kopije primerjali izdelavo kopije z uporabo stiskanja podatkov in brez nje.

3.5 Učinkovitost izdelave varnostne kopije v oblaku

Kot smo omenili že v razdelku 2.2, Amazon S3 lahko omejuje prepustnost v okviru posamične seje na 2,5 do 3,5 Mb/s, s čimer se posamičnim uporabnikom prepreči nesorazmerno rabo oblačnih virov. Vendar pa smo ugotovili, da je mogoče z uporabo pravilne kombinacije paralelizma in stiskanja podatkov pri izdelavi varnostne kopije doseči podatkovno prepustnost od 43 Mb/s do 55 Mb/s, kar odločilno vpliva na hitrost izdelave varnostne kopije.

V okviru analize učinkovitosti izdelave varnostne kopije podatkov v oblaku s podatkovno bazo Oracle smo izvedli več meritev, v katerih smo ugotavljali čas, ki je potreben za izdelavo varnostne kopije. Merili smo trajanje izdelave varnostne kopije podatkovne baze, ki se je nahajala na našem testnem strežniku, nato pa še v navideznem strežniku storitve EC2 [5]. Za obe podatkovni bazi smo opazovali vpliv stiskanja podatkov na čas izdelave varnostne kopije. Meritve smo izvedli tako za izdelavo popolne kot inkrementalne varnostne kopije. Velikost celotne varnostne kopije je bila 250 Gb, velikost inkrementalne varnostne kopije pa je bila 10 odstotkov sprememb podatkov v podatkovni bazi. Rezultate meritev trajanja izdelave varnostnih kopij prikazuje tabela 1.

Lokacija pod. Baze	Podatkovna prepustnost		Čas izdelave celotne varnostne kopije		Čas izdelava inkrement. varnostne kopije	
	Stiskanje		Stiskanje		Stiskanje	
	Ne	Da	Ne	Da	Ne	Da
Testni strežnik	10 MB/s	43 MB/s	< 6 ur	> 2 uri	< 1 ure	> 30 min
Navidezni strežnik v EC2	35 MB/s	55 MB/s	< 2 uri	> 1 ure	< 20 min	> 10 min

Tabela 1: Hitrost izdelave varnostne kopije podatkov v oblaku

Na podlagi izmerjenih časov ugotovimo:

- Čas izdelave celotne ali inkrementalne varnostne kopije podatkovne baze (brez uporabe stiskanja podatkov), ki se je nahajala na testnem strežniku, je 3-krat daljši, kot če se podatkovna baza nahaja v navideznem računalniku v EC2.
- Čas izdelave varnostne kopije podatkovne baze (z uporabo stiskanja podatkov), ki se je nahajala na testnem strežniku, je 2-krat (pri izdelavi celotne kopije) oziroma 3-krat (pri izdelavi inkrementalne kopije) daljši, kot če se podatkovna baza nahaja v navideznem računalniku v EC2.
- Čas izdelave celotne varnostne kopije na testnem strežniku je 3-krat daljši brez uporabe stiskanjain 2-krat daljši pri izdelavi inkrementalne varnostne kopije.
- Čas izdelave celotne ali inkrementalnevarnostne kopije podatkovne baze na navideznem strežniku v EC2 je 2-krat daljši brez uporabe stiskanja.

Iz navedenega lahko sklepamo, da na hitrost izdelave varnostne kopije podatkov močno vplivata predvsem podatkovna prepustnost svetovnega spleta in stopnja stiskanja podatkov. Pri tem naj še opozorimo, da podatkovna baza Oracle od različice 11g naprej uporablja t. i. napredne mehanizme za stiskanje podatkov, ki so z vidika uporabe CPU časa bistveno učinkovitejši kot pri prejšnjih različicah.

Na hitrost vpliva tudi UOP z vzporedno uporabo več prenosnih kanalov, ki omogočajo polno izkoristiti omrežje. Največjo učinkovitost smo dosegli pri uporabi 64 sočasnih kanalov. Podatkovna baza Oracle, od različice 11g naprej, namreč omogoča s hkratno uporabo več kanalov izdelovati varnostno kopijo ene podatkovne datoteke.

3.6 Ocena stroškov izdelave varnostne kopije podatkov v oblaku

Pri oceni stroškov [6] izdelave varnostne kopije podatkov v oblaku smo izhajali iz cen za uporabo oblačnih storitev S3 in EC2. Stroški storitve S3 vključujejo ceno hranjenja 325 Gb podatkov v oblaku (glej opis scenarija izdelave varnostnih kopij) in ceno uporabe storitve S3. Stroški storitve EC2 pa vključujejo ceno uporabe navideznega strežnika in ceno prenosa podatkov v oblak. Stroške smo ocenili za en mesec ob predpostavki, da smo morali na začetku izdelati popolno varnostno kopijo podatkovne baze, torej prenesti v oblak celotno varnostno kopijo (250 Gb), 3-krat v mesecu (tedensko) pa smo izdelali inkrementalno varnostno kopijo. Hitrost spletne povezave je bila 10 Mbit/s. Velikost inkrementalne varnostne kopije je znašala 25 Gb. Na spletni strani storitve S3 smo z orodjem za izračun stroškov izračunali, da se nam prenos celotne varnostne kopije podatkov z uporabo prenosnega diska ne splača, saj stroški takega prenosa znašajo 235 dolarjev (vključno s ceno prenosnega diska), pri prenosu iste količine podatkov prek 10 Mbit spletne povezave, ki znaša 25 dolarjev in traja 3 dni in 6 ur. Poleg tega tudi transport prenosnega diska v računalniški center podjetja Amazon traja 3–4 dni. Celotne stroške za izdelavo varnostne kopije podatkov v oblaku (uporaba storitve S3) prikazuje tabela 2.

Storitev S3			
Cena hrambe podatkov (cena prvega 1 TB/mesec znaša 0,14$/GB):			
Količina podatkov	**Čas hrambe (dnevi)**	**Izračun: 0,00452$/GB dan * št. dni * količina podatkov**	**Cena**
celotna varnostna kopija - 250 GB	31 dni	0,00452*31*250	35,00$
1. inkr. varnostna kopija	24 dni	0,00452*24*25	2,71$
2. inkr. varnostna kopija	17 dni	0,00452*17*25	1,92$
3. inkr. varnostna kopija	10 dni	0,00452*10*25	1,13$
Cena prenosa podatkov v oblak:			
1 x 250 GB		1 x 25$	25,00$
3 x 25 GB		3 x 2,5$	7,50$
SKUPAJ:			**73,26$**

Tabela 2: Ocena stroškov izdelave varnostne kopije podatkov v oblaku

Pri uporabi storitve EC2, kjer se je podatkovna baza Oracle nahajala na navideznem strežniku v oblaku, je cena izdelave varnostne kopije podatkov enaka, saj se podatki prav tako prenesejo v storitev S3. Prednost uporabe navideznega strežnika je predvsem v hitrosti izdelave varnostne kopije, saj se podatki prenašajo znotraj oblaka (ponudnika storitev Amazon), kjer nismo omejeni s podatkovno prepustnostjo svetovnega spleta, zato bi bila v našem primeru celotna varnostna kopija izdelana v manj kot treh dneh. Prav tako lahko omenimo tudi strošek za najem navideznega strežnika, ki za strežnik Extralarge, High-memory Instance z operacijskim sistemom Windows Server 2008 x64 znaša 0,62 $/h. Tako je cena za en mesec 461,28 dolarja, kar je v primerjavi s ceno fizičnega strežnika skoraj 10-krat manj. Cena testnega strežnika z enakim operacijskim sistemom, ki smo ga uporabili pri analizi, je na primer znašala 4200 dolarjev.

3.7 Hitrost in ocena stroškov izdelave klasične varnostne kopije podatkov

Čas izdelave klasične varnostne kopije podatkov smo izmerili tako, da smo sešteli čas, ki je potreben za izdelavo varnostne kopije na magnetni trak in čas za dostavo magnetnega traku na ločeno lokacijo. Pri tem smo merili čas izdelave celotne in inkrementalne varnostne kopije, in sicer z uporabo stiskanja podatkov in brez nje, podobno kot v razdelku 3.5. Uporabljali smo tračno enoto za zapisovanje na magnetni trak, storitve kurirske službe za dostavljanje magnetnih trakov na ločeno lokacijo in storitev hranjenja magnetnih trakov na ločeni lokaciji v trezorju. Pri izbiri tračne enote smo izhajali iz zahteve, da mora biti ta zmožna zapisati vse podatke (celotno ali inkrementalno kopijo) na en

magnetni trak. Izmerjene čase za izdelavo celotne in inkrementalne varnostne kopije prikazuje tabela 3.

	Čas izdelave varnostne kopije celotne podatkovne baze		Čas izdelava inkrementalne varnostne kopije	
	Stiskanje		Stiskanje	
	Ne	Da	Ne	Da
	< 1:15 ure	> 15 min	< 10 min	> 1:42 min
Transport na ločeno lokacijo in skladiščenje	< 3 ure	< 3 ure	< 3 ure	< 3 ure
Skupni čas	< 4:14 ure	> 3:15 ure	< 3:10 ure	> 3:1:4 ure

Tabela 3: Čas izdelave klasične varnostne kopije podatkov

Glede trajanja izdelave celotne in inkrementalne varnostne kopije ugotovimo, da:

- Minimalen čas za izdelavo celotne varnostne kopije podatkov znaša 3 ure in 15 minut, kar je v primerjavi s časom za izdelavo varnostne kopije celotne podatkovne baze v oblaku (2 ure) 62,5 odstotka več.
- Minimalen čas za izdelavo inkrementalne varnostne kopije podatkov je približno 3 ure in 2 minuti, kar je v primerjavi s časom za izdelavo inkrementalne varnostne kopije v oblaku (30 minut) 6-krat več.

Pri oceni stroškov za izdelavo klasične varnostne kopije podatkov na magnetni trak smo predvidevali, da za izdelavo varnostnih kopij potrebujemo tračno enoto, ustrezno število magnetnih trakov, storitev kurirske službe za prenos magnetnega traku na oddaljeno lokacijo in storitev najema trezorja za hrambo magnetnih trakov na oddaljeni lokaciji. Stroške smo podobno kot v razdelku 3.6 ocenili za en mesec ob predpostavki, da smo morali na začetku izdelati popolno varnostno kopijo podatkovne baze, 3-krat v mesecu (tedensko) pa smo izdelali inkrementalno varnostno kopijo. Celotne stroške za izdelavo klasične varnostne kopije podatkov na oddaljeni lokaciji prikazuje tabela 4.

Klasična izdelava varnostne kopije			
	Cena na enoto	**Število enot**	**Cena**
Tračna enota	2750$	1	2750$
Transport magnetnih trakov s kurirsko službo	40$	4	160$
Najem trezorja (1 leto)	240$	1	240$
Magnetni trak (400 GB) za celotno kopijo	45$	1	45$
Magnetni trak (400 GB) za inkrementalne kopije	45$	3	135$
SKUPAJ			**3330$**

Tabela 4: Ocena stroškov izdelave klasične varnostne kopije podatkov

Strošek klasične izdelave varnostne kopije po prej omenjenem scenariju bi v prvem mesecu izdelave varnostnih kopij znašal 3330 dolarjev, ker bi morali kupiti tračno enoto in ker je treba trezor najeti za najmanj eno leto. V vseh nadaljnjih mesecih (če se omejimo na obdobje enega leta) bi se ta strošek sicer znižal za ceno tračne enote in ceno najema trezorja. Tako bi pri uporabi omenjenega scenarija stroški padli na 340 dolarjev. Kljub temu vidimo, da je izdelava take varnostne kopije še vedno 4,6-krat dražja od izdelave varnostne kopije podatkov v oblaku.

4 SKLEP

Poslovni sistemi lahko uporabljajo zelo različne scenarije za izdelovanje varnostnih kopij. Zato je glede na pridobljene rezultate smiselno, da se ne prenaglijo in ne začnejo takoj mrzlično razmišljati o uporabi oblaka, temveč da najprej ugotovijo, kakšne so njihove performančne zahteve glede hitrosti izdelave varnostnih kopij in kakšni bodo stroški, povezani s tem. Šele nato lahko najdejo t. i. prelomno točko, na podlagi katere se odločijo, ali je za izdelovanje varnostnih kopij bolj smiselno uporabljati klasični način ali oblak.

Poleg same učinkovitosti in stroškov, ki smo jih obravnavali v tem prispevku, pa si morajo poslovni sistemi pri uporabi oblaka za potrebe izdelovanja varnostnih kopij odgovoriti še na več drugih pomembnih vprašanj [7]: Ali lahko zaupajo podatke ponudniku oblačne storitve [8]? Kaj se bo zgodilo s podatki, če ponudnik storitev preneha delovati? Ali je mogoče podatke prenesti "v drug oblak" – k drugemu ponudniku oblačnih storitev? Ali se podatki po prenehanju uporabe zares zavržejo? Ali so podatki v oblaku varni pred krajo? Obstaja torej množica vprašanj, na katera je treba, preden bo uporaba oblakov zares zaživela, odgovoriti v okviru nadaljnjih raziskav.

LITERATURA

[1] B. HAYES, CloudComputing, *Communicationsofthe ACM*, Vol. 51, No. 7, pp. 9-11, 2008

[2] A. REED, S. G. BENNET, SilverClouds, Dark Linings: A ConciseGuide to CloudComputing, *Prenticehall*, ISBN-13: 978-0-131-38869-7, 2010

[3] AmazonSimpleStorageService (Amazon S3), http://aws.amazon.com/s3/

[4] AmazonElasticComputeCloud (EC2),http://www.amazon.com/ec2/

[5] G. J. POPEK, R. P. GOLDBERG, Formalrequirementsforvirtualizablethirdgenerationarchitectures, *Communicationsof ACM*, Vol. 17, No. 7, pp. 412–421, 1974

[6] N. STINCHCOMBE, Cloudcomputing in thespotlight, Vol. 6, No. 6, pp. 30–33, 2009

[7] S. VRHOVEC, R. RUPNIK, A model forresistancemanagement in IT projectsandprograms, *Elektrotehniški vestnik*, Članek v recenziji

[8] D. SVANTESSON, R. CLARKE, Privacyandconsumerrisks in cloudcomputing, *ComputerLaw&SecurityReview*, Vol. 26, No. 4, pp. 391–397, 2010

Aljaž Zrnec je diplomiral leta 1999 in magistriral leta 2002 na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Leta 2006 je doktoriral s področja konstruiranja metodologij za razvoj programske opreme. Zaposlen je v Laboratoriju za podatkovne tehnologije kot predavatelj in asistent za področje podatkovnih baz. Na raziskovalnem področju se ukvarja s podatkovnimi bazami in računalništvom v oblaku. Je avtor ali soavtor številnih prispevkov v strokovnih in znanstvenih publikacijah.