Vzpostavitev podatkovne baze iz pogorišča

Valter Miščič

A1 Slovenjia, Ljubljana, Slovenija
valter.miscic@a1si

Vse pogostejše in obsežnejše naravne in tudi drugim katastrofe spremljajo naše življenje v zadnjem obdobju. Obsežni požari, povodnji in potresi uničujejo naša mesta, rakete uničujejo infrastrukturo. Ogrožena so naša življenja, premoženje in vse, kar smo ustvarjali desetletja in kar nam je najvažnejše in najdražje. Če pogledamo na te stvari iz oči naših podjetij, so najpomembnejša stvar prav gotovo njeni podatki. Firma, ki zgubi svoje najpomembnejše podatke, praktično izgubi vse. Firme se morajo na takšne dogodke pripraviti in svoje podatke ustrezno zaščititi. S podvojevanjem računskih centrov vključno z vso strojno in programsko opremo ter podatki se lahko dokaj dobro zaščitimo. Žal, vse firme nimajo tega privilegija. Dodatni računski center seveda stane in pri denarju se največkrat ustavi. Velikokrat pa gre zgolj za nezavedanje ali podcenjevanje te problematike. Vsekakor je dobro, da imamo pripravljen načrt okrevanja, da mu vsi sledimo in da neprestano vadimo postopke okrevanja.

Ključne besede:
restavriranje po katastrofi
rezervni računski center
podatkovne tehnologije
podvojeni sistemi
administracija podatkovnih baz

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-772-0
DOI https://doi.org/10.18690/um.feri.8.2023.22

1 Uvod

Vsem je jasno, da so danes podatki najpomembnejša stvar vsakega podjetja. Podatke čuvamo pred izgubo in zlorabo, skrivamo pred konkurenco. Za večino ljudi se zdi razpoložljivost podatkov samoumevna. Vedno pa obstaja možnost, da podatki niso razpoložljivi ali jih celo izgubimo. Problema se velikokrat zavemo šele ob izpadih informacijskih sistemov. Zgodi se, da so podatki začasno nedosegljivi: pride do okvare strojne opreme, napake v programski opremi ali do kake druge začasne težave, ki nam ne omogoča dostopa do podatkov. Take težave se večinoma rešijo v nekaj urah ali morda dneh. Smo kdaj pomislili, da lahko izgubimo vse, popolnoma vse: pogori nam računski center z vso opremo vred. Zgodi se katastrofa. Kaj bomo naredili v takem primeru. Imamo opremo, čas in znanje, da postavimo vse z ničle? Kaj, če za vedno ostanemo brez vseh podatkov. Podjetje zapremo, ljudi damo na cesto. Na take katastrofalne izpade se moramo pripraviti!

Sam sem administrator podatkovnih baz , zato bom problematiko opisal s stališča administratorja podatkovnih baz.

2 Naloge administratorjev

2.1 Najpomembnejša naloga administratorjev

Za vsako delovno mesto obstaja spisek del in nalog, ki jih mora opravljati. Te naloge so zapisane že ob razpisih za posamezno delovno mesto. Kot administratorju baz podatkov, mi je najpomembnejša naloga izvajanje arhiviranja podatkovnih baz in zmožnost njihovega restavriranja. To ne velja samo za administratorje baz, ampak velja na splošno za vse druge administratorje: sistemske inženirje, administratorje omrežja, aplikacij, itd.. Na vse ostale naloge se lahko pripravljamo več časa, se sproti učimo, dokumentiramo. Ko pa gre za restavriranje, se od nas pričakuje, da bomo hitri in učinkoviti. V takih trenutkih velja nekakšna napetost, živčnost in negotovost ne samo administratorjev, ampak tudi vseh, ki so od podatkov odvisni. Zato je pomembno, da imajo administratorji pogoje in izkušnje za uspešno restavriranje sistemov, za katere skrbijo.

2.2 Revizija dela administratorjev

Zaradi pomembnosti informatike se delo tistih, ki skrbijo zanjo, nenehno revidira. Do njih prihajajo najrazličnejši revizorji in ugotavljajo, če administratorji opravljajo svoje delo. Zanimivo je, da tudi revizije, ki se nanašajo na popolnoma specifične zadeve, vedno preverijo tudi delo informatikov. Zavedajo se, da predstavlja informatika veliko ranljivost in tveganje za podjetje. Med drugim se njihova vprašanja vedno dotaknejo tudi področja arhiviranja in restavriranja podatkovnih baz in vseh ostalih komponent informacijskega sistema. Vprašanja zgledajo nekako takole:

- Izvajate arhiviranje sistemov/podatkovnih baz/aplikacij?
- Beležite njihovo izvajanje?
- Izvajate monitoring nad arhiviranjem?
- Izvajate občasna restavriranja?

Vsak izmed administratorjev za svoje področje odgovori pritrdilno na vsa vprašanja. Večinoma je to tudi res. Vendar vsak administrator tudi pove, kakšni so predpogoji, da bo svoj del uspešno restavriral. Na primer, če hočem restavrirati podatkovno bazo, mora najprej sistemski inženir postaviti ali restavrirati strežnik, na katerega bom bazo restavriral. Administrator aplikacije pove, da mora za delovanje aplikacije najprej imeti dostop do restavrirane aplikacije. To je vsakomur jasno, vendar pa prav v teh odvisnostih včasih prihaja to zapletov. Računamo drug na drugega, nismo pa se nikoli popolnoma dogovorili, kaj kdo od koga vse pričakuje. Gre za pomembne malenkosti, ki se morda odkrijejo šele v primeru restavriranja.

Vsakršne revizije so koristne, čeprav jih informatiki ne maramo, ker lahko pokažejo na določene neustreznosti ali pa nas vsaj malo predramijo iz svoje samovšečnosti.

3 Dogodki s katastrofalnimi posledicami

3.1 Kakšne katastrofe se nam lahko zgodijo?

V zadnjem času smo na lokalni in svetovni ravni doživeli kar nekaj dogodkov, ki lahko vodijo v popolno katastrofo. Če jih naštejem samo nekaj:

- napad z raketami,
- poplave večjih razsežnosti,
- požari večjih razsežnosti,
- uničujoči potresi.

Na osebni ravni ti dogodki jemljejo naša življenja, našo imovino, uničujejo infrastrukturo. Za posameznika je to najbolj pretresljivo. Poleg tega lahko taki dogodki uničujejo tudi širšo infrastrukturo, cela mesta, tovarne. Za podjetja predstavlja najhujšo izgubo uničenje njenih dragocenih podatkov. Tega ne povrne nobena zavarovalnica in tega se ne da nikjer kupiti. Ne gre samo za izgubo podatkov. Podatke morda celo redno arhiviramo in bi jih lahko restavrirali. Pogubno je že, če ostanemo brez računskega centra.

Za postavitev novega centra, ki bi deloval v zadovoljivi funkcionalnosti bi potrebovali naslednje:

- pridobitev novega ustreznega prostora,
- nabava strojne opreme,
- vzpostavitev omrežja,
- priprava strežnikov,
- namestitev programske opreme in aplikacij,
- restavriranje baz,
- konfiguriranje aplikacij, baz, operacijskih sistemov.

Nepredstavljivo je, da bi nam pri današnjih kompleksnih arhitekturah to uspelo. Firme, ki se tega zavedajo, so na take dogodke bolje ali slabše pripravljene. Nekatere pa se ali sploh ne zavedajo ali pa zgolj niso pripravljene. Upam, da niste med njimi.

3.2 Kako se zaščititi pred takimi dogodki

Takšnih katastrofalnih dogodkov ne moremo predvideti in se jim ne moremo izogniti. Nanje pa smo lahko bolje ali slabše pripravljeni. Ko govorimo o uničenju celotnega računalniškega centra, imamo na razpolago različne scenarije okrevanja.

Najpogostejši in hkrati najslabši primer je, da se zanašamo zgolj na naše varnostne kopije. V tem primeru predvidevamo, da je verjetnost katastrofe majhna in bomo vzpostavili nov center z novo opremo in restavriranjem vseh komponent iz obstoječih varnostnih kopij. Vendar takšna rešitev sploh ni enostavna. Najprej je treba dobiti ustrezen prostor in nabaviti celotno novo opremo. Nabava nove opreme lahko traja mesece in tudi časovna stiska nam ne omogoča pogajanj za boljše cene.

Današnji informacijski sistemi so tako kompleksni, da je uresničitev te variante nepredstavljiva. Zamislimo si sistem s stotinami aplikacij in njihovimi povezavami do servisov, ki so povsod po svetu. Praktično nemogoče je, da bi firma to vzpostavila in preživela.

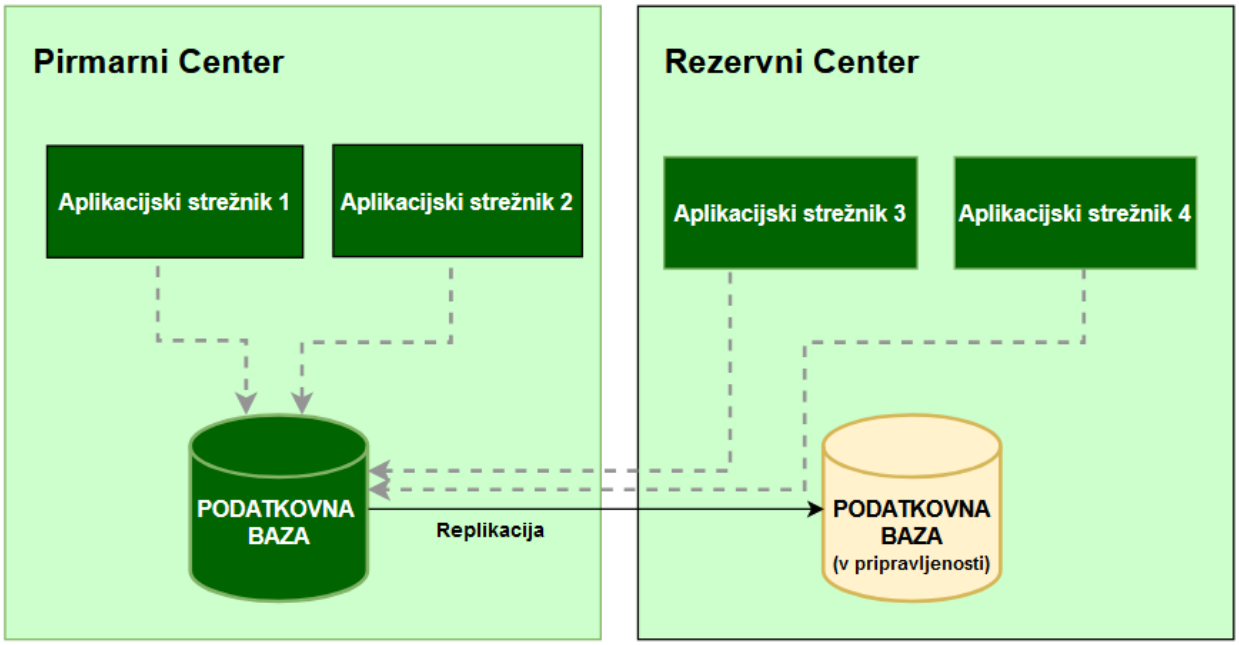
Drugi in tudi boljši pristop je, da poleg računskega centra (recimo mu primarni center) vzdržujemo še en t. i. rezervni center. Rezervni center mora biti opremljen s podobno opremo kot primarni center in živeti mora v sozvočju z njim. Imeti rezervni center z nekaj stare opreme nam ne bo dosti koristil. Morda smo pred leti res imeli takšne rezervne centre (zgolj zaradi boljšega občutka), vendar se je v zadnjem času z osveščanjem to drastično spremenilo. Rezervni centri so postali pravi rezervni centri in tudi v resnici zmorejo prenesti vse breme primarnih centov.

Pri rezervnih centrih je pomembna sama lokacija. Biti mora dovolj oddaljena od primarnega centa, da je ne bi zajela ista katastrofa kot primarni center. Sam prostor mora biti primeren za računski center. Biti mora ustrezno klimatiziran, na razpolago mora biti zadostno električno napajanje in podatkovno omrežje. Računalniško omrežje in požarno zidovje mora biti samostojno in neodvisno od primarnega centra. Strojna oprema mora biti zadostna in kompatibilna z opremo v primarnem centru.

Ko imamo strojno opremo v rezervnem centru postavljeno, je treba urediti še podatkovne baze in aplikacije. Rezervni center naj ne predstavlja samo prostor in opremo, ki čaka nekje v rezervi. Podatkovne baze naj bodo postavljene tako, da se na rezervni lokaciji vzdržujejo baze v pripravljenosti in jih kadarkoli lahko preklopimo iz primarne lokacije na rezervno in nazaj. Obstaja več načinov postavitev baz v pripravljenosti. Izberemo način, ki nam najbolj ustreza in nas zadovoljuje. Nekatere konfiguracije zahtevajo še dodatne licence, kar lahko dodatno podraži našo rešitev. Rezervni center predstavlja za podjetje praktično dvojni strošek za informatiko, zato ga gre izkoristiti.

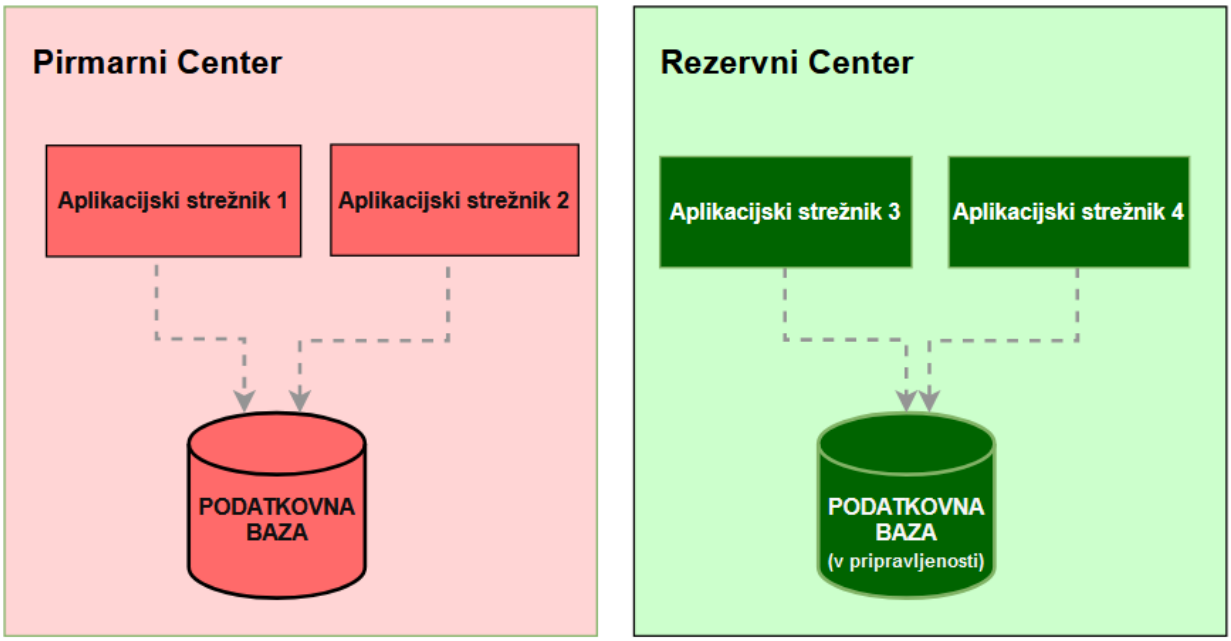
To je najlažje narediti z aplikacijskimi strežniki. Aplikacija, ki uporablja več aplikacijskih strežnikov, naj ima le te porazdeljene med obema centroma. Ob morebitnem izpadu primarnega centra, bodo aplikacijski strežniki na rezervni lokaciji že delovali le preklopili se bodo na bazo na rezervni lokaciji. Ker so aplikacijski strežniki na obeh lokacijah ves čas aktivni, se nam tudi ne more zgoditi, da bi ob nadgradnjah aplikacije pozabili na strežnike v pripravljenosti na rezervni lokaciji in bi ob morebitnem preklopu aplikacije le ta ne delovala pravilno.

Slika 1 prikazuje dobro postavljene aplikacije: oba centra sta aktivna, aplikacija deluje na dveh strežnikih na primarni lokaciji in na dveh strežnikih na rezervni lokaciji. Baza je aktivna na primarni strani, vse spremembe pa se sproti replicirajo na bazo v pripravljenosti na rezervni lokaciji.



Slika 1: Dobra postavitev podatkovne baze in aplikacijskih strežnikov.

Aplikacije morajo biti konfigurirane tako, da znajo delati s podatkovnimi bazami na primarni ali rezervni lokaciji brez intervencije administratorjev. Če bi morali vse aplikacije ročno preklapljati in konfigurirati v času aktiviranja rezervnega centra, bi nam to vzelo preveč časa. Aktivirati bi morali veliko ljudi, da bi vsak opravil svoje delo. V primeru izpada primarne lokacije se ali ročno ali samodejno aktivira podatkovna baza v pripravljenosti na rezervni lokaciji. Preživeli aplikacijski strežniki se namesto na primarno bazo povežejo z bazo, ki je bila do sedaj baza v pripravljenosti in je postala primarna baza.



Slika 2: Ob izgubi primarnega centra, prevzame glavno vlogo rezervni center.

Takšna arhitektura nam zagotavlja boljši spanec, s seboj pa prinaša tudi nekaj stranskih učinkov:

- stroški za računski center, opremo in licence se povečajo,
- več je dela,
- potrebujemo dodatni kader ali pa bolj obremeniti obstoječega.

Odločitev je vedno v naših rokah!

3.3 Kaj pa če nimamo vsega optimalno postavljenega

Morda imamo dobro postavljen rezervni center, vendar nimamo popolnoma vsega podvojenega. Razlogi za to so različni:

- Morda se nam zdi nepotrebno kompliciratiz razvojnimi in testnimi okolji.
- Nekatere produkcijske aplikacije niso nujno potrebne za preživetje podjetja.
- Stare aplikacija ne omogočajo takšne arhitekture.
- Strošek podvojevanja aplikacijskih strežnikov za nekatere aplikacije je prevelik.
- Prepletenost in kompleksnost aplikacij je že sama po sebi nevzdržna in podvojevanje takega sistema je praktično nemogoče.

V takem primeru moramo stvari postaviti od začetka iz obstoječih arhivov. Seveda ni nujno, da nam bo to sploh uspelo. Predstavljajmo si aplikacijo, ki nam jo je v okviru pogodbe namestil prodajalec sam. Potreboval je nekaj mesecev, da je postavil strežnike, podatkovne baze, aplikacijo in poskrbel za vse potrebne konfiguracije in spravil aplikacijo v pogon. Zdaj naj bi sistemski inženirji, administratorji baz in aplikacij to postavili v enem dnevu. To bo zelo težko izvedljivo. Dandanes imajo podjetja na desetine takšnih aplikacij. Nihče jih ne obvlada v popolnosti. Dokumentacija je morda slaba ali je sploh ni. Morda celo podpore za nekatere aplikacije nimamo več, ker so firme ta produkt opustile ali so celo propadle.

Ne glede na vse, bi moralo imeti vsako podjetje vsaj načrt, kako okrevati po katastrofalnem dogodku. Ta načrt mora priti v zavest vseh vpletenih. Morajo ga upoštevati pri svojem delu in tudi izvajati občasne požarne vaje. Vsaka vaja pokaže določene pomanjkljivosti, ki jih je treba neprestano odpravljati.

Postavitev z ničle je zahtevna. Prvi korak je, da uredimo omrežje:

- pridobiti je potrebno IP naslove,
- urediti DNS in
- postaviti pravila na požarnem zidovju.

Tu se že lahko zatakne. Zamislimo si, da je primarni center uničen. Kje imamo dokumentacijo o propustih na požarnem zidovju? Jo sploh imamo? Jo imamo morda na kakšnem strežniku na uničeni primarni lokaciji? Odpiranje požarnega zidovja zna biti precej dolgotrajno, tudi če dokumentacijo imamo. V razvejanem okolju je morda treba urediti požarno zidovje tudi na drugih lokacijah - drugih firmah in celo državah, kar vse vpliva na čas postavitve novega okolja.

Tudi če na rezervni lokaciji nimamo že pripravljenih rezervnih strežnikov, je dobro imeti vsaj pripravljene rezervne IP naslove z ustreznimi propustnostmi na požarnem zidovju. To nam prihrani precej časa pri restavriranju strežnikov tako aplikacijskih kot baznih.

To je osnova, preden sploh začnemo z restavriranjem strežnikov in podatkovnih baz. Zdaj nastopijo sistemski inženirji, ki morajo postaviti aplikacijske in bazne strežnike. Dandanes strežniki niso več fizični stroji, ampak večinoma uporabljamo virtualizacijske mehanizme, kar nam precej poenostavi delo, vendar je tu prvo vprašanje,

ki se postavi: koliko procesorjev je treba dodeliti strežniku, koliko pomnilnika, koliko diskovnega prostora? Pri malem številu strežnikov morda to celo poznamo, imamo dober občutek, vendar pri stotinah strežnikov je to nemogoče vedeti na pamet. Če dodelimo preveč resursov, jih bo morda zmanjkalo za druge, če jih dodelimo premalo, pa se morda aplikacije in baze ne bodo pobrale. Ker primarnega centra nimamo več, tam teh informacij ne moremo preveriti. Dobro je vse te podatke sproti pridobivati in jih hraniti nekje na varni lokaciji.

Sledi restavriranje naših strežnikov, podatkovnih baz in aplikacij. Tu pa najprej pade vprašanje: kje imamo arhive? Jih imamo zgolj v primarnem centru? V tem primeru bomo pri katastrofalnem dogodku izgubili tudi te. Vedno jih moramo imeti še na eni lokaciji. Najbolje je, da jih imamo tako na primarni kot rezervni lokaciji. Danes se za arhiviranje uporablja specializirano diskovno polje, ki omogoča samodejno preslikavo arhivov iz primarne lokacije na rezervno. V takem primeru postane restavriranje enostavnejše. Pri restavriranju baz je pomembno še, kje imamo katalog arhivov. Če smo ostali brez njega, bomo potrebovali malo več znanja in spretnosti, da bazo restavriramo. Zelo pomembno je neprestano utrjevanje spretnosti restavriranja. Večje firme imajo zaposleno večje število administratorjev baz in se znotraj ekipe oblikuje skupina, ki je zadolžena zgolj za arhiviranje in restavriranje baz. V manjših firmah je administratorjev manj in morajo početi vse, kar je povezano z administracijo baz, vendar kot sem že prej zapisal, vsak administrator mora vedeti, da je restavriranje baz njegova najpomembnejša zadolžitev, ki jo mora neprestano utrjevati.

Ko sta podatkovna baza in aplikacija restavrirani, bodo morda potrebne še nastavitve določenih konfiguracij.

Največkrat se izkaže, da je potrebno postoriti še marsikaj. Aplikacija morda sploh ne deluje ali pa deluje le deloma.

Pri restavriranju ne gre vedno vse gladko. Včasih je treba postopek večkrat ponoviti. Pri tem se nabere nekaj nesnage. To je treba za seboj takoj počistiti. Urediti je treba dokumentacijo in ne smemo pozabiti, da je treba novo okolje takoj spet arhivirati.

3.4 Biti popolnoma nepripravljen

Niti pomisliti si ne upam, da v svoji organizaciji ne bi imel nobene možnosti takojšnjega preklopa baz oz. aplikacij na rezervni center. Dogodek, ki bi uničil primarno informacijsko infrastrukturo, bi bil poguben za celotno podjetje. Tega nikomur ne priporočam.

Danes obstajajo možnosti oblačnih storitev. Morda si umislimo rezervni center v oblaku vsaj za najpomembnejše informacijske sisteme, da ne ostanemo popolnoma brez vsega. Oblačne storitve niso vedno prava možnost - morda zaradi zakonske regulative, morda ker se bojimo za svoje podatke, da ne bi bili izpostavljeni zlorabam.

4 Zaključek

Verjetno si nismo nikoli zamišljali, da bi zaradi naravne katastrofe ali teroristične akcije ostali brez celotne informatike v podjetju. Vendar možnosti katastrofe obstajajo - o tem se lahko prepričamo skoraj vsak dan.

Pomembno je, da:

- se tega zavedamo,
- imamo pripravljeno okolje, da bomo imeli v primeru katastrofe kar najmanj dela za povrnite,
- neprestano utrjujemo svoje znanje,
- težimo k posodabljanju aplikacij in ukinjanju arhaičnih aplikacij brez podpore,
- poenostavljamo svoje sisteme in
- izvajamo ustrezne požarne vaje, da bomo pripravljeni, če pride do katastrofe.