UNIVERZITET CRNE GORE
ELEKTROTEHNIČKI FAKULTET PODGORICA

Vladana Mrdak

Predlog heterogenog rješenja za kreiranje rezervnih kopija podataka na Linux platformama

- magistarski rad -

Mentor:
Prof. dr Božo Krstajić

Podgorica, maj 2016

PODACI I INFORMACIJE O MAGISTRANDU

Ime i prezime:	**Vladana Mrdak**
Datum i mjesto rođenja:	**07.07.1982.**
Naziv završenog osnovnog studijskog programa i godina završetka studija:	**Elektrotehnički fakultet, odsjek za Elektroniku, telekomunikacije i računare, 2006.**

INFORMACIJE O MAGISTARSKOM RADU

Naziv postdiplomskog studija:	**Elektronika, Telekominikacije i Računari**
Naslov rada:	**Predlog heterogenog rješenja za kreiranje rezervnih kopija podataka na Linux platformama**
Fakultet/Akademija na kojem je rad odbranjen:	**Elektrotehnički fakultet, Podgorica**

UDK, OCJENA I ODBRANA MAGISTARSKOG RADA

Datum prijave magistarskog rada:	**06.04.2015.**
Datum sjednice Vijeća na kojoj je prihvaćena tema:	**23.09.2015.**
Komisija za ocjenu teme i podobnosti magistranda:	**Doc. Dr Milutin Radonjic** **Prof. dr Bozo Krstajic** **Prof. dr Budimir Lutovac**
Mentor:	**Prof. dr Bozo Krstajic**
Komisija za ocjenu rada:	**Doc. Dr Milutin Radonjic** **Prof. dr Bozo Krstajic** **Prof. dr Budimir Lutovac**
Komisija za odbranu rada:	**Doc. dr Milutin Radonjic** **Prof. dr Bozo Krstajic** **Prof. dr Budimir Lutovac**
Lektor:	
Datum odbrane:	**25.5.2016**
Datum promocije:	**_____**

Rezime

Projektovanje adekvatnog rješenja za kreiranje rezervnih kopija podataka je složen zadatak koji utiče na pouzdano poslovanje svih kompanija sa razvijenim informacionim sistemom. Standardi daju opšte smjernice, dok najbolje prakse, preporuke i iskustva stručnjaka iz oblasti informacionih tehnologija daju važan aspekt čitavoj problematici. Različita rješenja mogu zadovoljavati postavljene uslove i standarde i biti jednako optimalna. Problemi sa kojima se suočava proces projektovanja rješenja za kreiranje rezervnih kopija podataka su mnogobrojni. Tehnologija svakodnevno napreduje dok je proces implementiranja novih ili ažuriranja implementiranih rješenja dugotrajan i materijalno zahtjevan. Trendovi se mijenjaju velikom brzinom, a može se desiti da se nakon izbora i implementacije rješenja izabrana tehnologija pokaže kao neadekvatna zbog povećanja cijene održavanja ili nedovoljne pouzdanosti.

Budući da raznorodni podaci zahtijevaju različit pristup pri izradi strategije za kreiranje rezervnih kopija podataka u zavisnosti od svojih funkcija i osobina, u radu će biti predloženo i analizirano heterogeno rješenje za backup i recovery na Linux operativnim sistemima. Rješenje će se zasnivati na D2D2T mehanizmu koji podrazumjeva kreiranje primarnog backup materijala na disku, a zatim kreiranje sekundarnog backup materijala na trakama. Biće razmatrana i opisana odgovarajuća SAN infrastruktura sa akcentom na uređaj za skladištenje podataka, odnosno *storage* uređaj. Pristupiće se implementaciji rješenja na više nivoa tretirajući različite tipove podataka na Linux operativnom sistemu u skladu sa definisanom backup politikom i strategijom. Backup rješenje biće realizovano kroz programiranje u *bash* i *korn shellu* čija je osnovna prednost inkorporiranje odgovarajućih alata za backup i automatizacija. Predloženo rješenje će se sastojati iz dva odvojena procesa u zavisnosti od kategorije podataka čije će se rezervne kopije čuvati.

Predlog rješenja za kreiranje rezervnih kopija standardnih podataka biće zasnovan na analizi postojećih *Open Source* alata za kreiranje rezervnih kopija dostupnih na Linux operativnim sistemima. Topologija rješenja će biti zasnovana na LAN mreži a u cilju odabira adekvatnog alata, izvršiće se opsežno testiranje mreže. Rad će takođe obuhvatati analizu rješenja za backup Oracle baze podataka kreiranjem potpunog snimka, odnosno klon (*clone*) kopije baze.

Predloženo heterogeno rješenje će biti analizirano i testirano tako da zadovoljava uslove predviđene backup politikom kompanije i usvojenom strategijom. Biće izvršena analiza koja će pokazati prednosti i mane predloženog rješenja.

Magistarski rad, pored rezimea i literature sadrži sledeće cjeline: kreiranje rezervnih kopija podataka i njihov oporavak (*backup* i *recovery*), strategije kreiranja rezervnih kopija podataka, tehnologije na kojima se zasnivaju backup i recovery koncepti, predlog heterogenog rješenja za backup i recovery podataka na Linux sistemima, implementacija heterogenog rješenja za backup i recovery podataka na Linux sistemima, zaključak i lista urađenih programa u *bash i korn shell*-u, kao konkretna implementacija predloženih strategija u formi priloga.

Abstract

Designing real data backup and recovery solution is a complex process that influences business operations of companies with any information system. Basic guidelines are determined by standards, but best practices, recommendations and experts' experience shape the whole aspect of backup and recovery issue. Different solutions can meet conditions and standards defined and prove to be equally optimal. There are numerous issues facing the process of designing backup and recovery solution. Technology advances rapidly as the process of implementing new or updating existent solutions remains slow and expensive. Trends change and old solutions are quickly replaced with new ones on the market. Some solutions may prove inadequate after its implementation due to expensive support or lack of reliability.

Considering that different data categories require different approach while constructing backup and recovery strategy, this thesis will propose and analyze heterogeneous backup and recovery solution on Linux operating systems. Solution will be based on D2D2T mechanism that includes saving primary backup on disk and secondary backup on tape. Adequate SAN infrastructure will be described focusing on storage device. Solution will be introduced through multiple levels handling different data categories on Linux operating system according to predefined backup policy and strategy. Backup solution will be performed through bash and korn shell programming whose basic advantage is incorporating specific backup tools and automatization. Proposed solution will have two separate processes depending on data category designated for backup.

Backup solution proposal of *standard* data will be based on analysis of Open Source backup tools available on Linux operating systems. LAN based topology will be used and extensive network testing will be performed to select proper backup tool. This thesis will also describe backup solution of *Oracle database* based on snapshot/clone session.

Proposed heterogeneous solution will be examined and tested to confirm conditions determined by company's backup policy and default strategy. Deep analysis will show advantages and disadvantages of proposed solution.

Master's thesis, beside Abstract and Literature contains following: Backup and recovery definitions and trends, Backup and recovery strategies, Backup and recovery technologies, Heterogeneous backup and recovery solution proposal on Linux OS, Heterogeneous backup and recovery solution implementation on Linux OS, Conclusion and Appendixes with list of performed shell programs.

Sadržaj

1. Kreiranje rezervnih kopija podataka i njihov oporavak

Backup je engleska riječ koja u bukvalnom prevodu znači podrška, rezerva, kopija. U terminologiji informacionih i komunikacionih tehnologija (*ICT*) *backup* podataka se odnosi na proces kopiranja i smiještanja podataka na odvojeni pouzdani medijum koji se može upotrijebiti za oporavak originalnih podataka u slučaju njihovog gubitka ili oštećenja. Backup je opšte korišćen izraz za postojanje rezervne kopije jednog ili više fajlova ili slike cijelog sistema kreirane kao alternativa u slučaju gubitka ili korupcije originalnih fajlova.

Backup predstavlja jedan od osnovnih termina u informacionim tehnologijama. Njegov značaj se ne prepoznaje na ličnom nivou dok nije kasno i dok se ne izgube godine fotografija, e-mail arhiva, poslovnih dokumenata... Međutim, na poslovnom nivou kreiranje rezervnih kopija podataka je neophodnost koja podržava i održava poslovanje pouzdanim. Kompanije kojima je sigurnost podataka i ispravan i kontinuiran rad sistema presudan za poslovanje, ulažu velike resurse u očuvanje svojih podataka i proces kreiranja rezervnih kopija podataka. Sredstva treba opravdati sa poslovnog stanovišta budući da zaštita podataka ne generiše profit već stvara troškove [1].

Osnovna svrha backupa je oporaviti podatke nakon njihovog gubitka. Gubitak podataka i nefunkcionisanje sistema određeni vremenski period može dovesti do prekida rada servisa i gubitka novca. Druga svrha backupa je povraćaj podataka iz preciziranog trenutka u vremenu koje je u nekim sferama poslovanja dio zakonske regulative. Zakonske regulative definišu vremenski period u kom je potrebno čuvati određene podatke.

U ICT terminologiji, *restore* i *recovery* označavaju proces povratka fajlova sa backup medijuma na njihovu originalnu lokaciju. *Recovery* se uglavnom odnosi na oporavak jednog ili više fajlova, dok je *restore* proces oporavka kompletnog sistema iz rezervne kopije cijelog sistema (*full system backup*).

Uglavnom, backup i recovery termini se odnose na razne strategije i procedure koje štite podatke od gubitka i definišu pravilno rekonstruisanje tih podataka u slučaju gubitka. To su usko vezani procesi koji se ne mogu posmatrati odvojeno. Pravilno planiranje oporavka podataka je uslovljeno pravilnim planiranjem strategije za backup. Backup proces nema svrhu ukoliko nije moguće odraditi *restore/recovery* proces i izvući podatke.

1.1. Poslovni inicijatori u backup i recovery trendovima

Kompanijama su potrebni jasni obrasci kako da vrednuju svoje investicije u rješenja za backup i recovery podataka. Pitanja koja se često postavljaju su:

- Koji su to inicijatori u poslovnom smislu koji podstiču kompanije da implementiraju rješenja za backup i recovery?
- Nakon implementacije, koje oblasti su imale najviše benefita sa operacione i ekonomske tačke gledišta?

Što je bolje rješenje za backup i recovery podataka, to su sigurniji podaci i postiže se bolja efikasnost u smislu ljudstva, procesa i opreme. Po istraživanjima koje je sprovela jedna od

vodećih kompanija u polju informacionih tehnologija (Symantec) [2] u kompanijama raznih veličina i profila, sledeći kriterijumi su bili presudni za planiranje i nabavku rješenja za backup i recovery podataka, a pokazali su najveću poslovnu vrijednost:

- **Porast količine podataka i upravljanje njima –** Jedan od najznačajnijih trendova u svijetu je porast obima podataka predviđenih za čuvanje, budući da njegova količina na godišnjem nivou u većini slučajeva (90% kompanija) raste od 10% do 60%. Mnogi su razlozi za porastom količine podataka kojima se raspolaže: papirni dokumenti se pretvaraju u elektronske, a servisi postaju povezani na Internet. Ukoliko je kompanija u mogućnosti da podrži rast količine podataka sa istim ljudstvom i infrastrukturom, rješenje za backup i recovery je skalabilno [2].
- **Eliminisanje redudantnih podataka –** Tehnikama deduplikacije se uveliko smanjuje količina podataka potrebna za čuvanje, čime se štedi prostor na storage uređajima i uređajima predviđenim za backup i recovery podataka [2].
- **Unapređenje uspješnosti backup operacija –** Neuspjele backup operacije opterećuju infrastrukturu i troše vrijeme za administraciju. Zbog toga je važno da procenat uspješnosti backup operacija bude što veći. Veće kompanije su zadovoljnije uspješnošću operacija koje kreiraju rezervne kopije podataka, dok više od trećine ispitanih kompanija imaju uspješnost oko 70%, tako da na ovom polju ima mjesta za napredak [2].
- **Vremenski prozor za backup –** Problem se javlja prilikom backupa velike količine podataka u malom vremenskom intervalu koji je definisan vremenskim prozorom. Odgovarajućim izborom rješenja za backup i recovery koja implementiraju nove tehnike (npr. deduplikacija, kompresija, itd.) i automatizuju procedure, ovaj prozor se može smanjiti povećavajući produktivnost i snižavajući cijenu rada, a istovremeno štedeći resurse.
- **Efikasnost koje pruža jedinstveno rješenje** – Standardizovanje opreme predviđene za backup smanjuje troškove predviđene za osposobljavanje ljudstva, konsoliduje i smanjuje troškove za licence, pojednostavljuje nadgledanje operacija i obezbjeđuje veću infrastrukturnu skalabilnost.

1.2. Tehnološki inicijatori u backup i recovery trendovima

Promjene u poslovnim strategijama značajno utiču na način na koji se kompanije odnose prema backup i recovery postupku kao i na način na koji upravljaju podacima i informacijama u svom posjedu. Tendencije i trendovi koji se mogu sagledati iz poslovne i iz perspektive infrastrukture informacionih tehnologija (IT) uključuju [3]:

- **IT kao servis** – Rukovodioci teže da krajnji rezultat bude IT kao servis, gdje IT obezbjeđuje najveću poslovnu vrijednost po najnižoj cijeni. Pomoću visoko automatizovane infrastrukture sa minimumom održavanja, IT se može usredsrediti na inovacije koje povećavaju profit, poboljšavaju korisničko iskustvo i minimizuju poslovne i pravne rizike. Na ovaj način svaki servis je u potpunosti definisan svojim komponentama, resursima i kvalitetom isporuke. Poslovne jedinice mogu odabrati i dobiti resurse kroz standardizovane, automatske kataloge ili na zahtjev značajno skraćujući vrijeme isporuke. Backup i recovery usluge su uključene u servisni katalog i predstavljene u kontekstu parametara važnih za oporavak podataka [3].

- **Big data** – je termin koji opisuje eksponencijalni rast i dostupnost velike količine struktuiranih i nestruktuiranih podataka. Tradicionalne IT kompanije treba da primijene isti nivo pouzdanosti, zaštite, čuvanja i dostupnosti „velikih podataka“ (*big data*) kao što su bile u mogućnosti da upravljaju tradicionalnim obimom posla. To se postiže primjenom odgovarajućih politika na različite tipove podataka u backup i recovery strategijama [3].
- **Konvergentna infrastruktura** – Danas se često sistemi integrišu na licu mjesta. Konvergencija nekada odvojenih tehnoloških komponenti pomaže u nabavci, razvoju i održavanju sistema, a integrisanje se vrši u operacije postojećeg datacentra. To uključuje sisteme za backup i recovery, oporavak od nesreće i arhiviranje [3].
- **Računarstvo u oblaku** (*Cloud computing*) – je paradigma koja se odnosi na sveprisutni, pogodni pristup mreži na zahtjev dijeljenim računarskim resursima kao što su mreže, serveri, uređaji za skladištenje podataka, aplikacije i servisi, a koji se mogu brzo pripremiti i osposobiti za produkcionu upotrebu. [4]. Oblak se može odnositi na privatne oblake unutar kompanija kao i na javne, odnosno „hibridne“ oblake koji kombinuju privatne i javne računarske resurse. Ipak, u svakom obliku oblak mora osigurati bezbjednost, backup i recovery i upravljanje informacijama tako da zadovolji poslovne zahtjeve kao i operacione ciljeve u smislu troškova.
- **Konsolidacija infrastrukture** – Ekonomski faktori, rast kompanije i ograničenja u postojećim datacentrima (npr. napajanje, hlađenje, prostor) su podstakli inicijative vezane za konsolidaciju infrastrukture. Virtuelizacija je aktuelna tehnika kojom se povećava efikasnost, smanjuje broj uređaja i omogućava mobilnost. Ipak, kako virtuelne sredine rastu, zaštita virtuelnih mašina postaje glavni problem. Postojeće okoline za backup mogu otežati proces virtuelizacije i ograničiti njene prednosti [3].
- **Društveni podaci i mobilnost** – Novi izazovi u informacionim tehnologijama se odnose na zaštitu, arhiviranje i analizu društvenih podataka. Dozvoljava se pristup važnim poslovnim aplikacijama i podacima različitim i novim korisničkim uređajima u radnoj sredini, uglavnom pametnim telefonima i tabletima. Fenomen BYOD („*Bring your own device*“ – Ponesi svoj uređaj) nameće potrebu kompanijama da obezbijede siguran pristup korporativnim podacima kao i da kontrolišu korisničke akcije sa novih uređaja u korporativnoj mreži. Backup i recovery igra veliku ulogu u tome kako kompanije efektivno omogućavaju produktivnost zaposlenima dok istovremeno spriječavaju korporativne rizike [3].

1.3. Backup kao vid zaštite podataka

Iako u informacionim tehnologijama ne postoji standardna definicija za “zaštitu podataka” i funkcije koje ona obuhvata, strategije za zaštitu podataka bi trebale razmotriti sledeće oblasti [1]:

- **Sigurnost podataka –** Spriječavanje neautorizovanog pristupa podacima, što može uključivati korišćenje tehnologija kao što je enkripcija kao i sigurnosne tehnologije zasnovane na aplikacijama.
- **Dostupnost podataka –** Podaci u svakom trenutku moraju biti dostupni poslovnim aplikacijama. To uglavnom povlači sa sobom upotrebu rješenja sa visokom dostupnošću (*high-availability*) koja se fokusiraju na eliminisanju

tačaka prekida (*single point of failure*) u putanjama podataka i/ili storage tehnologijama.

- **Backup i recovery podataka –** Obezbjeđivanje rezervne kopije podataka iz određenog trenutka u vremenu kako bi se uništeni podaci oporavili i kako bi se nastavile poslovne operacije.

Ove funkcionalne oblasti nisu nezavisne jedna od druge. Na primjer, backup baze podataka se kreira kako bi zadovoljio zahtjeve postavljene backup i recovery politikom. Međutim, može biti značajno enkriptovati rezervnu kopiju kako bi se zadovoljili zahtjevi za sigurnošću podataka, pogotovo ako se kopija nalazi na prenosnom medijumu za skladištenje podataka koja se iznosi iz datacentra i podložna je neautorizovanom pristupu [1].

U idealnom slučaju vrijednost podataka bi trebalo da odredi nivo zaštite koja je za njih predviđena [5]. Vrijedne podatke bi trebalo čuvati na opremi sa visokim stepenom dostupnosti, dok se manje vrijedni podaci mogu čuvati na jeftinijoj opremi koja je manje otporna na hardverske otkaze. Samim tim vrijednost podataka bi trebala biti porporcionalna ulaganju u odgovarajuću infrastrukturu, a otporna infrastruktura štiti od nepotrebnih oporavaka usljed hardverskih otkaza.

1.4. Politika koja definiše kreiranje rezervnih kopija

Prije izbora i implementacije rješenja za backup i recovery podataka, kompanije treba da usklade backup politiku sa poslovnim zahtjevima. Prilikom kreiranja backup politike treba voditi računa o internacionalnim standardima i zakonskoj regulativi države. Pored toga kompanije kreiraju svoje zahtjeve definišući period čuvanja (*retention*) i zaštite (*protection*) podataka neophodnih za nesmetano funkcionisanje poslovanja. Kako bi se važne informacije sačuvale i oporavile nakon gubitka, treba obezbijediti adekvatne kapacitete u smislu infrastrukture. Backup kopije podataka, softvera i slika sistema treba obezbijediti i testirati u skladu sa dogovorenom backup politikom.

Prema ISO/IEC 27002:2013 standardu [6], prilikom pravljenja backup plana treba uzeti u obzir da:

- treba da postoje tačni i potpuni zapisi backup kopija i odgovarajuće dokumentovane procedure za restore;
- tip i frekvencija backupa treba da odgovaraju poslovnim zahtjevima organizacije, sigurnosnim zahtjevima informacija koje se čuvaju, kao i važnosti informacija kako bi organizacija obezbijedila kontinuiran servis;
- kopije treba čuvati na dovoljno udaljenoj lokaciji kako bi se izbjegao gubitak podataka u slučaju nesreće na glavnoj lokaciji;
- rezervnim kopijama podataka treba obezbijediti odgovarajući nivo fizičke i ekološke zaštite koji odgovaraju standardima primijenjenim na glavnoj lokaciji;
- mediji za backup se moraju redovno testirati kako bi se osigurala njihova ispravnost ukoliko bude potrebe, kombinovano sa procedurama i vremenom neophodnim za oporavak podataka;
- rezervne kopije podataka bi trebalo enkriptovati u slučajevima kad je povjerljivost podataka značajna.

Operacione procedure treba da prate izvršavanje backupa i dokumentuju greške zakazanih akcija kako bi se osigurao kompletan proces prema odgovarajućoj backup politici.

U nastavku su date neke smjernice i najbolje prakse za razvoj efektivnog standardizovanog procesa implementacije rješenja za kreiranje rezervnih kopija podataka u kompanijama koje dopunjuju poznate standarde [6, 15] iz ove oblasti:

- Razviti backup i restore strategiju sa odgovarajućim resursima i osobljem i testirati ih. Dobar plan osigurava brzi i jednostavni oporavak podataka u slučaju gubitka.
- Dati odgovornosti za backup i restore operacije administratoru.
- Napraviti što detaljniju proceduru za oporavak podataka usljed gubitka.
- Čuvati tri kopije backup medijuma. Najmanje jednu kopiju čuvati van datacentra u odgovarajuće kontrolisanoj okolini.
- Periodično vršiti testne restore operacije kako bi se verifikovao ispravni backup proces. Ovakve testne operacije mogu otkriti hardverske probleme koje nije moguće dijagnostikovati prilikom verifikacije backup procesa.
- Osigurati storage uređaj i backup medijum kako bi se onemogućio administratoru drugog sistema oporavak ukradenih podataka.
- Izvršiti backup kompletnog sistema kao priprema za neočekivani otkaz uređaja.

Prije implementacije rješenja za backup i oporavak podataka, ICT organizacije treba pažljivo da definišu svoje ciljeve za sve klase svojih poslovnih podataka i da usklade tehnološku strategiju sa poslovnim zahtjevima. Način na koji se vrši backup za svaki pojedinačni sistem bi trebalo redovno testirati i osigurati tako da budu zadovoljeni standardi za kontinualnost poslovanja [6]. U slučaju vitalnih sistema i servisa, procedure za backup bi trebalo da pokriju sve sistemske informacije, aplikacije i podatke neophodne za oporavak kompletnog sistema u slučaju nesreće. Često treba uzeti u obzir zahtjeve kada period čuvanja bitnih poslovnih informacija treba biti trajan.

1.5. Klasifikacija podataka

Klasifikacija podataka predviđenih za zaštitu i čuvanje je interno definisana procedura u svakoj organizaciji koja definiše različite tipove podataka, a oslanja se na ISO/IEC 27002 standard [6], dok su rokovi čuvanja tih podataka u Crnoj Gori definisani nacionalnim zakonima (Zakon o elektronskim komunikacijama Crne Gore [7]).

Politika koja definiše klase podataka (*Data Protection Class - DPC*) proizilazi iz potrebe za boljim iskorišćenjem prostornih kapaciteta, boljim indeksiranjem i pretraživačkim mogućnostima. Kategorisanje i skladištenje svih podataka može imati veliku cijenu, a javljaju se i skriveni troškovi u vidu backup procesa, arhiviranja i pretraživanja velike količine nestruktuiranih i umnoženih podataka. Postoji nekoliko nivoa na kojima se podaci mogu procijeniti, uključujući finansijski, poslovni, regulatorni, zakonski i lični.

Posljedica klasifikacije podataka je potreba za slojevitom arhitekturom prostora za skladištenje podataka koja će omogućiti različite nivoe sigurnosti za svaki tip skladištenja: primarni, backup, *disaster recovery* i arhiviranje. Slojevita arhitektura je povoljnija, a pristup trenutnim podacima je brz i efikasan, dok su arhivirani i podaci predviđeni za skladištenje pohranjeni na jeftinijim medijumima koji ne moraju biti odmah dostupni *(offline)*. [8].

Vrlo je važno pravilno označiti odgovarajuće klase podataka kako bi se i IT sistemi klasifikovali u zavisnosti od informacije koju čuvaju u neenkriptovanoj formi. Važnost IT

sistema se određuje na osnovu najveće klase koja je predviđena za zaštitu na tom sistemu (tabela 1.1).

Tabela 1.1: *Klasifikacija IT sistema u smislu važnosti i zahtjeva za zaštitom*

Klasa zaštite	**Označavanje je zahtijevano u zavisnosti od klase zaštite**	**Povjerljivost**	**Važnost sistema**	**Dostupnost sistema**
Klasa 0	• Bez oznake	"Otvoreno"	Nevažan	Slaba
Klasa 1	• Može se označiti kao "Interno" ili "Za internu upotrebu" ali nije neophodno	"Interno"	Nevažan	Normalna
Klasa 2, Klasa 3	• Potrebno je jasno označiti "Povjerljivo" na svakoj stranici ili nosiocu informacije • Dokument treba sadržati datum na koji se označavanje odnosi (npr. posljednja korektura)	"Povjerljivo"	Važan	Trenutna
Klasa 3+	• Potrebno je jasno označiti "Strogo povjerljivo" na svakoj stranici ili nosiocu informacije • Dokument treba sadržati datum na koji se označavanje odnosi (npr. posljednja korektura) • Oznaka bi trebala biti vremenski ograničena	"Strogo povjerljivo"	Važan	Trajna

U tabeli u prilogu 1 dat je primjer klasifikacije podataka predviđenih za zaštitu u jednoj ICT organizaciji.

Npr. u Crnoj Gori je zakonom [7] propisano da se na važnim sistemima podaci čuvaju u roku do 2 godine od momenta ostvarenja komunikacije. Tu spadaju podaci koji se odnose na:

- saobraćaj, uključujući glas i internet, pa se samim tim odnosi i na logove (kako korisnika tako i zaposlenih). U ovu kategoriju spadaju i neuspjeli pozivi i njihovi logovi (ako su generisani),
- lokacije,
- identifikovanje komunikacione opreme korisnika (IMSI, IMEI, identifikacija ćelije...).

Takođe shodno zakonu [7] podaci o saobraćaju korisnika, obrađeni i uskladišteni treba da budu izbrisani ili napravljeni anonimnim nakon isteka roka od 5 godina. Sa druge strane, politika kompanija je da se svi podaci o zaposlenim čiji je vlasnik kadrovska služba (lični dosijei zaposlenih) čuvaju trajno.

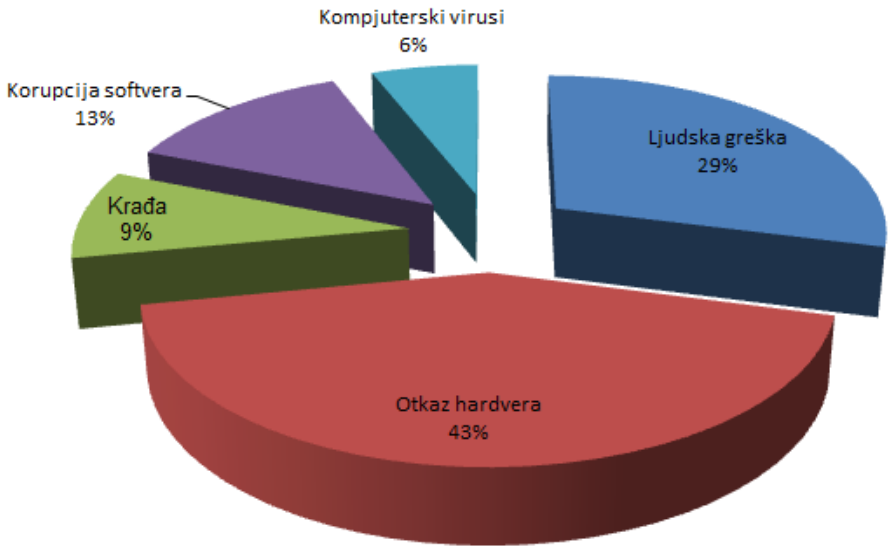
1.6. Uzroci za gubitak podataka

Postoji mnogo načina kako se podaci mogu izgubiti. Kao i svi elektronski uređaji, iako su hard diskovi predviđeni da traju određeno vrijeme, nisu imuni na probleme. Budući da uglavnom nisu „*solid state*" (uređaji bez pokretnih djelova), hard diskovi zavise od pokretnih djelova kako bi pristupili podacima. Pokretni djelovi uređaja se lako mogu oštetiti tako da podaci postanu nedostupni. Pored toga, korupcija softvera takođe može oštetiti fajlove. Strukture direktorijuma se mogu oštetiti uzrokujući nestanak kompletnih foldera. Fajlovi se mogu slučajno obrisati ili ih virusi mogu oštetiti. Konflikti programskih instalacija takođe mogu onemogućiti pristup aplikacijama ili fajlovima [9].

Uzroci za gubitak podataka se ipak mogu podijeliti u nekoliko kategorija [10]:

- Ljudska greška – brisanje programa ili fajlova greškom, greške u administriranju bazom;
- Kriminalne radnje uključujući krađu, industrijsku špijunažu, hakovanje;
- Prirodni, slučajni uzroci – uključujući nestanak struje, hardverski otkaz, iznenadna havarija softvera, softverski bagovi, virusi;
- Prirodne katastrofe kao što su požari, zemljotresi, poplave, itd...

Na slici 1.1 su u procentima prikazani uzroci za gubitak podataka u SAD, a proizašli su iz dva kombinovana izvora: osiguravajućih društava koja obeštećuju u slučaju gubitka podataka i istraživanja koje sprovodi kompanija koja se bavi oporavkom podataka [11].



Slika 1.1: *Uzroci za gubitak podataka [11]*

Frekvencija gubitka podataka i posljedice se mogu ublažiti preduzimanjem odgovarajućih mjera predostrožnosti. Različiti tipovi gubitka podataka zahtijevaju i različite mjere. Npr. redudantna napajanja i redudantni agregati štite samo od nestanka struje. Fajlsistemi sa hronološkim zapisom operacija koje procesuiraju podatke (*journaling file system*) i RAID štite samo od određenih tipova softverskih i hardverskih otkaza. Iako ne štite od korisničkih grešaka ili sistemskih otkaza, stalni backup-i podataka su vrlo važan resurs prilikom oporavka podataka. U zavisnosti od načina na koji su se izgubili ili oštetili podaci, može zavisiti i način njihovog oporavka. Bez odgovarajuće backup strategije, oporavak bi zahtijevao reinstalaciju programa i regenerisanje podataka, što je sa poslovnog stanovišta neprihvatljivo.

2. Strategije kreiranja rezervnih kopija podataka

Kompanije više nisu izolovane u isključivo tehnološkoj ulozi u poslovim sredinama, tako da moraju prihvatati poslovne vrijednosti kao osnovu za određivanje raznih strategija. Ovo se takođe odnosi i na *backup* i *recovery* strategiju [2].

Korporativni podaci rastu velikom brzinom. Baze podataka se udvostručavaju na godišnjem nivou, IT resursi se vrlo brzo mijenjaju, a kompanije nisu u mogućnosti da ih prate jednakom brzinom. Internet aplikacije i globalni biznisi su uspostavili dvadesetčetvoročasovni poslovni dan drastično smanjujući vrijeme u kom je dozvoljen prekid poslovanja (*downtime*) kako bi se izvele redovne procedure za backup podataka. Ne tako davno, *backup* podataka je bio dosta jednostavan proces. Svake noći bi se trake za *backup* iznosile van datacentra, a *backup* administrator vodio računa da su poslovni procesi neprekinuti. U slučaju potrebe za oporavkom, trake bi se vraćale u uređaje i administrator bi im pristupao. Danas su procesi za backup i recovery značajno drugačiji. Postupak kreiranja rezervnih kopija podataka i njihovog oporavka je evoluirao u složeni zadatak koji se nameće kompanijama zahtijevajući da informacije budu trenutno dostupne, usklađenost sa regulatornim tijelima i potrebu za umreženim datacentrima. Kao rezultat toga, kompanije pristupaju izradi adekvatne strategije kreiranja rezervnih kopija podataka kako bi bile u mogućnosti da efikasno očuvaju procese sa dovoljno dobrim nivoom zaštite i osiguraju oporavak podataka [5].

2.1. Kriterijumi za kreiranje backup strategije

Prije razvoja efektivne strategije za backup i oporavak podataka, ICT organizacije bi trebale eksplicitno definisati svoje kriterijume za sve tipove svojih poslovnih podataka u smislu:

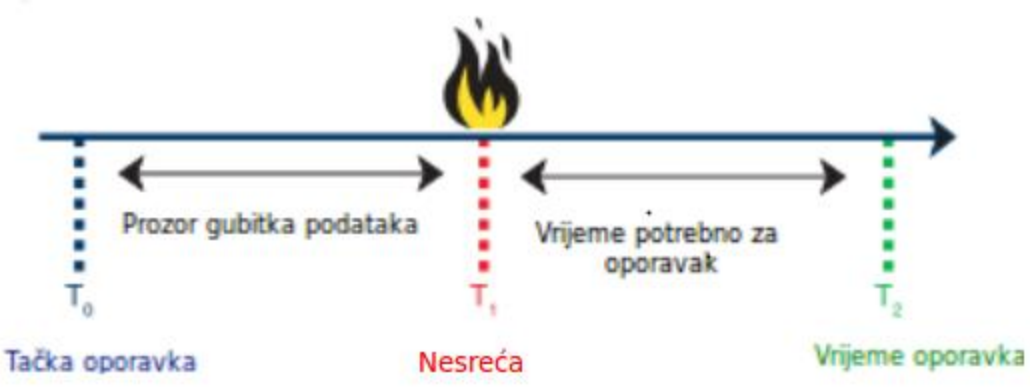
- ***Recovery Point Objective (RPO)***: RPO opisuju dva ključna parametra:
    a. **broj transakcija koje se mogu izgubiti** - Ovaj parametar se može odnositi na aktuelni broj poslovnih transakcija ili na vremensku jedinicu (kao što su sati). Ovim parametrom se definiše prihvatljivi gubitak podataka.
    b. **trenutak u vremenu od kojeg mora biti moguće oporaviti podatke** – Ovaj parametar uglavnom definiše periode čuvanja zaštićenih podataka.
- ***Recovery Time Objective (RTO)***: RTO definiše kojom brzinom se funkcije poslovanja moraju vratiti u prvobitno stanje prije gubitka podataka. RTO označava vrijeme potrebno za oporavak funkcionalnosti poslovanja, što ne mora uvijek da znači vrijeme potrebno za oporavak samih podataka.

Dok se ovi parametri ne definišu, kompanija neće biti u mogućnosti da predvidi da li će odabrano rješenje zadovoljiti njene zahtjeve poslovanja [1].

Slika 2.1 ilustruje ovaj koncept i definiše tri tačke u vremenu:

- T_0 je vrijeme u kom se podrazumijeva da su sačuvani podaci ispravni. To je tačka oporavka i predstavlja stanje u koje će se podaci vratiti nakon oporavka.
- T_1 je vrijeme u kom se dogodila nesreća. Interval između T_0 i T_1 je prozor gubitka podataka. RPO odgovara veličini ovog prozora. Što je manji ovaj prozor, to je više podataka sačuvano.
- T_2 je vrijeme u kojem su podaci u potpunosti oporavljeni. Interval između T_1 i T_2 je vrijeme oporavka, odnosno vrijeme u kojem je sistem bio nedostupan. RTO odgovara ovom intervalu, odnosno vremenu trajanja zastoja poslovanja

(*downtime*). Što je kraće ovo vrijeme, sistem se brže postavlja u funkcionalno stanje.



Slika 2.1: *Odnos između tačke oporavka, nesreće i vremena oporavka [12]*

Većina današnjih kompanija ima RPO vrijednost nula ili blizu nule za aplikacije koje su neophodne za poslovanje kompanije. Gubitak bilo koje transakcije je neprihvatljiv. Međutim, nisu svi podaci neophodni za opstanak firme tako da RPO može imati drugačije vrijednosti u zavisnosti od aplikacije [5].

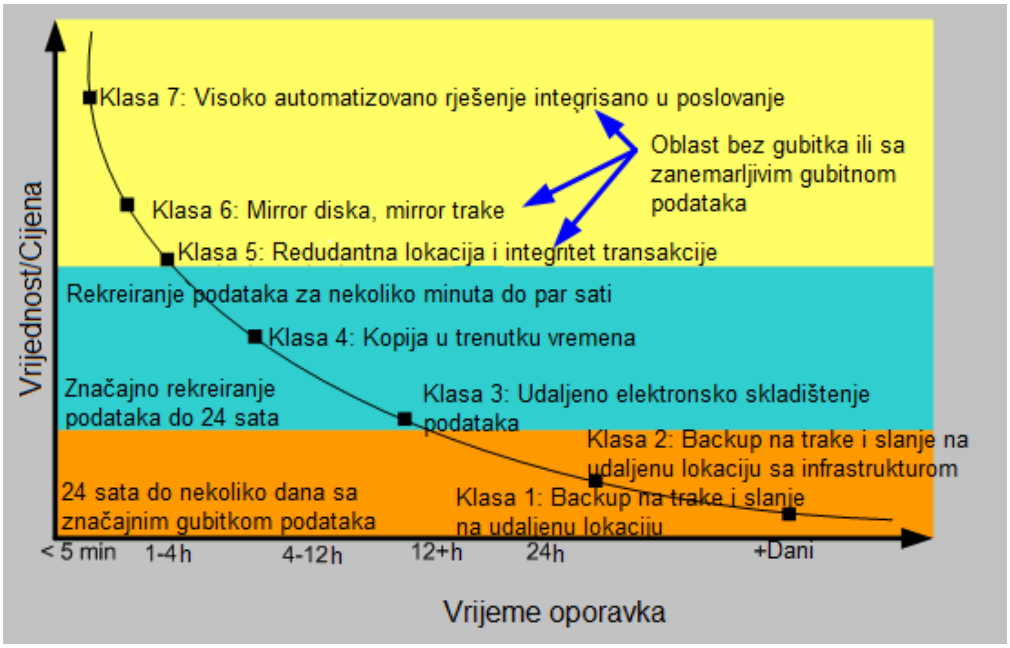
Kao dodatak RPO i RTO kriterijumima, operacije za kreiranje rezervnih kopija podataka su ograničene parametrom backup prozor (*backup window*) koji definiše vrijeme potrebno za izvršenje backup operacija na svim serverima. Uobičajeno je da se aplikacije zamrznu odnosno da se svi fajlovi i unosi zatvore i postave u stanje mirovanja kako bi bili spremni za backup. Međutim, kompanije čije operacije moraju biti aktivne dvadeset četiri sata, sedam dana u nedelji, nemaju mogućnost zaustavljanja svojih aplikacija tako da ne tolerišu backup prozor. U tom slučaju se koristi backup softver koji pravi kopije otvorenih fajlova, i iako se oni mogu promijeniti za vrijeme trajanja backup operacije, njihova prvobitna verzija ostaje sačuvana.

2.2. Sedmoklasni sistem servisa

Dok svi korporativni podaci imaju neku vrijednost, nema potrebe da svi podaci budu trenutno dostupni za oporavak poslovanja u slučaju njihovog gubitka. Vrlo je važno napraviti prioritete među poslovnim podacima i aplikacijama i pridružiti klase podataka nivoima oporavka. RPO i RTO parametri se mogu značajno razlikovati u odnosu na tip aplikacije, a dimenzionisanje taktike oporavka prema poslovnim zahtjevima smanjuje troškove i pojednostavljuje proces oporavka.

Prva svjetska organizacija IT profesionalaca, IBM korisnička grupa SHARE je uspostavila sistem višestrukih klasa zaštite podataka, od klase bez zaštite do kontinualne zaštite i dostupnosti, koji se koristi za identifikovanje raznih metoda oporavka IT sistema esencijalnih za poslovanje kompanije. Iako je originalni koncept nastao 1992. godine, on se i danas koristi kao najdetaljniji model za zaštitu podataka [13]. Detaljan opis klasa je dat u prilogu 2.

Slika 2.2 ilustruje koncept sedam klasa zaštite podataka na vremenskoj osi i osi koja predstavlja njihovu materijalnu vrijednost [14]. Svrha ove podjele je u tome da se svakoj aplikaciji u određenom poslovanju dodijeli odgovarajuća klasa. Prioritizacija poslovnih podataka i aplikacija i njihovo postavljanje u odgovarajuće klase je najteži ali osnovni korak u kreiranju efikasne strategije za backup podataka.



Slika 2.2: *Sistem višestrukih klasa zaštite podataka [14]*

Sadržaj dokumenta koji pokriva nivoe servisa (*SLA - Service Level Agreement)* ili internih i eksternih ugovora o obezbjeđivanju određenih usluga kao što je kreiranje rezervnih kopija podataka, treba da pokriva detalje vezane za odgovornost, pouzdanost servisa i vrijeme odgovora odnosno kvalitet obezbjeđivanja servisa [6].

2.3. Kategorije aplikacija i servisa predviđenih za backup

Kao što je već rečeno, prije izrade strategije, važno je napraviti detaljnu analizu cjelokupnog sistema i izvršiti kategorizaciju svih aplikacija i servisa po tipu i važnosti. U zavisnosti od važnosti servisa za funkcionisanje kompanije definišu se parametri relevantni za čuvanje rezervnih kopija, a u zavisnosti od tipa servisa, definiše se način na koji treba kreirati rezervne kopije.

Kriterijumi za kategorizaciju servisa po važnosti treba da budu [15]:

- **Poslovna kritičnost servisa** – važnost servisa za poslovanje i kako nefunkcionisanje određenog servisa utiče na redovne poslovne aktivnosti.
- **Zavisni servisi** – ukoliko drugi važni servisi zavise od ovog servisa, onda se i on smatra jednako važnim.

Najznačajnije kategorije podataka definisane po tipu servisa za koje treba obezbijediti rezervne kopije su:

- **Sistemski backup –** Ova kategorija uključuje backup operativnog sistema servera. Potrebno ga je izvršiti nakon svake promjene operativnog sistema kako bi se sistem mogao vratiti u zadnje funkcionalno stanje u slučaju oštećenja. Promjene uključuju *upgrade, update* ili bilo koju izmjenu u konfiguracionim fajlovima. Backup bi trebalo pohraniti na lokaciji odvojenoj od servera kako bi joj se moglo pristupiti u slučajevima kad server nije funkcionalan. Sistemski backup sistema je vrlo značajan jer je teško nanovo instalirati sistem da u potpunosti odgovara zadnjem funkcionalnom stanju

(odgovarajuća verzija OSa, *patch* nivo, *update* nivo pojedinačnih paketa), budući da vitalne aplikacije zahtijevaju tačno određenu verziju operativnog sistema.

- **Backup standardnih fajlova i servisa –** Ova kategorija uključuje rezervne kopije standardnih fajlova i servisa koji se mogu čuvati kao obični fajlovi. Primjer su aplikacije na Linux operativnim sistemima, kako integrisane (Apache, DNS server, DHCP server, Mail serveri...), tako i specijalno razvijene za potrebe poslovanja. Ovakvo kreiranje rezervnih kopija je najjednostavnije i ne zahtijeva specijalizovane softvere za backup podataka, iako oni uveliko olakšavaju proces kopiranja.
- **Backup aplikacije –** Ovaj backup se odnosi na podatke aplikacije i njene konfiguracije koje nije moguće oporaviti iz sistemskog ili servisnog backupa. Primjeri ove kategorije uključuju aplikacije na Windows operativnom sistemu kao što su *Microsoft Exchange, Active Directory, Cisco Call Manager* itd.
- **Backup baze podataka –** Rezervna kopija baze se kreira i čuva u cjelini. Ovo je izuzetno značajna kategorija podataka jer predstavlja osnovu svih kritičnih aplikacija u kompanijama, optimalno skladišteći, organizujući i upravljajući velikom količinom podataka. Primjeri baza podataka su Oracle, MSSQL Server, MySQL, PostgreSQL, Sybase, IBM DB2...
- **Backup virtuelnih mašina –** Kopije virtuelnih mašina se mogu kreirati kao slike (*image*), ili se virtuelne mašine mogu tretirati kao fizički sistemi i tako backupovati.

2.4. Oporavak IT sistema u slučaju nesreće

Backup predstavlja osnovu za oporavak IT sistema u slučaju nesreće i backup procedure bi trebale biti dio plana za "oporavak od nesreće" (*disaster recovery plan* - DRP). Pomoću DRP procedura moguće je rekonstruisati kompleksne kompjuterske konfiguracije kao što su klasteri, aktivni direktorijumi, serveri sa bazama podataka, itd. koji čine osnovu IT sistema. Oporavak od nesreće (*Disaster Recovery - DR*) i kontinualnost poslovanja (*Business Continuity - BC*) su strategije - BCDR strategije koje definišu mogućnost kompanije da nastavi pružanje podrške za svoje proizvode i servise na prihvatljivom nivou nakon nesreće koja je oštetila njen IT sistem [15].

Nivoi servisa (SLA) treba da definišu i dokumentuju RTO i RPO ciljeve za svaki poslovni proces, a onda da ih povežu sa osnovnim poslovnim aplikacijama. Sledeći zadatak je određivanje kako se ovi poslovni procesi odnose na poslovne korisnike koji ih svakodnevno upotrebljavaju, a nakon toga treba odrediti odnos prema samim IT sistemima. Slika 2.3 ilustruje tipični BCDR proces na visokom nivou [16].

Slika 2.3: *Tipični proces planiranja BCDR strategije*

Akcije na dnevnom nivou koje treba preduzeti za oporavak podataka dešavaju se za vrijeme uobičajenih poslovnih operacija i razlikuju se od DRP procedura koje uključuju akcije za

oporavak ukoliko je čitav datacentar ugrožen i oštećen. Sa akcijama ovog tipa administratori sistema se susreću na dnevnoj osnovi i one ne treba da predstavljaju izazov.

2.4.1 PLANIRANJE KONTINUITETA POSLOVANJA

Kontinuitet poslovanja (*Business Continuity - BC*) je definisan kao mogućnost organizacije da nastavi pružanje podrške za svoje proizvode i servise na prihvatljivom nivou nakon razarajuće nesreće. Upravljanje kontinuitetom poslovanja (*Business Continuity Management - BCM*) je definisano kao sveobuhvatni upravljački proces koji identifikuje potencijalne prijetnje i posljedice koje te prijetnje mogu imati na poslovne operacije. Ovaj proces obezbjeđuje okvir za izradu otpornosti jedne organizacije tako da bude u mogućnosti da efikasno podrži i održi njene funkcionalnosti, aktivnosti, reputaciju i vrijednosti nakon nesreće. Detaljno je definisan u standardu ISO 22301 [15].

Kontiuitet poslovanja se postiže kroz rigorozno planiranje strategije i razvoj procesa. BC proces planiranja dijelom određuje količinu kritičnih procesa, troškove zastoja poslovanja i rizike sa kojima se suočava kompanija. Rizici opravdavaju sredstva koja su potrebna kompaniji kako bi ugradila dostupnost, otpornost na nesreće i sposobnost oporavka od nesreće u svoju IT infrastrukturu. Prateća IT infrastruktura je blisko povezana sa procesom planiranja oporavka od nesreće (DRP) [13].

2.4.2 DISASTER RECOVERY

Oporavak od nesreće (*Disaster Recovery - DR*) predstavlja osnovni aspekt mnogo šireg koncepta kojeg predstavlja kontinuitet poslovanja (*Business Continuity*). Planiranje kontinuiteta poslovanja mora uključivati osoblje, objekte, udaljene kancelarije, napajanje, transport, telefon, komunikacionu opremu, kao i infrastrukturu u datacentru. Planiranje oporavka od nesreće je užeg karaktera i fokusira se na pristup podacima, tako da uzima u obzir servere, storage uređaje, mrežu i infrastrukturu u datacentru. Uključuje dodatnu opremu kao što su agregati ili redudantni sistemi koji će podržati primarni datacentar i obezbijediti lokaciju namijenjenu za oporavak ukoliko je primarni datacentar u potpunosti oštećen [5].

Nesreće (disaster) je teško predvidjeti i uglavnom u tim slučajevima dolazi do djelimičnog ili potpunog oštećenja hardvera. U ovu svrhu IT organizacije angažuju timove koji prave specijalne planove, takozvane DRP (*Disaster Recovery Plan*) procedure sa detaljnim opisom ponašanja i akcija koje treba preduzeti da bi se neki IT sistem oporavio od ovakvog gubitka.

Plan za oporavak od nesreće se često posmatra kao polisa osiguranja. Za današnje kompanije, DR je uslov za njihov opstanak. Ako zastoj u poslovanju (*downtime*) košta kompaniju veliku zaradu, svaki trenutak više nefunkcionalnog poslovanja čini kompaniju osjetljivom na konkurenciju, uništava brend i dovodi do gubitka korisnika. IT administratorima se postavlja složeni zadatak kako da kreiraju funkcionalni plan za oporavak od nesreće koji će uvijek biti pod pritiskom budžetskih ograničenja i konstantnog rasta podataka neophodnih za zaštitu [5].

Iako scenarija za oporavak od nesreće mogu koristiti zajedničke elemente, profili praktičnih DR scenarija se mogu uveliko razlikovati od kompanije do kompanije. Mala ili srednja preduzeća, na primjer, mogu imati jedan storage uređaj na svojoj produkcionoj lokaciji i vršiti sinhronu ili asinhronu replikaciju podataka na udaljeni storage uređaj. Velike kompanije mogu imati nekoliko desetina ovakvih uređaja raspoređenih u različitim datacentrima, a podaci se mogu replicirati na jedan ili više strateški raspoređenih DR lokacija. Dodatno, replikacija podataka može biti samo jedan element u kompleksnoj strukturi DR strategije koja može

uključivati mehanizme kontinualne zaštite podataka i centralizovanog skladištenja traka. Kompleksnost DR topologija tako zavisi od poslovnih zahtjeva kompanije i količine i vrste podataka koje treba obezbijediti u slučaju gubitka.

2.4.3 OSNOVNE DEFINICIJE BCDR KONCEPTA

Važni termini koji definišu i uključeni su u BCDR koncept su:

- **Analiza uticaja na poslovanje *(Business Impact Analysis - BIA)*** - se sprovodi kako bi se utvrdili uticaji povezani sa prekidima određenih funkcija i aktivnosti u nekoj kompaniji – u to su uključeni operativni, finansijski, zakonski i regulatorni uticaji. Primjeri uticaja nesreće mogu biti izgubljeni korisnici, prekovremeni rad, angažovanje dodatne pomoći na rješavanju problema, kazne i penali, otežano prikupljanje prihoda, itd..
- **Analiza rizika** - identifikuje funkcije i vrijednosti koje su važne za poslovanje kompanije, a onda procjenjuje vjerovatnoću prekida tih funkcionalnosti. Kada se jednom rizik procijeni, mogu se postaviti ciljevi i strategije kojima se minimizuju uticaji neizbježnih rizika i eliminišu rizici koji se mogu izbjeći.
- **Otpornost na nesreću (*Disaster Tolerance*)**- definiše sposobnost okruženja da izdrži velike poremećaje u sistemima i važnim poslovnim procesima. Otpornost na nesreću treba da bude ugrađena u okruženje na različitim nivoima; u obliku hardverske redudanse, klaster rješenja, visoko dostupnih rješenja, višestrukih datacentara, eliminišući jedinstvenu tačku prekida.
- **DR „vruća“ lokacija (*DR hotsite*)** - predstavlja datacentar lokaciju sa dovoljno hardverske opreme, komunikacionih interfejsa i kontrolisanog prostora sposobnu da relativno brzo obezbijedi podršku za procesuiranje kopija podataka.
- **DR „topla“ lokacija (*DR warmsite*)** - predstavlja datacentar lokaciju ili kancelarijske prostorije djelimično opremljene hardverom, komunikacionom opremom, napajanjem i klima uređajima sposobne da podrže backup operacije.
- **DR „hladna“ lokacija (*DR coldsite*)**- predstavlja datacentar lokaciju ili kancelarijske prostorije umrežene i opremljene klima uređajima, napajanjem, komunikacionom opremom i prostorom kako bi podržale instalaciju i funkcionisanje opreme neophodne za pokretanje poslovnih procesa.
- **Oporavak na „golom metalu“ (*Bare Metal Recovery*)** - opisuje proces postavljanja kompletnog sistema u njegovo originalno stanje u nekom trenutku prije nesreće, uključujući sistem i particije za podizanje sistema (*boot*), sistemska podešavanja, aplikacije i podatke.
- **Visoka dostupnost (*High Availability*)** - opisuje sposobnost sistema da nastavi sa funkcionisanjem određeni vremenski period iako se neka nesreća dogodila, obično sa vrlo visokim procentom od 99,999%. Visoka dostupnost se implementira u IT infrastrukturu smanjujući jedinstvene tačke prekida (*single points of failure – SPOF*) upotrebljavajući redudantne komponente. Slično, klasteri i uparene aplikacije na dva ili više sistema obezbjeđuju visoko dostupno računarsko okruženje [13].

2.5. Makro i mikro pristup kreiranju backup strategije

Vrlo je važno da procesi za backup i oporavak podataka budu u pozadini kako ne bi imali uticaja na standardne procese poslovanja i njihove korisnike. Zbog kompleksne prirode dizajna

rješenja za backup i oporavak podataka, kompanije uglavnom pristupaju izradi strategije kreiranja rezervnih kopija podataka i sa „makro“ i sa „mikro“ stanovišta [1].

- „Makro” pristup se bavi analizom dostupne infrastrukture u smislu hardvera i softvera, kao i mogućnostima za njeno proširenje. Makro dizajn je pristup na visokom nivou (*high-leve*l) koji uključuje faktore kao što su fizička lokacija backup servera (server koji upravlja backup procesom) u odnosu na podatke koje treba kopirati i čuvati, broj istih kopija podataka, kao i tip uređaja za backup koji će se koristiti. IT organizacije uglavnom koriste ovakav pristup kako bi odredili veličinu potrebne infrastrukture. Na ovom nivou planiranja, ključan je odabir infrastrukture i softvera za backup. Budući da treba uložiti značajna sredstva, jednom odabranu infrastrukturu i softver nije lako promijeniti ni sa materijalnog ni sa administratorskog stanovišta. Nakon odabira softvera, ključne odluke koje treba donijeti su:
    - da li će backup serveri i backup klijenti biti na istim ili udaljenim fizičkim lokacijama
    - da li treba kreirati sekundarne kopije postojećih backup imidža i na koji način
    - koju vrstu medijuma za skladištenje podataka treba odabrati; magnetske trake, diskove, VTL, itd.
- “Mikro” pristup uzima u obzir zahtjeve koje postavljaju raznorodni podaci: pojedinačne aplikacije, serveri, skupovi podataka... U ovom stadijumu se odlučuje koja će se kombinacija tipova backupa primijeniti i u kom vremenskom intervalu. Kako nemaju svi podaci istu važnost, različite strategije će se primjenjivati na različitim kategorijama podataka nakon što se oni klasifikuju. Neke od ključnih odluka koje treba donijeti su:
    - Da li će prenos podataka od klijenta do servera za backup ići kroz LAN, SAN ili direktno na medijum za skladištenje (bez mreže);
    - Da li je potrebno koristiti dodatni softver sa standardnim softverom za jednostavniji backup pojedinačnih aplikacija (API agent);
    - Koja kombinacija tipova backupa će se primijeniti na pojedine grupe podataka;
    - Kada i koliko često treba kopirati i pohranjivati podatke;
    - Koliko dugo treba čuvati slike backup procesa;
    - Metode zakazivanja backup akcija, i sl.

Pravilno osmišljeno rješenje za backup i recovery se mora zasnivati na razumnom operacionom modelu. Operacioni model definiše broj sati u toku 24 sata dostupnih za završetak određenih backup operacija i operacija za oporavak [1].

3. Tehnologije na kojima se zasnivaju backup i recovery koncepti

3.1. Infrastruktura mreže za kreiranje rezervnih kopija podataka

Određivanje veličine infrastrukture i planiranje kapaciteta su ključne komponente uspješno realizovanog okruženja za kreiranje rezervnih kopija podataka i njihov oporavak, uključujući i proaktivno planiranje kapaciteta kako bi se podržao kontinuirani rast kompanije. Sa strane kapaciteta, dva aspekta su kritična:

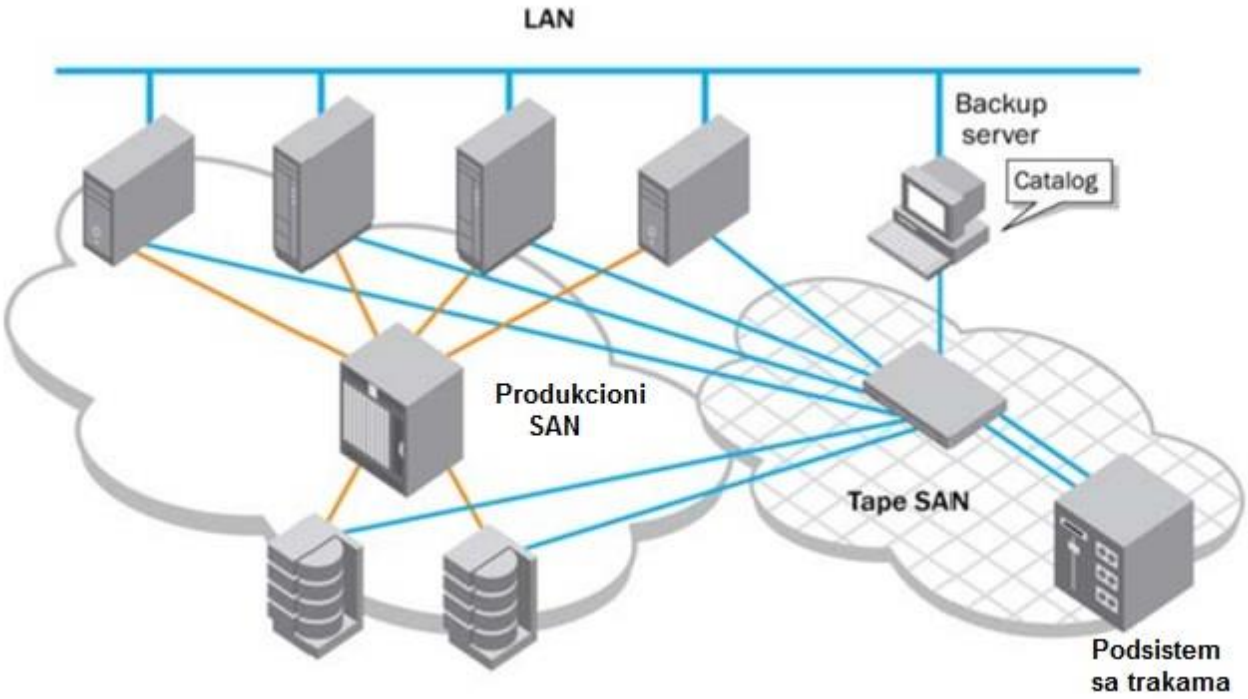
- **Protok (*Bandwidth*)** - Kopirana količina podataka u vremenu. Ovaj parametar uglavnom predstavlja broj gigabajta ili terabajta iskopiranih za jedan dan. Njega određuje količina podataka koju treba zaštititi i način na koji se štiti.
- **Skladište (*Storage*)** - Ukupni kapacitet svih kreiranih slika koje predstavljaju rezervne kopije podataka koje će održavati softver za backup. Ovaj parametar proizilazi iz količine podataka koja se štiti kao i parametara čuvanja koji se definišu za podatke. [1].

U velikim datacentrima, vitalne aplikacije uvijek rade na visoko performantnoj *Fibre Channel* (FC) SAN mreži. *Storage Area Network* (SAN) je posebna mreža koja obezbjeđuje pristup konsolidovanim uređajima za smiještanje podataka, a funkcioniše preko Fibre Channel (FC) tehnologije velikih brzina (2, 4, 8 ili 16 Gb/s). *Fibre Channel* tehnologija obezbjeđuje skup generičkih servisa niskog nivoa na koji se mogu mapirati arhitektura mreže i hostova. Obezbjeđuje interfejs za serijski transfer podataka preko bakarne parice i/ili optičkog kabla. Mrežne komande i I/O protokoli (kao što su SCSI komande) se mapiraju na FC konstrukciju i onda enkapsuliraju i transportuju u FC frejmovima. Ovaj proces omogućava prenos više različitih protokola velikim brzinama kroz isti fizički medijum. FC tehnologija omogućava pristup uređajima na nivou bloka, dozvoljavajući host sistemu da identifikuje uređaj povezan na mrežu kao svoj lični. Primarno se koristi za povezivanje uređaja za skladištenje podataka (*storage* uređaji), a na taj način je moguće koristiti sve aplikacije, npr. softvere za backup, za upravljanje volumenima (*volume management*), za upravljanje disk uređajima (*raw disk management*), bez modifikacija [17].

Fibre Channel Storage Area Network isključivo koristi *Fibre Channel* za prenos komandi, podataka i statusnih informacija. Sastoji se od individualne strukture (eng. *fabric*) ili više struktura međusobno povezanih koristeći funkcije rutiranja. Struktura SAN mreže (*fabric)* je skup FC portova koji dijele isti 24-bitni adresni prostor. Informacije o portovima koji su povezani (logovani) na određenu strukturu se distribuiraju svim elementima u toj strukturi [17].

Protok podataka u produkcionoj SAN mreži se karakteriše visokim I/O ili uglavnom kratkim transakcijama. Sa izuzetkom video striming sadržaja i aplikacija koje sadrže velike slike (npr. medicinske ili geofizičke slike), većina uobičajenih poslovnih transakcija kroz SAN je kratka i tako otpornija na kratkotrajne probleme u mreži kao što su zagušenje ili prekid. Nasuprot tome, kreiranje kopija podataka karakteriše konstantan protok blokova podataka od inicijalne tačke do ciljanog medijuma. Bilo koji prekid u prenosu backup podataka može uzrokovati prekid kompletne operacije. Datacentri su zbog toga opremljeni odvojenom mrežom koja služi za backup, kako bi se minimizovala mogućnost prekida backup procesa i kako bi se ovaj saobraćaj odvojio od produkcione SAN mreže [5].

Iako se u SAN mreži koja služi za backup podataka ne nalaze isključivo podsistemi sa trakama, ona se uslovno rečeno naziva „tape“ SAN, odnosno SAN sa trakama, budući da su trake prvobitni i izvorni medijum za kreiranje rezervnih kopija podataka. U poglavlju 3.4.1 su detaljnije opisani mehanizmi u tradicionalnim tehnologijama za backup.



Slika 3.1: *SAN sa trakama namijenjen za backup izoluje backup proces iz produkcione SAN mreže*

Kao što je prikazano na slici 3.1, „tape“ SAN (SAN sa trakama) koji je namijenjen za backup podataka se može implementirati zajedno sa produkcionom SAN mrežom kako bi se izolovao saobraćaj za backup od ostalih transakcija. Iako implementacija odvojene SAN mreže zahtijeva dodatne uređaje i povećava obim upravljačkog posla, značajno se povećava stabilnost operacija i osigurava uspješan backup proces [5].

3.2. Zaštita podataka u SAN Infrastrukturi

Budući da su podaci najvažnija komponenta funkcionisanja neke kompanije, centralni zadatak IT strategije je pronalaženje načina za njihovu zaštitu i očuvanje integriteta. Podaci se nalaze na nekom tipu medijuma za skladištenje: disk u stabilnom obliku (*solid state disk – SSD*), traka, optički medijum, a posebno je značajan disk medijum u formi uređaja za skladištenje podataka (*storage array*). Zbog toga je akcenat zaštite podataka na storage uređaju. Nivoi zaštite podataka i pristupnih mehanizama, od pristupa blokovima sa visokim procentom dostupnosti do distribuiranih fajl sistema, su izgrađeni na osnovama ojačanog storage uređaja i nastavljaju se do aplikativnog nivoa [5].

Strateški pristup sveobuhvatnoj zaštiti podataka uključuje paletu rješenja koje predstavljuju osnovne cjeline povezanog ekosistema. Očuvanje podataka kroz replikaciju podataka ili backup nema puno smisla ako se podaci gube u loše projektovanoj mreži ili zbog otkaza u mreži. Zbog toga, jednako je važno osigurati pristup podacima koliko je važno očuvati njihov integritet. Za SAN mreže, alternativne putanje sa mehanizmima preuzimanja aplikacija u

slučaju otkaza sistema (*failover* mehanizmi) su vitalne za ostvarivanje visoko dostupnog pristupa podacima, a visoka dostupnost (*high availability – HA*) omogućava konzistentnu implementaciju servisa za zaštitu podataka [5].

Vrlo važni aspekti SAN topologije su rezilijentnost i redudansa strukture SAN mreže. Glavni cilj je ukloniti bilo koju tačku prekida. Rezilijentnost je sposobnost mreže da nastavi funkcionisanje i/ili da se samostalno oporavi od otkaza [18]. Ona predstavlja otpornost mreže na pojedinačne otkaze u sistemu. Sa druge strane, redudansa se odnosi na udvojene komponente, čak i čitave strukture, kako bi se eliminisale jedinstvene tačke prekida (*single point of failure*) u mreži. Redudantni sistem uključuje višestruke kanale kako bi obezbijedio alternativne putanje u slučaju pojedinačnih otkaza. Da bi se konstruisala rezilijentna mreža, ona obično mora sadržati redudantne komponente i linkove.

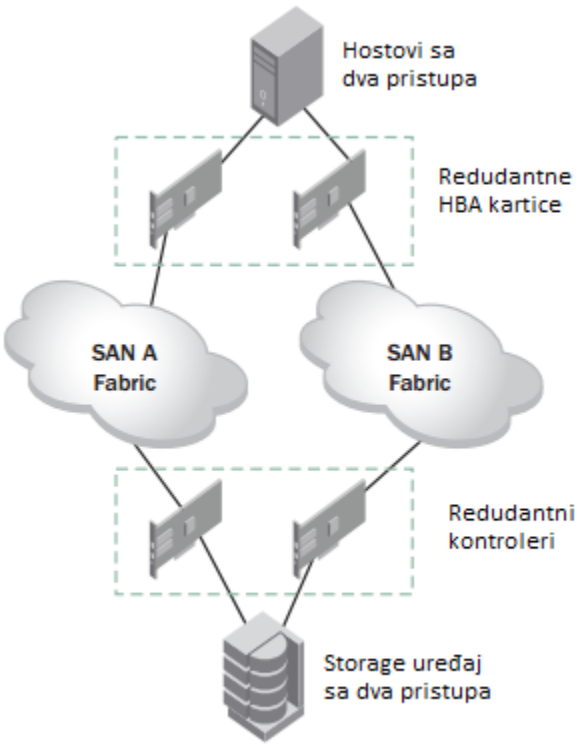
Ključ visoke dostupnosti i ispravne instalacije opreme na visokom nivou leži u redudansi. Eliminišući jedinstvenu tačku prekida, obezbjeđuje se nastavak poslovanja kroz predvidljive i nepredvidljive događaje. Kompletna mreža treba biti redudantna, sa dvije potpuno odvojene strukture koje ne dijele nijedan mrežni element.

Multipath je tehnika koja poboljšava performanse i štiti od grešaka, a definiše više od jedne fizičke putanje između procesora u serveru i njegovih storage uređaja. Serveri i storage uređaji treba da su povezani na obije strukture istovremeno koristeći neki oblik *multipath* rješenja, tako da se podaci mogu neprimjetno transportovati kroz obije mreže u aktivnom/aktivnom ili aktivnom/pasivnom režimu. *Multipath* tehnika obezbjeđuje alternativne putanje ukoliko se neka od putanja prekine zbog bilo kakvog problema u mreži. U idealnom slučaju, mreže treba da su identične, a minimalni zahtjev je da su zasnovane na istoj arhitekturi svičeva. U nekim slučajevima, ove mreže se nalaze na istoj lokaciji. Ipak, kako bi se osiguralo DR rješenje, često se koriste dvije odvojne lokacije, ili za kompletne mreže, ili za pojedine djelove svake mreže.

Nezavisno od fizičke lokacije, treba da postoje dvije različite mreže zbog kompletne mrežne redudanse. Ukratko, preporuke za projektovanje SAN mreže kako bi se ostvarila visoka dostupnost i rezilijentnost aplikacija su:

- Redudansa ugrađena u strukturu kako bi se izbjegla jedinstvena tačka prekida,
- Serveri povezani sa storage uređajem kroz redudantne strukture (Slika 3.2),
- Multipath rješenje između servera i storage uređaja,
- Redudatne strukture zasnovane na sličnoj arhitekturi,
- Odvojeni serverski nivo i nivo za skladištenje podataka zbog nezavisne ekspanzije,
- Svičevi u središtu (core) mreže treba da budu jednakih ili većih performansi u odnosu na periferne svičeve,
- Definisanje glavnog sviča u mreži koji treba da posjeduje najbolje performanse [18].

Kao što je već spomenuto, uvijek treba da postoje najmanje dva slična ako ne identična elementa u SAN mreži kako bi se obezbijedila redudansa i unaprijedila rezilijentnost. Na slici 3.2, predstavljena je uprošćena SAN mreža koja se sastoji od dvije redudantne strukture [18]. Svaka konekciona linija predstavlja najmanje dvije fizičke mrežne konekcije. Kao dodatak redudantnim strukturama, redudantni linkovi treba da povezuju različite ploče, različite grupe portova, različite HBA kartice, različite kontrolere, kako bi se u slučaju otkaza uvijek mogla pronaći funkcionalna alternativna putanja od izvora do destinacije.



Slika 3.2: *Primjer povezivanja uređaja kroz redudantne strukture*

Rješenja za zaštitu podataka zavise od stabilnog transporta kroz SAN mrežu koji je istovremeno predvidljiv i upravljiv. Ipak ni najpažljivije projektovan SAN ne može osigurati dostupnost i integritet podataka ako su uređaji za skladištenje podataka osjetljivi na gubitak podataka ili korupciju. Za aplikacije na nivou kompanija, storage uređaji se moraju projektovati tako da obezbijede performantnost, kapacitet, integritet podataka i visoku dostupnost. To znači da arhitektura samog storage uređaja treba da uključuje osobine rezilijentnosti kako bi uvećala njegovu dostupnost i kako bi zaštitila podatke od gubitaka usljed otkaza disk komponenti [5]. U najmanju ruku disk uređaji treba da sadrže redudantna napajanja, redudantne ventilatore, odmah zamjenjive adaptere i interne diskove. Interni dizajn sistema (sistemska matična ploča) takođe ne smije sadržati jedinstvene tačke prekida [13] tako da mora postojati redudansa u smislu kontorlera, I/O putanja, konekcija na mrežu, itd.

Vrlo važan koncept za zaštitu podataka u storage tehnologiji je RAID (*Redundant Array of Inexpensive Disks*), tehnika virtuelizacije skladištenja podataka koja kombinuje više disk komponenti u logičke jedinice kako bi postigla redudansu i poboljšanje performansi. Velika prednost RAIDa je transparentnost sistemu koji ga koristi; sistem od skupa diskova pod RAIDom vidi samo jedan disk i tako omogućava jedostavnu zamjenu u slučaju otkaza bez administratorske intervencije [19]. RAID podsistemi obično koriste tri tehnike redudanse:

- **Ogledanje (*Mirroring*)** - Kada se podaci ogledaju, sistem naizmjenično piše na odvojene hard diskove ili nizove diskova (*drive arrays*). Ako se jedan disk ošteti, sistem i dalje može nesmetano čitati podatke sa drugog logičkog volumena (*logical volume*).
- **Paritet (*Parity*)** - je tehnika koja se koristi da bi odredila da li su podaci izgubljeni ili prepisani. U RAID implementacijama, diskovi mogu biti posebno namijenjeni ili djelimično upotrijebljeni za paritet podataka. Suštinski, višestruki volumeni dijele podatke sa paritetom.
- **Dijeljenje na trake (*Striping*)** - je tehnika koja ravnomjerno raspoređuje podatke na više fizičkih diskova u nizu. Logička grupa podataka se dijeli u inkremente veličine

blokova ili bajtova i sekvencijalno upisuje preko više diskova. Ova tehnika unapređuje I/O performanse tako što više diskova može istovremeno pristupiti logičkoj sekvenci podataka, ali ne obezbjeđuje redudansu podataka [13].

Serverske tehnologije bi takođe trebale obezbjeđivati najveću moguću redudansu i skalabilnost. Kao i u storage tehnologijama, standardi za arhitekturu platformi treba da uključuju redudantna napajanja, redudantne ventilatore, odmah zamjenjive PCI uređaje i odmah zamjenjive interne diskove. Interni dizajn sistema bi trebalo da eliminiše sve jedinstvene tačke prekida [13].

Na transportnom nivou, individualni serveri su opremljeni redudantnim HBA (*Host Bus Adapter*) karticama koje su povezane na SAN (*Storage Area Network*) optičku infrastrukturu. Host Bus Adapter, skraćeno HBA je interfejs koji povezuje server sa ostalim mrežnim i storage uređajima u optičkoj infrastrukturi. Povezivanje je paralelno, i na primarnu i na sekundarnu strukturu, tako da u slučaju otkaza bilo koje tačke u putanji (HBA, port konekcija, port na sviču, svič ili port na storage uređaju) postoji alternativna putanja koja osigurava kontinualni pristup.

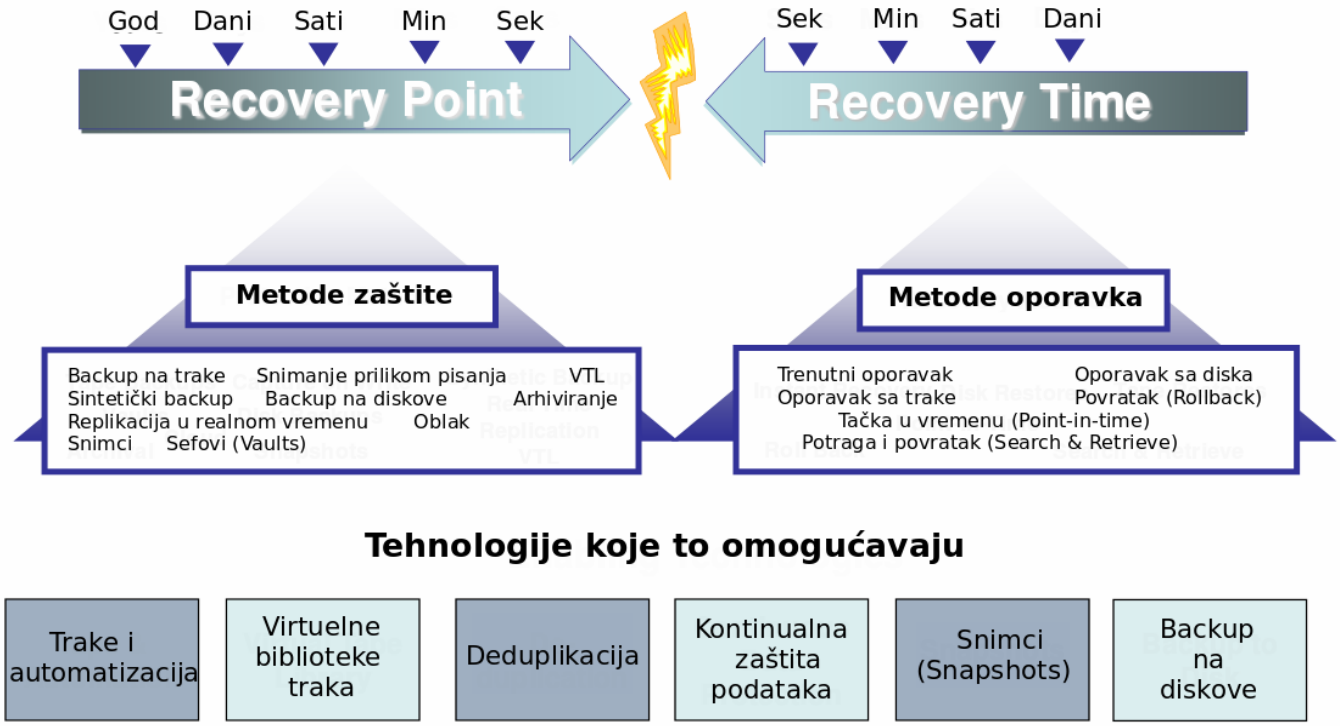
Postoji broj softverskih aplikacija koje omogućavaju povezivanje više servera u klastere kako bi se obezbijedila visoka dostupnost. Klaster rješenja u vidu softvera uglavnom nadgledaju sistemske resurse i uređaje pomoću protokola koji razmjenjuje sistemske (*heartbeat)* poruke. U zavisnosti od definisanih događaja, nedostatak određenih sistemskih resursa uzrokuje prelazak (*failover)* aplikacionog okruženja sa jednog servera na drugi [13].

3.3. Mehanizmi za skladištenje kopija podataka

Evolucija storage uređaja u smislu kapaciteta, brzine pristupa i cijene je značajno uticala na razvoj različitih tehnologija za kreiranje rezervnih kopija podataka. Donedavno postojalo je tek par mogućnosti u izboru arhitekture rješenja, pa su tako paralelno bili zastupljeni i sistemi sa diskovima i sa trakama. U zadnjih nekoliko godina desio se veliki napredak u razvoju disk tehnologija koji je značajno smanjio cijenu disk jedinice. Tehnologije kao što su virtualizacija storage-a, deduplikacija podataka i replikacija podataka donose nove mogućnosti. Prostor za skladištenje podataka zasnovan na disku dobija veliku ulogu na polju zaštite podataka koje je nekada bilo rezervisano isključivo za rješenja zasnovana na trakama [25].

Kako organizacije moraju biti spremne za oporavak od nesreće, DR je značajno uticao na razvoj storage sistema. Zahtijevani nivo zaštite podataka traži rješenja koja će varirati u tehnološkoj sofisticiranosti; od magnetnih traka koje se ručno prenose, kroz elektronske verzije kopija podataka, do rješenja koja pružaju potpune replikacije i distribuirane sisteme [26]. IT organizacije mogu izabrati i kombinovati brojne tehnologije koje su danas dostupne; od tradicionalnih do vodećih aktuelnih rješenja.

Na slici 3.3 ilustrovani su aktuelni mehanizmi za zaštitu i oporavak podataka posmatrani kroz RPO i RTO parametre. U zavisnosti od veličine RPO parametra, sledeće metode zaštite se globalno primjenjuju: backup na trake, snimanje prilikom pisanja, VTL, sintetički backup, backup na diskovima, arhiviranje, replikacija u realnom vremenu, oblak, snimci, sefovi (eng. *vaults*). U zavisnosti od vremena koje je potrebno za oporavak podataka, dostupne su sledeće metode oporavka: trenutni oporavak, oporavak sa diska, oporavak sa trake, povratak (eng. *rollback*), tačka u vremenu (eng. *point-in-time*), potraga i povratak (eng. *Search & Retrieve*).



Slika 3.3: *Ilustracija mehanizama za zaštitu podataka zasnovanih na oporavku*

Tehnologije koje realizuju nabrojane metode zaštite i oporavka su opisane u nastavku poglavlja.

3.3.1 TRADICIONALNE PLATFORME ZA KREIRANJE REZERVNIH KOPIJA PODATAKA

Tradicionalni backup mehanizmi koriste trake kao primarni medijum za backup. Kreiranje rezervnih kopija podataka na trake (*Tape-based backup*) je najstarija forma čuvanja podataka dostupna poslovanjima i koristi se još od sredine '60 godina. Stare i dobrostojeće kompanije koriste ovaj vid backupa dugi niz godina i ostaju mu vjerni jer nije potrebno značajno mijenjati infrastrukturu u datacentru zbog proširenja [27].

Slika 3.4: *Backup server kopira podatke sa diska primarnog storage-a na traku [29]*

Traka je ekonomski pristupačan medijum za skladištenje podataka, mala je i omogućava jednostavan prenos podataka na udaljenu lokaciju. Međutim, mehanizmu kreiranja kopija podataka na trake nedostaju brzina, pouzdanost, fleksibilnost i jednostavnost, osobine koje su neophodne kompanijama u njihovim rješenjima za zaštitu podataka. Takođe, isključivo kreiranje

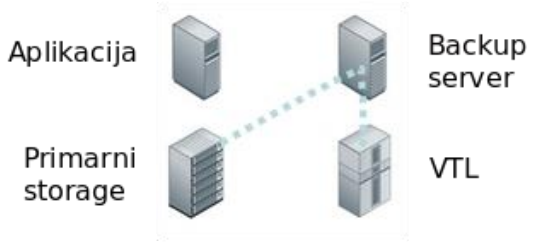
kopija podataka na trake nije više adekvatno rješenje budući da postoji veliki rizik da se trake izgube, a administracija backup i recovery operacija je dosta složena [28].

Fizička biblioteka podataka - PTL (*Physical Tape Library*) je uređaj koji se sastoji od robotske ruke, traka i slotova. Robotska ruka postavlja kertridže na odgovarajuće mjesto za upis i prihvata komande od računara na kom se nalazi softver za backup. Slotovi drže kertridže sa trakama. Ovi uređaji mogu pohraniti ogromne količine podataka, od 20TB do 2,1EB. Oni su isplativo rješenje za slučaj skladištenja velikog broja podataka, ali mogu biti jako spori zbog svog sekvencijalnog pristupa podacima i velikih kapaciteta. Ovim uređajem uglavnom upravlja softver za backup i recovery koji kontroliše robotiku. HP je vodeći proizvođač ovakvih uređaja sa svojom MSL serijom [30].

Backup na trake je linearni proces kojeg usporava konstantno izlaganje trake glavi za čitanje i upis. Iako po specifikaciji trake, njena brzina upisa može dostizati vrijednost do 800MB/s (za tip trake LTO-5), maksimalna brzina zavisi od ograničenja kojeg postavlja fizika pokretnih djelova i magnetne trake [62]. Ako uzmemo u obzir da diskovi dozvoljavaju trenutne operacije upisa/čitanja, iako po specifikaciji dostižu znatno manje brzine (SSD disk 280MB/s), dolazi se do zaključka da je disk medijum značajno brži od trake, čineći traku „uskim grlom“ u backup i restore procesu.

Budući da su backup na trake i softver za backup sveprisutni u datacentru, bilo je teško zamijeniti ih alternativnom tehnologijom. U tu svrhu razvijeni su VTL uređaji koji omogućavaju nizovima diskova da se ponašaju kao tradicionalni uređaji sa trakama [5].

Virtuelna biblioteka podataka - VTL (*Virtual Tape Library*) je uređaj koji se koristi u svrhe backupa i oporavka podataka a zasnovan je na virtuelizaciji prostora za skladištenje podataka. VTL predstavlja storage komponentu (obično storage uređaj zasnovan na hard diskovima) kao biblioteku traka i tako omogućava integraciju sa postojećim softverom za backup. VTL uglavnom koristi SAS ili SATA diskove zbog njihove relativno povoljne cijene. Podaci su organizovani u jednom od RAID nivoa zbog dalje zaštite od otkaza diska. VTL je sofisticiraniji uređaj od PTLa; smiještajući podatke na diskovima umjesto na trake, povećavaju se performanse operacija za backup i operacija za oporavak podataka. Ova jedna razlika može značajno smanjiti backup prozor i unaprijediti vrijeme oporavka, budući da se podaci procesuiraju brzinom diska umjesto brzinom trake.



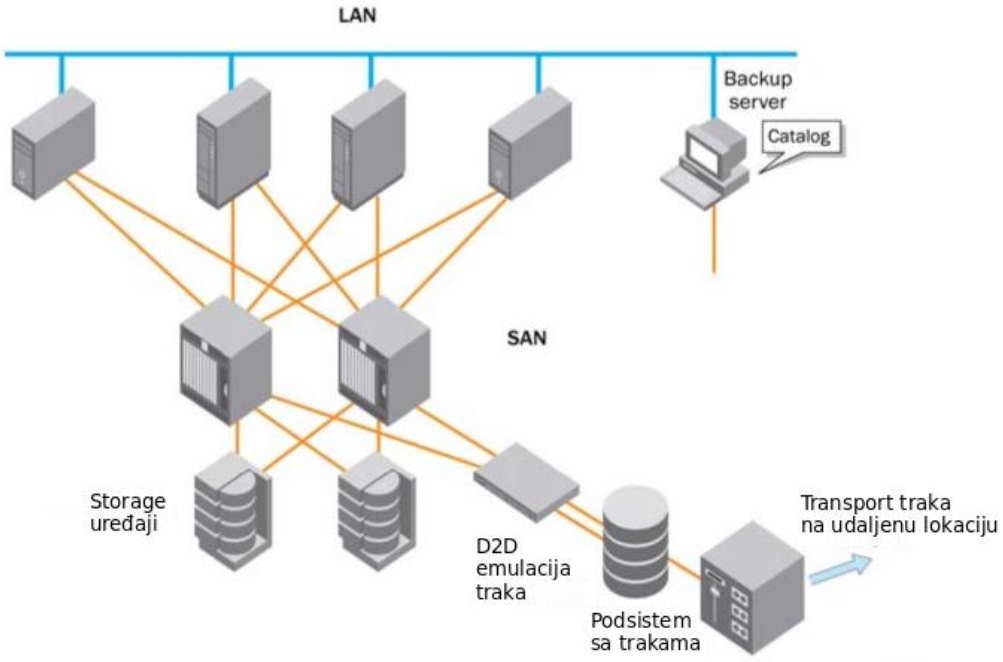
Slika 3.5: *Backup server kopira podatke sa diska primarnog storage-a na VTL [29]*

Kako emulacija trake disk na disk (*disk-to-disk - D2D*) eliminiše uska grla koja postavlja mehanika trake, moguće je značajno smanjiti backup prozor. Povraćaj podataka sa D2D je takođe ubrzan. D2D emulacija trake se može konfigurisati sa dodatnim uređajem ili integrisati u specijalizovani disk kontroler. Sa strane backup aplikacije, krajnji uređaj izgleda kao konvencionalni podsistem sa trakama. Ovo znači da je moguće implementirati D2D rješenje bez većih promjena na postojeći sistem [5].

Backup sistemi zasnovani na diskovima se odnose na tehnologiju koja omogućava backup velikih količina podataka na prostor na diskovima (*backup-to-disk – B2D* i *disk-to-disk – D2D*) čineći disk primarnim backup medijumom. Oni omogućavaju brže izvršavanje procesa

backupa i oporavka podataka nego trake, a pri tom eliminišu mnogobrojne probleme vezane za transport traka. Ovi sistemi imaju mogućnosti deduplikacije i kompresije i koriste RAID kao jedan od mehanizama zaštite podataka [31]. Potencijalni nedostatak ovog mehanizma je što se prilikom njegove implementacije mogu zahtijevati promjene u postojećim procesima i operacijama vezanim za backup. Neki od značajnih proizvoda u ovoj oblasti su EMC DataDomain i HP StoreOnce uređaji.

Emulacija traka D2D može funkcionisati zajedno sa konvencionalnim podsistemom sa trakama koji bi služio za dugoročno arhiviranje, kao što je prikazano na slici 3.6. Kada se jednom podaci iskopiraju na D2D rješenje, odatle se mogu ponovo kopirati na podsistem sa trakama i odnijeti na udaljenu lokaciju. U ovom slučaju uređaj sa trakama više ne predstavlja usko grlo za backup proces budući da je inicijalni backup već odrađen na disk. D2D2T mehanizam (*disk-to-disk-to-tape*) ne eliminiše traku već pomaže da se prevaziđu njena ograničenja u smislu performansi procesa kreiranja rezervnih kopija i oporavka podataka. Imajući na umu trend porasta količine podataka koju treba čuvati i regulatorne obaveze prema zaštiti podataka, D2D2T mehanizam ubrzava proces i osigurava dugoročnu zaštitu podataka [5].



Slika 3.6: *Kombinacija D2D emulacije traka sa konvencionalnim podsistemom sa trakama*

3.3.2 KONCEPT SNIMKA

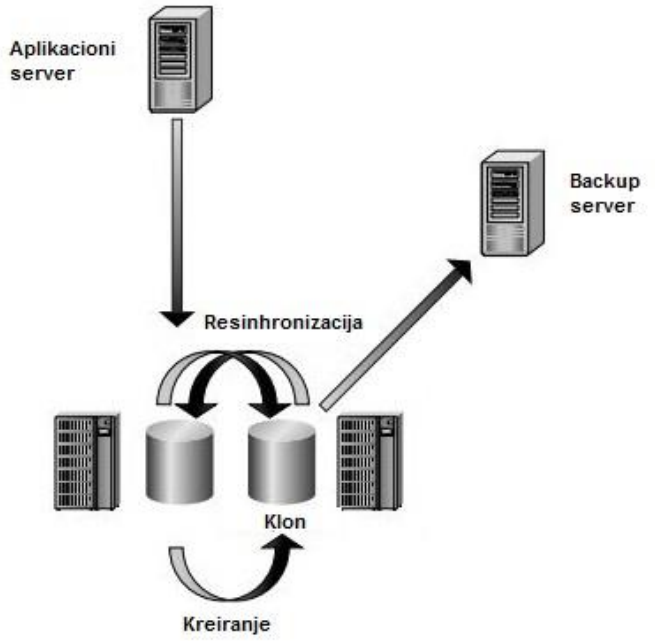
Sistemi sa diskovima godinama obezbjeđuju backup i recovery funkcionalnosti, koristeći kapacitet storage sistema za kreiranje kopija primarnih podataka u svrhe oporavka. Snimak (*snapshot*) je trenutna kopija podataka na diskovima koja obuhvata originalne podatke u određenoj tački u vremenu. Snimci mogu biti samo za čitanje (*read-only*) ili i za čitanje i za upis (*read-write*), a još su poznati i pod imenom *checkpoint*, tačka u vremenu (*Point-in-Time*), stabilna slika (*Stable Image*). Njima se upravlja na nivou storage uređaja [23].

Snimak obično ima neku od formi:

- **Potpuni snimak ili klon (*Full-copy snapshot ili clone*)** - Klon je potpuna kopija LUN-a (blok format) ili volumena – *volume* (fajl format) na odvojeni niz diskova na disk sistemu. U ovom slučaju potrebno je 100% kapaciteta prostora na kojem se nalaze

originalni podaci kako bi se napravila potpuna kopija. Nakon prve kopije, neki sistemi omogućavaju inkrementalno ažuriranje tako da se kreira novi klon na istom mjestu samo upisivanjem promijenjenih blokova (slika 3.7).

- **Diferencijalni snimak (*Pointer-based snapshot*)** - Ova vrsta snimka je slična klonu sa tim izuzetkom što se ne kreira potpuna kopija primarnog LUNa/volumena već niz pokazivača na lokaciju originalnih podataka. Kad se originalni podaci mijenjaju, pravi se njihova kopija prije ažuriranja („kopija na upis“) i snimak odražava novu lokaciju ovih podataka. Kao rezultat, snimak zasnovan na pokazivaču ne mora zauzimati jednaki prostor kao veličina originalnog LUNa/volumena.
- **Udaljena replikacija (*Remote mirroring/replication*)** - Uključuje kopiranje podataka sa jednog storage uređaja na drugi. Uglavnom ova dva storage sistema moraju biti slični sistemi (isti proizvođač i ista linija proizvoda). Postoje dvije vrste replikacije: sinhrona i asinhrona. Kod sinhrone replikacije, svaka upisna transakcija na primarnoj lokaciji se replicira na udaljenoj lokaciji prije nego što stigne potvrda da je upis završen. Tako se osigurava konzistentnost podataka i na primarnoj i na udaljenoj lokaciji. Kod asinhrone replikacije, transakcije se upisuju na primarnoj lokaciji i postavljaju u status čekanja za prenos na udaljenu lokaciju. Zbog toga udaljeni sistem može biti u zaostatku za primarnim sistemom od nekoliko sekundi do par sati u zavisnosti od brzine upisa, latencije, protoka i ostalih faktora.
- **Snimci i udaljeno ogledanje (*Snapshot* i *remote mirroring*)** - Organizacije mogu kombinovati funkcije snimaka i udaljenog ogledanja kako bi omogućili dodatne opcije za oporavak podataka. Snimak na primarnoj lokaciji se može replicirati asinhrono na udaljenu lokaciju kako bi se omogućila udaljena kopija podataka u određenoj tački u vremenu [1].



Slika 3.7: *Ilustracija potpunog snimka – klona [42]*

Jedna od slabih strana rješenja zasnovanih na storage tehnologijama je to što su ona uglavnom vezana za određenog proizvođača (i često za određeni model) storage sistema.

Takođe, snimci uzeti na produkcionom storage uređaju mogu opteretiti produkciju. U tabeli 3.1 je data uporedna analiza klona i diferencijalnog snimka [22].

Tabela 3.1: *Uporedna analiza klona i diferencijalnog snimka*

Snimci	**Klon - Potpuni snimak**	**Diferencijalni snimak**
Prednosti	- Minimalni uticaj na performanse - Nezavisne kopije dostupne za DR	- Manji utrošak prostora na storage uređaju - Smiješta se na jeftinije diskove
Mane	- Veći utrošak prostora na diskovima - Nema geo-redudantnu zaštitu	- Uticaj na performanse - Zavistan od primarne kopije
Aplikacije	- Oporavak od nesreće - Backup prozor blizu nule - Najbrži restore - Podaci se mogu opet iskoristiti	- Izvor backup-a - Backup prozor blizu nule - Brzi restore - Može pomoći u ponovnom iskorišćavanju podataka

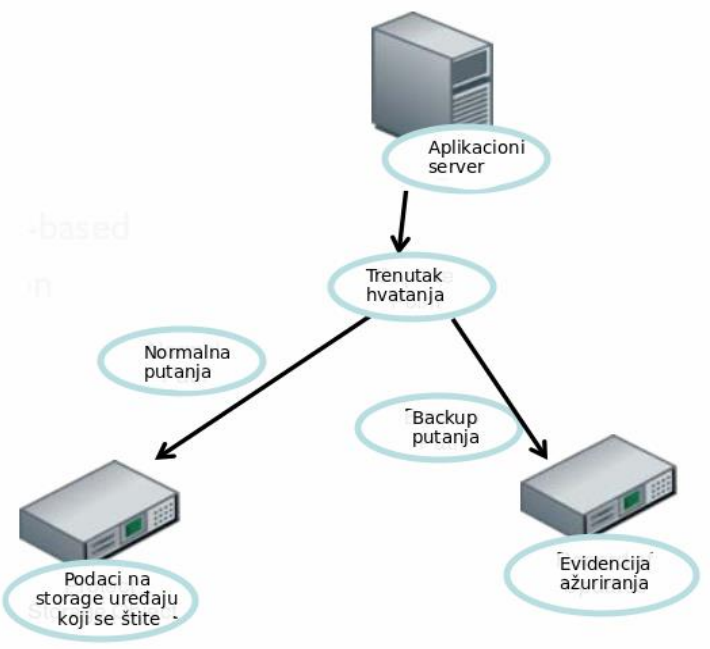
BCV stoji za Business Continuance Volume a termin je prvi put upotrijebljen od strane EMC korporacije. Jednostavnom skriptom na nivou storage uređaja diskovi se repliciraju tako što se napravi klon ili snimak (snapshot) jednog ili grupe diskova koji odmah postaju upotrebljivi kao nezavisna cjelina i mogu se prezentovati bilo kojem serveru istog operativnog sistema. Klonovi moraju biti postavljeni u stanje samo za čitanje *(read-only*) ukoliko se žele upotrijebiti za oporavak podataka, koji se vrši reverzibilnom akcijom kloniranja. Resursi koje uzima BCV kopija su dodatni prostor na storage uređaju namijenjen za klon veličine originalnih diskova. Kako je prostor na storage uređaju ograničen resurs i zahtijeva znatna novčana ulaganja, obično se ovakve kopije smiještaju na sporim i najjeftinijim diskovima. Primjer ovakvog uređaja za skladištenje podataka je EMC storage uređaj VMAX 10K Symmetrix koji je korišćen u ovom radu.

3.3.3 KONTINUALNA ZAŠTITA PODATAKA

Kako IT organizacije sve više razumiju značaj svojih podataka, isključivo backup na trake više nije adekvatan mehanizam za kreiranje rezervnih kopija podataka; ne samo što rastu zahtjevi za administraciju kako broj kopija podataka raste, već se javlja problem brzine, pouzdanosti, fleksibilnosti i jednostavnosti.

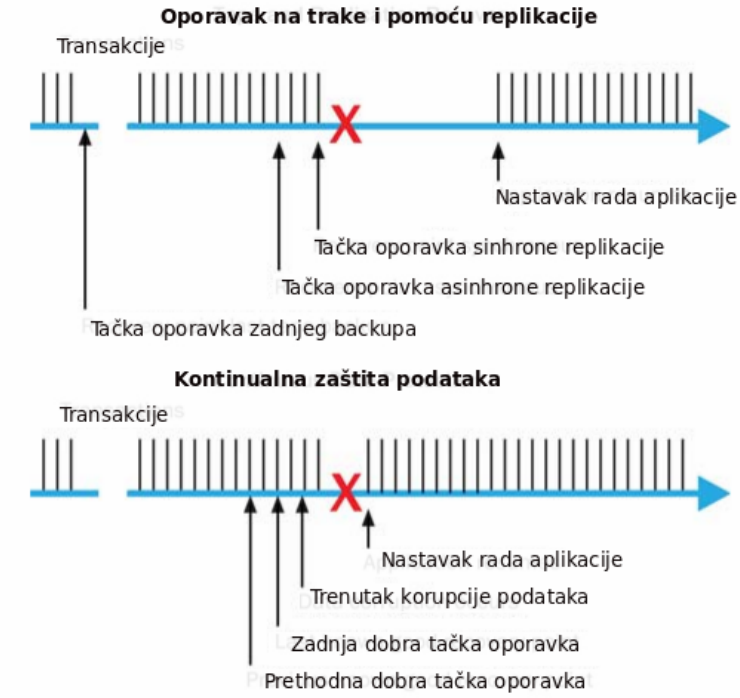
Kontinualna zaštita podataka (*Continuous Data Protection* - CDP) je proces koji omogućava organizacijama da kontinualno prate modifikacije svojih podataka kroz vrijeme čuvajući promjene nezavisno od njihovog izvora i omogućavajući oporavak podataka iz tačno određenog vremenskog trenutka u prošlosti (slika 3.8). CDP sistemi mogu biti zasnovani na bloku, fajlu ili aplikaciji i obezbjeđuju granularnost objekata za koje treba izvršiti operaciju oporavka. CDP koncept smanjuje kompleksnost sistema za zaštitu podataka i eliminiše potrebu za kompletnim, inkrementalnim i diferencijalnim backupom tako što trenutno čuva podatke i kopira ih na disk u realnom vremenu [32].

CDP nije potpuna zamjena za tradicionalni backup već važna komponenta dobro osmišljene strategije za kreiranje rezervnih kopija podataka i njihov oporavak. Tradicionalni mehanizmi za backup i replikaciju podataka obezbjeđuju zaštitu protiv gubitka kompletnog storage uređaja, otkaza sistema, gubitak čitavog datacentra. Nasuprot tome, CDP nije predviđen za oporavak od katastrofe već se fokusira na korupciju podataka koja nastaje prilikom promjena transakcionih podataka u vremenu. CDP se zbog toga nalazi bliže aplikacionom nivou i u velikim datacentrima više različitih CDP jedinica može istovremeno vršiti backup više različitih aplikacija [5].



Slika 3.8: *Implementacija CDP mehanizma za kreiranje rezervnih kopija podataka [21]*

Budući da je prava kontinualna zaštita podataka vođena promjenama podataka umjesto promjenama u vremenu, tačka oporavka (RPO) je promjenjiva. Frekvencija nadgledanja i logovanja promjena podataka se razlikuje od rješenja do rješenja, ali sva CDP rješenja omogućavaju promjenjivu tačku oporavka koja olakšava sami oporavak i osigurava integritet podataka kada aplikacija nastavi sa radom [5].



Slika 3.9: *CDP omogućava finiju granularnost za oporavak podataka u slučaju korupcije*

Na slici 3.9, tačke oporavka za mehanizme backupa na trake i replikacije podataka su vremenski tačno određene. Za traku, tačka oporavka (RPO) je zadnji inkrementalni backup. Za asinhronu replikaciju podataka, tačka oporavka je zadnji završeni upis baferovanog I/O na sekundarni uređaj. Za sinhronu replikaciju podataka, tačka oporavka je zadnja transakcija upisana i na primarni i na sekundarni uređaj, čak iako su ti podaci korumpirani. Vremena oporavka (RTO) su takođe fiksna i za trake zavise od količine podataka koju treba oporaviti, a prilikom replikacije podataka treba logički odvojiti primarni od sekundarnog pristupa podacima.

Promjene podataka koje CDP prati na primarnom storage uređaju se smiještaju na odvojeni storage sistem koji se nalazi ili na lokaciji u glavnom datacentru ili na udaljenoj lokaciji u sekundarnom (DR) datacentru. Količina dodatnog prostora na storage uređaju kojeg zahtijeva CDP je određena brzinom promjena podataka i frekvencijom nadgledanja tih promjena. Periodično nadgledanje zasnovano na tehnologiji snimka (*snapshot*) se zove „skoro CDP“ (*near CDP*) i opisuje se kao „frekventno nadgledanje i praćenje promjena koje nije kontinualno“. Skoro CDP se tako bolje opisuje kao periodična zaštita podataka (*periodic data protection – PDP*). Pravi CDP, nasuprot tome, konstantno prati i bilježi promjene podataka i u skladu sa tim ažurira CDP katalog [5].

3.4. Topologije mreže za kreiranje rezervnih kopija podataka

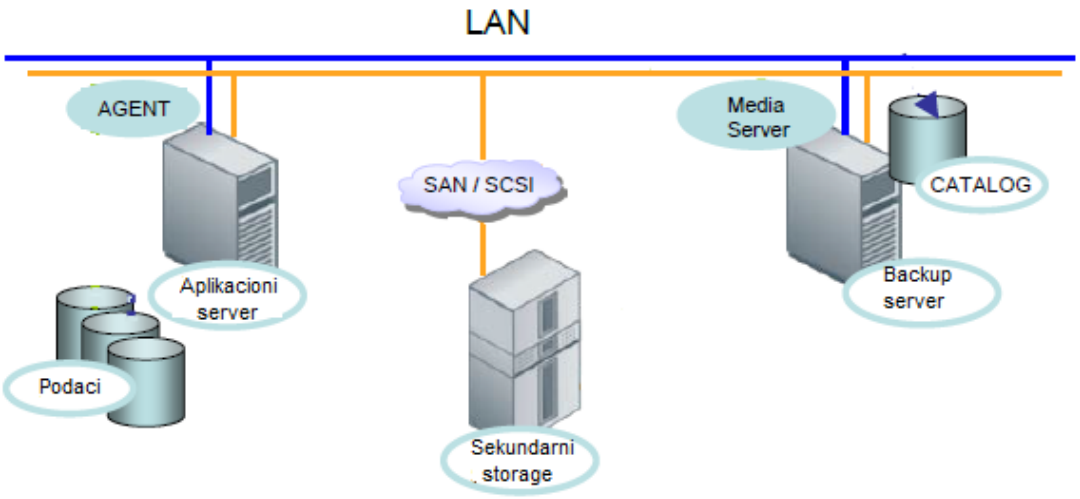
Kreiranje rezervnih kopija podataka na trake je bio jedan od inicijatora za kreiranje SAN tehnologije. Prije pojave SAN mreže, kreiranje rezervnih kopija podataka sa storage uređaja preko Ethernet mreže protoka 100Mb/s je bilo presporo i nije bilo mogućnosti za čuvanje svih potrebnih podataka. Kao i prvi transport preko gigabitne mreže, optička mreža (*Fibre Channel*) je omogućila protok i alternativnu mrežnu infrastrukturu kako bi odvojila backup operacije od LAN mreže. Nakon toga, razvoj tehnologije koja koristi SCSI proširene kopije (*SCSI Extended Copy*) je omogućio kreiranje rezervnih kopija podataka direktno preko SAN mreže i tako oslobodio individualne servere od obavljanja backup operacija [5].

Iako je zadnjih nekoliko godina uvriježeno mišljenje da je backup na trake zastareli način, on i dalje istrajava kao glavni oslonac zaštite podataka [20]. Kada se jednom podaci prebace na traku, ona se može transportovati van datacentra i skladištiti, a ima dovoljan rok trajanja koji može biti i do 30 godina. Čak i datacentri koji koriste novije tehnologije za primarne backup operacije na kraju često implementiraju krajnji backup na trake.

Glavne komponente u mreži predviđenoj za kreiranje rezervnih kopija podataka su:

- **Backup server** - centralni server za kreiranje kopija podataka obično predstavlja jedinstvenu tačku administracije. On sadrži *Metadata* katalog, odnosno informacije o strukturi fajlova i unosima koji su bili kopirani.
- **Media server ili tačka za skladištenje podataka** - skuplja podatke iz Agenta i čita i piše na sekundarni storage uređaj.
- **Agent** - upravlja kolekcijom podataka i *Metadata* katalogom. Obično je to klijent koji se nalazi na serveru čiji se podaci kopiraju (aplikacioni server).
- **Aplikacioni server** - server na kom se nalaze podaci koje treba čuvati. Podaci mogu biti struktuirani ili nestruktuirani.
- **Sekundarni storage uređaj** - ciljani medijum, odnosno destinacija za skladištenje kopija podataka. [21]

Na slici 3.10 dat je pojednostavljen i opšti prikaz glavnih komponenti u topologiji backup mreža. U zavisnosti od topologije, komponente se mogu nalaziti na različitim mjestima u mreži.

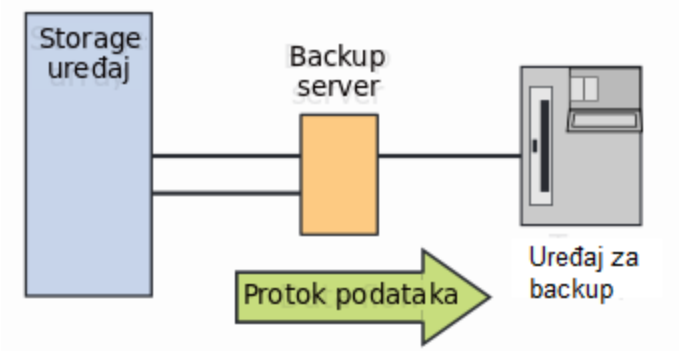


Slika 3.10 : *Glavne komponente u topologiji backup mreže*

U narednim poglavljima su opisane i sistematizovane razne topologije mreža za kreiranje rezervnih kopija podataka.

3.4.1 TOPOLOGIJA DIREKTNO POVEZANOG BACKUP-A

Mnoge organizacije su počele sa jednostavnom backup infrastrukturom koja se naziva direktno povezana (*direct-attached*) ili topologija zasnovana na hostu (*host-based*). Svaki backup klijent ima svoj uređaj za backup, a backup operacije se obavljaju direktno sa diska backup klijenta na njegov uređaj za backup (slika 3.11).



Slika 3.11: *Protok podataka u topologiji direktno povezanog backupa [24]*

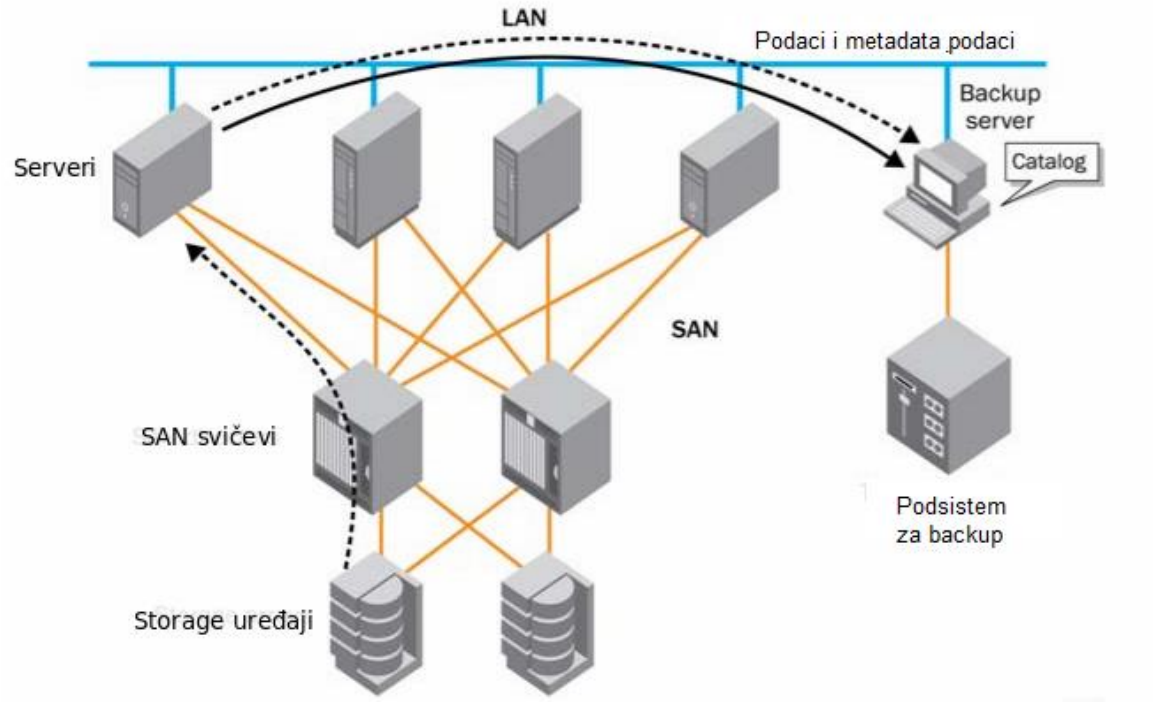
Ključna prednost ovakvog rješenja je brzina. Ovakav pristup optimizuje brzinu kreiranja kopija i njihov oporavak, budući da su uređaji za backup blizu izvora podataka i namijenjeni isključivo hostu. Međutim, ovakav pristup utiče na performanse hosta i aplikacije, pošto kreiranje kopija podataka troši resurse u vidu I/O propusnog opsega, memorije i procesora. Direktno povezana backup topologija je uglavnom predviđena za manje okoline i nikako nije preporučena za veće organizacije. Mane ovakvog pristupa su [24]:

- veliki broj neiskorišćenih traka,
- veliki broj uređaja za backup koji se istovremeno koriste,

- teška upravljivost, u smislu količine uređaja, procesa i alata za kreiranje rezervnih kopija,
- slaba mogućnost nadgledanja backup procesa,
- backup medijumi na raznim lokacijama koji otežavaju postupak oporavka i održavanje kontinuiteta poslovanja.

3.4.2 BACKUP TOPOLOGIJE ZASNOVANE NA LAN MREŽI

U topologiji zasnovanoj na LAN mreži, backup server služi kao repozitorijum za *Metadata* katalog i nalazi se ispred podsistema za backup kao centralna kontrolna tačka za sve backup procese (slika 3.12). Iako metadata podaci ne stvaraju opterećenje na LAN mreži, kontinualni protok gigabajta podataka od produkcionog servera ka backup serveru može značajno oslabiti funkcije aplikacija na LAN mreži. Primarni cilj ovakve topologije je da centralizuje backup resurse.



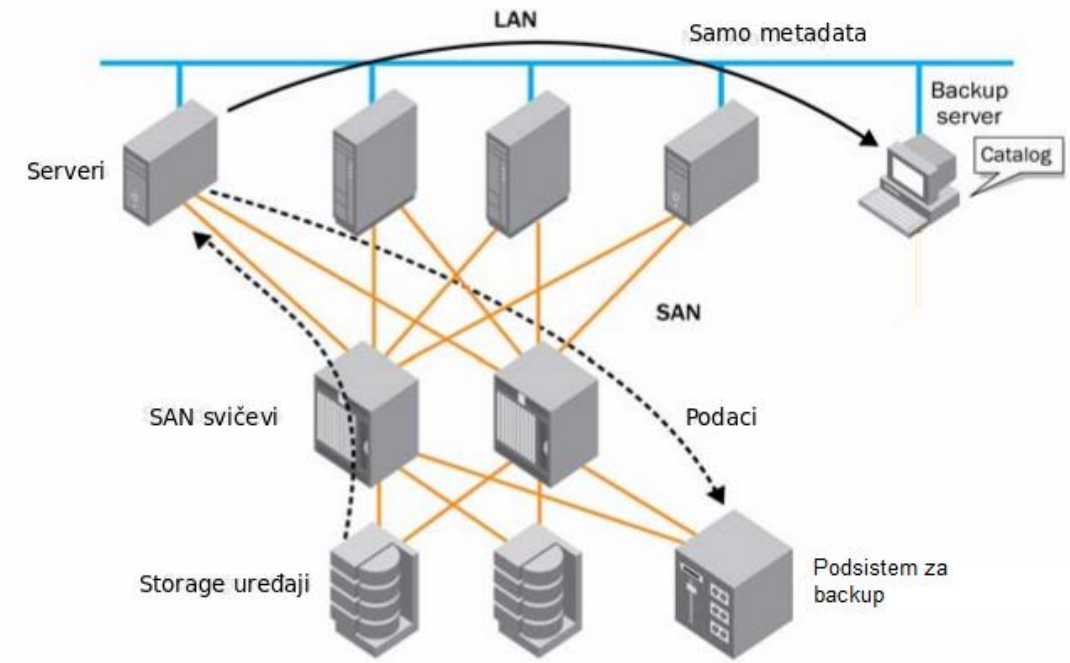
Slika 3.12: *Backup topologija zasnovana na LAN mreži [5]*

Tradicionalna backup rješenja zasnovana na LAN mreži vrše kreiranje rezervnih kopija fajlova. Svaki server na LAN mreži može imati gigabajte na storage uređajima koje treba sačuvati kroz backup. Backup server daje instrukcije svakom aplikacionom serveru preko Agenta da inicira backup proces, šaljući podatke preko LAN mreže backup serveru. Ovakav tip backup procesa uključuje višestruke konverzije; prvo aplikacioni server čita blokove SCSI podataka sa diska, onda ih sastavlja u fajlove i paketira fajlove za slanje preko LAN mreže. Na strani backup servera dolazni paketi se sastavljaju u fajlove, a fajlovi se rastavljaju u blokove kako bi se upisali na trake. Originalni blokovi podataka sa servera čije podatke treba sačuvati se na taj način više puta konvertuju prije nego što se na destinaciji pojave u formi bloka: blok > fajl > paket > fajl > blok. Višak koji stvaraju SCSI i mrežni protokoli značajno utiču na performanse u smislu procesora sa obije strane LAN mreže. Ograničeni protok na LAN mreži (obično 1Gb/s Ethernet) može dodatno povećati backup prozor [5].

3.4.3 BACKUP TOPOLOGIJE ZASNOVANE NA SAN MREŽI

Ideja da se putanja podataka ukloni sa LAN mreže i smjesti u SAN mrežu sa znatno boljim performansama je riješila problem saobraćaja na LAN mreži i ograničenje backup prozora. Ovi faktori su uticali na razvoj SAN mreže u kompanijskim datacentrima.

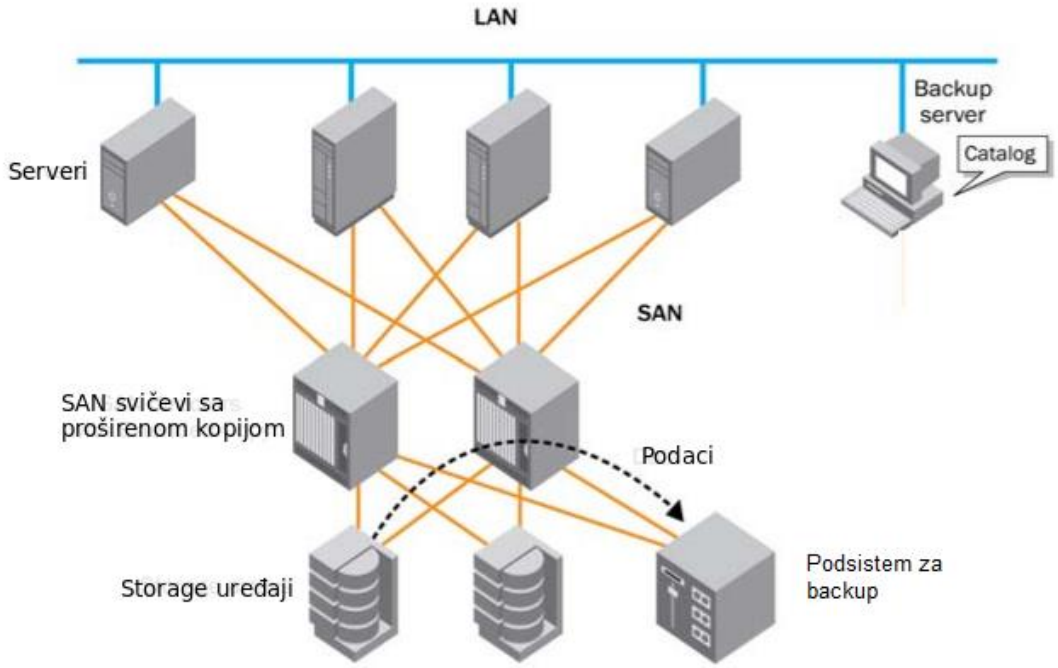
Slika 3.13 ilustruje topologiju backup mreže koja se zasniva na SAN mreži (*LAN-free, SAN-based*). Ciljani podsistem za backup je implementiran na storage mreži kako bi se ostvarila direktnija putanja između produkcionog servera i trake. Metadata i podaci predviđeni za backup su u odvojenim putanjama kako bi se rasteretio saobraćaj u LAN mreži i optimizovao protok backup podataka kroz SAN mrežu. Kao u topologiji koja je zasnovana na LAN mreži, backup server je odgovoran za čuvanje podataka o backup procesu (*metadata*), a razlika je u tome što produkcioni server može zatražiti podatke sa storage uređaja i kopirati ih direktno na podsistem za backup. Kako u ovom slučaju LAN mreža više nije usko grlo, backup prozor postaje mnogo fleksibilniji. Ipak, u oba rješenja (zasnovano na LAN mreži i bez LAN mreže), aplikacioni server ostaje u putanji backup procesa, čitajući podatke sa storage uređaja i upisujući podatke na traku što utiče na njegove performanse [5].



Slika 3.13: *Ilustracija topologije backup mreže bez LAN-a [5]*

3.4.4 TOPOLOGIJA BACKUP MREŽE BEZ SERVERA

Sledeći evolutivni korak u topologiji backup mreža bez LAN-a je topologija bez servera (*Serverless* ili *Server-free*). U ovoj topologiji backup uzima direktniju putanju između storage uređaja i uređaja za backup eliminišući produkcioni server iz backup procesa i putanje kojom se transportuju podaci za backup, oslobađajući tako resurse servera za aplikaciju. Kao što je prikazano na slici 3.14, mehanizam proširene kopije u SAN mreži obavlja ulogu inicijatora i destinacije u ime aplikacionog servera kako bi vršila operacije upisa i čitanja za backup proces. Mehanizam proširene kopije se može nalaziti u SAN svičevima, može biti dodatni uređaj povezan na SAN ili ubačen u podsistem za backup. Backup server je još uvijek neophodan kako bi upravljao metapodacima i nadgledao status backup procesa [5].



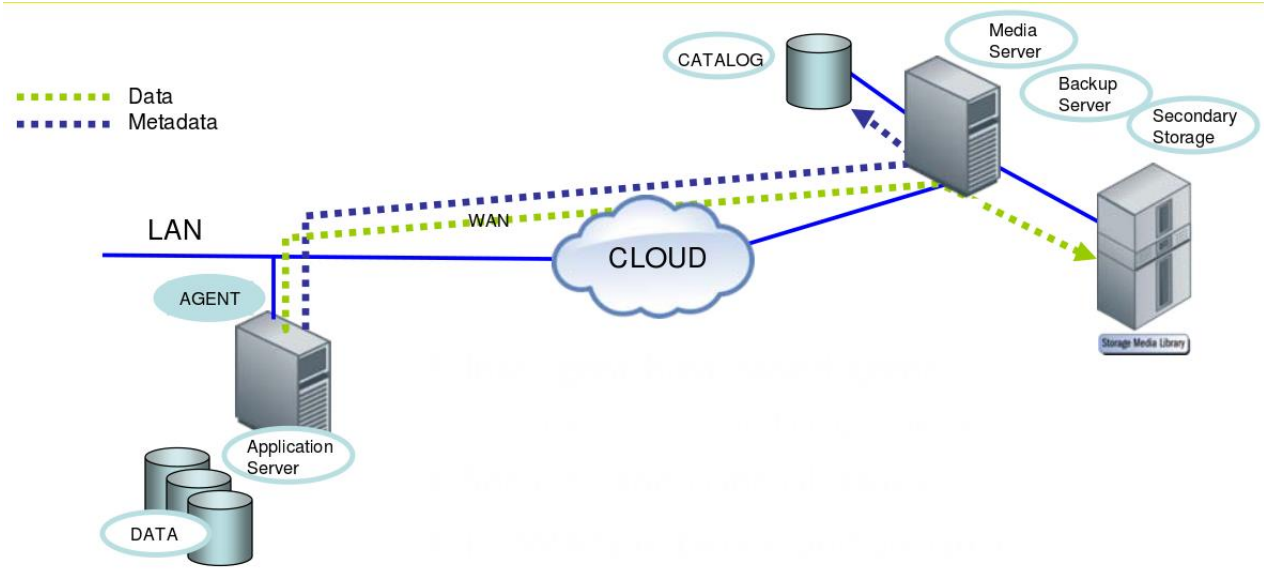
Slika 3.14: *Ilustracija topologije backup mreže bez servera [5]*

3.5. Backup u oblaku (Cloud backup)

Obim podataka je značajno porastao u zadnjoj dekadi i iako su tehnologije za skladištenje podataka postale relativno dostupne, ne mogu izdržati trku sa ovim porastom. Ekspanzija storage infrastrukture je kontinualan i skup proces. Oslobađanje prostora na storage uređajima nikada nije laka odluka, budući da treba ispoštovati poslovne i regulatorne zahtjeve a istovremeno posjedovati efektivne mehanizme za backup i oporavak od nesreće. Tradicionalni način kreiranja rezervnih kopija podataka i njihov oporavak je veoma skup i zahtjevan iz više razloga koji uključuju održavanje infrastrukture, cijenu rada, cijenu nekretnina, dodavanje i poboljšavanje postojeće infrastrukture, kao i rizik od nesreća koje mogu postaviti velike zahtjeve postojećim strategijama i mehanizmima za skladištenje podataka [33].

Kompanije koje obezbjeđuju backup servis prebacuju enkriptovane podatke pomoću sigurnih mrežnih protokola u udaljene datacentre koristeći posebne izlazne tačke iz mreže (*cloud storage gateways),* i u jednom potezu podaci se arhiviraju, backupuju i štite od nesreća. Na slici 3.15 je dat primjer kreiranja rezervnih kopija podataka u oblaku. Podaci se sa aplikacionog servera pomoću agenta koji kontroliše proces prebacuju preko WAN mreže na infrastrukturu za backup koja se nalazi na udaljenoj lokaciji u datacentru kompanije koja pruža backup servis [21]. Agent je inteligentni klijent koji se nalazi na aplikacionom serveru i čuva promjene i jedinstvene blokove. Većina rješenja posjeduje mogućnost „snimka“ („*snapshot*“) i time olakšava povraćaj podataka sa udaljene lokacije u slučaju otkaza.

Skladištenje podataka u oblaku je uzrokovalo značajne promjene na polju *backup* i *recovery* tehnologija. Kako posjeduje značajne prednosti u smislu skalabilnosti, fleksibilnosti, dostupnosti, mogućnosti nadgledanja i cijene, vjeruje se da ima budućnost u mnogim organizacijama [34]. Može biti lak, jednostavan i pristupačan način da se kreiraju rezervne kopije podataka i skladište van datacentra.



Slika 3.15: *Kreiranje rezervnih kopija podataka u oblaku [21]*

Vrlo je važno da kompanije imaju jasnu viziju i strategiju kad implementiraju rješenja u oblaku. Iako je to sigurna i pristupačna opcija, prebacivanje podataka kompletnog poslovanja u oblak se može pokazati vrlo riskantnim. Bezbjednost podataka, konzistencija aplikacija, zaštita podataka, nejasni SLA ugovori i podrška su neki od problema kojih kompanija mora biti svjesna prilikom izbora kompanije koja pruža backup servis. Ipak, kako količina podataka u kompanijama raste vjeruje se da je ovo rješenje budućnosti [33], kao i tendencija da se primarno skladište podataka (*storage*) takođe prebaci u oblak.

3.6. Aplikacije za kreiranje rezervnih kopija podataka

Dok visoko performantna SAN infrastruktura i dodatni servisi, kao što je proširena kopija, olakšavaju efikasno kreiranje rezervnih kopija podataka sa storage uređaja, aplikacija koja inicira i upravlja backup procesom može varirati od proizvođača do proizvođača. Nekad je teško potvrditi uspješnost backup operacije i validnost traka koje su potrebne za proces oporavka. Dodatno, standardne operacije za kreiranje rezervnih kopija podataka mogu čuvati različite kopije podataka koje se vremenom nisu mijenjale i tako povećati količinu backup podataka i dužinu trajanja backup procesa. Proizvođači aplikacija za kreiranje rezervnih kopija podataka svojim softverima ugrađuju dodatne servise kao što su verifikacija, snimak aktivne baze podataka, deduplikacija podataka, backup na bazi promijenjenih blokova, itd.. Kako količina podataka za backup raste, zadatak sigurnog kreiranja rezervnih kopija podataka u prihvatljivom vremenskom intervalu postaje sve teži [5].

Većina IT organizacija koristi tradicionalne aplikacije za backup i oporavak podataka koje upravljaju backup infrastrukturom. One se zasnivaju na jednom ili više tipova servera za backup i backup klijenata. Klijenti za backup se instaliraju na serverima čije podatke treba čuvati i podaci se šalju kroz ethernet ili FC infrastrukturu backup serveru, koji ih onda skladišti na specijalne uređaje predviđene za backup. Primjeri takvog rješenja su komercijalni softveri IBM Tivoli Storage Manager (TSM), Symantec NetBackup (NBU), EMC NetWorker, CommVault Simpana i HP Data Protector. Samim tim što su fleksibilni, skalabilni i ne zavise od elemenata u infrastrukturi, ovakva rješenja zahtjevaju velike resurse i nije ih lako promijeniti nakon što se

implementiraju. Podržavaju veliki broj operativnih sistema, jednostavna su za korišćenje i dobro organizovana pomoću kataloga i drugih raspoloživih konfiguracionih fajlova. [1].

3.6.1 METODE PRISTUPA PODACIMA PREDVIĐENIM ZA ZAŠTITU

Aplikacije za kreiranje rezervnih kopija podataka mogu vršiti kopiranje podataka sa primarnog diska na više načina:

- **Backup na nivou fajla** - Bilo koja promjena na fajlu će uzrokovati ponovni backup čitavog fajla. Otvoreni fajlovi često zahtijevaju poseban tretman softvera kako se ne bi zaobišli u procesu ili nekonzistentno kopirali. Prednosti su lakoća izvršavanja operacija backup i restore, a mane su prenos ogromne količine podataka.
- **Backup na nivou bloka** - Kopiraju se samo blokovi u fajlu koji su promijenjeni. Zbog toga mora postojati klijent koji prati i otkriva promjene na blokovima. Prednosti su smanjena količina podataka predviđena za backup, smanjeni uticaj na mrežu, brzina, dok su mane povećana kompleksnost i uticaj na performanse na strani na kojoj se nalazi klijent [21].

U tabeli 3.2 je dat primjer mehanizama za zaštitu podataka zasnovanih na bloku i njihova uporedna analiza u smislu vrijednosti parametara RPO i RTO.

Tabela 3.2: *Mehanizmi zaštite podataka zasnovani na bloku [5]*

Tip zaštite podataka	Zaštita protiv	RTO	RPO
RAID	Otkaza diska	Trenutna	Bez gubitaka
Ogledanje (Mirror)	Otkaza linka, diska ili niza diskova	Trenutna	Bez gubitaka
Pravi CDP	Korupcije podataka	Sekunde, minuti	Bez gubitaka
Skoro CDP/Snimak	Korupcije podataka	Sekunde, minuti	Mali gubitak
Sinhrona replikacija	Sistemski otkaz	Sekunde, minuti	Bez gubitaka
Asinhrona replikacija	Sistemski otkaz	Sekunde, minuti	Mali gubitak
D2D emulacija traka	Otkaz storage uređaja	Minuti	Gubitak od zadnjeg backupa
Lokalni backup na trake	Otkaz storage uređaja	Minuti - sati	Gubitak od zadnjeg backupa

3.6.2 KONZISTENCIJA PODATAKA PRILIKOM KREIRANJA REZERVNIH KOPIJA PODATAKA

Aplikacija je konzistentna kada su podaci potpuni i validni u istoj tački u vremenu. Konzistencija kreiranih kopija predviđenih za backup se postiže na nekoliko načina:

- **Hladni backup *(Cold ili Offline backup)*** - predstavlja backup kada je aplikacija ugašena. Gašenjem aplikacije osigurava se konzistencija podataka, keš podaci su iskopirani na disk a sve transakcije ugašene. Mane su veliki backup prozor, a prednosti jednostavnost i pristupačnost u cijeni.
- **Atomski ili backup otporan na otkaze *(Crash consistent backup)*** - predstavlja snimak kompletne aplikacije u istom trenutku vremena, a ne obuhvata snimak memorije ni I/O operacija koje tek treba da se obrade. Ovo je metod koji najčešće koriste

komercijalni softveri i često je dovoljan za oporavak aplikacija koje ne zavise od baze podataka. Nema backup prozor.

- **Backup konzistentne aplikacije *(Application consistent ili Online backup)*** - predstavlja backup aplikacije dok je aktivna, a moguće je neke njene djelove postaviti u ugašeno stanje (*offline*). Uglavnom se koristi za aplikacije koje nemaju backup prozor i moraju biti dostupne 24x7. Primjer ovakvog backupa je baza podataka koja se postavlja u posebno „stanje za backup“ (*backup mode*) u kom nema promjena nad njenim fajlovima već isključivo u kešu i u logovima. Nakon backup operacije, sve promjene zapisane u kešu i logovima se primjenjuju na odgovarajuće podatke u bazi. Ovaj backup obezbjeđuje potpunu konzistentnost [22, 23].

3.6.3 TRADICIONALNI TIPOVI KREIRANJA REZERVNIH KOPIJA PODATAKA

Aplikacije za kreiranje rezervnih kopija podataka se moraju nositi sa različitim tipovima podataka različite važnosti, na različitim klijentima, serverima, storage uređajima, sa odgovarajućim nivoom obezbjeđenja za podatke koji se kopiraju. Zbog bolje performantnosti i efikasnosti, aplikacije omogućavaju razne tehnike za smanjenje količine podataka koja se mora čuvati. Iako svaka aplikacija ima svoj sistem za vršenje backup operacije, tri opšta tipa backup procesa se implementiraju i uglavnom koriste u većini programa:

- Kompletni backup
- Inkrementalni backup
- Diferencijalni backup

3.6.3.1 Kompletni (Full) backup

Kompletni backup je početna pozicija svih ostalih backupa i sadrži sve podatke u direktorijumima i fajlovima koji su selektovani da budu kopirani. Pošto kompletni backupi sadrže sve informacije, češći kompletni backupi uzrokuju jednostavnije i brže operacije oporavka. Međutim, kompletni backup zauzima i najviše prostora i veličina mu uvijek raste, budući da sadrži kompletnu sliku izvornih podataka [35].

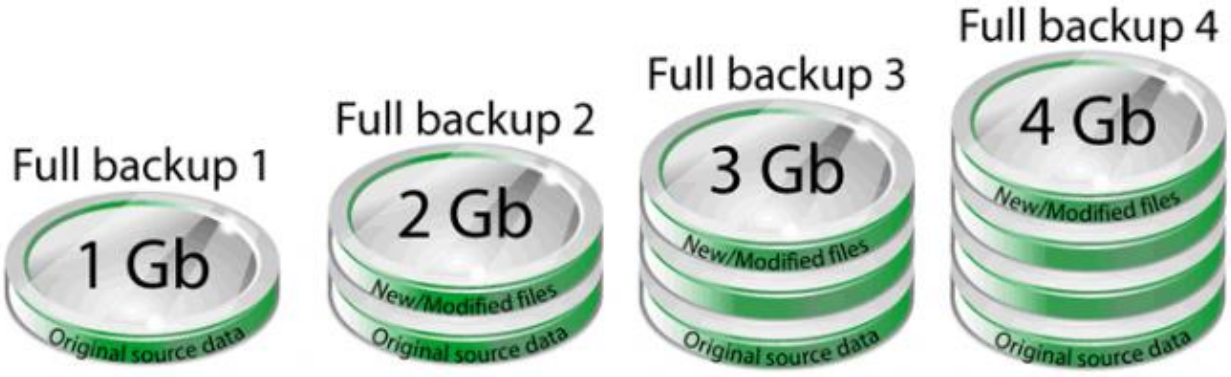
Prednosti su:

1. Restore je najbrži;
2. Svi kopirani podaci su smješteni na jednom mjestu i omogućavaju jednostavnije rukovanje prostorom, tako da ovaj tip backupa nudi najviše zaštite.

Mane su:

1. Proces kopiranja podataka je najsporiji u poređenju sa ostalim tipovima backupa, budući da treba kopirati kompletnu količinu podataka;
2. Zahtjevi za prostorom za skladištenje podataka su najveći u poređenju sa drugim tipovima backup procesa. U današnje vrijeme diskovi ne moraju biti skupi, tako da ova stavka ima malo uticaja prilikom dizajniranja rješenja.

Na slici 3.16 je dat prikaz zauzeća prostora prilikom kompletnog backupa za proces koji bi se izvršio 4 puta:



Slika 3.16: *Ilustracija rasta zauzeća prostora prilikom kompletnog backupa [35]*

3.6.3.2 Inkrementalni backup

Inkrementalni backup čuva sve promjene koje su se desile od zadnjeg backupa, bez obzira na tip. Najmanje vremena mu je potrebno da završi operacije backupa budući da kopira samo razlike. Na osnovu toga je nazvan inkrementalni backup, svaki backup je inkrement prethodnog backupa [35].

Prednosti inkrementalnog backupa su:

1. najbrži tip backupa;
2. čuva prostor za skladištenje podataka u poređenju sa drugim tipovima;
3. svaki backup inkrement može sadržati različitu verziju fajla.

Mane ovakvog backupa su:

1. kompletna restore operacija je mnogo sporija u poređenju sa ostalim tipovima backupa; za kompletni restore potreban je kompletan backup i svi inkrementi nakon toga;
2. kako bi se oporavila zadnja verzija individualnog fajla, prvo se mora pronaći inkrement koji to sadrži.

Na sledećoj slici je dat prikaz zauzetog prostora prilikom inkrementalnog backupa za proces koji bi se izvršio 4 puta:

Slika 3.17: *Ilustracija rasta zauzeća prostora prilikom inkrementalnog backupa [35]*

Restore operacija može trajati jako dugo, jer sistem mora pronaći zadnji kompletni backup kao i svaki inkrementalni backup koji je napravljen od zadnjeg kompletnog backupa.

3.6.3.3 Diferencijalni backup

Diferencijalni backup čuva sve promjene koje su se desile od zadnjeg kompletnog backupa. Time je znatno skraćeno vrijeme za restore u odnosu na inkrementalni backup. Ipak, ako se diferencijalni backup izvrši veliki broj puta, njegova veličina može premašiti veličinu određenu kompletnim backupom [35].

Prednosti diferencijalnog backupa su:

1. restore operacija je brža nego restore operacija inkrementalnog backupa, jer su potrebna samo dva fajla, zadnji kompletan backup i zadnji diferencijalni;
2. manje vremena je potrebno za ovaj tip backupa nego za kompletni backup;
3. zahtjevi za prostorom za skladištenje podataka su manji u poređenju sa prostorom kojeg zahtijeva kompletni backup.

Mane su:

1. restore operacija je sporija nego kod kompletnog backupa;
2. proces kopiranja podataka je sporiji u poređenju sa inkrementalnim backupom;
3. zahtjevi za prostorom za skladištenje podataka su veći u poređenju sa prostorom kojeg zahtijeva inkrementalni backup.

Diferencijalni backup treba koristiti ako postoji dovoljno vremena za izvršavanje backupa. Na sledećoj slici je dat prikaz diferencijalnog backupa u smislu zauzeća prostora za proces koji bi se izvršio 4 puta:

Slika 3.18: *Ilustracija rasta zauzeća prostora prilikom diferencijalnog backupa*

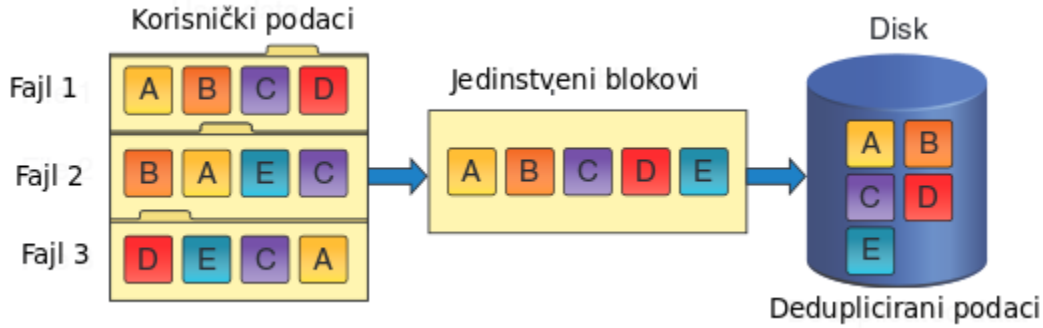
3.6.4 DEDUPLIKACIJA

Na prostorima za skladištenje, velika količina podataka je redudantna ili malo izmijenjena u odnosu na neki drugi blok podataka. Postoji mnogo tehnika koje eliminišu redudansu među podacima, a jedna od najpopularnijih je deduplikacija podataka [28]. Tokom prethodnih godina, ova metoda je postala standardna funkcionalnost u softverima za backup i uređajima za backup zasnovanim na disku.

Deduplikacija podataka je metoda koja čuva prostor na storage uređaju eliminišući redudantne podatke. Na storage medijumu kao što je disk čuva se samo jedna jedinstvena instanca podatka. Redudantni podatak je zamijenjen pokazivačem na taj jedinstveni podatak.

Deduplikacija se vrši na fajlovima. Bilo koji redudantni podatak u fajlovima se čuva samo jednom. Proces deduplikacije pretražuje sve fajlove koji imaju redudantne djelove

podataka i čuva samo jedinstvene blokove u disku, dodajući pokazivač kad god se blok ponovi. Kao rezultat toga, smanjuje se kapacitet potreban za skladištenje fajlova. Stvarno smanjenje podataka predviđeno za čuvanje može značajno varirati od organizacije do organizacije i od aplikacije do aplikacije, a zavisi od brojnih faktora od kojih su najvažniji: brzina kojom se podaci mijenjaju, frekvencija backup procesa i arhiviranja i koliko dugo podaci treba da su dostupni. Uglavnom se postižu nivoi redukcije podataka od 10:1 do 50:1 [28].



Slika 3.19: *Ilustracija procesa deduplikacije podataka*

Na slici 3.19 je prikazan proces deduplikacije podataka [24]. Algoritam deduplikacije detektuje podatak koji se ponavlja tako što kreira kriptografski *hash* podataka za skladištenje. *Hash* je prikaz fiksne dužine poruke proizvoljne dužine. Na ovaj način se smanjuje kompleksnost poređenja dva bloka podataka ili dva zapisa, jer je veličina *hash*-a mnogo manja od veličine samog podatka. Za svaki dolazeći zapis, prvo se računa *hash* a onda traži u bazi već postojećih hash zapisa na sistemu. Ako unos postoji, znači da postoji i podatak, tako da se kreira samo referenca na podatak umjesto skladištenja kompletnog podatka. U suprotnom, čitav podatak se skladišti na disku a hash upisuje u svoju bazu [28].

Prednosti deduplikacije su:

- Smanjeni zahtjevi za prostorom za skladištenje, dakle smanjeni zahtjevi za diskovima, napajanjem i rashladnim uređajima;
- Duži periodi čuvanja diskova;
- Smanjena količina podataka koja se šalje preko mreže.

Nedostatak ovog procesa može biti uticaj na performanse sistema kada je veliki procenat dedupliciranih podataka. Zbog toga se ova metoda uglavnom primjenjuje u rješenjima za backup i arhiviranje podataka više nego u primarnim storage rješenjima. Takođe, čin deduplikacije transformiše inicijalne podatke i tako unosi određenu dozu rizika da podaci nisu konzistentni.

3.7. Virtuelizacija prostora na uređajima za skladištenje podataka

Virtuelizacija prostora obezbjeđuje logičku apstrakciju fizičkog prostora za skladištenje. To je jednostavna, konzistentna prezentacija kompleksne infrastrukture cjelinama koje koriste te resurse [43]. Još 2001. godine, SNIA organizacija je uspostavila definiciju termina „virtuelizacija“ kako bi omogućila krajnjim korisnicima i proizvođačima storage uređaja jedinstveno tlo za diskusiju ove teme [42]. SNIA definicije virtuelizacije prostora su:

- Čin apstrakcije, prikrivanja ili izolovanja internih funkcija *storage* podsistema ili servisa od aplikacije, host računara ili opšteg mrežnog resursa u svrhu omogućavanja aplikaciji upravljanje prostorom ili podacima nezavisno od mreže.

- Aplikacija virtuelizacije *storage* servisa ili uređaja u svrhu ujedinjavanja funkcija ili uređaja kako bi se sakrila kompleksnost ili dodale nove mogućnosti nižim nivoima storage resursa.

Storage tehnologije igraju važnu ulogu u povećanju performansi, dostupnosti i upravljivosti prostorom na uređajima za skladištenje podataka [41]. Uglavnom, tri su osnovne prednosti virtuelizacije [42]:

- Unapređenje u upravljanju prostorom za skladištenje u heterogenim IT okolinama;
- Unapređenje dostupnosti i eliminacija prekida funkcionalnosti pomoću automatskog upravljanja;
- Unaprijeđeno iskorišćenje prostora na uređajima.

Ukoliko se storage infrastruktura posmatra kao niz tehnologija od kojih svaki nivo ima svoju ulogu u transformaciji I/O zahtjeva, mogu se izdvojiti tri pristupa virtuelizacije prostora:

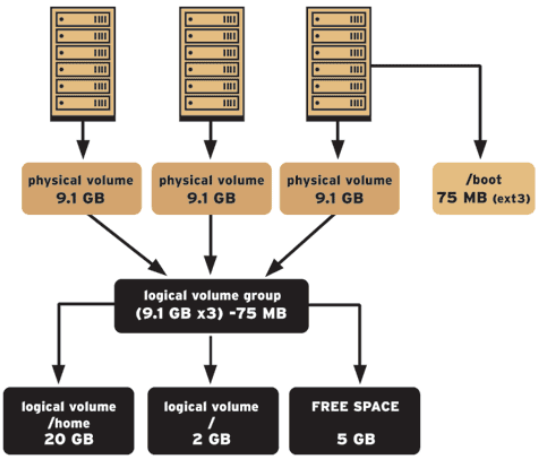
- Virtuelizacija na nivou hosta;
- Virtuelizacija na nivou storage sistema;
- Virtuelizacija na nivou mreže.

3.7.1 VIRTUELIZACIJA PROSTORA NA NIVOU SERVERA

Jedna od najranijih formi virtuelizacije prostora nije potekla iz storage infrastrukture već od servera, odnosno serverskog operativnog sistema [44]. Tip virtuelizacije prostora na nivou servera je uglavnom povezan sa alatima za logičko upravljanje volumenima (*Volume Manager*) koji se nalaze na serverima, sa različitim nivoima sofisticiranosti u zavisnosti od operativnog sistema. Najčešće se upotrebljavaju u sledećim slučajevima [42]:

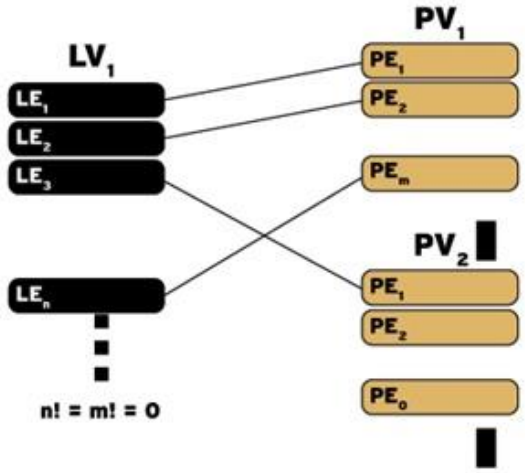
- Za agregaciju fizičkog prostora u formi više LUN-ova kako bi se formirao jedan veliki LUN koji operativni sistem vidi kao jedan disk;
- Za implementaciju softverskog RAID-a i ostalih naprednih funkcionalnosti, uključujući snimke i udaljenu replikaciju;
- Za upravljanje i održavanje disk resursa koji su pod kontrolom operativnog sistema.

Jedan od vrlo važnih alata na Linuxu je upravo *Logical Volume Manager (LVM)* koji služi za kreiranje logičkog prostora nad fizičkim prostorom i upravljanje njime.



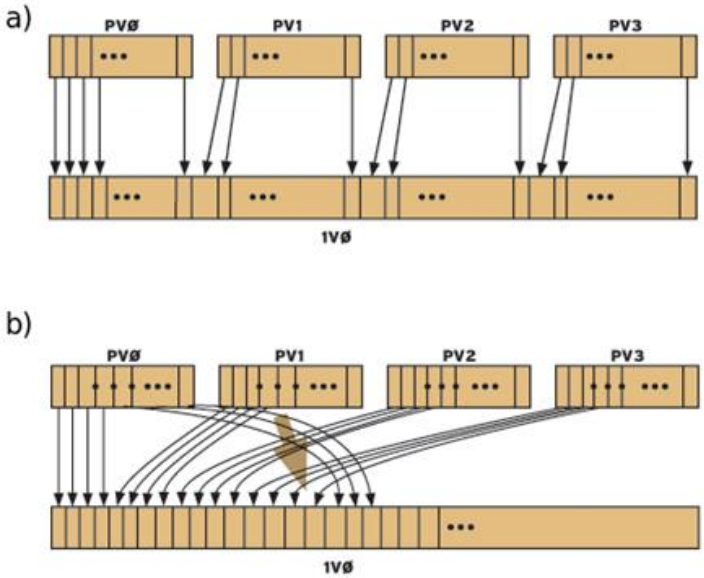
Slika 3.20: *Unutrašnja organizacija prostora pomoću LVMa*

Pomoću LVM alata, „logičke“ particije se protežu preko fizičkih hard diskova i može im se mijenjati veličina po potrebi. Fizički disk se dijeli na jedan ili više fizičkih volumena (*physical volume - pv*), a onda se kreiraju logičke grupe volumena (*volume group – vg*) kombinujući fizičke volumene kao što je prikazano na slici 3.20. Logička grupa volumena može biti skup fizičkih volumena sačinjenih od mnoštva fizičkih diskova [41].



Slika 3.21: *Mapiranje logičkih jedinica na fizičke jedinice*

Svaki PV se sastoji od određenog broja fizičkih jedinica fiksne veličine (*physical extent – PE*); na sličan način svaki LV se sastoji od određenog broja logičkih jedinica fiksne veličine (*logical extent – LE*). LE i PE su uvijek iste veličine, a podrazumijevana vrijednost na odgovarajućem Linux kernelu je 4MB. LV se kreira tako što se logičke jedinice mapiraju na fizičke jedinice tako da se reference na logičke blokove razrješavaju na fizičkim blokovima. Cilj ovakvog mapiranja je postizanje odgovarajućih performansi, skalabilnosti i dostupnosti [41]. Na slici 3.21 je prikazano mapiranje logičkih prostora na fizičke prostore.



Slika 3.22.a) *LVM linearno mapiranje*
b) *LVM mapiranje u linijama (4 fizička prostora po liniji)*

Na primjer, nekoliko PV jedinica se može objediniti u jedan veliki logički volumen (LV) kao što je prikazano na slici 3.22.a. Ovaj pristup se naziva linearno mapiranje i dozvoljava kreiranje fajlsistema na više različitih diskova. Drugi pristup je linijsko mapiranje (*striped mapping*) u kom se linije (grupe susjednih fizičkih jedinica) drugih PV mapiraju na jedan LV, kao što je prikazano na slici 3.22.b. Linijsko mapiranje dozvoljava jednom LV da postigne kombinovane performanse dva PV i često se koristi kako bi se postigle veće brzine prenosa podataka sa i na diskove [41].

Kroz ove različite tipove logičko-fizičkih mapiranja, LVM postiže 4 važne prednosti nad običnim fizičkim particionisanjem [41]:

1. Veličina logičkih volumena se može mijenjati *online* dok im pristupa fajlsistem ili baza, tako da ne postoji funkcionalni prekid prilikom promjene prostora.
2. Podaci (potencijalno korumpirani ili oštećeni) sa jednog fizičkog uređaja se mogu migrirati na drugi uređaj koji je noviji, brži ili otporniji, dok je originalni volumen u funkciji i dostupan.
3. Logički volumeni se mogu kontruisati dodavanjem fizičkih diskova kako bi se povećale performanse (pomoću linijskog mapiranja) ili obezbijedila redudansa (pomoću ogledanja diskova).
4. Moguće je kreirati snimke logičkih volumena (LV) kako bi se obezbijedila slika prostora u određenom trenutku vremena i kreirala precizna kopija.

Mane ovakvog pristupa su takođe višestruke:

1. Kompleksna administracija na samom hostu budući da se rezervacija prostora mora izvršiti na svakom hostu pojedinačno [42].
2. Kompleksna administracija usljed toga što svaki operativni sistem implementira različiti tip fajlsistema i alata za upravljanje volumenima [44].
3. Proces upravljanja diskovima oduzima aplikacijama značajne resurse u vidu CPU i memorije [44].
4. Otežan i nestabilan proces podizanja operativnog sistema usljed bug grešaka na samom LVM alatu koji je inkorporiran u operativni sistem [45].
5. Na sporim medijumima (kao što su magnetni diskovi) koji moraju da pretražuju praznine među PE jedinicama za vrijeme velikih sekvencijalnih upisa ili čitanja, smanjene su I/O performanse usljed eksterne fragmentacije kada se PE jedinice na storage uređajima ne alociraju uzastopno [45].

3.7.2 VIRTUELIZACIJA NA NIVOU STORAGE SISTEMA

Storage uređaji visoke klase su uvijek imali mogućnosti virtuelizacije kako bi unaprijedili resurse fizičkog prostora. Jedan od takvih primjera je RAID funkcionalnost koju posjeduje skoro svaki storage uređaj nezavisno od klase, funkcionalnost snimka, ili virtuelizacija prednjih portova za konekciju kako bi se omogućilo višestrukim operativnim sistemima da koriste isti fizički port [44].

Virtuelizacija na nivou storage sistema ne zavisi od tipa servera omogućavajući tako storage uređaju podršku za heterogene servere bez obzira na operativni sistem ili aplikaciju koja se na njima nalazi. Mana ovakvog pristupa je ta da se funkcije virtuelizacije ograničavaju na jedan uređaj; npr. izvorni volumen koji je korišćen za snimak i sami snimak održava isti uređaj, a snimak postaje neupotrebljiv u slučaju hardverskog otkaza. U nekim slučajevima funkcije virtuelizacije se pružaju na nekoliko različitih uređaja, ali su ova rješenja ipak ograničena na uređaje istog proizvođača [42].

Često se tehnologije virtuelizacije na hostu i na storage sistemu kombinuju kako bi se omogućila fleksibilnost LVM alata na nivou servera i performanse hardverske RAID funkcionalnosti [42].

3.7.3 VIRTUELIZACIJA NA NIVOU MREŽE

Prednosti prethodna dva pristupa virtuelizaciji se mogu kombinovati kako bi se omogućila virtuelizacija na nivou SAN strukture. Virtuelizacija na nivou mreže podržava upravljanje prostorom na nivou datacentra i u stanju je da podrži heterogeni SAN sa širokom paletom host platformi i storage uređaja. Obično se implementira koristeći specijalizovani uređaj „crna kutija“ (*black-box*) u SAN strukturi i agent koji se instalira na hostu (u zavisnosti od načina implementacije virtuelizacije). Tipične funkcije koje uključuje ovakav pristup virtuelizacije su:

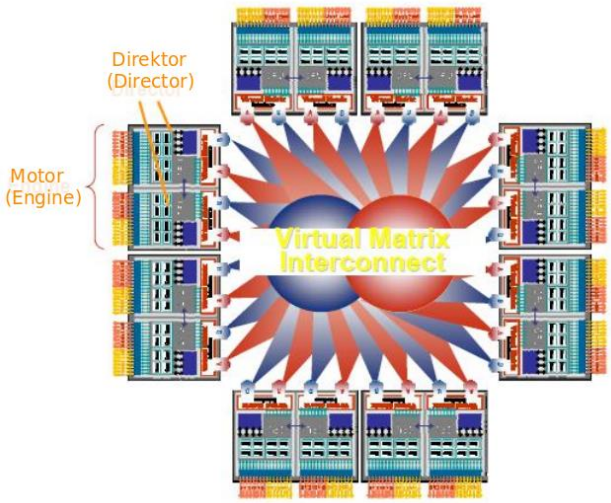
- Kombinovanje nekoliko LUN-ova sa jednog ili više različitih uređaja u jedan LUN prije predstavljanja hostu;
- Dijeljenje jednog LUN-a sa storage uređaja u više malih virtuelnih LUN-ova i predstavljanje različitim hostovima;
- Sinhrona i asinhrona replikacija u SAN mreži kao i preko WAN linkova;
- Sigurnost uređaja kako bi se obezbijedio pristup LUN-u tačno određenom hostu

Ostale funkcije uključuju keširanje, napredno upravljanje volumenima, prostor za skladištenje na zahjtev i QoS funkcionalnosti, a njihova dostupnost varira i zavisi od proizvođača opreme.

3.8. Primjer uređaja za skladištenje rezervnih kopija podataka

Cilj storage rješenja je da budu povoljna, performantna, skalabilna i pouzdana. Primjer storage uređaja visoke klase (eng. *high-end*) koji će biti korišćen u ovom radu je VMAX 10k Symmetrix proizvođača EMC. Njegova arhitektura skalabilno obezbjeđuje performanse i kapacitet pomoću Symmetrix VMAX motora (*engine*) koji čine cjeline za izgradnju u okviru storage uređaja. Svaki motor ima dvostruki integrisani *Virtual Matrix Director* koji obezbjeđuje sopstveni CPU, memoriju, keš resurse zajedno sa portovima na prednjoj strani prema hostu i portovima na zadnjoj strani prema fižičkom prostoru za skladištenje (slika 3.23).

Slika 3.23: *Arhitektura storage uređaja*



U jednom storage uređaju može biti do 8 motora koji su potpuno međusobno povezani dijeleći resurse radi boljeg iskorištenja kapaciteta i boljih performansi [38].

Fundamentalni fizički prostor za skladištenje u VMAX sistemu se sastoji od 3 osnovna nivoa za skladištenje koji počivaju na različitim tehnologijama diskova, od najbolje performantnih do najlošije performantnih [38]:

- **Nivo 1 – SSD diskovi (*EMC Flash Drives* - EFD)**
- **Nivo 2 – FC diskovi (*Fibre Channel Drives)***
- **Nivo 3 – SATA diskovi (*SATA II 7200 RPM)***

Ovako dimenzionisani nivoi skladištenja obezbjeđuju najoptimalnije performanse i cijenu po gigabajtu na osnovu čega se u zavisnosti od važnosti podataka određuje tip koji će se smiještati na pojedinačnim nivoima. Nivoi fizičkog skladišta se implementiraju pomoću različitih RAID nivoa (npr. RAID 1, RAID5 (3+1) ili (7+1) i RAID6 (6+2) ili (14+2)) ili pomoću virtuelne RAID arhitekture, naprednog mehanizma pomoću kojeg se RAID nivoi virtuelno mijenjaju. Automatsko nivelisanje se postiže kroz FAST/VP mehanizam ugrađen u storage uređaj koji nadgleda iskorišćenje raspoloživog prostora na različitim diskovima i omogućava migraciju podataka kroz različite nivoe u zavisnosti od količine operacija za čitanje i upis nad određenim podacima. Podaci kojima se češće pristupa se migriraju na veći nivo, dok se podaci koji se puno ne koriste migriraju na niži nivo [38].

Pet najznačajnijih karakteristika diskova su kapacitet, cijena, tip interfejsa (npr. SCSI, ATA, FC, SATA), performanse (npr. vrijeme pristupa, IOPS, vrijeme prenosa) i pouzdanost [39]. SSD (*Solid State Drives*) diskovi zahvaljujući silikonskoj tehnologiji bez pokretnih djelova značajno skraćuju vrijeme odgovora i time nude najbolje performanse u odnosu na ostale diskove. Izuzetno su značajni za aplikacije (npr. Oracle baze podataka) kojima trebaju visoke performanse u vidu što manjeg kašnjenja prilikom pristupa podacima i što veće mogućnosti za izvršenje input/output operacija po sekundi (IOPS). Ipak, u odnosu na ostale diskove izuzetno su skupi i mnogo su manjeg kapaciteta [40].

FC i SATA su hard diskovi koji koriste *Fibre Channel* i *Serial ATA* tehnologije respektivno za komunikaciju sa storage uređajem. SATA diskovi su veliki, spori diskovi sa najdužim vremenom odziva u odnosu na ostale diskove i zbog toga su i najslabiji. U tabeli 3.3 je dato poređenje među diskovima zastupljenim na konkretnom storage uređaju, gdje se jasno vidi razlika u performansama i kapacitetu.

Tip diska	Vrijeme odziva operacija čitanja	Kapacitet
SSD	1ms	200GB
15K FC	6ms	450GB
SATA	12ms	2TB

Tabela 3.3: *Poređenje diskova po performansama i kapacitetu*

Funkcionalnosti storage uređaja variraju u zavisnosti od proizvođača i modela. Nekada su ovakvi uređaji bili jednostavne kutije sa fizičkim diskovima, dok su danas sofisticirani računari sa mogućnošću virtuelizacije prostora. Razvijene su razne opcije pomoću kojih se trenutno kreiraju replike produkcionog prostora koje se mogu upotrijebiti u razne svrhe; za razvoj aplikacije, u testne svrhe, izvještavanje, kao i za backup podataka.

4. Predlog heterogenog rješenja za backup i recovery podataka na Linux sistemima

Neophodno je pažljivo planirati svaki aspekt sistema za kreiranje rezervnih kopija podataka i sa stanovišta parametara usvojenih u strategiji i sa stanovišta funkcionalnosti. U ovom poglavlju predloženo je heterogeno rješenje za kreiranje rezervnih kopija standardnih tipova podataka i baza podataka na Linux sistemima. Predlog se zasniva na D2D2T modelu kreiranja rezervnih kopija podataka koji kombinuje prednosti diska i trake kako bi se optimizovao backup proces, unaprijedila pouzdanost backup materijala i smanjilo vrijeme oporavka.

U kompanijama sa razvijenim informacionim sistemom gdje postoji integrisana backup (*„tape" SAN*) infrastruktura, praksa je da se primarna rezervna kopija čuva na trakama. Mana ovakvog pristupa je dugotrajnost restore operacije za velike količine podataka koja može trajati nekoliko sati ili čak čitav dan. U slučaju prestanka funkcionalnosti servisa, kada se poslovanje mora oporaviti u najkraćem mogućem roku, restore operacija sa trake ne može zadovoljiti zahtjevnije DR parametre. Zbog toga se predlog zasniva na uvođenju još jednog koraka u čitav proces, takozvani „backup u nivoima" (eng. *disk staging*) koji prvo kopira podatke na disk kao primarni medijum, a zatim se pomoću već postojeće backup infrastrukture podaci smiještaju na trake koje predstavljaju sekundarni medijum.

Cilj je obezbijediti brzi pristup backup materijalu na diskovima u slučaju kada je potrebna restore operacija i kreirati dugotrajni backup na trakama koji je izdržljiviji. Na ovaj način se dobijaju dva ista backup materijala, na različitim medijumima, od kojih svaki obezbjeđuje prednosti za ono za šta je namijenjen; backup na diskovima nudi brzi restore u slučaju potrebe, dok backup na trakama omogućava dugoročno skladištenje podataka. Iako se za ovakav tip backup procesa troši dva puta više prostora, to obezbjeđuje dodatnu redudansu i sigurnost da su podaci očuvani. Ova metoda se koristi za kreiranje rezervnih kopija raznih tipova podataka, ali se proces na prvom nivou kopiranja sa diska na disk razlikuje u zavisnosti od tipa podataka čije se rezervne kopije čuvaju. Različiti tipovi podataka kao što su standardni fajlovi i Oracle baze podataka zahtijevaju različit pristup pri izradi strategije za kreiranje rezervnih kopija podataka u zavisnosti od svojih funkcija i osobina i na to treba posebno obratiti pažnju prilikom izbora tehnologije za backup.

Budući da je proces kreiranja rezervnih kopija podataka na trake standardizovan proces u backup infrastrukturi opisan u poglavlju 3.6, ovaj rad će se fokusirati na procedure primarnog backupa koje odgovaraju D2D mehanizmu a variraju u zavisnosti od tipa podataka. Za primarni backup standardnih podataka predložen je model kreiranja rezervnih kopija podataka koji pomoću *open source* alata preko LAN mreže kopira podatke sa originalne lokacije na objedinjenu backup lokaciju koja se nalazi na diskovima na storage uređaju. Za primarni backup baze podataka predložen je koncept potpunog snimka, odnosno kloniranje diskova na kojima se nalazi baza podataka na nivou storage uređaja. Poželjno je da se originalna i backup lokacija nalaze na različitim storage uređajima, čime se uvodi nivo zaštite u slučaju otkaza samog uređaja ili pristupnih portova. Ukoliko su i primarni i sekundarni podaci na istom storage uređaju, zaštita je predviđena samo usljed korupcije podataka ljudskom intervencijom, ali ne i usljed svih tipova hardverskog otkaza. U ovom predlogu koristiće se jedinstveni storage uređaj za primarni backup podataka, budući da se sekundarni backup smiješta na trake u backup infrastrukturi koja je na odvojenoj lokaciji u odnosu na originalne podatke i primarni backup materijal.

Nakon implementacije novog sistema u IS kompaniji, pristupa se planiranju i implementaciji rješenja za kreiranje rezervnih kopija podataka za taj sistem. Kako za svaki novi

sistem treba obezbijediti infrastrukturu za funkcionisanje nove aplikacije, tako treba obezbijediti način i kapacitete za kreiranje rezervnih kopija podataka u skladu sa politikom kompanije.

Ulazni podaci uslovljeni politikom kompanije i infrastrukturom koja već postoji u kompaniji odgovaraju na pitanja „makro“ i „mikro“ pristupa izrade strategije za kreiranje rezervnih kopija podataka [poglavlje 2.5.]. To su parametri koje treba pažljivo analizirati i koji određuju smjer razvoja predloga za kreiranje rezervnih kopija:

- Frekvencija backup operacija, period zaštite podataka i vrijeme oporavka koji proističu iz RTO i RPO parametara;
- Preporučena infrastruktura;
- Količina i kategorije podataka predviđenih za backup;
- Dostupni alati za kreiranje rezervih kopija podataka;
- Način skladištenja rezervnih kopija podataka.

4.1. Frekvencija backup operacija i period zaštite podataka

Nakon utvrđivanja RTO i RPO parametara za svaki tip podataka, prema njima kompanije u sklopu svoje politike o očuvanju i zaštiti podataka definišu frekvenciju backup operacija, period zaštite podataka i vrijeme oporavka. Predlog heterogenog rješenja obuhvata tri tipa podataka koji se različito tretiraju u zavisnosti od njihove funkcije i tipa servisa:

- sistemski podaci,
- aplikacioni podaci,
- baze podataka.

Na Linuxu se sistemski i aplikacioni podaci posmatraju kao standardni fajlovi, a servisi se mogu čuvati kao obični fajlovi prostim kopiranjem [poglavlje 2.3, Backup standardnih fajlova i servisa]. Za razliku od Linux operativnog sistema, npr. Windows operativni sistem i aplikacije na njemu je bolje čuvati kao sliku, odnosno bit-po-bit kopiju čitavog sistema [eng. *image*].

Često kompanije usvajaju politiku koju generalizuju u odnosu na tip podataka. Tako npr. politika kompanije može biti da je frekvencija pravljenja kopija sistemskih podataka jednom mjesečno i da se čuvaju zadnje dvije kopije. Za podatke aplikacije u produkciji uglavnom se usvaja politika kreiranja dnevnog inkrementalnog backupa, a potpuni backup se sprovodi jednom sedmično sa periodom zaštite od 2 sedmice.

Rješenje koje se predlaže uvodi primarni nivo backup mehanizma za standardne podatke D2D čiji period zaštite može biti do nekoliko dana u zavisnosti od potrebe i prostora raspoloživog za čuvanje rezervnih kopija. Ovaj parametar se definiše u skripti koja kreira proces backup operacije, dok se frekvencija backup operacije definiše u crontab fajlu. Raspon frekvencije backup operacije može biti od nekoliko puta dnevno do jednom u nekoliko dana. To znači da broj backup materijala kompletnog sistema koji se čuva odgovara periodu zaštite pomnoženom sa frekvencijom backup operacija. Nakon toga treba primijeniti sekundarni backup na trake koji treba da prati usvojenu politiku kompanije za određeni tip podatka.

Pored kopija standardnih podataka, često je potrebno obezbijediti konzistentan i siguran backup baze podataka u izuzetno zahtjevnoj okolini koja ne dozvoljava prekid poslovanja. Operacije kreiranja rezervnih kopija baze podataka i njen oporavak mogu biti izuzetno zahtjevne zato što je kompletan sistem u stvari veliki skup referenci. Njihova veličina može dostizati nekoliko TB, a moraju se čuvati u cjelini kako bi ostali konzistentni.

Za baze podataka se definiše drugačija politika čuvanja podataka u odnosu na sistemske i podatke aplikacije. Usvojena politika kompanije za ovaj tip podataka može uključivati kombinaciju različitih tipova backupa, npr. da se inkrementalni backup baze vrši svakodnevno sa

periodom zaštite 13 dana, potpuni backup se vrši sedmično sa periodom zaštite 4 sedmice, dok se jednom mjesečno vrši potpuni backup koji se čuva permanentno. Za ovakav vid zaštite i čuvanja rezervnih kopija, budući da su neophodni veliki resursi u vidu prostora, mora postojati namijenjena backup infrastruktura koja kopije čuva na trakama.

Rješenje koje se predlaže za bazu podataka uvodi primarni nivo D2D backup mehanizma koji kreira klon, nakon čega se standardnim postupkom po usvojenoj politici može sa klona kreirati sekundarna kopija baze podataka na trake. Predlaže se svakodnevno osvježavanje klon sesije, što znači da u tom slučaju postoji samo jedna kopija primarnog backup materijala i ona se mijenja jednom dnevno.

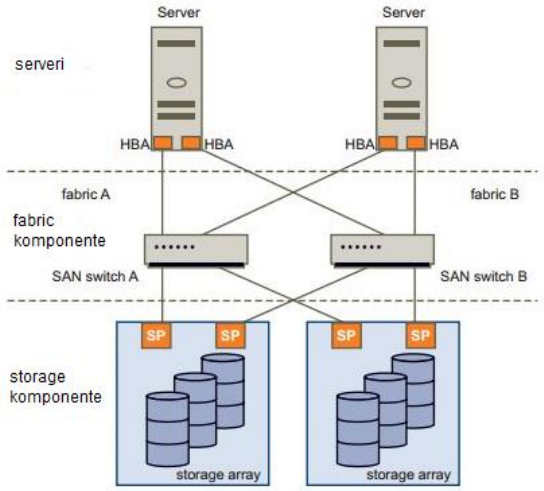
4.2. Preporučena infrastruktura

Heterogeno rješenje uključuje kreiranje potpunih rezervnih kopija više servera koji pripadaju jednoj logičkoj cjelini na kojima se nalazi prioritetna aplikacija. Serveri mogu biti različitih konfiguracija. Na serverima treba da bude instaliran Linux operativni sistem baziran na RPM sistemu za pakovanje paketa (*Red Hat Package Manager*), poželjno RHEL ili Centos. Zbog optimalnog iskorišćenja resursa, operativni sistem na serverima treba da bude instaliran sa minimumom potrebnih programa za funkcionisanje bez grafičkog interfejsa. Na taj način se smanjuje količina podataka predviđena za sistemski backup.

Imena svih servera i njihove IP adrese treba da budu definisane na korporativnom DNS uređaju radi lakše administracije i međusobne komunikacije. Kako velika količina podataka koja se prenosi tokom backup operacija ne bi zauzela kapacitete LAN mreže koja je neohodna za pravilno funkcionisanje prioritetnog servisa, po mogućstvu treba izabrati servere tako da posjeduju više mrežnih interfejsa. Primarni mrežni interfejsi se tako koriste za funkcionisanje glavne aplikacije, a dodatni gigabitni mrežni adapteri služe isključivo za backup operacije. Na taj način se backup saobraćaj izoluje i rasterećuje mreža za funkcionisanje glavne aplikacije. Aliasi imena servera koji odgovaraju dodatnim mrežnim adapterima i njihove IP adrese takođe treba definisati na korporativnom DNS uređaju i koristiti ih u daljem definisanju strategije i implementacije rješenja za kreiranje rezervnih kopija podataka. IP adrese interfejsa predviđenih za backup na svim serverima treba definisati tako da se nalaze u istoj VLAN mreži kao i IP adresa backup servera kako bi se izbjegao uticaj *firewall* uređaja na performanse mreže.

Pojednostavljena topologija preporučene SAN mreže je prikazana na Slici 4.1 [49]. Kostur SAN topologije po pravilu čine FC (*Fibre Channel* - optički) sviječevi koji treba da budu u paru zbog redudanse, formirajući dvije strukture (*fabric*). Heterogeno rješenje se oslanja na postojanje storage uređaja koje je povezano na SAN i opisano u poglavlju 3.8. Preporuka je da svi serveri imaju ugrađene HBA (*Host Bus Adapter*) kartice koje su povezane na SAN (*Storage Area Network*) optičku infrastrukturu, primarno zbog toga da bi serverima bio dostupan prostor na storage uređaju. Svi uređaji se preko HBA kartica povezuju i na jednu i na drugu strukturu. Na FC sviču treba kreirati zone u kojima se nalaze portovi servera i kontrolera na storage uređaju kako bi se omogućila vidljivost servera i prostora na storage uređaju. *Fibre Channel* (FC) infrastruktura se implementira prema preporukama iz poglavlja 3.2, kako bi bila redudantna i visoko dostupna, poštujući pravila koncepta „bez tačke prekida“.

Da bi kompanije mogle da odgovore na zahtjeve i standarde koje kreiraju trendovi i politika kompanije, poželjno je da posjeduju backup infrastrukturu. Predlog heterogenog rješenja se zasniva na postojanju backup infrastrukture kroz koju se kreiraju sekundarne kopije podataka koje se smiještaju na trake. Uopšteno o backup infrastrukturi dato je u poglavlju 3.1.



Slika 4.1: *Topologija FC SAN infrastrukture*

4.3. Kategorije podataka predviđene za kreiranje rezervnih kopija podataka

Specijalizovani softveri za backup koji upravljaju backup infrastrukturom uglavnom pružaju podršku za različite tipove podataka. Međutim, budući da se primarni backup D2D ne oslanja na specijalizovani softver koji bi podatke skladištio na specijalnim uređajima predviđenim za backup, već na mehanizme koji skladište podatke na storage uređaju, svaka kategorija podataka se mora posebno analizirati. Predlog heterogenog rješenja uključuje dvije najčešće kategorije podataka na Linux operativnim sistemima, standardne podatke i baze podataka.

4.3.1 STANDARDNI FAJLOVI

Kako predlog rješenja za standardne podatke pripada tipu backupa na nivou fajla, jer se zasniva na kopiranju fajlova preko LAN mreže, tako je potrebno analizirati podatke sa strane operativnog sistema i na nivou fajla.

Prosto, sa stanovišta kreiranja rezervnih kopija podataka, Linux operativni sistem se sastoji isključivo od standardnih fajlova. Postoji nekoliko vrsta fajlova na Linuxu: regularni fajl, direktorijum, link, karakter specijalni fajl, imenovani pipe i blok uređaj; međutim nije potrebno kreirati rezervne kopije svih tipova standardnih podataka.

Npr. direktorijumi su fajlovi sa listom imena ostalih fajlova u njemu. Da bi se kreirale rezervne kopije standardnih podataka, potrebno je kreirati rezervne kopije pojedinačnih fajlsistema koji sadrže regularne fajlove i direktorijume. Fajlsistem je u stvari direktorijum sa imenom mount-point direktorijuma određenog volumena. Prilikom izvršavanja backup operacije treba preskočiti nekoliko direktorijuma na root (/) particiji kao što su /dev, /sys, /media, /proc, /lost+found, jer sadrže specijalne tipove fajlova i ostale koji nisu regularni fajlovi. Ovi fajlovi nisu potrebni za oporavak sistema, već ih generiše kernel automatski prilikom svakog podizanja sistema.

Standardni fajlovi se po kategoriji aplikacija i servisa mogu podijeliti na sistemske fajlove u vlasništvu *super-user* korisnika (*root*) i korisničke fajlove, odnosno fajlove u vlasništvu aplikacije. Kao preporuka najbolje prakse, sistemski fajlovi se uglavnom smještaju na lokalnim

diskovima, dok se fajlovi aplikacije smiještaju na diskovima na storage sistemu koji su vidljivi odgovarajućem serveru. Da bi se osigurao backup standardnih fajlova, dovoljno je napraviti njihovu prostu kopiju dok je fajl zatvoren i niko mu ne pristupa i sačuvati je.

4.3.2 FIZIČKA STRUKTURA BAZE

Predlog rješenja za baze podataka pripada tipu backupa na nivou bloka, jer se zasniva na kreiranju klon sesije koja podatke kopira na nivou storage uređaja. Zbog toga je potrebno analizirati podatke sa strane storage uređaja odnosno organizacije diskova, ali je takođe potrebno znati koji fajlovi su ključni za funkcionisanje baze i gdje se nalaze.

Baza podataka je skup podataka koji se posmatraju kao cjelina. Svrha baze podataka je čuvanje i pristup određenim informacijama i ona je ključ dobro organizovanih informacija. Uglavnom server baze pouzdano upravlja velikom količinom podataka u višekorisničkom okruženju tako da više korisnika može istovremeno pristupati istim podacima. Takve operacije nisu moguće sa standardnim fajlovima. Kako bi se dao predlog za kreiranje rezervnih kopija baze podataka, treba detaljno analizirati njenu strukturu. U nastavku rada je predstavljena struktura Oracle baze podataka kao primjer, budući da je ona često osnova kritičnih aplikacija koje funkcionišu na Linux operativnom sistemu u velikim IS kompanijama [64].

Vrlo je važno osigurati konzistentnu kopiju baze podataka. Konzistentnost podataka se odnosi na tačnost i integritet podataka i kopija podataka. Specijalizovani softveri za backup podataka uglavnom imaju ugrađene funkcionalnosti za backup Oracle baze podataka.

Fajlovi koji čine Oracle bazu podataka su organizovani na sledeći način [51]:

- **Kontrolni fajlovi** - Sadrže podatke o samoj bazi odnosno informacije o njenoj fizičkoj strukturi. Ovi podaci su kritični i bez njih se ne mogu otvoriti „fajlovi sa podacima“ kako bi se pristupilo podacima u bazi. Mogu sadržati i metapodatke vezane za backup baze.
- **Fajlovi sa podacima** - Sadrže korisničke ili aplikacione podatke baze podataka kao i metapodatke.
- **Online redo log fajlovi** - Dozvoljavaju oporavak instance baze podataka. Ukoliko baza prestane da funkcioniše usljed neke greške i nijedan fajl nije izgubljen, instanca može oporaviti bazu pomoću informacija u ovim fajlovima.

Dodatni fajlovi koji su važni za uspješno funkcionisanje Oracle baze podataka su:

- **Parameter fajl** - definiše kako je instanca konfigurisana i kada se pokreće.
- **Fajl sa šiframa** - dozvoljava sistemskim korisnicima administraciju baze udaljenim pristupom.
- **Backup fajlovi** - se koriste za oporavak baze usljed oštećenog hardvera ili ukoliko se obrišu ili oštete originalni fajlovi.
- **Arhivirani redo log fajlovi** - sadrže aktuelnu istoriju promjena nad podacima (redo) koje generiše instanca. Pomoću ovih fajlova i backup fajlova baze moguće je oporaviti izgubljene fajlove sa podacima.

Oracle baza posjeduje integrisani alat „rman backup“. On je osnova svih specijalizovanih tradicionalnih alata za backup baza podataka opisanih u poglavlju 3.6. „RMAN backup“ komanda podržava backup sljedećih tipova fajlova:

- Datafajlovi i kontrolni fajlovi,
- Server parameter fajlovi,
- Arhivirani redo log fajlovi,
- RMAN backup fajl.

Iako baza zavisi i od drugih tipova fajlova, kao što su mrežni konfiguracioni fajlovi, fajlovi koji sadrže šifre, sadržaj Oracle home direktorijuma, ovi fajlovi se ne čuvaju pomoću RMANa, već kao standardni fajlovi [52].

Prilikom izvršavanja operacije kreiranja rezervnih kopija baze podataka za vrijeme njenog funkcionisanja bilo kojim specijalizovanim softverom za backup, neophodno je fajlove sa podacima postaviti u takozvani „backup status“ (*backup mode* ili *hot backup mode*). Kada se baza nalazi u ovom statusu, slika kompletnog bloka se upisuje u redo log fajlovima prije njegove modifikacije kako bi se osigurala konzistentnost kompletne baze [Backup konzistentne aplikacije, poglavlje 3.6.2]. Ukoliko se backup baze izvršava pomoću RMAN alata, nije potrebno postavljati bazu u ovaj status, jer ovaj alat poznaje strukturu baze i format blokova sa podacima, tako da neće kreirati kopije oštećenih blokova koji nastaju nepotpunim ažuriranjem podataka [52].

4.4. Alati za kreiranje rezervnih kopija podataka

Za bilo koji tip backup operacije potreban je alat za backup. Alat može biti komercijalni softver ili određena *open source* komanda na Linuxu, a i komercijalni softver može biti skup komandi koji se izvršavaju na komandnoj liniji Linux operativnog sistema. Da bi komanda na linuxu mogla da obavlja automatizovanu funkciju backup operacije, potrebno je da se upakuje u formu skripte.

Skripta predstavlja skup komandi koje se smiještaju u običan tekstualni fajl sa pravima izvršavanja. Ljuska (eng. shell) čita ovaj fajl i izvršava komande kao da se nalaze na komandnoj liniji. *GNU/Linux shell* (ljuska) je poseban interaktivni program koji omogućava korisnicima da pokreću programe, upravljaju fajlovima na fajlsistemu i procesima na Linux sistemu. To je interfejs operativnom sistemu koji se ponaša kao komandni interpreter.

Postoji mnogo različitih tipova shell-ova na Linuxu, svaki napravljen da služi nekoj posebnoj svrsi i sa svojom istorijom. Većina Linux distribucija sadrži više od jednog shell-a, iako je uvijek jedan osnovni i glavni. Neki shell-ovi su korisniji za kreiranje skripti i programa, dok su drugi bolji za upravljanje procesima. Ovo su dva osnovna tipa shell-a korišćena u daljem razmatranju:

- ***Bash shell (/bin/bash)*** – osnovni (*default*) komandni interpreter u svim Linux distribucijama razvijen u okviru GNU projekta kao zamjena za standardni Unix shell. Nazvan je po tvorcu prvobitnog shella na Unixu Stivu Bournu, a samo ime „*Bourne again shell*“ je igra riječi koja znači „ponovo rođeni shell“. Sve više postaje popularan medju tradicionalnim Unix korisnicima. Takođe je osnovni shell u Cygwin okruženju, koje obezbjeđuje GNU alate pod Microsoft Windows operativnim sistemom [37].
- ***Korn shell (ksh)*** – programski shell kompatibilan sa bash-om koji podržava napredne programske funkcije kao što su asocijativni nizovi i operacije sa realnim brojevima (*floating-point* aritmetika). Napisan je od strane Davida Korna, 1983. godine. Uveliko se koristi kako za skripte, tako i za interaktivno izvršavanje komandi. Zajedničke funkcionalnosti ksh i Bourne shella su iskorišćene za definisanje POSIX standarda za */bin/sh.*

Predlog heterogenog rješenja se bazira na skriptama koje se postavljaju na backup serveru i u sebi integrišu alate koji pokreću proces za backup podataka. Skripta koja izvršava backup standardnih podataka na Linux operativnom sistemu uključujući i sistemske podatke je pisana u *bash shell* interpreteru, dok je skup skripti koji kreira klon baze podataka napisan u *korn shell* interpreteru. Skripte treba da budu neinteraktivne kako bi se mogle postaviti u *crontab* fajl za automatsko i periodično izvršavanje.

4.4.1 ALATI ZA KREIRANJE REZERVNIH KOPIJA STANDARDNIH PODATAKA

Na Linux operativnom sistemu postoji nekoliko raspoloživih komandi koje mogu kopirati standardne podatke u zavisnosti od potreba i zahtjeva. U procesu razmatranja alata koji bi bili podesni za backup velikog broja podataka, uzete su u obzir tri komande: *scp, tar i rsync.* Sve tri komande su potpuno različitog koncepta, iako se sve mogu koristiti za backup podataka. Ovo su njihove osnovne karakteristike:

- ***scp*** - označava sigurno kopiranje (eng. *secure copy*) i služi za sigurni transfer podataka između uređaja na mreži. Funkcioniše po istom principu kao cp komanda, sa tom razlikom što su kod scp komande izvor ili destinacija udaljeni uređaj.
- ***tar*** - standardni alat koji služi za arhiviranje podataka na Unixu. On takođe označava i format fajla kojeg obrađuje taj alat. Inicijalno razvijen kako bi pisao podatke na sekvencijalnim I/O uređajima kao što su trake za backup, u današnje vrijeme se koristi kako bi se veliki broj fajlova sakupio u jedan veći fajl i tako distribuirao ili pohranio, čuvajući sistemske informacije kao što su prava korisnika i grupa, datumi i strukture direktorijuma [61]. Kako je kompresija vrlo mala, pomoću *tar* komande se ne štedi značajno prostor.
- ***rsync*** - *Rsync* je backup alat na komandnoj liniji, koji može da izvršava D2D backup lokalno i na udaljenoj mašini i pri tom čuva sistemski specifične atribute kao što su prava, datumi, ACL, strukture direktorijuma, itd. Poznat je po svom *delta-transfer* algoritmu koji smanjuje količinu podataka predviđenu za prenos preko mreže i tako šalje samo razlike između izvornih fajlova i već postojećih fajlova na destinaciji [50]. Za razliku od Windows operativnog sistema koji koristi archive bit kako bi utvrdio da li je fajl već prošao kroz proces backupa, *rsync* na Linuxu pronalazi fajlove koji su promijenili veličinu ili zadnje modifikovano vrijeme i njih prenosi, dok ostale atribute mijenja direktno na destinacionim fajlovima ukoliko algoritam pokaže da fajlove ne treba ažurirati.

Alati *scp* i *rsync* su u svom izvornom obliku zasnovani na SSH protokolu, a samim tim koriste iste metode autentikacije i obezbjeđuju jednak nivo sigurnosti. Komandu *tar* treba kombinovati sa *ssh* komandom kako bi se ostvario prenos arhiviranih podataka preko LAN mreže.

Budući da se predlog rješenja za kreiranje rezervnih kopija standardnih podataka zasniva na kopiranju podataka preko LAN mreže, preporuka je testirati brzinu i vrijeme koje je potrebno za prenos podataka od izvora do destinacije za svaki od navedenih alata. Informacija koja se dobije na taj način može biti vrlo korisna pri izboru adekvatnog alata za kreiranje rezervnih kopija standardnih podataka.

Za validaciju heterogenog rješenja predlaže se testna okolina koja se sastoji od dva servera koji su povezani gigabitnim kablom na isti mrežni uređaj, što je najjednostavnija i najčešća varijanta LAN mreže. Za simuliranje stvarnog okruženja i strukture direktorijuma stvarnog skupa podataka, predlaže se kreiranje šest različitih struktura fajlova približno jednake ukupne veličine 8GB. Na taj način je osmišljeno šest testnih scenarija sa različitim strukturama fajlova, kako bi se utvrdilo koja je najbolja opcija za prenos velike količine podataka i koliko brzina prenosa zavisi od organizacije fajlova koje treba prenijeti kroz LAN mrežu.

Za kreiranje prvog fajla može se koristiti dd komanda koja fajl popunjava slučajnim podacima kako ne bi došlo do kompresije podataka i to za svaki scenario pojedinačno:

1. za kreiranje fajla 8GB # dd if=/dev/urandom of=output.8gb bs=64M count=128
2. za kreiranje fajla 800MB # dd if=/dev/urandom of=output.800mb bs=64M count=13
3. za kreiranje fajla 80MB # dd if=/dev/urandom of=output.80mb bs=8M count=10

4. za kreiranje fajla 8MB # dd if=/dev/urandom of=output.80mb bs=1M count=8
5. za kreiranje fajla 800KB # dd if=/dev/urandom of=output.800k bs=800 count=1024
6. za kreiranje fajla 80KB # dd if=/dev/urandom of=output.80k bs=80 count=1024

Za prvi scenario kreira se jedan fajl veličine 8GB. Za drugi scenario kreira se fajl od 800MB, i deset puta umnoži kako bi se dobila ukupna veličina od 8GB. U trećem scenariju kreira se fajl od 80MB, umnožava 10 puta, a nakon toga se folder u kom su smješteni ti fajlovi umnožava 10 puta kako bi se dobila ukupna veličina od 8GB. Za svaki naredni scenario nakon kreiranja inicijalnog fajla, fajlovi se umnožavaju tako da se dobije jedan nivo direktorijuma više u odnosu na prethodni scenario, odnosno deset puta više fajlova. Zadnji, šesti scenario najviše odgovara stvarnom okruženju, budući da je ono uglavnom sastavljeno od velike količine malih fajlova.

Nakon toga je potrebno, za svaki scenario pojedinačno, kompletnu strukturu fajlova prenositi preko mreže od jednog servera do drugog servera deset puta pomoću navedenih alata. Testiranje se zasniva na mjerenju vremena potrebnog za prenos podataka ukupne veličine 8GB i brzina protoka koja se tom prilikom ostvaruje.

Tabela 4.1. prikazuje usrednjeno vrijeme u minutima koje je potrebno za prenos fajlova i brzinu prenosa fajlova u MB/s za svaki alat pojedinačno u opisanoj testnoj okolini.

Tabela 4.1: *Testiranje brzine prenosa podataka preko LAN mreže*

Scenario	Struktura fajlova	Ukupna količina podataka (KB)	scp		rsync		rsync inc		tar + ssh	
			vrijeme (min)	protok (MB/s)	vrijeme (min)	protok (MB/s)	vrijeme (min)	protok (MB/s)	vrijeme (min)	protok (MB/s)
1	1 x 8GB	8388612	1:04	128	9:00	15	0	∞	8:07	16,82
2	10 x 800MB	8519724	1:05	138	8:34	16	0	∞	8:11	16,9
3	100 x 80MB	8192044	0:58	137	8:16	16,12	0	∞	8:05	16,16
4	1000 x 8MB	8192444	0:58	137	8:17	16,1	0	∞	7:48	17
5	10250 x 800K	8204548	1:25	94,26	8:17	16,12	0	∞	8:05	16,52
6	101000 x 80k	8124888	3:18	40,07	7:04	18,7	0	∞	7:20	18

Kako bi se dobilo tačno vrijeme prenosa podataka predlaže se korišćenje komande *time* ispred glavne komande na komandnoj liniji. Pored standardnog izlaza glavne komande, *time* komanda u polju *real* daje stvarno vrijeme koje je potrebno da podaci stignu od izvora do destinacije. Nakon toga, protok u MB/s se računa pomoću formule:

„Ukupna količina podataka"(KB)/vrijeme(s)/1024.

U opisanoj testnoj okolini, najbolje rezultate je ostvario scp alat koji dostiže brzinu jednaku kapacitetu mrežnog linka prilikom prenošenja velikih fajlova. Međutim, primjećuje se da što su fajlovi manji, ovaj alat pokazuje slabije performanse. U šestom scenariju, koje najviše odgovara nekom realnom okruženju i koje se uglavnom sastoji od velikog broja malih fajlova, performanse su 3 puta lošije nego prilikom prenošenja velikih fajlova. Alati *rsync* i *tar + ssh* su ostvarili približno jednake rezultate u svakom scenariju. Vrijeme prenosa 8GB podataka za svaki scenario varira od 7 do 9 minuta, dok se brzina prenosa podataka kreće od 15 do 18 MB/s, što ne predstavlja značajnu razliku. Primijećuje se da struktura fajlova i njihove pojedinačne veličine ne utiču na vrijeme prenosa za alate *rsync* i *tar+ssh*, već samo ukupna veličina podataka koja se kopira. „*Rsync inc*" kolona predstavlja rezultate inkrementalnog backup procesa kada na

destinaciji već postoje iskopirani fajlovi; u tom slučaju proces traje nemjerljivo kratko jer sistem odmah ustanovi da se podaci nalaze na destinaciji.

Iako je komanda scp pokazala najbolje rezultate na testu mrežnih performansi, ona nema dovoljno dobru kontrolu nad pravima, atributima, ACL listama i proširenim atributima kao što to imaju tar i rsync. Takođe nema mogućnost inkrementalnog kreiranja rezervnih kopija podataka, tako da bi se svaki put iznova kopirali svi fajlovi sa izvora na destinaciju. Nedostaci tar komande su prepis svih fajlova/foldera istog imena na destinaciji prilikom ekstrakcije, bez obzira na parametre kao što su vrijeme modifikacije ili prava pristupa koji su se možda u međuvremenu promijenili. Neki stariji kerneli su prijavljivali probleme prilikom arhiviranja direktorijuma većih od 8GB, a u predloženom rješenju razmatrani su fajlsistemi značajno veći od toga.

Iako su tar i rsync pokazali slične rezultate u testiranju prenosa podataka preko mreže, rsync se pokazao kao najbolji izbor, jer iako pojedinačno kopira svaki fajl, ima mogućnost upoređivanja fajlova na izvorištu i fajlova na destinaciji prije slanja preko mreže, tako da po potrebi može kopirati samo razlike. Još jedna velika prednost rsync alata je što ukoliko se konekcija prekine i ponovo pokrene, operacija se nastavlja od trenutka prekida za razliku od drugih alata koji je pokreću ispočetka.

Da bi funkcionisao, *rsync* treba da postoji i na serverskoj i na klijentskoj strani komunikacije. Ovaj paket je uključen u standardnu Linux instalaciju i ne treba ga dodatno instalirati. Moderni *rsync*, koristeći *ssh* protokol kao podrazumijevani protokol za transfer podataka sa udaljene mašine, ostvaruje enkripciju podataka preko mreže, tako da su i sigurnosni zahtjevi zadovoljeni [50]. Više o ovom alatu i o opcijama koje treba koristiti je u prilogu 3.

Na tržištu postoji značajan broj komercijalnih i besplatnih softvera koji koriste rsync alat i zasnovani su na njemu. Iako je rsync inicijalno razvijen na Linuxu, neki od ovih softvera su prilagođeni i za ostale operativne sisteme kao što su Windows i MacOS.

Skripte koje u sebi integrišu rsync alat su predviđene da se mogu upotrijebiti na bilo kojem Linux sistemu i nisu određene hardverom. Testirane su na Red Hat i Centos distribucijama operativnog sistema, kao i na fizičkim i virtuelnim mašinama. Njihov kod se nalazi u prilogu 4.

4.4.2 ALATI ZA KREIRANJE KLON SESIJA

Kako određeni storage uređaji posjeduju ugrađene mehanizme za kreiranje snimaka, u predloženom rješenju iskoristiće se prednosti takvog mehanizma za kreiranje rezervnih kopija baza podataka. Postoji niz dokumenata koji potvrđuju da je ovakav pristup najbolja praksa i da je ovakav tip uređaja optimalno prilagođen za funkcionisanje baza i njenih kopija [53, 54, 55, 56, 58, 59]. Klon kopije su prigodne u situacijama kada je potrebno više kopija produkcionih podataka u svrhu oporavka, testiranja, backupa ili izvještavanja. Upotreba kloniranih kopija smanjuje korišćenje i povećava brzinu pristupa produkcionih diskova tako što usmjerava određene korisnike na klonove umjesto na produkcione podatke. Predloženo rješenje razmatra kreiranje jednog klona koji će se osvježavati na dnevnom nivou. Nakon kreiranja klona baze koji predstavlja primarnu kopiju, sekundarna kopija se kreira sa primarne pomoću specijalizovanog tradicionalnog softvera za kreiranje rezervnih kopija i smiješta na trakama.

Solution Enabler (SE) je specijalizovana biblioteka komandi formatirana na UNIXu koja služi za upravljanje, konfigurisanje i nadzor uređaja/diskova u datoj storage okolini. *Symcli* (*Symmetrix Command Line*) je dio ovog softvera koji služi za interakciju sa predstavljenim storage uređajem preko komandne linije i koji se koristi za „kloniranje“. Da bi se ostvarila komunikacija između servera gdje je alat instaliran i storage uređaja, serveru moraju biti vidljivi specijalni uređaji, takozvani Čuvari Vrata (*Gatekeepers*), koji omogućavaju izvršavanje komandi na serveru i dobijanje odgovarajućih informacija od storage uređaja [57]. U predloženom

rješenju, ovaj komercijalni softver takođe razvijen od strane EMC korporacije, treba biti instaliran na backup serveru. Na istom serveru je potrebno postaviti skripte pisane u *Korn shell*-u kako bi mogle koristiti SE softver.

Mehanizmi za kloniranje imaju dvije svrhe:

- kopirati podatke sa izvornog uređaja na krajnji uređaj;
- garantovati konzistentnu kopiju u vremenu na krajnjim uređajima bez prekida procesuiranja podataka na izvornim diskovima.

Komanda za kreiranje i aktiviranje klona koja pripada skupu alata *symcli* je *symclone*. Mehanizam za kloniranje koristi nekoliko različitih opcija za kreiranje kopija izvornih diskova u tački vremena koji zavise od vrste kopije na destinacionim diskovima, vremena kada se podaci kopiraju i toga što prokreće proces kopiranja. Tri metode za sinhronizaciju destinacionih diskova su:

- ***Precopy*** - ili kopiranje u pozadini, sinhronizuje izvorne podatke sa destinacionim prije nego što se destinacija aktivira.
- ***Copy*** - kopiranje počinje kada se destinacija aktivira i završava kada su svi blokovi iskopirani na destinacione diskove.
- ***Nocopy*** - kao i kod copy opcije, proces kopiranja počinje nakon aktivacije sesije ali se podaci kopiraju samo kada host/server inicira I/O operacije. Ova opcija ne dozvoljava procese u pozadini.

Klon se prvo kreira a potom aktivira. Podaci su dostupni backup serveru odmah nakon aktivacije klona. U predloženom rješenju se koristi opcija *precopy* kako bi se podaci u potpunosti iskopirali prije njihove upotrebe. Iako nije potrebno čekati završetak operacije kreiranja klona za aktivaciju, to je još jedna mjera opreza kako bi podaci bili konzistentni.

```
a)  # symclone -sid $SID -file $CTL -noprompt -precopy -differential create >>
    $LOGFILE 2>&1
b)  # symclone -sid $SID -file $CTL -noprompt -precopy recreate >> $LOGFILE 2>&1
c)  # symclone -sid $SID -file $CTL  -noprompt activate   >> $LOGFILE 2>&1
```

Kod 4.1: *Preporučene symclone komande za kreiranje i aktivaciju klona*

U Kodu 4.1 predložene su komande koje se koriste za inicijalno kreiranje potpunog snimka, inkrementalno kreiranje potpunog snimka i njegovu aktivaciju. Komanda a) u Kodu 4.1 kreira potpuni klon sa opcijom –precopy, odnosno kreira sesiju među izvornim i destinacionim diskovima. Nakon kreiranja sesije, više nije potrebno izvršavati ovu komandu nad istim diskovima. Sesija je inicijalno morala biti kreirana pomoću –differential opcije, da bi se nakon toga periodično mogla rekreirati. Druga komanda b) služi za kreiranje inkrementalnog klona u sesijama kad je potpuni klon već kreiran, odnosno kopira samo blokove koji su se promijenili od kad je zadnji put aktiviran klon. Treća komanda c) služi za aktivaciju klona, bez obzira na način na koji je klon kreiran, odnosno da li je potpuni ili inkrementalni. Varijabla $SID sadrži 3 cifre i predstavlja identifikacioni broj konkretnog Symmetrix storage uređaja. Varijabla $CTL predstavlja konfiguracioni fajl sa listom symdev identifikatora izvornih i krajnjih diskova. Više o *symclone* komandi i korišćenju *symcli* softvera je na *man* stranicama i u bijelim knjigama [53, 56, 57].

Procesi kopiranja u pozadini i pristupanja zaštićenim blokovima na izvornim diskovima od strane aplikacionog servera kontrolišu proces kloniranja. Kada se blok prvi put upiše na izvorni disk a još uvijek nije kopiran na destinacioni disk, prvo se mora upisati na destinacioni disk kako bi se upis na izvornim diskovima potvrdio. Ovaj proces se ne primjenjuje na svaki

sljedeći upis na blokove koji su već kopirani. Takođe, ukoliko se bloku na destinaciji pristupi prije nego što je kopiran, prvo se mora kopirati sa izvornih diskova na destinacione. Ovaj proces uzrokuje dodatnu aktivnost na izvornim diskovima i može biti uzrok opterećenja na produkciji.

Sistem skripti koji u sebi integriše *symclone* komandu i obavlja operacije kloniranja izdijeljen je u nekoliko cjelina u zavisnosti od funkcije:

- **bin/** - je direktorijum gdje su smještene izvršne skripte, programi i funkcije;
- **config/** - je direktorijum gdje su smješteni konfiguracioni fajlovi;
- **jobs/** - je direktorijum gdje su smještene glavne skripte koje koriste programe i funkcije iz bin/;
- **logs/** - je direktorijum gdje se smiještaju log ispisi svake izvršene akcije.

U prilogu 5 su date skripte koje u zavisnosti od ulaznih parametara mogu obavljati obije funkcije, kreirati klon za potrebe backupa i kreirati klon za potrebe izvještavanja ili testiranja.

4.5. Način skladištenja rezervnih kopija podataka

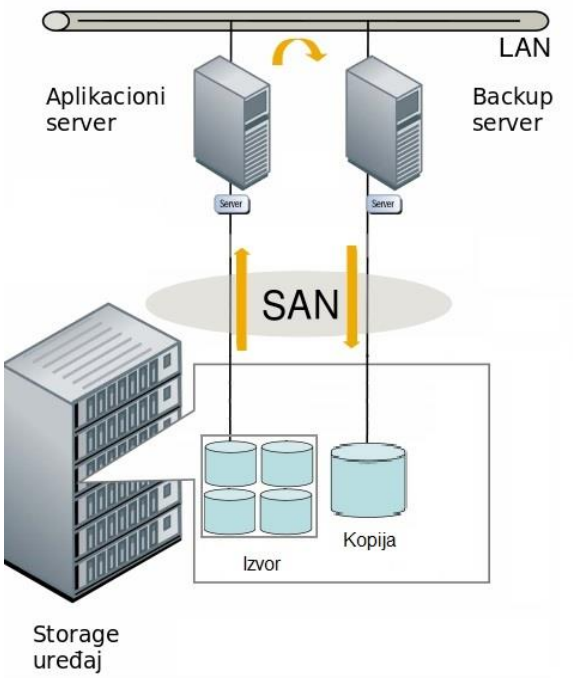
Heterogeno rješenje predlaže upotrebu jedinstvenog storage sistema kao repozitorijuma za čuvanje primarnih kopija podataka. Pošto se sekundarne kopije podataka svakako čuvaju na trakama u backup infrastrukturi, u slučaju hardverskog otkaza jedinstvenog storage uređaja podaci ostaju dostupni za oporavak.

U slučaju kreiranja primarnih kopija standardnih podataka, backup proces u predloženom rješenju ne zavisi od tipa repozitorijuma za skladištenje. Potrebno je backup serveru obezbijediti dovoljno veliku particiju kako bi se smjestili svi podaci koje je potrebno čuvati. Kako je preporuka da se resursi za backup proces ne troše na brzinu upisa podataka, poslužio bi bilo koji tip storage uređaja dovoljnog kapaciteta.

Budući da se za baze podataka kreiraju primarne kopije u obliku klon sesija, ovaj tip backupa zavisi od funkcionalnosti integrisanih u konkretnom storage uređaju. Ukoliko bi se razmatrala mogućnost za kreiranjem istovjetnih kopija na udaljenom storage uređaju kako bi se obezbijedili podaci na DR lokaciji, potrebno je obezbijediti još jedan identični model storage uređaja i dodatne licence što zahtijeva značajna ulaganja.

4.5.1 SKLADIŠTENJE REZERVNIH KOPIJA STANDARDNIH PODATAKA

Razmatrane *open source* komande za kreiranje rezervnih kopija standardnih fajlova vrše kopiranje preko LAN mreže, tako da je za backup standardnih fajlova usvojena topologija zasnovana na LAN mreži. Na slici 4.2 prikazana je putanja standardnih podataka u backup procesu sa originalnih diskova na backup disk. Podaci čije rezervne kopije treba kreirati su kroz SAN infrastrukturu predstavljeni aplikacionim serverima. Kako bi se kreirale njihove rezervne kopije, preko LAN mreže se šalju backup serveru koji ih na prijemu smiješta na diskove koji se takođe nalaze na storage uređaju. Pošto se backup proces obavlja na nivou fajla, ne postoji način da se ova putanja skrati i da se razmjena obavi direktno na nivou storage uređaja.



Slika 4.2: *Prikaz originalnih i backup diskova na storage uređaju*

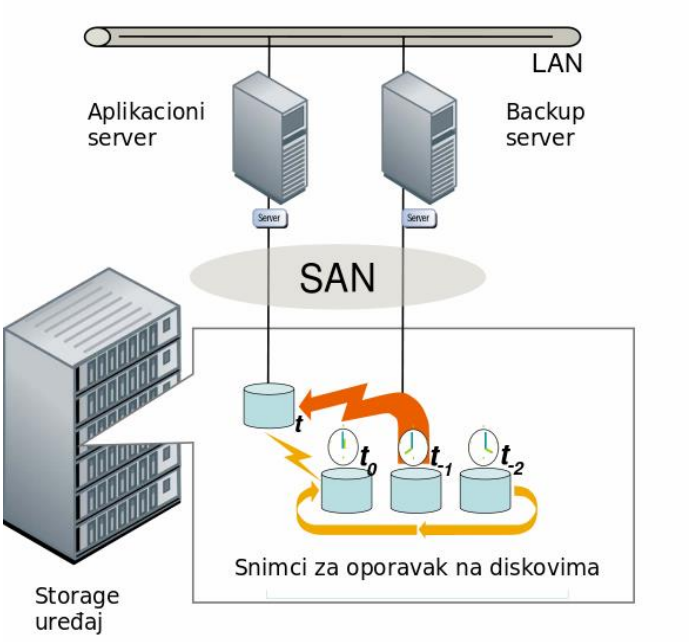
U svrhu kreiranja primarne kopije standardnih podataka, backup serveru se predstavlja jedna particija na storage uređaju za potrebe skladištenja backup materijala. Na njoj se kreira fajlsistem dovoljno veliki da skladišti više dnevnih kopija kompletnog sistema čiji je broj definisan periodom zaštite.

4.5.2 SKLADIŠTENJE REZERVNIH KOPIJA BAZA PODATAKA

BCV funkcionalnosti su integrisane u storage uređaju u vidu *TimeFinder* softvera. On omogućava trenutno kreiranje višestrukih kopija baze podataka, takozvane snimke i trenutnu dostupnost tih podataka nakon izvršenja *restore* operacije. Kako bi se zaštitili podaci kritični za određeno poslovanje vrlo približno trenutku u kom se dogodio otkaz, backup koji koristi BCV funkcionalnosti je preferirana metoda koja iskorištava potencijale storage uređaja bez dodatnog ulaganja. *TimeFinder* softver omogućava kreiranje kopija na istom storage uređaju.

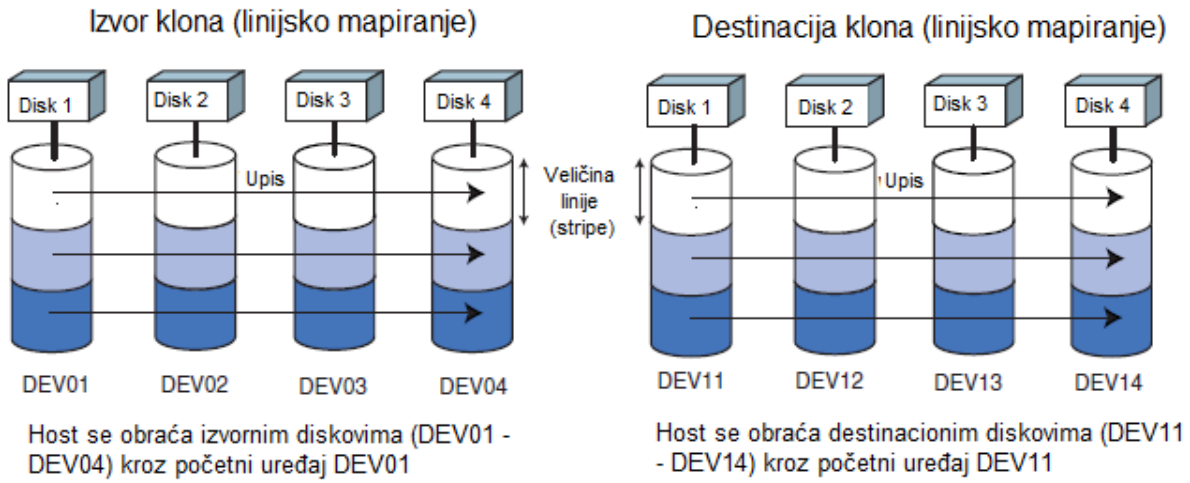
Za implementaciju rješenja koje kreira rezervne kopije baze podataka predlaže se funkcija koja kreira potpune snimke, odnosno klonove. Time će se primijeniti topologija backup mreže bez servera (*Server-free backup*) opisane u poglavlju 3.4.4. Na slici 4.3 ilustrovan je proces kreiranja klonova u različitim trenucima u vremenu, t_0, $t\text{-}_1$, i $t\text{-}_2$ [23].

Za razliku od potpunog snimka odnosno klona, diferencijalni snimak kreira logičke kopije zasnovane na pokazivačima kopirajući samo promjene na originalnim diskovima tako da zauzima manje prostora na fizičkim uređajima. Međutim, ovakav način nije preporučen za scenarija koja uključuju oporavak podataka budući da nisu nezavisna u odnosu na produkcione podatke.



Slika 4.3: *Prikaz originalnog i klon diskova na storage uređaju [23]*

Da bi se na destinacionom (backup) serveru mogao mapirati klon baze podataka, na storage uređaju treba kreirati potpuno istu nezavisnu strukturu diskova, koja mora biti vidljiva ovom serveru (Slika 4.4 [53]).



Slika 4.4: *Meta-uređaji konfigurisani kao klon parovi*

Svaki disk prilikom kreiranja na storage uređaju će dobiti svoj WWN, jedinstveni univerzalni identifikator od 16 bajta koji u sebi sadrži informacije o proizvođaču, modelu i tipu storage uređaja, kao i jedinstveni trocifreni broj koji određuje konkretni storage uređaj. Zadnjih 8 cifara u WWN identifikatoru svakog diska određuju konkretan disk na storage sistemu. Ova izolovana informacija se prevodi u SYMDEV identifikator i koristi se u konfiguracionim fajlovima prilikom operacija sa diskovima.

Za svaki pojedinačni klon potrebno je odvojiti prostor na storage uređaju u vidu strukture diskova identične izvornim diskovima. Izvorni i krajnji diskovi mogu biti različitog tipa, a originalne podatke treba smjestiti na kvalitetnijim diskovima kako bi izvorna aplikacija imala što bolje performanse, dok se klon kopija treba smjesti na diskovima lošijeg kvaliteta budući da je operacija kloniranja pozadinska i ne smije ugrožavati rad glavne aplikacije.

Izvorne diskove treba mapirati na produkcionom serveru kao što je slučaj u predloženom rješenju. Nije neophodno da se destinacioni diskovi mapiraju serveru budući da se kopiranje obavlja na nivou storage uređaja. To zavisi od svrhe kopije. Ukoliko se diskovi nigdje ne montiraju, oni mogu služiti samo za potrebe restore operacije budući da se podacima ne može pristupiti, a diskovima može pristupiti samo softver koji upravlja diskovima. Iako bi zbog konzistencije backup materijala bilo sigurnije da se klonirani diskovi nigdje ne montiraju, predlaže se da su destinacioni diskovi vidljivi backup serveru. Razlog tome je kreiranje sekundarne kopije pomoću specijalizovanog softvera koja se smiješta na trakama.

5. Implementacija heterogenog rješenja za backup i recovery podataka na Linux sistemima

U ovom poglavlju izložen je proces implementacije i validacije predloženog rješenja u realnom okruženju.

Kompanija u kojoj treba implementirati predloženo rješenje za kreiranje rezervnih kopija podataka pripada velikim kompanijama sa više od 500 zaposlenih. Pripada tipu telekomunikacionog operatera koji opslužuje desetine hiljada korisnika. Kompanija ima razvijeni informacioni sistem i jasno definisane ciljeve i standarde. SAN i LAN infrastrukture su implementirane prema preporukama najbolje prakse, kao i namijenjeni SAN sa trakama, odnosno backup infrastruktura sa specijalizovanim softverom za backup. Kompletna infrastruktura je smještena u datacentru sa razvijenom pomoćnom infrastrukturom u smislu redudantnog napajanja, agregata, klimatizacije, fizičkog pristupa.

Obim podataka koji se obrađuje u informacionom sistemu je reda nekoliko stotina terabajta. Neki od tipova aplikacija na Linux operativnom sistemu pripadaju kompleksnim aplikacijama za naplatu, narudžbu, nabavku, medijaciju, analizu podataka, izvještavanje, itd... Za sve njih treba obezbijediti adekvatno rješenje za backup podataka kako bi se zadovoljili standardi i regulacioni zahtjevi i omogućio oporavak u slučaju potrebe.

Predloženo rješenje se primjenjuje na konkretni sistem koji se sastoji od više uređaja i na kojem se nalazi prioritetna aplikacija čije podatke treba očuvati sa mogućnošću oporavka njene funkcionalnosti. Tip funkcionalnosti originalne aplikacije nije važan sa aspekta kreiranja rezervnih kopija podataka. Kompatibilnost aplikacije određuje operativni sistem i bazu podataka, a implementacija rješenja se fokusira na Linux kao operativni sistem i Oracle kao bazu podataka. Sama aplikacija povlači sa sobom nekoliko parametara koje treba pažljivo analizirati i predlog prilagoditi u skladu sa tim.

Kako bi se heterogeno rješenje za kreiranje rezervnih kopija podataka implementiralo prema predlogu, sprovedeni su sljedeći koraci:

- **Vremenska organizacija backup operacija** - koja je određena definisanom frekvencijom backup operacija i periodom zaštite podataka;
- **Analiza infrastrukture primijenjene za funkcionisanje glavne aplikacije** - aplikacija uslovljava infrastrukturu u smislu servera i storage uređaja na kojoj će funkcionisati, a koja se treba uklopiti u postojeću infrastrukturu;
- **Analiza kapaciteta potrebnog za skladištenje rezervnih kopija** - kategorija, organizacija i količina podataka su takođe uslovljeni implementiranom aplikacijom, a na osnovu njih se određuje kapacitet koji je potrebno obezbijediti kako bi se skladištile rezervne kopije tih podataka;
- **Primjena alata za kreiranje rezervnih kopija** - korišćenjem skripti u bash i korn shell komandnom interpreteru, sa osvrtom na neinteraktivnu komunikaciju između backup servera i aplikacionih servera.
- **Prostorna organizacija backup operacija** - koja se oslanja na način skladištenja rezervih kopija standardnih i baza podataka, a uzima u obzir primijenjenu infrastrukturu uslovljenu implementiranom aplikacijom.

Koraci primjenjeni za validaciju heterogenog rješenja su:

- **Testiranje operacije oporavka** - kojim se osigurava uspješnost kompletnog procesa kreiranja rezervnih kopija podataka nakon implementiranja rješenja na postojeći sistem;
- **Analiza primijenjenog rješenja** - sa osvrtom na performanse i trajanje backup operacija kako bi se ustanovili nedostaci u cilju poboljšanja predloženog rješenja.

5.1. Vremenska organizacija backup operacija

Kako se za kreiranje rezervnih kopija standardnih podataka i baze podataka koriste različiti mehanizmi i različite skripte, to su ova dva procesa vremenski odvojena. Frekvencija i period zaštite sekundarne backup operacije za standardne podatke i baze podataka su implementirani prema preporukama u poglavlju 4.1.

Frekvencija primarne backup operacije standardnih podataka definisana u crontab fajlu je jedan dan, a period zaštite definisan u kodu skripte je tri dana. To znači da se na primarnom backup medijumu čuvaju tri backup materijala. Iskustvo autora ovog rada je pokazalo da je to dovoljno vremena da se uoči greška ili korupcija u podacima i ispravi pomoću primarnog backupa. Parametri se jednostavno mogu izmijeniti u slučaju potrebe, međutim time se povećava prostor koji je potrebno odvojiti za čuvanje primarnog backup materijala. Ukoliko je potrebno oporaviti starije podatke, oni se nalaze na sekundarnom backup materijalu na trakama.

Skripta za backup standardnih podataka kompletnog sistema je postavljena u *crontab* fajlu *root* korisnika na backup serveru *servrepdb* kao što je prikazano u kodu 5.1. Skripta se automatski izvršava svakog jutra u 2 sata sa izuzetkom nedjelje i ponedjeljka. Budući da su subota i nedjelja neradni dani i tada nema promjena na sistemu od strane korisnika, nedelja i ponedeljak se preskaču u rasporedu kako bi se izbjegla tri ista uzastopna backupa.

```
00 2 * * 2-6 /root/Scripts/backup_all.sh
```

Kod 5.1: *Unos u crontab fajlu koji definiše automatsko izvršavanje skripte backup_all.sh u 2:00 svim danima osim nedjelje i ponedeljka*

Glavna skripta koja pokreće proces inkrementalnog kloniranja je takođe automatizovana postavljanjem u crontab fajl root korisnika na serveru *servrepdb* i izvršava se svako veče u 00:20 kao što je prikazano u kodu 5.2.

```
00 20 * * * /opt/emc/clon_scripts/jobs/clone_refresh.ksh
```

Kod 5.2: *Automatsko izvršavanje skripte clone_refresh.ksh u 00:20*

Kompletan proces se prati i snima, a log informacije se smiještaju u poseban fajl određen datumom tako da je u svakom trenutku moguće provjeriti uspješnost operacije kloniranja.

Metodom kloniranja se kreira samo jedna kopija produkcione baze koja se montira na backup serveru i osvježava se svakodnevno, što znači da su frekvencija primarne backup operacije baze podataka i period zaštite jedan dan. Ostale kopije se kreiraju na trakama u skladu sa definisanom politikom.

Noćni termin za obije backup operacije je izabran iz više razloga tako da se ne preklapa:

- sistem je tada najmanje opterećen korisničkim akcijama,
- dodatna aktivnost prouzrokovana backup operacijom nije smetnja korisnicima koji tada ne koriste sistem,

- sistem prolazi kroz minimum promjena tako da je mala vjerovatnoća da dodje do korupcije podataka ukoliko više procesa istovremeno pristupa istim podacima.

5.2. Analiza primijenjene infrastrukture

Predlog heterogenog rješenja je primijenjen na sistem od šest servera na kojima kao cjelina funkcioniše prioritetna aplikacija. Aliasi imena servera odražavaju njihovu funkciju u konkretnom sistemu na kom radi glavna aplikacija:

- **serv01db** - server na kom se nalazi baza podataka;
- **servepc, serv01sdp, serv01app, serv02app, serv03app** - serveri na kojima se nalaze segmenti aplikacije
- **servrepdb** - backup server

Potrebno je kreirati rezervne kopije operativnog sistema odnosno sistemskih podataka svih servera, Oracle baze podataka na serveru *serv01db* i podataka glavne aplikacije na serverima *servepc, serv01sdp, serv01app, serv02app, serv03app*. Backup server *servrepdb* igra ulogu media servera za primarni backup, pokrećući backup operacije i usmjeravajući backup podatke na odgovarajuće lokacije.

Na svim serverima je instaliran operativni sistem distribucije RHEL 6.4 (*Red Hat Enterprise Linux*). Specifikacije svih aplikacionih servera su:

- OS: RHEL 6.4
- CPU: 2 x 6 Core Xeon E5-2640
- Memorija: 128GB DDR3
- Harddisk: 2x300GB u RAID 1 konfiguraciji

Backup server koji je dio postojeće infrastrukture je identične specifikacije kao aplikacioni serveri.

Iako svaki operativni sistem posjeduje svoj originalni multipath softver u vidu drajvera, često se koriste komercijalni proizvodi (*third party*) koji posjeduju bolje performanse i stabilniji su. Primjeri takvih softvera su Symantec Veritas Dynamic Multipathing (VxDMP) i EMC PowerPath. Na datim serverima korišćen je originalni linux softver za multipath koji je uključen u standardnu distribuciju RHEL 6 u obliku rpm paketa device-mapper-multipath-0.4.9-72.el6.x86_64 zbog nekoliko prednosti:

- za njegovu primjenu ne treba izdvajati dodatna sredstva,
- kako je dio standardne Linux distribucije, potpuno je kompatibilan sa sistemom,
- relativno jednostavno se konfiguriše, a njegova funkcionalnost je na solidnom nivou.

Storage uređaj koji će se koristiti i kao primarni i kao sekundarni storage uređaj je opisan u poglavlju 3.8. Povezan je na SAN infrastrukturu i vidiljiv svim serverima po preporukama visoke dostupnosti. Njegove karakteristike su sljedeće:

- Model: Symmetrix Vmax 10k,
- Konfiguracija: 2 motora (engine),
- Keš: 128GB po motoru
- Diskovi: 16 x 200GB flash drive R5(3+1), 1 rezervni
  140 x 300GB 15K FC drive R1, 4 rezervna
  32 x 2000GB 7.2K SATA R6(6+2), 2 rezervna

5.3. Analiza kapaciteta potrebnog za skladištenje rezervnih kopija po kategorijama podataka

Kapacitet predstavlja prostor koji je potrebno odvojiti na diskovima kao primarnom i trakama kao sekundarnom backup medijumu. U narednom poglavlju prikazana je analiza fajlsistema, volume grupa i diskova, kao i detaljan postupak računanja kapaciteta koji je potreban za skladištenje rezervnih kopija po kategorijama podataka koje će se razmatrati u ovom predlogu. Kategorije podataka na Linux operativnom sistemu koje obuhvata predlog heterogenog rješenja su standardni fajlovi i baze podataka.

5.3.1 KAPACITET POTREBAN ZA SKLADIŠTENJE STANDARDNIH PODATAKA

Kako bi se utvrdio kapacitet potreban za skladištenje standardnih fajlova, razmatraće se organizacija fajlsistema na kojima se nalaze standardni podaci na svim serverima.

Fajlsistemi na lokalnim diskovima koji predstavljaju operativni sistem, organizovani su na svim serverima pojedinačno pomoću LVM alata u jednu *volume* grupu vg00 koja se nalazi na hard disku servera. Informacije o fajlsistemima operativnog sistema su date u tabeli 5.1. Kada se saberu sve vrijednosti u koloni „Veličina fajlsistema“, dobija se količina alociranog prostora na lokalnim diskovima. Ona iznosi oko 60GB po serveru, odnosno 360GB za svih šest servera. Ova vrijednost predstavlja prostor koji je potrebno odvojiti na uređajima za skladištenje podataka kako bi se sačuvala jedna rezervna kopija svih operativnih sistema.

Tabela 5.1: *Informacije o fajlsistemima operativnog sistema*

Mount-point direktorijum fajlsistema	Opis fajlsistema	Veličina fajlsistema	Ime volume grupe	Veličina volume grupe	Server
/	root fajlsistem	2GB	vg00	279GB	serv01db, serv01sdp, servepc, serv01app, serv02app, serv03app
/boot	fajlovi za podizanje sistema	200MB			
/var	log fajlovi i privremeni fajlovi	7GB			
/usr	korisničke komande, biblioteke, dokumentacija	4.5GB			
/opt	fajlovi sa podacima	40GB			
/home	lični direktorijumi svih korisnika sistema	1GB			
/tmp	privremeni fajlovi	2GB			

Pošto se u /tmp fajlsistemu nalaze privremeni i pomoćni fajlovi, za njih nije potrebno organizovati rezervne kopije. Zbir veličina svih fajlsistema operativnog sistema je manji od ukupne količine prostora dostupnog na VG; ostavljena je mogućnost za eventualno proširenje bilo kojeg fajlsistema po potrebi dok je sistem u operativnom stanju pomoću LVM alata.

Fajlsistemi aplikacije su organizovani kao što je prikazano u tabeli 5.2.

Tabela 5.2: *Informacije o fajlsistemima aplikacije*

Mount-point direktorijum fajlsistema	Server	Veličina fajlsistema	Ime volume grupe	Veličina volume grupe
/oravl01	serv01db, serv01sdp, servepc, serv01app, serv02app, serv03app	15GB	vguser	zavisi od servera
/ctmuser1	serv01sdp, servepc, serv01app, serv02app,	100GB		

	serv03app			
/ctmuser2	servepc, serv01app, serv02app, serv03app	100GB		
/ctmuser3	servepc, serv01app, serv02app, serv03app	300GB		
/ctmuser9	serv03app	50GB		
/dba	serv01app	100GB		

Kada se saberu sve vrijednosti u koloni „Veličina fajlsistema“ na svim serverima, dobija se ukupna količina alociranog prostora na diskovima na storage sistemu. Ona iznosi:

```
6 x 15 + 5 x 100 + 4 x 100 + 4 x 300 + 50 + 100 = 2340GB
```

Vrijednost 2340GB predstavlja ukupni prostor na svim fajlsistemima odvojen za potrebe glavne aplikacije, odnosno maksimalnu veličinu koju može imati jedna rezervna kopija same aplikacije na kompletnom sistemu. Ova vrijednost se treba uzeti u obzir prilikom računanja kapaciteta potrebnog za skladištenje podataka aplikacije.

Prilikom projektovanja prostora kojeg će glavna aplikacija upotrijebiti kako ne bi došlo do zagušenja fajlsistema i kako bi se uračunao rast podataka u vremenu, uzeto je da maksimalna količina podataka koja će biti smještena na fajlsistemima odgovara 70% alociranog prostora i prema tome je modelirana infrastruktura. Kako je za sistemski backup alocirano 360GB ukupno, za backup aplikacije 2340GB i računa se da će biti upotrijebljeno 70% ukupnog alociranog prostora, sledećom računicom se dolazi do broja koji predstavlja kapacitet potreban za 3 dana procesuiranja backup operacija standardnih fajlova:

```
(2340GB + 360GB) * 0,7 * 3 = 5670GB
```

Fajlsistemi baze se razmatraju odvojeno u odnosu na fajlsisteme na kojima se nalaze standardni fajlovi.

5.3.2 KAPACITET POTREBAN ZA SKLADIŠTENJE ORACLE BAZE PODATAKA

Baza MASTER predstavlja izvornu Oracle bazu podataka čiju je rezervnu kopiju potrebno obezbijediti i nalazi se na serveru *serv01db*. *Volume* grupe na kojima se nalazi originalna baza podataka su organizovane u nekoliko cjelina u zavisnosti od njihove funkcije i tipa podataka na njima kao što je prikazano u tabeli 5.3.

Tabela 5.3: *Organizacija volume grupa baze podataka MASTER*

Tip podataka	**Ime volume grupe**
Fajlovi sa podacima baze	Vgmasterdbdata
Archive log fajlovi	Vgmasterdbarc
Redo log fajlovi A	vgmasterdbredoA
Redo log fajlovi B	vgmasterdbredoB

Svaka *volume* grupa je sastavljena od 4 diska koji se nalaze na storage uređaju a vidljivi su izvornom serveru *serv01db*. Pomoću LVM alata svaka grupa diskova je linijskim mapiranjem objedinjena u jednu logičku volume grupu (VG). Ovakva praksa daje značajno bolje performanse jer se istovremeno pristupajući na četiri lokacije, ostvaruju 4 puta veće brzine pristupa diskovima na storage uređaju. Nakon toga su pojedinačne volume grupe izdijeljene na logičke volume i napravljene su particije na kojima se nalaze odgovarajući fajlsistemi.

U tabeli 5.4 date su informacije o svim fajlsistemima i *volume* grupama baze MASTER, kao i kapacitetu kojeg zauzimaju na storage uređaju.

Tabela 5.4: *Organizacija fajlsistema i volume grupa baze MASTER*

Mount-point direktorijum fajlsistema	Opis fajlsistema	Veličina fajlsistema (GB)	Ime volume grupe	Veličina volume grupe	Broj linijskih (stripe) jedinica	Veličina diska u grupi (GB)	Ukupan prostor na storage sistemu
/pkgmasterdbprod/redologa	Redo log fajlovi A	15	vgmasterdbredoA	15	4	4	16
/pkgmasterdbprod/redologb	Redo log fajlovi B	15	vgmasterdbredoB	15	4	4	16
/pkgmasterdbprod/oradata1	Fajlovi sa podacima, kontrolni fajl	50	vgmasterdbdata	520	4	130	520
/pkgmasterdbprod/oradata2	Fajlovi sa podacima, privremeni fajlovi	50					
/pkgmasterdbprod/oradata3	Fajlovi sa podacima	200					
/pkgmasterdbprod/oradata4	Fajlovi sa podacima	200					
/pkgmasterdbprod/oracle	Fajlovi sa podacima	20					
/pkgmasterdbprod/oraclearch	Arhivirani redo log fajlovi	500	vgmasterdbarc	500	4	130	520

Zbir svih veličina u koloni „Ukupan prostor na storage sistemu“ daje ukupan prostor na storage sistemu alociran za potrebe baze podataka MASTER i iznosi 1072GB. Sastoji se od 4 grupe diskova od kojih se na svakoj nalazi različita *volume* grupa. *Volume* grupe *vgmasterdbdata* i *vgmasterdbarc* se nalaze na po četiri diska veličine 130GB, dok se *volume* grupe *vgmasterdbredoA* i *vgmasterdbredoB* nalaze na po četiri diska veličine 4GB.

Veličina upotrebljivog prostora na svim fajlsistemima nakon njihovog kreiranja je 1036GB i ova vrijednost predstavlja korisni prostor na diskovima koji je moguće upotrijebiti za smiještanje fajlova. Razlika od 5% prostora između alociranog i upotrebljivog prostora na fajlsistemu rezervisana je za potrebe samog fajlsistema [*mkfs.ext4 man page*]. Na fajlsistemima, iskorišćeni prostor koji prikazuje operativni sistem predstavlja prostor koji je prilikom kreiranja baze MASTER alociran za nju i iznosi ukupno oko 580GB. Efektivna veličina baze je oko 130GB i jedino je ova veličina promjenjiva u vremenu a informacija o njoj se dobija iz sistema.

5.4. Primjena alata za kreiranje rezervnih kopija podataka

5.4.1 SKRIPTE ZA BACKUP STANDARDNIH PODATAKA

Backup rješenje za šest Linux servera u opisanom sistemu je realizovano kroz automatsko izvršavanje dvije skripte pisane u *bash shellu*:

- */root/Scripts/backup_all.sh,*
- */root/Scripts/backup_fs.sh.*

Skripte se nalaze na backup serveru *servrepdb.* Skripta *backup_all.sh* sadrži listu svih servera u sistemu i poziva skriptu *backup_fs.sh* za svaki server pojedinačno. Ona je postavljena u *crontab* fajlu za automatsko izvršavanje.

Skripta *backup_fs.sh* je napravljena tako da vrši backup kompletnog servera na udaljenoj lokaciji, odnosno svih njegovih fajlsistema. Inkorporira funkciju koja koristeći rsync alat vrši kreiranje rezervnih kopija svih pojedinačnih fajlsistema preko LAN mreže na jednom serveru.

Udaljeni pristup serverima je opisan u poglavlju 5.4.3. i predstavlja standardni mehanizam za razmjenu informacija među računarima pod Linux operativnim sistemom.

Kodovi obije skripte se nalaze u prilogu 4.

5.4.2 PROCEDURA KREIRANJA KLONOVA

Inicijalna zamisao prilikom kreiranja klonova je bila da isti klon posluži u svrhu backupa i u svrhu izvještavanja kako bi se uštedio prostor na storage uređaju i smanjila količina pristupa produkcionim diskovima. Međutim, u istom okruženju nije sigurno imati dvije baze sa istim imenom iako se nalaze na različitim serverima, tako da je klon baza podataka predviđena za izvještavanje zahtijevala promjenu svog imena i parametara. Ukoliko se ime baze i njeni parametri promijene, to više nije ista baza i taj klon više ne može poslužiti u svrhu operacije oporavka. Zbog toga se procedura za kloniranje razlikuje u zavisnosti od svrhe klon kopije.

Da bi operacija kloniranja bila uspješna a podaci na destinaciji bili konzistentni i pripremljeni za backup na trake, važno je ispratiti sledeći redosljed:

1. Gašenje klonirane Oracle baze na backup serveru.
2. Demontiranje (umount) fajlsistema klonirane baze.
3. Deaktiviranje LV i VG klonirane baze.
4. Provjera da nema aktivnih grupa volumena prije početka procesa kloniranja.
5. Inkrementalno kloniranje diskova.
6. Postavljanje produkcione Oracle baze podataka na aplikacionom serveru u „hot backup“ status.
7. Aktiviranje klona.
8. Završetak „hot backup“ statusa produkcione baze.
9. Aktiviranje VG i LV na kloniranim diskovima.
10. Montiranje (mount) fajlsistema na kloniranim diskovima.
11. Podizanje klonirane Oracle baze podataka u status samo za čitanje (read-only mode).

Klon Oracle baze podataka je postavljen u status samo za čitanje *(read-only*) kako bi se mogao upotrijebiti za oporavak podataka. Gledano iz ugla baze podataka, potpuni klon postaje nezavisna baza u odnosu na svoj izvor, tako da je važno onemogućiti upis kako bi podaci ostali netaknuti.

Proces inkrementalnog kloniranja MASTER baze podataka traje oko 10 minuta u prosjeku. Vrijeme trajanja ovog procesa zavisi od količine promjena na blokovima diskova produkcione baze. U prilogu 5 data je istorija log fajlova procesa kloniranja iz koje se može vidjeti trajanje ove operacije po danima.

Nakon što je prva kopija kreirana na diskovima u vidu klona, pristupa se kreiranju druge kopije na uređaju sa trakama u backup infrastrukturi uz pomoć specijalizovanog softvera koji ima integrisanu podršku za Oracle baze podataka. Postupak kreiranja rezervnih kopija podataka na trake uz pomoć softvera kao što je HP Data Protector je opisan u poglavlju 3.6. Vrijeme trajanja backup operacije na trake iste baze zavisi od efektivne veličine baze. Da bi se MASTER baza u potpunosti sačuvala na trake, potrebno je oko 40 minuta. Dok se kod procesa kloniranja kopiraju razlike u blokovima na izvornim i destinacionim diskovima na storage uređaju, backup na trake se izvršava pomoću specijalizovanog softvera koji vrši backup na nivou fajlova i time uzima u obzir efektivnu vrijednost Oracle baze.

Ukoliko je klon predviđen za testiranje ili izvještavanje, uvode se novi koraci promjene imena grupa volumena, logičkih volumena, fajlsistema, baze i parametara baze, po sledećem redosljedu:

1. Gašenje klonirane Oracle baze na backup serveru.

2. Demontiranje (umount) fajlsistema klonirane baze.
3. Deaktiviranje LV i VG klonirane baze.
4. Provjera da nema aktivnih grupa volumena prije početka procesa kloniranja.
5. Inkrementalno kloniranje diskova.
6. Postavljanje produkcione Oracle baze podataka na aplikacionom serveru u „hot backup“ status.
7. Aktiviranje klona.
8. Završetak „hot backup“ statusa produkcione baze.
9. Promjena imena LV i VG.
10. Aktiviranje novih LV i VG na kloniranim diskovima.
11. Montiranje (mount) fajlsistema na kloniranim diskovima.
12. Podizanje klonirane Oracle baze podataka.
13. Promjena imena i parametara Oracle baze.

Sistem skripti koji može kreirati obije varijante klona, i klon samo za čitanje i klon koji mijenja imena volume grupa, fajlsistema i baze, je postavljen u direktorijum /opt/emc/clone_scripts/ servera *servrepdb*, a kod se nalazi u prilogu 5.

5.4.3 PRISTUP UDALJENOM RAČUNARU

Secure Shell (SSH) je komandni interfejs baziran na Unixu i mrežni protokol koji korisnicima omogućava uspostavljanje sigurnog komunikacionog kanala između dva računara koristeći nesigurnu računarsku mrežu. Pristup serveru/računaru preko SSH protokola omogućava korisnicima izvršavanje operacija na Linux komandnoj liniji. Za pristup sa Unix računara na Unix, mehanizmi su već ugrađeni u postojeće shellove. Početni računar je ssh klijent, dok je krajnji računar ssh server.

Da bi komande koje se pokreću na backup serveru mogle automatski da se izvršavaju na udaljenom računaru, odnosno aplikacionom serveru, bez interakcije administratora, potrebno je omogućiti autentikaciju bez šifri (*passwordless*) koji je osnovni metod autentikacije preko ssh protokola. To se postiže upotrebom ssh ključeva. Na izvornom serveru, pod odgovarajućim userom se kreira par privatni/javni ssh ključ bez šifre (*passphrase*) pomoću komande *ssh-keygen.* Pošto posebni argumenti nisu specificirani, kreiran je skup RSA enkriptovanih ključeva u *~HOME/.ssh/* direktorijumu root korisnika. Fajl id_rsa je privatni ključ i on ostaje u .ssh/ direktorijumu, dok je id_rsa.pub javni ključ čiji se sadržaj kopira u fajl *~HOME/.ssh/authorized_keys* na udaljenom serveru. Važno je da kompletna struktura direktorijuma koji sadrži fajl *authorized_keys* na udaljenom serveru ima odgovarajuća prava inače ovakva autentikacija neće biti moguća. Najčešći uzrok nemogućnosti ostvarivanja ovakve komunikacije je u pravima upisa na *~HOME/* direktorijumu koji su greškom definisani za ostale (eng. *others*), kao i za nepravilno postavljena prava na .ssh/ direktorijumu i *authorized_keys* fajlu.

Za potrebe funkcionisanja skripti za backup pomoću rsync komande, iskopiran je javni ključ sa *root@servrepdb* na root naloge ostalih aplikacionih servera čije rezervne kopije podataka treba kreirati. U to je uključen i ključ na root nalogu servera baze *serv01db* za potrebe funkcionisanja skripte koja pravi snimak baze.

5.5. Prostorna organizacija backup operacija

Pošto su performanse backup operacija manje važne u odnosu na pouzdanost podataka, odvojen je prostor na storage uređaju kojeg čine SATA diskovi sa najlošijim karakteristikama. Resurs storage uređaja kojeg čine brzi i kvalitetni diskovi su rezervisani za potrebe funkcionisanja same aplikacije. Iako fizički prostor na storage uređaju čine fizički diskovi, prostor koji se dodjeljuje serverima je virtuelizovan i kreiran pomoću alata koji upravljaju storage uređajem [poglavlje 3.7.2.]. Maksimalna veličina virtuelnog diska koju je moguće kreirati pomoću softvera za virtuelizaciju prostora na storage uređaju je 240GB [59, str 7.].

5.5.1 REPOZITORIJUM STANDARDNIH PODATAKA

Prilikom razmatranja najbolje varijante za konfigurisanje prostora na storage uređaju, a kako bi se u datim okolnostima dobile najbolje performanse za prostor veličine 5,6TB koji je potreban za smiještanje rezervnih kopija standardnih podataka, upotrijebljeni su mehanizmi za virtuelizaciju prostora na nivou servera i na nivou storage uređaja.

Prva opcija je podrazumijevala konfigurisanje skupa od 24 diska veličine 240GB na storage uređaju koji se onda linijski mapiraju mehanizmom za virtuelizaciju prostora na serveru (LVM) kako bi se dobio jedan objedinjeni disk – logički volume (LV) /dev/vgbackup/backup veličine 5,6TB. Tim postupkom su se postigle najbolje performanse, budući da je omogućen istovremeni pristup svim diskovima. Međutim, ovakav pristup se nije pokazao praktičnim i skalabilnim jer je vrlo brzo trebalo proširiti prostor predviđen za backup na 6TB, a zbog linijskog mapiranja to se nije moglo učiniti prostim dodavanjem prostora u VG. Zbog toga se pristupilo drugoj opciji koja predstavlja kombinovanu metodu virtuelizacije; prvo je pomoću softvera koji virtuelizuje prostor na storage sistemu kreirano 5 grupa diskova sastavljenih od 4 diska veličine 240GB i jedna grupa od 8 diskova veličine 150GB. Nakon toga su diskovi linijskom metodom mapiranja direktno na storage uređaju objedinjeni u velike diskove od 960GB, odnosno 1200GB i tako mapirani serveru. Serveru je na taj način vidljivo ukupno 6 velikih diskova. Zatim je na serveru pomoću LVM alata linearnom metodom virtuelizacije kreiran jedan veliki disk od 6000GB ~ 5,87TB:

```
5*(4*240GB) + (8*150GB) = 5*960GB + 1200GB = 6000GB / 1024 = 5,87TB
```

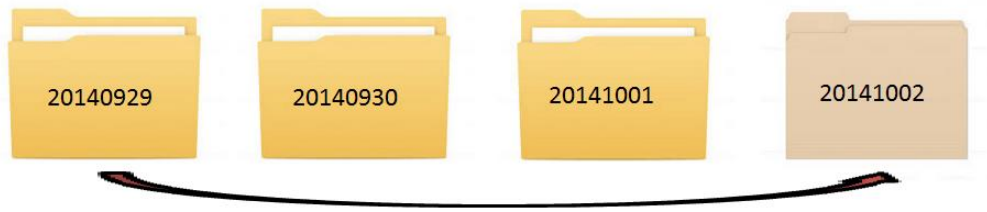
Nakon kreiranja logičkog volumena (LV), odnosno particije, disk je postavljen u ext4 format pomoću mkfs.ext4 komande i tek onda montiran na sistem na odgovarajući mount-point direktorijum /backup, kako bi se dobio upotrebljivi prostor, odnosno fajlsistem. Prilikom računanja potrebnog prostora, potrebno je uzeti u obzir da ~5% ukupnog prostora [*mkfs.ext4 man page*] koristi sami fajlsistem, tako da se dobije manje iskoristivog prostora nego što je očekivano:

```
5,87TB x 0,95 ~ 5,6TB
```

To znači da je konfigurisan fajlsistem upotrebljivog prostora veličine 5,6TB koji se može koristiti za skladištenje rezervnih kopija fajlova. Prostor dobijen ovakvom metodom se u slučaju potrebe jednostavno može proširiti linearnim dodavanjem diskova u volume grupu, a particija i fajlsistem /backup se mogu proširiti dok su aktivni (*online)* bez potrebe demontiranja (*umount*) prostora. Velika prednost je mogućnost proširivanja fajlsistema koji je u aktivnom stanju (*online*), budući da je teško naći vremenski prostor u kom on ne mora biti dostupan i u kom se može spustiti radi akcija proširenja. Određeno linijsko mapiranje u cilju poboljšanja performansi se ipak ostvaruje na samom storage uređaju na virtuelnim diskovima.

Nakon što je fajlsistem za skladištenje standardnih podataka kreiran na particiji veličine 5,87TB prezentovanoj sa storage uređaja i montiran na novokreirani mount-point direktorijum /backup na backup serveru, kreirani su direktorijumi sa imenima svakog servera pojedinačno. U svakom pojedinačnom direktorijumu kreiran je novi direktorijum *FS/*. Nakon toga su u *FS/* direktorijumu kreirani direktorijumi čija imena označavaju datum kada je izvršen backup podataka. Ove direktorijume kreira skripta *backup_fs.sh* pomoću komande *`date +%Y%m%d`* tako da se njegovo ime sastoji od trenutne godine, mjeseca i dana. Izabran je takav redosljed kako bi se direktorijumi uvijek sortirali po starosti bez obzira na prelazak u novi mjesec ili novu godinu.

Efekat inkrementalnog backup-a u smislu vremena potrebnog za izvršavanje skripte se postiže pomoću određene sekvence u skripti, iako se zauzima prostor kompletnog backupa. Rotaciona šema funkcioniše tako što se nakon tri dana folder sa zadnjim backup materijalom preimenuje u današnji i u njemu se odradi inkrementalni backup (Slika 5.1).



Slika 5.1: *Logički prikaz rotacione šeme u skripti*

Kako nijedna komanda nema mogućnost čuvanja isključivo promjena i samo jednog kompletnog backupa, došlo se do prelaznog rješenja; čuvaju se 3 zadnja kompletna backup-a, što jeste 3 puta više prostora, ali je vrijeme kopiranja skraćeno samo na razlike. Na taj način se dnevni backup od ~2TB preko LAN mreže završi za 3 sata u prosjeku, a pri tom nema potrebe definisati dodatne procedure koje brišu stare podatke (*cleanup procedure*).

5.5.2 REPOZITORIJUM ORACLE BAZE PODATAKA

Kako se rješenje za kreiranje rezervnih kopija baza podataka zasniva na tipu backupa na nivou bloka, kapacitet koji je potreban za skladištenje baze podataka odgovara veličini izvornih diskova i iznosi 1072GB. Izvorna baza je smještena na kombinaciji SSD i FC diskova koji predstavljaju kombinaciju diskova sa najboljim performansama, dok je klon kopija baze smještena na najslabijim SATA diskovima. Diskovi na kojima se nalazi kopija baze podataka su konfigurisani tako da su vidljivi isključivo backup serveru.

U tabeli 5.5 data je veza između fajlsistema i *volume* grupa na kojima se nalazi izvorna baza MASTER i diskova na storage uređaju. Kolona „Mount-point direktorijum fajlsistema“ ujedno predstavlja organizaciju fajlsistema izvorne baze grupisanih u četiri volume grupe od kojih je svaka sastavljena od četiri fizička diska koje definiše WWN identifikator na strani Linux servera i SYMDEV identifikator na strani storage uređaja.

Tabela 5.5: *Veza između fajlsistema baze MASTER i diskova na storage uređaju*

Mount-point direktorijum fajlsistema	Ime volume grupe	SYMDEV	DISK WWN	Alias diska
/pkgmasterdbprod/redologa	vgmasterd	0645	360000970000298700871533030363435	cluster_vgmasterdbredoA_dsk01

	bredoA	0647	360000970000298700871533030363437	cluster_vgmasterdbredoA_dsk02
		0646	360000970000298700871533030363436	cluster_vgmasterdbredoA_dsk03
		0648	360000970000298700871533030363438	cluster_vgmasterdbredoA_dsk04
/pkgmasterdbprod/redologb	vgmasterdbredoB	064A	360000970000298700871533030363441	cluster_vgmasterdbredoB_dsk01
		0649	360000970000298700871533030363439	cluster_vgmasterdbredoB_dsk02
		064B	360000970000298700871533030363442	cluster_vgmasterdbredoB_dsk03
		064C	360000970000298700871533030363443	cluster_vgmasterdbredoB_dsk04
/pkgmasterdbprod/oradata1	vgmasterdbdata	0642	360000970000298700871533030363432	cluster_vgmasterdbdata_dsk01
/pkgmasterdbprod/oradata2		0643	360000970000298700871533030363433	cluster_vgmasterdbdata_dsk02
/pkgmasterdbprod/oradata3		0644	360000970000298700871533030363434	cluster_vgmasterdbdata_dsk03
/pkgmasterdbprod/oradata4		0641	360000970000298700871533030363431	cluster_vgmasterdbdata_dsk04
/pkgmasterdbprod/oracle				
/pkgmasterdbprod/oraclearch	vgmasterdbarc	064D	360000970000298700871533030363444	cluster_vgmasterdbarc_dsk01
		064E	360000970000298700871533030363445	cluster_vgmasterdbarc_dsk02
		0650	360000970000298700871533030363530	cluster_vgmasterdbarc_dsk03
		064F	360000970000298700871533030363446	cluster_vgmasterdbarc_dsk04

Dok je WWN univerzalna oznaka koju koristi Linux server, SYMDEV je translirana WWN oznaka koju koristi konkretni storage uređaj i njegovi alati kao što je Symcli, u svojim konfiguracionim fajlovima. Veza između ova dva parametra je linearna, a zakonitost se nalazi u tabeli 5.6. Npr. WWN diska *cluster_vgaprmdbarc_dsk01* je 360000970000298700871533030363444, zadnjih 8 cifara su 30363444, a kada se grupišu po dvije cifre: 30, 36, 34, 44 i mapiraju prema tabeli, dobija se: 0, 6, 4, d, odnosno SYMDEV 064D.

Tabela 5.6: *Linearna zavisnost između SYMDEV i WWN parametara*

	Moguće opcije															
Dio WWN identifikatora	30	31	32	33	34	35	36	37	38	39	41	42	43	44	45	46
Translacija u SYMDEV	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

U tabeli 5.7 prikazana je konfiguracija i međusobni odnos izvornih diskova na serveru serv01db i destinacionih diskova koji su predstavljeni backup serveru *servrepdb*.

Tabela 5.7: *Konfiguracija produkcionih i klon diskova*

Izvorni uređaji						
Server	**Ime VG**	**Broj diskova**	**Kapacitet pojedinačnog diska (GB)**	**Ukupni kapacitet diska (GB)**	**Tip fizičkih diskova (Bound Pool)**	**Izvorne WWN oznake (Symdev)**
serv01db	vgmasterdbdata	4	130	520	SSD/FC 300GB	0641, 0642, 0643, 0644
serv01db	vgmasterdbarc	4	130	520	SSD/FC 300GB	064D, 064E, 064F, 0650
serv01db	vgmasterdbredoA	4	4	16	SSD/FC 300GB	0645, 0646, 0647, 0648
serv01db	vgmasterdbredoB	4	4	16	SSD/FC 300GB	0649, 064A, 064B, 064C
Destinacioni uređaji						

Server	Ime VG	Broj diskova	Kapacitet pojedinačnog diska (GB)	Ukupni kapacitet diska (GB)	Tip fizičkih diskova (Bound Pool)	WWN oznaka na destinaciji (Symdev)
servrepdb	vgmasterdbdata	4	130	520	SATA 2000GB	0723, 0724, 0725, 0726
servrepdb	vgmasterdbarc	4	130	520	SATA 2000GB	072F, 0730, 0731, 0732
servrepdb	vgmasterdbredoA	4	4	16	SATA 2000GB	0727, 0728, 0729, 072A
servrepdb	vgmasterdbredoB	4	4	16	SATA 2000GB	072B, 072C, 072D, 072E

Konfiguracioni fajl kojeg koristi symcli alat je tekstualni fajl koji sadrži tabelu u koju su upisani SYMDEV identifikatori; prva kolona sadrži SYMDEV identifikatore izvornih diskova, dok su u drugoj koloni mapirani odgovarajući SYMDEV identifikatori destinacionih diskova na kojima se nalazi klon. SYMDEV identifikatori moraju biti pravilno mapirani po odgovarajućem redosljedu inače operacija kloniranja neće biti uspješna, a moguće je i uništenje podataka na diskovima. Nakon kloniranja, na destinacionim diskovima nije potrebno iznova kreirati LVM strukturu, već je ona kopirana zajedno sa ostalim podacima.

Nakon što se na storage uređaju kreira struktura diskova identična izvornim diskovima, potrebno je napraviti vezu među ovim diskovima i kreirati prvi potpuni klon. U tom trenutku se stvara veza među izvornim i destinacionim diskovima prema tabeli u konfiguracionom fajlu koja nadalje postoji i omogućava proces inkrementalnog kloniranja. Kada se ova veza raskine, u tom trenutku se prekida odnos original – klon i dobijaju se dvije nezavisne grupe diskova.

Prvo kloniranje najduže traje i zavisi od veličine baze, jer treba iskopirati svaki blok na nivou storage uređaja. Prvo kloniranje konkretne MASTER baze je trajalo 44 minuta, budući da je ukupna veličina svih njenih diskova preko 1TB.

5.6. Testiranje operacije oporavka podataka

5.6.1 OPORAVAK STANDARDNIH PODATAKA

Jedna od najvažnijih tema za planiranje oporavka podataka je pravilno planiranje metode za backup. Kao što je već rečeno, infrastruktura je uglavnom zaštićena od hardverskih otkaza implementacijom koncepta „bez tačke prekida“. Storage kao uređaj ima određene vidove zaštite svih podataka od otkaza jednog ili više diskova, kontrolera, portova i ostalih njegovih segmenata. Budući da je u ovom slučaju najveći uzročnik gubitka podataka ljudski faktor ili korupcija softvera ili baze, izgubljeni podaci će se nalaziti na makar jednoj od 3 dnevne kopije na primarnom backup repozitorijumu. Ukoliko se kasno otkrije gubitak fajlova, starije backup materijale je moguće pronaći na trakama.

Zbog dobro planirane backup strategije, restore je vrlo jednostavna operacija. Vrši se reverzibilnom *rsync* komandom koja je inicijalno poslužila za backup podataka. Primjer oporavka jednog direktorijuma na *serv01app* serveru za proizvoljni datum, npr. 14. septembar 2014. godine je predstavljen u kodu 5.3.

```
# /usr/bin/rsync -avzx --progress --delete --exclude={/lost+found} --inplace --ignore-
errors --blocking-io --numeric-ids --timeout=1500
/backup/serv01app/FS/20140914/ctmuser1/ root@serv01app:/ctmuser1/
```

Kod 5.3: *Primjer oporavka direktorijuma sa standardnim podacima*

Budući da se podaci vraćaju na originalnu lokaciju, vrijeme oporavka zavisi od količine podataka koju treba povratiti i od najsporije karike u čitavom procesu. Pošto je brzina upisa na disk na storage uređaju veća od brzine mreže, a brzina mreže je približno 100MB/s, brzina restore operacije je limitirana rsync funkcijom kako je prikazano testiranjem mreže i dostiže

vrijednosti do 16MB/s. Ovo je najveći nedostatak ove funkcije i predstavlja usko grlo u slučaju operacije restore, jer se tako ne mogu iskoristiti kapaciteti mreže i diskova sa storage uređaja u smislu brzine oporavka podataka. Ipak, kako bi backup trebala biti sporedna operacija, zahvaljujući manjoj brzini prenosa, oslobođeni su resursi servera za nesmetano funkcionisanje glavne aplikacije.

5.6.2 OPORAVAK SISTEMSKIH PODATAKA

Root particija je veličine 2GB na svim serverima i nalazi se na lokalnim diskovima zajedno sa ostalim sistemskim particijama u volume grupi vg00. Ovakvo particionisanje i mala veličina root particije omogućavaju olakšan restore sistemskih podataka. Korupcija root particije u opisanim okolnostima je dosta rijedak slučaj jer se na sistemima instaliranim i podešenim za određene svrhe vrlo rijetko vrše modifikacije na root nalogu.

Ukoliko je prilikom korupcije sistemskih podataka operativni sistem i dalje funkcionalan, oporavak je moguće odraditi direktno pomoću rsync komande, kopiranjem oštećenih/obrisanih fajlova. Restart sistema je neophodan kako bi se utvrdila postojanost operativnog sistema.

Ukoliko je došlo do korupcije sistemskih podataka, a sistem nije funkcionalan i ne može se podići, treba reinstalirati sistem na približno istu distribuciju operativnog sistema i sa istim rasporedom LVM particija, a nakon toga izvršiti *restore* svih podataka pomoću *rsync* komande na svaki fajlsistem pojedinačno, uključujući i *root*. Restart sistema je takođe neophodan kako bi se utvrdila postojanost sistema.

5.6.3 OPORAVAK BAZE PODATAKA

Restore operacija se vrši nad istim diskovima koristeći reverzibilnu operaciju kloniranja i iste konfiguracione fajlove. Nije potrebno terminirati originalnu klon sesiju među diskovima kako bi se izvršila operacija oporavka ukoliko je inicijalna sesija kreirana pomoću opcije – *differential*, kao što je slučaj prilikom ove implementacije. Takođe, podatke je moguće vratiti i na potpuno nove diskove, ali je za to prvo potrebno terminirati originalnu sesiju.

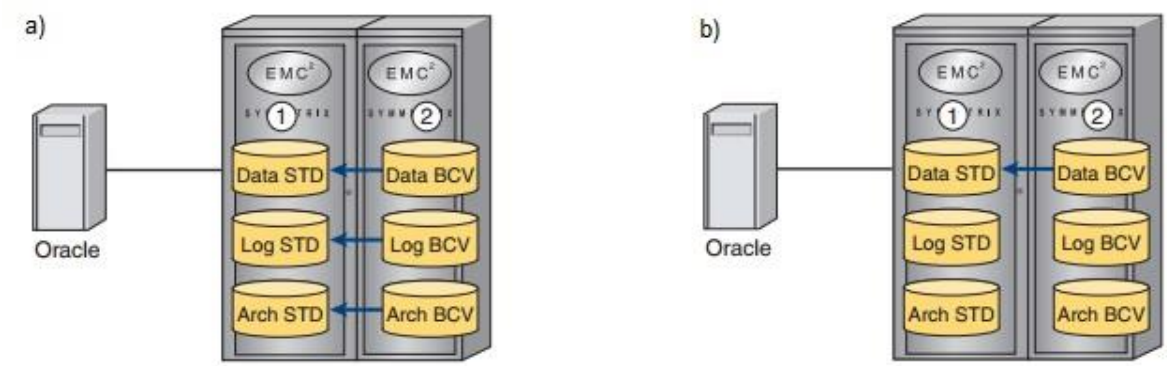
U sledećoj tabeli 5.8 date su smjernice koje treba pratiti kako bi se oporavila baza podataka prilikom oštećenja:

Tabela 5.8: *Scenarija i smjernice za izvršavanje restore operacija*

Scenario	**Smjernice za izvršavanje restore operacije**
Brisanje/korupcija tabele koja nije kritična za poslovanje. Produkcija može funkcionisati bez nje, sa određenim nedostacima.	Nastaviti produkciju i izvršiti restore tabele tokom dana sa klonirane kopije.
Brisanje/korupcija kritične tabele bez koje produkcija ne može nastaviti funkcionisanje.	Zaustaviti produkciju i izvršiti restore baze do sekunde u kojoj je tabela bila oštećena oporavljanjem samo fajlova sa podacima.
Korupcija baze usljed fizičkih oštećenja (npr. korupcija diska).	Opcija 1 – oporaviti bazu pomoću klon kopije. Opcija 2 – izvršiti restore operaciju sa traka.

Prije bilo kakve akcije koja zahtijeva operaciju oporavka podataka koristeći *symcli* softver, baza se mora spustiti a fajlsistemi demontirati. Operativni sistem ne bi trebalo da sadrži nijednu informaciju u svojoj memoriji koja se odnosi na prethodnu strukturu baze podataka.

Na slici 5.2.a je prikazan proces oporavka baze podataka kada se oporavlja baza u tački vremena. U tom slučaju se pored diskova koji sadrže fajlove sa podacima, oporavljaju strukture diskova na kojima se nalaze arhivirani log fajlovi, redo log fajlovi i kontrolni fajlovi. Ukoliko je zahtijevan potpuni restore, oporavljaju se samo strukture diskova koje sadrže fajlove sa podacima, a nakon toga primjenjuju arhivirani log fajlovi i redo log fajlovi sa originalne lokacije. Ovaj scenario je prikazan na slici 5.2.b



Slika 5.2: *Oporavak baze podataka iz klonirane sesije [55]*

Procedura za oporavak baze u tački vremena, odnosno oporavak svih kloniranih diskova koristi isti kontrolni fajl kao procedura za kloniranja diskova. U kontrolnom fajlu se nalazi lista svih diskova baze podataka: diskovi sa podacima baze, diskovi sa arhiviranim log fajlovima i diskovi sa redo log fajlovima. Uspješan oporavak baze zavisi od sljedećih koraka:

1. Verifikovati stanje kloniranih uređaja i potvrditi da su diskovi u aktivnom stanju.
2. Ugasiti Oracle bazu podataka na izvornim (produkcionim) diskovima.
3. Demontirati fajlsisteme produkcione baze kako bi se osiguralo da nema informacija u serverskom kešu.
4. Inicirati proces restore operacije klona.
5. Pokrenuti proces oporavka baze podataka. Moguće je pokrenuti proces prije nego što su podaci u potpunosti iskopirani na izvorne diskove.
6. Nakon završetka procesa oporavka, terminirati klon sesiju.

U kodu 5.4 date su komande za verifikovanje, oporavak i terminaciju klon sesije, gdje $SID predstavlja identifikacioni broj konkretnog storage uređaja, $CTL kontrolni fajl, a $LOGFILE fajl u koji se snimaju sve log informacije u svrhu kontrole i praćenja procesa.

```
# symclone -sid $SID -file $CTL -noprompt query >> $LOGFILE 2>&1
# symclone -sid $SID -file $CTL -noprompt restore >> $LOGFILE 2>&1
# symclone -sid $SID -file $CTL -noprompt terminate >> $LOGFILE 2>&1
```

Kod 5.4: *Komande za verifikovanje, oporavak i terminaciju klon sesije respektivno*

Postupak potpunog oporavka Oracle baze podataka je identičan, sa tom razlikom što se koristi kontrolni fajl u kom se nalazi samo lista diskova koji čine *vgmasterdbdata* grupu volumena, odnosno lista diskova sa podacima baze.

Takođe je moguće oporaviti bazu direktno iz backup materijala koji je smješten na trake. Ovakav oporavak bi trajao isto koliko i inicijalni potpuni backup na trake i zavisio bi od efektivne veličine baze koja iznosi oko 130GB. Brzina SAN mreže preko koje se vrši backup je oko 60MB/s, tako da bi oporavak sa trake fajlova sa podacima ovakve baze trajao oko 40 minuta.

5.7. Analiza rješenja za kreiranje rezervnih kopija podataka

5.7.1 ANALIZA RJEŠENJA ZA KREIRANJE REZERVNIH KOPIJA STANDARDNIH PODATAKA

Opisano backup rješenje standardnih podataka je skalabilno, a može se proširiti jednostavnim dodavanjem diskova sa storage uređaja ukoliko za to postoje kapaciteti. Fleksibilnost se ogleda u tome da prilikom dodavanja novih fajlsistema na bilo koji server, skripta ih automatski prepoznaje i vrši njihov backup na standardnoj lokaciji. Dodavanje novih servera je takođe jednostavno, dodavanjem nove linije u skripti koja se automatski pokreće iz *crontab* fajla. Iskorišćena je postojeća infrastruktura, mada je prostor na storage uređaju vrijedniji od prostora na uređajima za backup. Iskorišćene su sposobnosti *rsync Open Source* programa da vrši inkrementalni backup kako bi se skratilo vrijeme izvršavanja i rasteretila *Ethernet* mreža preko koje se vrši prenos fajlova. Postoji određena *logging* komponenta, tako da je jednostavno utvrditi razlog ukoliko se desio prekid u izvršavanju skripte. Vodi se evidencija u log fajlovima o svim fajlovima koji su kopirani i vremenu koje je potrebno za njihovo kopiranje. Budući da postoje 3 dnevne kopije, izgubljeni podaci će se nalaziti na nekoj od tih kopija.

U tabeli 5.9 predstavljeni su parametri koji opisuju proces kreiranja rezervnih kopija standardnih podataka u smislu trajanja procesa i brzine prenosa podataka u toku jedne sedmice. Sedmica dana predstavlja dovoljan uzorak budući da nema velikih odstupanja u dnevnim operacijama. Prosječno trajanje backup procesa je 3 sata i 36 minuta, dok je prosječna količina podataka koje se prenesu kroz mrežu 16,9GB. U prosjeku se za noć obradi 1,3TB, bez sistemskih fajlova koji uglavnom ostaju nepromijenjeni. Ubrzanje koje se postiže primjenom delta transfer algoritma je u prosjeku 85 puta. Prosječna efektivna brzina prenosa podataka je 1,35MB/s, što predstavlja vrijednost koja neznatno utiče na performanse i opterećenje mrežnih i serverskih resursa. Kada se uzme u obzir količina obrađenih podataka koja bi se u svakom drugom slučaju, korišćenjem ostalih alata za backup, kompletna prenosila preko mreže, dobija se vrijednost od 107MB/s, što je dosta velika vrijednost i predstavlja dobre performanse.

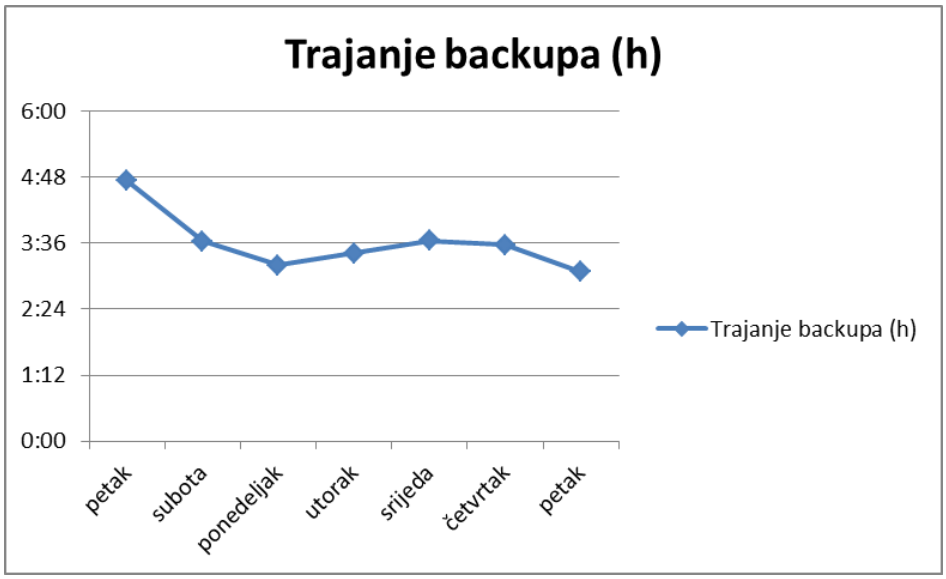
Tabela 5.9: *Parametri vezani za kreiranje rezervnih kopija standardnih podataka*

Dan	Početak backup procesa	Kraj backup procesa	Trajanje	Količina prenesenih podataka (GB)	Ukupno obrađeno podataka (GB)	Ubrzanje (obrađeno/ preneseno)	Brzina prenosa promijenjenih fajlova (MB/s)	Ukupna brzina prenosa (MB/s)
Petak	2:00	6:44	4:44	14,11737857	944,1001507	66,87503252	0,848368289	56,73465694
Subota	2:00	5:38	3:38	30,81375664	1148,53075	37,2733115	2,412330795	89,91555717
Ponedeljak	2:00	5:12	3:12	14,13659596	1388,847344	98,24482133	1,256586307	123,4530973
Utorak	2:00	5:25	3:25	15,89742116	1366,573116	85,96193699	1,323492623	113,7699895
Srijeda	2:00	5:39	3:39	13,33782264	1430,965555	107,2862935	1,039416316	111,5151239
Četvrtak	2:00	5:34	3:34	16,75654647	1652,861479	98,63974551	1,336347631	131,8169903
Petak	2:00	5:05	3:05	13,21607022	1342,188086	101,5572756	1,219212243	123,8198739
Prosjek			3:36	16,89651309	1324,86664	85,11977385	1,347964887	107,289327

Prvi uzorkovani petak ukazuje na znatno veće vrijeme izvršenja backup operacije koje iznosi 4 sata i 44 minuta i lošiju statistiku performansi od ostalih dana. U log fajlovima se vidi da je uzrok tome jedan fajlsistem na kome je u tom trenutku bilo 387GB korisnih podataka. Bilo je potrebno 3 sata 12min za inkrementalni backup čija je delta iznosila 9,5GB, a brzina prenosa je

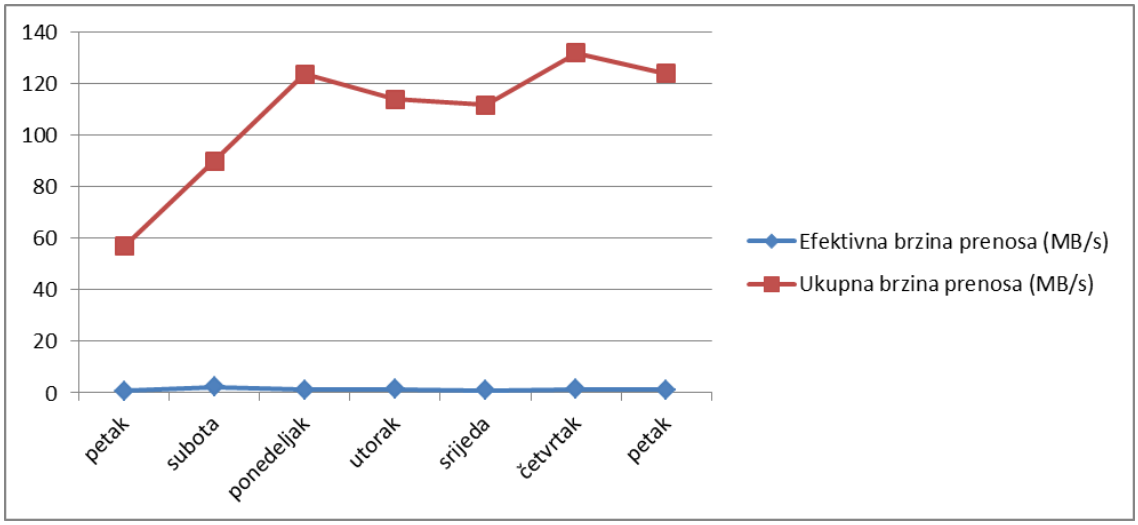
iznosila 853295.34 b/s što je jako sporo i ne poklapa se sa rezultatima dobijenim prilikom testiranja mreže u poglavlju 4.4.1. Uzrok takvog ponašanja može biti zagušenje u mreži ili opterećenost serverskih resursa, ali se ono iz priloženih logova nije moglo detaljnije utvrditi.

Na slici 5.3 grafički je predstavljeno trajanje backup operacija po danima u sedmici.



Slika 5.3: *Trajanje backup procesa standardnih podataka u satima*

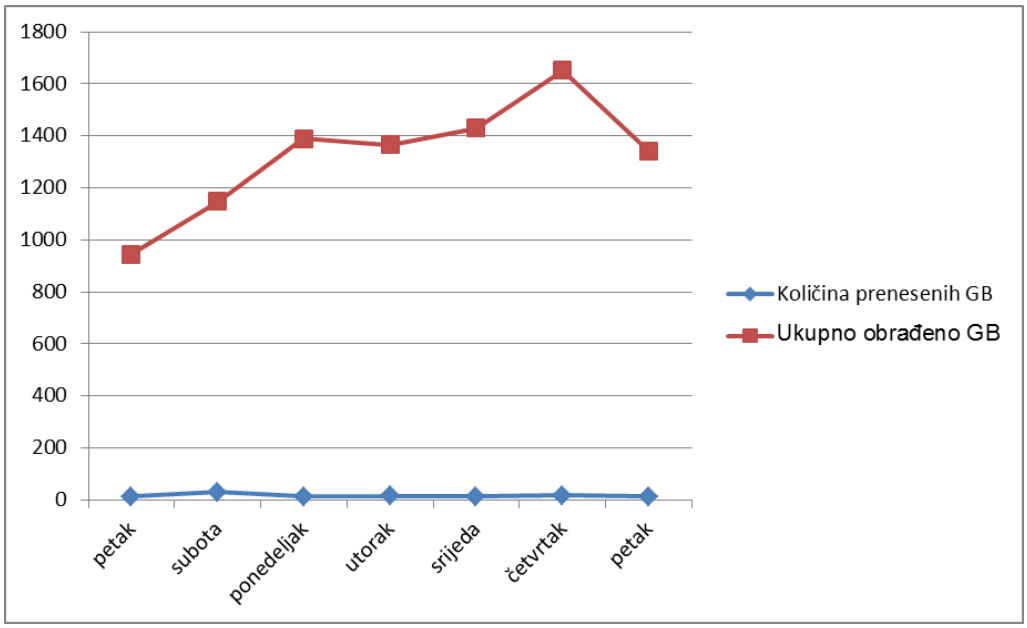
Na slici 5.4 grafički su predstavljene efektivna i ukupna brzina prenosa podataka u MB/s. Može se zaključiti da je ogromna ušteda u resursima prilikom korišćenja rsync delta transfer algoritma budući da plava kriva predstavlja efektivnu brzinu koja se ostvaruje prilikom prenosa stvarne količine podataka, dok crvena kriva predstavlja hipotetičku brzinu koja bi se postizala ukoliko bi se za isto vrijeme vršio potpuni backup svake noći.



Slika 5.4: *Poređenje efektivne i ukupne brzine prenosa podataka*

Na slici 5.5 grafički je predstavljeno poređenje ukupne količine podataka predviđenih za backup i količine prenesenih podataka u gigabajtima. I u ovom slučaju važi prethodni zaključak,

količina prenesenih podataka nemjerljiva je u odnosu na ukupnu količinu podataka za koju je trebalo organizovati kreiranje rezervnih kopija.



Slika 5.5: *Poređenje ukupne količine podataka predviđenih za backup i količine prenesenih podataka u GB*

Bez obzira na prikazane uštede u resursima, nije se postigla očekivana brzina prenosa podataka preko mreže. Prilikom testiranja mreže korišćenjem tar i rsync alata postigla se prosječna brzina od 16MB/s, dok statistika implementiranog rješenja pokazuje prosječnu brzinu 1,34MB/s što je 10 puta lošije, a približno 100 puta lošije od mogućnosti koje pruža kapacitet linka. U skladu sa tim je i vrijeme trajanja backup operacije 10 puta slabije od očekivanog. Pretpostavka autora ovog rada je da problem leži u loše postavljenim kernel parametrima vezanim za mrežu, ali tačna dijagnostika bi zahtijevala detaljniju analizu operativnog sistema što ne spada u domen ovog rada.

Ukoliko administratori ne vode računa o prostoru, dešava se da se particija prepuni podacima i da backup operacija ne bude uspješna. U tom slučaju, proces se ne završi do kraja i mora ručno da se terminira. Zato je neophodno svakodnevno provjeravati log fajlove. Poboljšanje rješenja bi moglo biti u pravcu transparentnosti, budući da ne postoji notifikacija koja obavještava o uspješnosti backup operacije. Postavljanje automatskog obavještavanja na e-mail i/ili SMS o uspješnosti izvršenog backupa bi značajno unaprijedilo izloženo rješenje. Takođe, ne postoji grafički interfejs, već se sve informacije dobijaju sa komandne linije, što čini rješenje nepreglednim i nerazumljivim za korisnike koji ne rade na Linux operativnom sistemu, te bi to mogao biti sledeći korak u razvoju ovog rješenja.

5.7.2 ANALIZA RJEŠENJA ZA KREIRANJE REZERVNIH KOPIJA ORACLE BAZA PODATAKA

Predstavljeno rješenje za kreiranje rezervnih kopija Oracle baza podataka je jedno od standardizovanih rješenja koje nosi nekoliko prednosti. Konzistentnost Oracle baze je jedna od najvažnijih karakteristika ovakvog rješenja, budući da je baza izuzetno osjetljiva struktura koja mora da se čuva u cjelosti. Standardni podaci se ne suočavaju sa ovakvim zahtjevom, budući da je njihova struktura jednostavna za kopiranje. Ovakvo rješenje za kreiranje rezervnih kopija

podataka je moguće primijeniti i na standardne podatke, međutim to nije praksa jer se troši previše resursa u vidu prostora na storage uređaju. Takođe, proces kloniranja je isti na svim operativnim sistemima koji su kompatibilni sa Oracle bazom podataka, budući da se kopiranje vrši na nivou blokova na storage uređaju, a ne na samom operativnom sistemu.

Najveća prednost ovakvog rješenja leži u skraćenom vremenu za oporavak podataka. Oporavak sa traka uglavnom traje nekoliko sati u zavisnosti od veličine baze, dok oporavak putem kloniranja u ovom slučaju traje svega nekoliko minuta. U tabeli 5.10 predstavljeni su parametri vezani za trajanje procesa kloniranja u toku jednog mjeseca. Druga kolona predstavlja promjene u megabajtima koje su se desile tokom dana od kad je zadnji put napravljen klon baze. To je razlika na dnevnom nivou koju je potrebno kopirati da bi baza bila ažurirana prilikom kloniranja, odnosno veličina inkrementalnog backupa u vidu blokova podataka.

Tabela 5.10: *Parametri procesa kloniranja baze MASTER*

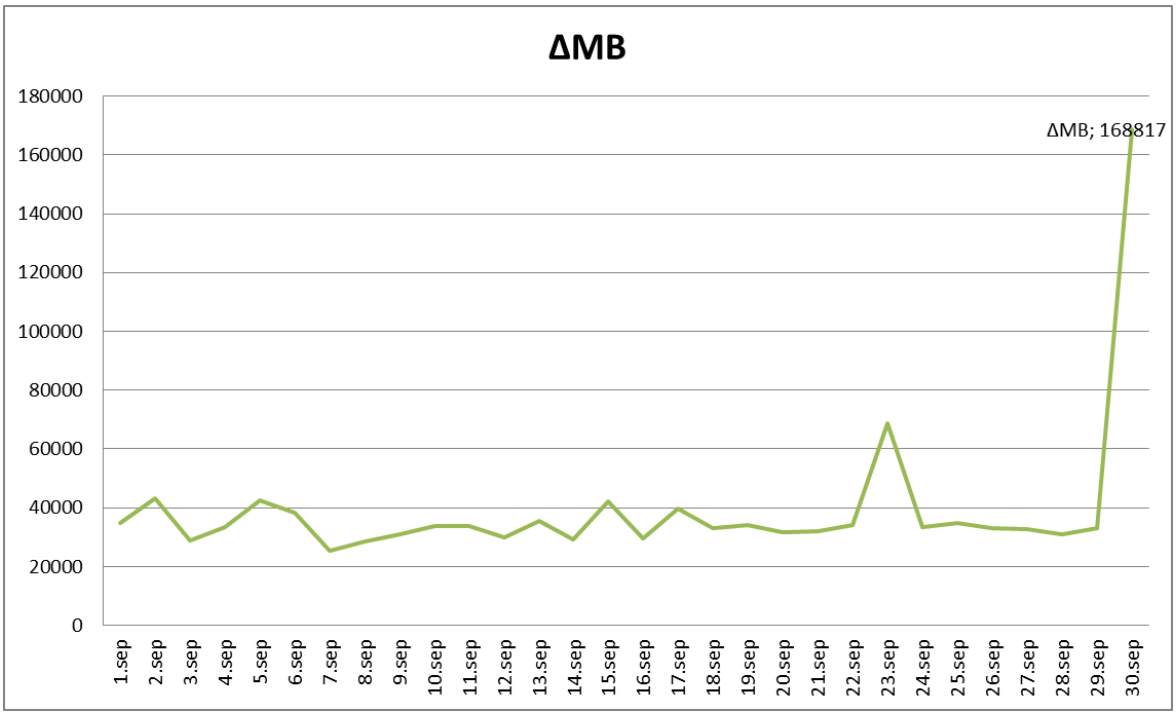
MASTER baza	ΔMB	Trenutak spuštanja baze	Početak kloniranja	Završetak kloniranja	Završetak podizanja baze	Trajanje kompletnog procesa	Trajanje procesa kloniranja
1.sep	34940,1	0:30:41	0:30:51	0:38:38	0:39:13	0:08:32	0:07:47
2.sep	43127,1	0:26:27	0:26:38	0:40:59	0:41:32	0:15:05	0:14:21
3.sep	28790.9	0:29:31	0:29:43	0:38:24	0:38:51	0:09:20	0:08:41
4.sep	33322.3	0:27:12	0:27:23	0:35:58	0:36:31	0:09:19	0:08:35
5.sep	42658.6	0:31:38	0:31:49	0:42:24	0:42:45	0:11:07	0:10:35
6.sep	38255.6	0:31:30	0:31:42	0:42:24	0:42:43	0:11:13	0:10:42
7.sep	25327.6	0:23:47	0:23:58	0:31:53	0:32:12	0:08:25	0:07:55
8.sep	28386.1	0:28:25	0:28:36	0:37:07	0:37:40	0:09:15	0:08:31
9.sep	30926.8	0:28:01	0:28:12	0:39:47	0:40:06	0:12:05	0:11:35
10.sep	33862.1	0:30:20	0:30:32	0:38:05	0:38:27	0:08:07	0:07:33
11.sep	33793.2	0:31:10	0:31:21	0:38:58	0:39:26	0:08:16	0:07:37
12.sep	29841.0	0:30:21	0:30:32	0:38:07	0:38:28	0:08:07	0:07:35
13.sep	35423.4	0:28:39	0:28:50	0:42:49	0:43:24	0:14:45	0:13:59
14.sep	29038.6	0:28:18	0:28:30	0:37:13	0:37:49	0:09:31	0:08:43
15.sep	42064.4	0:30:03	0:30:14	0:45:21	0:45:57	0:15:54	0:15:07
16.sep	29511.7	0:29:29	0:29:40	0:37:26	0:38:02	0:08:33	0:07:46
17.sep	39790.9	0:31:21	0:31:31	0:42:19	0:42:53	0:11:32	0:10:48
18.sep	32912.6	0:27:22	0:27:33	0:36:18	0:36:36	0:09:14	0:08:45
19.sep	34053.7	0:31:03	0:31:16	0:39:42	0:40:00	0:08:57	0:08:26
20.sep	31699.9	0:24:45	0:24:56	0:33:44	0:34:03	0:09:18	0:08:48
21.sep	31869.5	0:28:02	0:28:13	0:35:48	0:36:10	0:08:08	0:07:35
22.sep	34076.5	0:34:09	0:34:19	0:46:07	0:46:39	0:12:30	0:11:48
23.sep	68623.9	0:36:31	0:36:42	0:47:31	0:48:06	0:11:35	0:10:49
24.sep	33315.4	0:27:06	0:27:18	0:34:58	0:35:16	0:08:10	0:07:40
25.sep	34789,2	0:30:05	0:30:15	0:38:50	0:39:26	0:09:21	0:08:35
26.sep	33051,9	0:30:03	0:30:15	0:37:56	0:38:16	0:08:13	0:07:41
27.sep	32626,4	0:27:50	0:28:01	0:35:38	0:35:58	0:08:08	0:07:37
28.sep	31002,5	0:26:23	0:26:24	0:34:46	0:35:04	0:08:41	0:08:22

29.sep	32978,6	0:28:09	0:28:19	0:36:45	0:37:21	0:09:12	0:08:26
30.sep	168817	0:53:43	0:53:54	1:34:57	1:35:22	0:41:39	0:41:03
Prosjek	51416,6					0:11:04	0:10:27

Skripta za kloniranje ne pokreće proces kloniranja MASTER baze u isto vrijeme, već to zavisi od nekih njenih prethodnih akcija. U koloni 3 je dat trenutak kada počinje spuštanje baze MASTER koje u prosjeku traje 10tak sekundi. Nakon toga kreće proces kloniranja i tek kada se potpuno završi, baza se automatski podiže, što u prosjeku traje nekih 20tak sekundi. Iz tabele se takođe zaključuje da je trajanje procesa kreiranja rezervne kopije baze podataka primjenom opisanog rješenja u prosjeku 10tak minuta, a isto toliko traje proces oporavka, budući da je on reverzibilna operacija kloniranja. I prilikom operacije kreiranja rezervnih kopija i prilikom operacije oporavka, moguće je klon aktivirati odmah nakon akcije rekreiranja, tako da se baza može odmah podići dok se proces kopiranja obavlja u pozadini. Međutim, zbog sigurnosti u ovom slučaju izabran je postupak ponovnog kreiranja klona u potpunosti, i tek nakon što su svi podaci iskopirani slijedi njegova aktivacija. Ovakav postupak povećava vrijeme trajanja operacije kloniranja.

U tabeli je prikazan prosjek svakodnevnih promjena na podacima baze MASTER i on iznosi 51416,6MB. Prosječno vrijeme koje je potrebno za završetak procesa kloniranja iznosi 10 minuta i 27 sekundi, dok trajanje kompletnog procesa iznosi prosječno 11 minuta i 4 sekunde.

Na slici 5.6 dat je grafički prikaz razlike količine podataka koja se kopira na dnevom nivou, odnosno delte u MB.

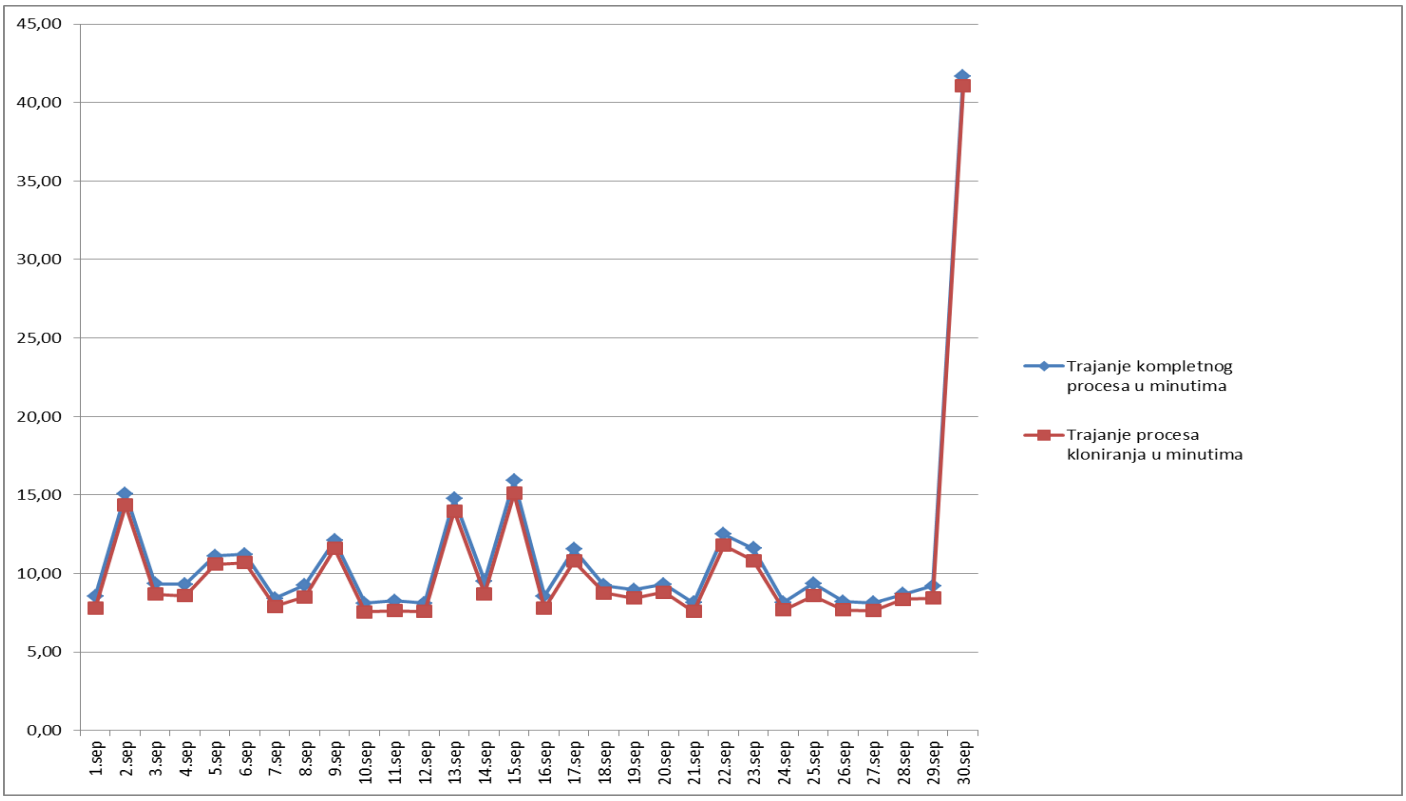


Slika 5.6: *Grafički prikaz količine podataka u MB koji se dnevno kopiraju tokom jednog mjeseca*

Na slici 5.7 dat je grafički prikaz trajanja kompletnog procesa i procesa kloniranja po danima u periodu od jednog mjeseca. Razlika između ova dva procesa nije više od 1 minut, a to je vrijeme koje je potrebno da se klon baza spusti i nakon završetka procesa podigne. Uočava se

linearna zavisnost između delte količine podataka i vremena trajanja procesa kloniranja. Što je delta veća, to je vrijeme trajanja procesa kloniranja duže.

Kako se kopiranje podataka obavlja na nivou storage sistema, nema prenosa podataka kroz LAN ili SAN što značajno rasterećuje mrežu. Može se desiti da storage sistem bude opterećen usljed velikog broja operacija koje izvršava. Zbog toga se biraju noćni sati za automatsko izvršavanje operacije kloniranja tako da se što više rastereti period u kojem obični korisnici pristupaju produkcionoj bazi podataka.



Slika 5.7: *Grafički prikaz trajanja procesa kloniranja tokom jednog mjeseca*

Razvijeno je opsežno zapisivanje i snimanje log informacija koje u potpunosti prate proces kreiranja klonova, tako da je prilikom svakog izvršavanja skripte moguće utvrditi eventualni problem. Međutim, i za ovo rješenje ne postoji grafički interfejs, tako da je za njegovo upravljanje neophodno poznavanje Linux operativnog sistema i LVM alata. Notifikacija se šalje prilikom neuspješnog izvršavanja skripte tako da proces nije potrebno svakodnevno kontrolisati.

Mane ovakvog rješenja su dvostruki prostor kojeg backup materijal zauzima, budući da se skladišti i na diskovima i na trakama. Međutim ovo istovremeno predstavlja i prednost jer daje dvostruku sigurnost da su podaci očuvani i konzistentni. Svrha kopije zavisi od tipa medijuma na kojem se kopije čuvaju; ukoliko je potreban trenutni oporavak, upotrijebiće se kopije na diskovima, a ukoliko je potrebno doći do podataka iz određenog perioda, za oporavak će se upotrijebiti kopije na trakama.

Zaključak

U ovom radu je predstavljen predlog heterogenog rješenja koji je primijenjen na realno okruženje konkretne kompanije prikazujući kompletan proces kreiranja rezervnih kopija podataka od planiranja strategije do implementacije i validacije rješenja. Temeljno je izložena sistematizacija terminologija, metodologija i tehnologija u oblasti koja tretira sisteme i načine za kreiranje rezervnih kopija podataka i njihov oporavak.

Predloženo rješenje je heterogeno jer tretira i objedinjuje kreiranje rezervnih kopija dvije različite kategorije podataka, standardne podatke i Oracle baze podataka na Linux operativnim sistemima, u skladu sa prethodno definisanom backup politikom kompanije. Ono se zasniva na mehanizmu D2D2T kreiranja rezervnih kopija podataka. D2D2T mehanizam se sastoji od dva koraka, backup sa diska na disk (primarni backup) i backup sa diska na traku (sekundarni backup). Ovaj rad se fokusira na primarni backup podataka čiji je medijum disk, budući da je sekundarni backup standardizovani proces koji pomoću integrisane backup infrastrukture smiješta podatke na trake. Primarni backup standardnih podataka se zasniva na *Open Source* alatu *rsync*, a primarni backup Oracle baze podataka na konceptu snimka. Alati za primarni backup podataka su inkorporirani u formu skripte na Linux operativnom sistemu i automatizovani tako da se kompletan proces odvija bez ljudske interakcije.

Koristeći postojeću infrastrukturu, predloženo rješenje kombinuje prednosti diska i trake u cilju optimizacije backup procesa, unaprijeđenja pouzdanosti backup materijala i smanjenja vremena oporavka.

Prednosti rješenja za kreiranje rezervnih kopija standardnih podataka su skalabilnost, fleksibilnost i rasterećenje mrežnih resursa. Jednostavnom modifikacijom skripte rješenje je moguće proširiti dodavanjem novih servera čije je kopije potrebno čuvati. Kapacitet potreban za čuvanje podataka je jednostavno nadograditi dodavanjem diskova i proširenjem particije za backup bez prekida funkcionalnosti. Fleksibilnost se ogleda u tome da prilikom dodavanja novih fajlsistema na bilo koji server, skripta ih automatski prepoznaje i vrši njihov backup na standardnoj lokaciji. Iskorišćene su sposobnosti *Open Source* programa *rsync* da vrši inkrementalni backup kako bi se skratilo vrijeme izvršavanja i rasteretila Ethernet mreža preko koje se vrši prenos fajlova.

Prednosti rješenja za kreiranje rezervnih kopija baza podataka se ogledaju u skraćenom vremenu za oporavak podataka, očuvanju konzistentnosti kopije baze i rasterećenju mrežnih resursa. Primjenom koncepta snimka, kompletan oporavak baze podataka od nekoliko terabajta traje svega nekoliko minuta. Kako se kopiranje podataka obavlja na nivou storage sistema, nema prenosa podataka kroz LAN ili SAN što značajno rasterećuje mrežu. Razvijen je detaljan proces kontrole i nadgledanja tako da je u svakom trenutku moguće utvrditi razlog za eventualni problem.

Dok je rješenje za kreiranje kopija standardnih podataka nezavisno u odnosu na modele korišćenih uređaja, predloženo rješenje za kreiranje rezervnih kopija baza podataka zasnovano je na korišćenju EMC Symmetrix modela *storage* uređaja i njegovih funkcionalnosti i to predstavlja značajan nedostatak. Nadalje, mane rješenja su dvostruki prostor kojeg backup materijal zauzima, budući da se skladišti i na diskovima i na trakama. Međutim ovo istovremeno predstavlja i prednost jer daje dvostruku sigurnost da su podaci očuvani i konzistentni. Za predloženo rješenje nije razvijen GUI, tako da je za upravljanje, kontrolu i nadgledanje backup procesa neophodno poznavanje Linux operativnog sistema i LVM alata. U opisanoj realizaciji predloženog rješenja, nedostatak je korišćenje jednog storage uređaja za smiještanje originalnih podataka i primarnog backup materijala čime on predstavlja „jedinstvenu tačku prekida“.

Kompletno rješenje je moguće realizovati na odvojenom storage uređaju na udaljenoj lokaciji. Ovaj nedostatak u konkretnoj primjeni nadomješćuje sekundarna backup operacija koja sekundarni backup materijal čuva na odvojenoj lokaciji na trakama.

Ovaj rad se može razvijati u pravcu unapređenja predloženog rješenja kroz razvoj grafičkog interfejsa koji bi dato rješenje učinio dostupnim širem spektru korisnika. Razvoj novih rješenja otvorenog koda koji su široko primjenjivi i finansijski isplativiji, a ne zavise od proizvođača i modela uređaja, bi mogao biti cilj budućih radova na ovu temu. Nadalje, razvoj adekvatnih rješenja u specifičnim sredinama i jačanje svijesti o značaju kreiranja rezervnih kopija podataka bi trebalo tretirati u daljim istraživanjima. S obzirom na kompletnost izložene materije rad može poslužiti kao osnov za dalje analize i primjene u naučno-istraživačkim i komercijalnim svrhama.

Literatura

[1] Brocade Communications Systems, Inc. (2007) Data Protection: Understanding the Benefits of Various Data Backup and Recovery Techniques, dostupno na http://www.officeproductnews.net/sites/default/files/DataProtection_WP_00.pdf [pristupano 23. novembra 2015.]

[2] The Alchemy Solutions Group (2009) Backup and Recovery, dostupno na http://eval.symantec.com/mktginfo/enterprise/customer_successes/b-bva_mrr_backup_and_recovery.en-us.pdf [pristupano 21.aprila 2015.]

[3] DuBois Laura (2012), Backup and Recovery Changes Drive IT Infrastructure and Business Transformation, dostupno na http://www.emc.com/collateral/software/white-papers/ar-backup-and-recovery-changes-drive-it.pdf [pristupano 23. novembra 2015.]

[4] Mell Peter, Grance Timothy (2011), The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145, dostupno na http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [pristupano 23. novembra 2015.]

[5] Clark, Tom (2008), Strategies For Data Protection, Brocade Communications Systems, dostupno na http://www.brocade.com/downloads/documents/books/Strategies_for_Data_Protection_First_Edition.pdf [pristupano 23. novembra 2015.]

[6] ISO/IEC 27002:2013, Information technology - Security techniques - Code of practice for information security controls

[7] Službeni list Crne Gore (2013), Zakon o elektronskim komunikacijama, Podgorica: "Službeni list Crne Gore, broj 40/2013", str. 74-77

[8] Cobb, M. (2009) How to create a data classification policy, ComputerWeekly.com, dostupno na http://www.computerweekly.com/tip/How-to-create-a-data-classification-policy [pristupano 23. novembra 2015.]

[9] Christensson, P. (2008) Backup, http://www.techterms.com/definition/backup

[10] Guidance Consulting Inc. (2012) Data Recovery - the importance of data backups, http://www.guidance-consulting.com/articles/60-importance-of-data-backups-.html

[11] David M. Smith (2003), The Cost of Lost Data, Graziado Business Review, Pepperdine University, http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/

[12] Xiotech (2006), Tiered Data Protection and Recovery, Xiotech Corporation, dostupno na http://fredv3.sharepointspace.com/downtime/Shared%20Documents/wp070311_TieredDR[1].pdf [pristupano 23. novembra 2015.]

[13] Brooks, C. Bedernjak, M. Juran, I. Merryman, J. (2002) Disaster Recovery Strategies with Tivoli Storage Management, International Technical Support Organization, dostupno na http://www.redbooks.ibm.com/redbooks/pdfs/sg246844.pdf [pristupano 23. novembra 2015.]

[14] Recovery Specialties, LLC (2007), Business Continuity: The 7-tiers of Disaster Recovery, dostupno na http://recoveryspecialties.com/7-tiers.html [pristupano 23. novembra 2015.]

[15] ISO 22301:2012, Societal security - Business continuity management systems – Requirements

[16] VMWare (2008) A Practical Guide to Business Continuity & Disaster Recovery with VMware Infrastructure 3, Revision: 20080912, Item: VMB-BCDR-ENG-Q308-001, dostupno na https://www.vmware.com/files/pdf/practical_guide_bcdr_vmb.pdf [pristupano 23. novembra 2015.]

[17] Lippitt, M. Smith, E. (2014) Networked Storage Concepts and Protocols, verzija 3.0, EMC techbook, part number H4331.5, dostupno na https://www.emc.com/collateral/hardware/technical-documentation/h4331-networked-storage-cncpts-prtcls-sol-gde.pdf [pristupano 23. novembra 2015.]

[18] Brocade (2013) SAN Design and Best Practices, verzija 2.3, dostupno na http://www.brocade.com/downloads/documents/best_practice_guides/san-design-best-practices.pdf [pristupano 23. novembra 2015.]

[19] Arpaci-Dusseau, Remzi H.; Arpaci-Dusseau, Andrea C. (2014), Operating Systems: Three Easy Pieces [Poglavlje: RAID], http://pages.cs.wisc.edu/~remzi/OSTEP/file-raid.pdf, Arpaci-Dusseau Books

[20] Fouarge, J. (2015) Tape is dead! Long live the tape! – Part I, dostupno na http://www.novastor.com/blog/tape-dead-long-live-tape-part/ [pristupano 23. novembra 2015.]

[21] Holliman, F. Iehl, J (2012) Introduction to Data Protection: Backup to Tape, Disk and Beyond, Storage Networking Industry Association, dostupno na

http://www.snia.org/sites/default/education/tutorials/2012/spring/data/FrankHolliman_%20Introduction_to_Data_Protection.pdf [pristupano 23. novembra 2015.]
[22] Fishman, M. (2012) Trends in Data Protection and Restoration Technologies, Storage Networking Industry Association, dostupno na http://www.snia.org/sites/default/files/MichaelFishman_Trends_in_Data_Protection-r9.pdf [pristupano 23. novembra 2015.]
[23] Schwegmann, A. (2010) Trends in Application Recovery, Storage Networking Industry Association, dostupno na http://www.snia.org/sites/default/education/tutorials/2010/fall/virtualization/AndreasSCHWEGMANN_Trends-in-Application-Recovery-v4-FINAL.pdf [pristupano 23. novembra 2015.]
[24] Dharma, R. Sake, S. Manuel, M. (2013) Backup and Recovery in SAN, verzija 1.2, EMC Techbooks, Part number H8077.2, dostupno na http://www.emc.com/collateral/hardware/technical-documentation/h8077-backup-recovery-san-tb.pdf [pristupano 23. novembra 2015.]
[25] Beech, D. (2009) The evolving role of disk and tape in the data center, Sylvatica whitepaper, dostupno na http://www.lto.org/wp-content/uploads/2014/07/BestPractices_Whitepaper_July2009.pdf [pristupano 23. novembra 2015.]
[26] Morris, R. J. T. Truskowski, B. J. (2003) The evolution of storage systems, IBM Systems Journal, Vol 42, No 2, dostupno na http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.8984&rep=rep1&type=pdf [pristupano 23. novembra 2015.]
[27] TechAdvisory.org (2014) 3 Business Backup Options, dostupno na http://www.techadvisory.org/2014/05/3-business-backup-options/ [pristupano 23. novembra 2015.]
[28] Kaurav, N. (2014) An Investigation on Data De-duplication Methods And it's Recent Advancements, Proc. of the Intl. Conf. on Advances In Engineering And Technology, Institute of Research Engineers and Doctors, ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-112
[29] Dutch, M. Freeman, L. Mcneal, T. Nagle, G. (2011) Trends in Data Protection, SNIA Data Protection and Capacity Optimization (DPCO) Committee, dostupno na http://sniadataprotectionblog.org/data-protection/trends-in-data-protection-2/ [pristupano 23. novembra 2015.]
[30] Hewlett-Packard (2014) HP StoreEver MSL Tape Libraries, dostupno na http://www8.hp.com/us/en/products/tape-automation/product-detail.html?oid=3936307#!tab=features [pristupano 23. novembra 2015.]
[31] ComputerWeekly (2008) Disk-based backup technology review, dostupno na http://www.computerweekly.com/report/Disk-based-backup-technology-review [pristupano 23. novembra 2015.]
[32] Hanavan, P. (2007) An Overview of Continuous Data Protection, http://www.infosectoday.com/Articles/Continuous_Data_Protection.htm#author
[33] Choudhury, A. (2014) Why organisations should consider cloud-based backup and recovery, Cloud Tech, dostupno na http://www.cloudcomputing-news.net/news/2014/apr/01/organisations-should-consider-cloud-based-backup-and-recovery/ [pristupano 23. novembra 2015.]
[34] Illsley, R. (2014) Ovum Decision Matrix: Selecting an Enterprise Backup and Recovery Solution, 2014–2015, product code: IT0022-000104, dostupno na http://www.autonomy.com/assets/global/pdf/campaigns/white-papers/ovumdecision2014.pdf [pristupano 23. novembra 2015.]
[35] Softland (2012) Backup types, dostupno na http://www.backup4all.com/kb/backup-types-115.html [pristupano 23. novembra 2015.]
[36] Richard Blum (2008), Linux Command Line and Shell Scripting Bible, Publisher: Wiley, ISBN: 978-0-470-25128-7
[37] Steve Parker (2011), Shell Scripting: Expert Recipes for Linux, Bash and more, Publisher: Wrox, ISBN: 978-1-4571-0681-1
[38] Bonuchi, S. Brown, T. Crevar, M. (2012) Best Practices for SAS® on EMC® SYMMETRIX® VMAX™ Storage, dostupno na https://support.sas.com/resources/papers/EMC_SAS_VMAX_Best_Practices.pdf [pristupano 23. novembra 2015.]
[39] Chan, K. (2006) A Comparison Of Disk Drives For Enterprise Computing, ;login: issue: June 2006, Volume 31, Number 3, dostupno na https://www.usenix.org/legacy/publications/login/2006-06/openpdfs/chan.pdf [pristupano 23. novembra 2015.]
[40] Kasavajhala, V. (2011) Solid State Drive vs. Hard Disk Drive Price and Performance Study, dostupno na http://www.dell.com/downloads/global/products/pvaul/en/ssd_vs_hdd_price_and_performance_study.pdf [pristupano 23. novembra 2015.]

[41] Mauelshagen, H. O'Keefe, M. (2005) The Linux Logical Volume Manager, Red Hat Magazine, Issue #9 July 2005, dostupno na https://www.redhat.com/magazine/009jul05/features/lvm2/ [pristupano 23. novembra 2015.]
[42] Bunn, F. Simpson, N. Peglar, R. Nagle, G. (2004) Storage Virtualization, SNIA Technical Tutorial, dostupno na http://www.snia.org/sites/default/files/sniavirt.pdf [pristupano 8. decembra 2015.]
[43] EMC (2005) Networked storage Virtualization, EMC White Paper, part number H1533.1, dostupno na https://education.emc.com/academicalliance/student/Networked%20Storage%20Virtualization.pdf [pristupano 8. decembra 2015.]
[44] De Luca, A. Bhide, M. (2010) Storage Virtualization For Dummies, Hitachi Data Systems Edition, Wiley Publishing, Inc. Indianapolis, Indiana
[45] World Heritage Encyclopedia (2014) Logical Volume Management, licensed under CC BY-SA 3.0, dostupno na http://community.worldheritage.org/article/WHEBN0000438425/management [pristupano 8. decembra 2015.]
[46] Lewis, AJ, (2006) Logical Volume Manager HOWTO, dostupno na http://tldp.org/HOWTO/LVM-HOWTO/ [pristupano 8. decembra 2015.]
[47] Mrdak V., Krstajić B., "Primjer implementacije rjesenja za backup i recovery podataka," *Informacione Tehnologije 2015*, Žabljak, Februar 2015.
[48] Guidance Consulting Inc. (2012) Data Recovery - Finding a right data backup method, http://www.guidance-consulting.com/articles/67-finding-a-right-data-backup-method-.html
[49] VmWare (2006), VMware Infrastructure 3: SAN Conceptual and Design Basics, dostupno na http://www.vmware.com/pdf/esx_san_cfg_technote.pdf [pristupano 23. novembra 2015.]
[50] Wayne Davison (2014) rsync(1) - Linux man page, dostupno na http://linux.die.net/man/1/rsync [pristupano 23. novembra 2015.]
[51] Oracle (2008), Oracle Database Online Documentation 10g Release 2 (10.2), dostupno na http://docs.oracle.com/cd/B19306_01/server.102/b14220/intro.htm [pristupano 23. novembra 2015.]
[52] Oracle (2008), 7 RMAN Backup Concepts, dostupno na http://docs.oracle.com/cd/B28359_01/backup.111/b28270/rcmcncpt.htm [pristupano 23. novembra 2015.]
[53] EMC (2012) EMC Symmetrix TimeFinder for VMAX 10K/VMAXe Series Product Guide, P/N 300-012-411, REV A03
[54] Udgith Mankad, Russell Kimkaran (2013), Implementing Local Replication Using EMC TimeFinder And Recoverpoint And Coexistence Of Rp/Cdp With SRDF On Symmetrix Vmax, dostupno na https://www.emc.com/collateral/white-papers/h8981-vmax10k-timefinder-recoverpt-local-repl-wp.pdf , Applied Technology Whitepaper
[55] Dar, Y. (2011) Oracle Databases od EMC Symmetrix Storage Systems, verzija 1.3, EMC Techbook, H2603.3, dostupno na http://www.emc.com/collateral/hardware/solution-overview/h2603-oracle-db-emc-symmetrix-stor-sys-wp-ldv.pdf [pristupano 23. novembra 2015.]
[56] EMC (2014) EMC Symmetrix VMAX Using EMC SRDF/TimeFinder and Oracle 11g, Part Number h6210.2, dostupno na http://www.emc.com/collateral/hardware/white-papers/h6210-symmetrix-vmax-srdf-timefinder-oracle-database-wp.pdf [pristupano 23. novembra 2015.]
[57] Symantec (2007) How to install and verify EMC Solutions Enabler in a Symantec i3 context, dostupno na https://clientui-kb.symantec.com/resources/sites/BUSINESS/content/live/TECHNICAL_SOLUTION/52000/TECH52779/en_US/290178.pdf [pristupano 23. novembra 2015.]
[58] EMC (2010) EMC TimeFinder Product Description Guide, dostupno na http://www.emc.com/collateral/software/timefinder.pdf [pristupano 12. decembra 2015.]
[59] EMC, VMWare (2010) Implementing EMC Symmetrix Virtual Provisioning with Vmware vSphere: Applied Technology, part number h6813.2, dostupno na https://community.emc.com/docs/DOC-14685 [pristupano 25. januara 2016.]
[60] Christian Kuhtz (1999) tune2fs(8) - Linux man page, http://linux.die.net/man/8/tune2fs
[61] John Gilmore, Jay Fenlason (2010) tar(1) - Linux man page, http://linux.die.net/man/1/tar
[62] Snyder, S. (2015) Tape Backup vs Hard Disk Backup: What Does the Future Hold?, dostupno na https://www.storagecraft.com/blog/tape-backup-vs-hard-disk-backup-what-does-the-future-hold/ [pristupano 12.decembra 2015.]
[63] Browning, J. (2007) Why Oracle Is So Important, Oracle Storage Guy Blog [online], 18. jul, dostupno na http://oraclestorageguy.typepad.com/oraclestorageguy/2007/07/why-oracle-is-s.html [pristupano 14. januara 2016.]

Skraćenice i pojmovi

IT	Informacione tehnologije (eng. *Information Technology*)
IS	Informacioni sistem (eng. *Information System*)
DRP	„oporavak od nesreće“ je skup procedura koje treba poštovati u slučaju nesreće kao što su zemljotresi, poplave, bombardovanja kako bi se oporavila i očuvala IT infrastruktura i nastavio nesmetan rad IT sistema (eng. *Disaster Recovery Plan).*
DNS	eng. *Domain Name Server*
BCV	klon diska/ova na storage uređaju koji postaje nezavistan od svog izvora i kao takav se može koristiti u svrhu backupa (eng. *Business Continuity Volume).*
VTL	uređaj koji služi za backup podataka, zasnovan je na diskovima koji emuliraju fizičke trake (eng. *Virtual Tape Library).*
RAID	tehnologija virtuelizacije skladištenja podataka koja kombinuje više disk komponenti u logičke jedinice kako bi postigla redudansu i poboljšanje performansi (eng. *Redundant Array of Independent Disks*).
LAN	skup računara i povezanih uređaja koji dijele iste komunikacione linkove ka serveru (eng. *Local Area Network*).
VLAN	logička grupa servera i ostalih uređaja na mreži konfigurisana u istom LANu uprkos njihovoj geografskoj poziciji (eng. *Virtual Local Area Network*).
UAT	zadnja faza testiranja nekog softvera prije nego što se njegova upotreba odobri i pusti u produkciju (eng. *User Acceptance Tests*).
SAN	posebna mreža koja obezbjeđuje pristup konsolidovanim urešđajima za smiještanje podataka (eng. *Storage Area Network*).
HBA	interfejs/kartica koja povezuje server/kompjuter sa ostalim mrežnim i storage uređajima, uglavnom za povezivanje na FC infrastrukturu (eng. *Host Bus Adapter).*
LUN	broj koji služi za identifikaciju logičke jedinice koja predstavlja uređaj definisan SCSI protokolom ili protokolom koji obuhvata SCSI, kao što su *Fibre Channel* ili iSCSI (eng. *Logical Unit Number).*
SCSI	skup standarda za fizičko povezivanje i prenos podataka između kompjutera i periferijalnih uređaja (eng. *Small Computer System Interface).*
FC	mrežna tehnologija velikih brzina (2, 4, 8 ili 16 Gb/s) koja se primarno koristi za povezivanje storage uređaja (eng. *Fibre Channel).*
SSD	uređaj za smiještanje podataka koji koristi integrisana kola kao memoriju kako bi trajno upisao podatke – vrlo brzi disk i izuzetno skup (eng. *Solid State Drive)*
FC disk	disk zasnovan na *Fibre channel* tehnologiji.
SATA	najsporiji tipovi diskova koji mogu biti većih kapaciteta (eng. *Serial ATA).*
Video streaming	termin koji označava emitovanje digitalnog programa preko Interneta krajnjem korisniku (eng. *video* streaming).
LVM	softver na Linuxu koji upravlja diskovima i sličnim storage uređajima na tom operativnom sistemu (eng. *Logical Volume Manager).*
SNIA	neprofitna organizacija koja promoviše standarde i tehnologije u storage industriji, obezbjeđuje edukacione servise, tehničke radne grupe i sertifikuje profesionalce u IT branši (eng. *Storage Networking Industry Association*).
WAN	geografski raširena telekomunikaciona mreža. Termin upućuje na telekomunikacionu mrežu veće strukture od LAN mreže (eng. *Wide Area*

	Network).
QoS	kvalitet servisa predstavlja ukupne performanse telefonske ili računarske mreže, a posebno se osvrće na performanse koje vide krajnji korisnici u mreži (eng. *Quality of Service*).
Firewall	Vatreni zid, služi za kontrolisanje toka saobraćaja između mreža i računara koji se nalaze u različitim sigurnosnim segmentima.
IEEE	profesionalna asocijacija smještena u Nju Jorku, posvećena naprednim tehnološkim inovacijama (eng. *Institute of Electrical and Electronics Engineers* – čita se kao AI-Triple-I).
SUS	Jedinstvena Unix specificacija je oficijalna definicija Unix sistema i predstavlja jedinstveni skup standarda za kompjuterske operativne sisteme koji se kvalifikuju za ime „UNIX“. SUS je razvijen i održava ga Austin Grupa, a zasnovano na ranijem radu IEEE i Open Grupe (eng. *Single Unix Specification*.
Open Grupa	dobavljač i industrijski konzorcijum sa preko 400 organizacija članica. Najpoznatiji je kao certifikaciono tijelo za Unix zaštitni znak i publikacija SUS tehničkih standarda.
open source	predstavlja softver čiji je kod otvoren i dostupan sa licencom koja dozvoljava njegovo proučavanje, promjenu i distribuciju bilo kome i u bilo koju svrhu.
cli	komandna linija (eng. *command line)*
ACL	omogućava dodatni, fleksibilniji mehanizam prava na fajlsistemu. One su dodatak Unix pravima na fajlovima i omogućavaju postavljanje specifičnih prava za bilo kojeg korisnika ili grupu na bilo koji fajl (eng. *Access Control Lists).*
SSH	kriptografski mrežni protokol koji služi za sigurnu komunikaciju, udaljeni pristup preko komandne linije, izvršavanje komandi sa udaljenog hosta i ostale mrežne operacije između dva umrežena kompjutera (eng. *Secure Shell).*
I/O	komunikacija između informacionog sistema (npr. računara) i spoljašnjeg svijeta, čovjeka ili nekog drugog informacionog sistema (eng. *input/output).*
Blocking I/O	I/O zahtjev koji označava da se kontrola ne vraća aplikaciji dok se I/O ne izvrši (eng. *Blocking input/output).*
ID	broj identifikacije za korisnika ili grupu na Unix sistemima
IP	eng. *Internet Protocol*
TCP	protokol koji zajedno sa IP protokolom šalje pakete podataka između kompjutera na Internetu. Zajedno, TCP and IP protokoli definišu pravila za prenos informacija kroz mrežu (eng. *Transmission Control Protocol).*
URL	formatirani tekstualni string kojeg koriste Web pretraživači, email klijenti i ostali softveri kako bi identifikovali izvor na Internetu (eng. *Uniform Resource Locator*).
RSA	jedan od prvih upotrebljivih kriptosistema sa javnim ključevima korišćen za razmjenu podataka na siguran način.
DB	baza podataka, u ovom radu se podrazumijeva da je to Oracle (eng. *Database).*
bug	je greška u kompjuterskom programu ili sistemu zbog koje se dobijaju pogrešni ili neočekivani rezultati ili neočekivano ponašanje. Većina grešaka je posljedica ljudskih grešaka u programiranju ili dizajnu koda.

Prilozi

Prilog 1

Tabela P.1: *Primjer klasifikacije tipova podataka*

Klasa 0 zaštite podataka / Klasa zaštite za "otvorene" informacije
• Opšte informacije ili sintetički generisani podaci bez reference na određenu osobu • Podaci u kojima su reference na konkretnu osobu obrisane postupkom anonimizacije • Javne informacije o osobi dostupne na Internetu za koje se bez sumnje može pretpostaviti da je osoba pristala na njeno neograničeno objavljivanje i indeksiranje od strane pretraživačkih mehanizama (Primjer: Podaci o osobi na društvenim mrežama za koje je dozvoljeno neograničeno objavljivanje i indeksiranje) **Podaci o zaposlenima**: • Podaci o zaposlenom za koje je zaposleni dao saglasnost za objavljivanjem bez ograničenja: intervju sa CEO, osoba zadužena za odnose sa javnošću, autor tehničkog rada, itd.
Klasa 1 zaštite podataka / Klasa zaštite za "interne" informacije
Pseudonimi koji se mogu personalizovati od strane odgovornog tijela Podaci o mogućim potrošačima Lični podaci objavljeni od strane ili u saglasnosti sa osobom sa neograničenom dozvolom za korišćenje: • Javno dostupni imenici • Javno dostupni lični podaci na društvenim mrežama: slike, tekstovi, rezimei, itd., koji nisu odobreni za indeksiranje od strane pretraživačkih mehanizama ili neograničeno objavljivanje • Javno dostupni lični podaci na društvenim mrežama kojima se može pristupiti kroz zatvorenu grupu korisnika nakon registracije • Objavljena lista članova nekog kluba, školskog razreda, kompanije, gdje se ne može pretpostaviti da je svaki član dao saglasnost za neograničenim objavljivanjem • Podaci osobe koja se javila na poslovni oglas (podaci su ograničeni na korišćenje samo kao dio aplikacije) **Podaci o zaposlenima:** • Poslovna adresa zaposlenog, broj telefona, e-mail, pripadnost organizacionoj jedinici, nalog i podaci potrebni za logovanje osim u slučaju nadgledanja ponašanja i učinka
Klasa 2 zaštite podataka / Klasa zaštite za "povjerljive" informacije
Detalji telekomunikacionog ili telemedia ugovora: • Imena stranke u ugovoru: adresa, prezime, ime; adresa stranke iz ugovora: Ime i broj ulice, poštanski broj, grad; • Primalac računa: adresa, prezime, ime, adresa ispostave računa; • Datum rođenja • Nacionalnost, jezik, broj računa; • Identifikacija linije, DSL-a, iznajmljene linije, pristupni podaci za servise • FTP podaci; telefonski brojevi (mobilni, fiksni, DSL telefonski brojevi); • DSL zamjena telefonskog broja • Tip ugovora; pretplata, plan, opcije, proizvodi, dodatni servisi, zaključenje ugovora, obavijest o isteku ugovora • Stanje na računu (*prepaid*), naknade, plaćanja, iznos računa, pretplate; • Status ugovora (aktivni/neaktivni); identifikacioni brojevi uređaja, IMEI, MAC, serijski broj, revizija, verzija softvera • Pretplatnički broj ID - ICC-ID, IMSI • Broj lične karte, broj pasoša i ostalih identifikacionih dokumenata • Kreditna zaduženja, korespodencije, istorija korespodencije uključujući kontakte, kopije dokumenata, Itd. **Detalji ugovora bez telekomunikacionog ugovora**

- Imena stranke u ugovoru: adresa, prezime, ime; ime i broj ulice, poštanski broj, grad;

- Predmet kupovine/iznajmljivanja
- Serijski broj uređaja, verzija softvera,
- Dodatni podaci kao što je e-mail, dodatni fiksni telefonski broj, itd.,
- Ime potencijalnog korisnika: adresa, prezime, ime; ime i broj ulice, poštanski broj, grad;
- Zakupljeni servisi
- Ime agenta/brokera: adresa, prezime, ime; ime i broj ulice, poštanski broj, grad;
- Status agenta/brokera, popusti,
- GPS pozicioni podaci

Obični podaci zaposlenog:

- Ime, kućna adresa, kvalifikacije, biografija, datum zaposlenja, radno vrijeme/odmori i odsustvo sa posla, porezi, izdržavanje djece, zdravstveno osiguranje, godine staža, penzioni plan, ostale aktivnosti

Klasa 3 zaštite podataka / Klasa zaštite za "povjerljive" informacije

Saobraćaj i potrošnja podataka (ili individualni podaci dobijeni iz zapisa o saobraćaju)

- Fiksni/mobilni/DSL telefonski brojevi A pretplatnika, Fiksni/mobilni/DSL telefonski brojevi B pretplatnika
- Dodijeljena fiksna/promjenjiva IP adresa, identifikacija sesije
- Ciljna IP adresa, korišćeni (SIP) proxy/gateway, URL, peer
- WAP/Internet APN
- Početak, kraj i trajanje Internet konekcije (datum, vrijeme)
- Prenešena količin a podataka
- Korišćeni servisi
- Tačke završetka poziva
- SS7 podaci, QoS dodaci, e-mail zaglavlje
- Lokalizacija informacija, identifikacija ćelije, GK koordinate, pozivni broj ukoliko postoji
- Identifikacija mobilnih pretplatnika - ICC-ID, IMSI
- Komunikaciona oprema korisnika - IMEI, MAC, serijski broj, revizija, operativni sistem, pretraživač, verzija softvera
- Vrijeme korišćenja servisa (npr. logovanje na Musicload)
- IP i GPS podaci prilikom korišćenja servisa
- Djelovi teksta ili multimedijalne poruke kao što je e-mail zaglavlje
- SMS, MMS ili Instant Messenger poruke;
- Korišćeni pseudonimi

Itd.

Sadržaj poruke

- Telekomunikacioni sadržaj zaštićen Zakonom o elektronskim komunikacijama
- Sadržaj konverzacija govornih servisa
- Sadržaj data servisa
- Snimci govora, fax podaci (T-Net Box)
- Signalni podaci (bip tonovi)
- Djelovi teksta ili multimedijalnih poruka kao što je sadržaj e-maila, priloga u e-mailu, SMSa, MMSa, čat sesije

Itd.

Osjetljivi podaci

- Zdravstveni podaci, religija, pripadnost sindikatu, etnička i rasna pripadnost, političko opredjeljenje, filozofska ubjeđenja, podaci o seksualnom životu;
- Izvještaji o prethodnim osudama, zakonski prekršaji ili tekuće istrage
- Lični podaci o bankovnim i kreditnim računima

Osjetljivi podaci o zaposlenom

- Podaci o plati, finansijske okolnosti

Prilog 2

U ovom prilogu detaljno su opisane klase u sedmoklasnom sistemu servisa:

- **Klasa 0** - (*No offsite data backup*) je klasa podataka bez rezervnih kopija podataka ili mogućnosti za oporavkom.
- **Klasa 1** - (Offsite *backup with no hotsite - PTAM*) Backup podataka bez redudantne lokacije se odnosi na kreiranje rezervnih kopija podataka i slanje na udaljenu lokaciju za skladištenje. Na udaljenoj lokaciji nema servera ni uređaja na kojima bi se podaci mogli oporaviti. Pošto skladištenje traka sa kopijama podataka u sefovima uglavnom obavljaju kuriri, ova klasa se obično opisuje kao kamionski metod pristupa (*Pickup Truck Access Method – PTAM*). Iako ovo nije skupa opcija, može biti teška za upravljanje zbog velike količine traka koje se skladište. Uobičajeno vrijeme oporavka je više od sedmice.
- **Klasa 2** - (*Offsite backup with hotsite - PTAM+hotsite*) Backup podataka sa redudantnom lokacijom se odnosi na kreiranje rezervnih kopija podataka i slanje na udaljenu lokaciju gdje se nalazi infrastruktura u smislu servera i procesora. Za oporavak podataka je potrebno pokrenuti infrastrukturu sa već kreiranim kopijama podataka. Uobičajeno vrijeme oporavka je više od jednog dana.
- **Klasa 3** - (*Electronic vaulting*) Elektronsko skladištenje je nadogradnja klase 2 (kopije podataka na udaljenoj lokaciji, plan oporavka od nesreće, redudantna lokacija). Dodatno podržava elektronsko skladištenje značajnih podataka sa mogućnošću bržeg oporavka sa trake. Redudantna lokacija je stalno aktivna i tako povećava troškove, ali je zato vrijeme oporavka smanjeno na jedan dan.
- **Klasa 4** - (*Point-in-time copy*) Kopija u trenutku vremena predstavlja sliku (*snapshot*) podataka u vremenu pripremljenu za prenos na udaljeni disk. Definiše se kao dva datacentra sa elektronskim skladištenjem između obije lokacije i uvodi obavezu aktivnog upravljanja podacima koji se skladište na udaljenoj lokaciji. U ovom scenariju opterećenje poslovanja se može rasporediti među lokacijama. Vrijeme oporavka je obično do jednog dana.
- **Klasa 5** - (*Transaction integrity*) Integritet transakcije se odnosi na podatke na udaljenoj lokaciji koji moraju biti konzistentni u odnosu na produkciju. Ova klasa uključuje sve zahtjeve klase 4 (kopije podataka na udaljenoj lokaciji, plan oporavka od nesreće, aktivna redudantna lokacija, elektronsko skladištenje) s tom razlikom što su kopije podataka u stanju slike (*image*). U rješenjima ovog tipa skoro da nema gubitaka među podacima, ali postojanje ovakvog rješenja zavisi isključivo od aplikacije. Vrijeme oporavka je obično manje od 12 sati.
- **Klasa 6** - (*Zero or little data loss*) Nula ili minimalni gubitak podataka se odnosi na asinhronu ili sinhronu kopiju disk-na-disk između produkcije i udaljene lokacije. Ovakvo rješenje nudi najveći nivo tačnosti kopije i zasniva se na nekom obliku replikacije podataka na dva ili više diskova (*Disk Mirroring).* Vrijeme oporavka je nekoliko minuta.
- **Klasa 7** - (*Highly automated, business-integrated solution*) Visoko automatizovano rješenje integrisano u poslovanje predstavlja sinhronu kopiju disk-na-disk sa automatskim oporavkom sistema i aplikacija. Rješenja ove klase uključuju sve glavne komponente rješenja klase 6 sa dodatkom integrisanog automatizma.

Prilog 3

Rsync nudi brojne opcije koje kontrolišu svaki aspekt njegovog ponašanja i dozvoljavaju veoma fleksibilne specifikacije fajlova predodređenih za kopiranje. Radi optimalnijeg i preglednijeg funkcionisanja rsync alata, u predloženom rješenju izabrane su sljedeće opcije koje će se koristiti prilikom njegove implementacije:

-a : *archive mode* – izvršava se backup svih poddirektorijuma, simboličkih linkova, itd.;

-v : *verbose mode* – detaljniji ispis izvršavanja komande;

-z : kompresija podataka prije prenosa;

-x : ne prelazi granice datog fajlsistema;

--progres : prikazuje napredak prilikom transfera – ispisuje listu fajlova koji su se kopirali;

--delete : brisanje fajlova na destinaciji kojih nema na izvorišnoj lokaciji;

--exclude={/dir1,/dir2...} : isključuje date direktorijume iz liste za backup;

--inplace : ažuriranje fajlova na destinaciji koji su kopirani u ranijim transferima;

--ignore-errors : brisanje čak i kada postoje I/O greške;

--blocking-io : upotreba blocking I/O za udaljeni shell;

--numeric-ids : pomoću ove opcije rsync će sačuvati brojčane ID-eve korisnika i grupa umjesto njihovih imena i povezaće ih na oba kraja;

--timeout : podešavanje maksimalnog vremena u sekundama za koje rsync čeka na prenos podataka. Ukoliko se ništa ne prenese u specificiranom vremenu, rsync će završiti izvršavanje. Podrazumijevani timeout je 0, što znači da ga nema (Detaljnije na *rsync man* stranicama [50]).

Prilog 4

U nastavku je dat kod skripte koja se koristi za kreiranje standardnih kopija podataka, a čiji je proces opisan u poglavlju 5.4.1.

Kod skripte /root/Scripts/backup_all.sh je dat u kodu P.1.

Kod P.1: *Kod skripte /root/Scripts/backup_all.sh*

```
#!/bin/bash

/root/Scripts/backup_fs.sh -d /backup –H serv01db
/root/Scripts/backup_fs.sh -d /backup -H serv01sdp
/root/Scripts/backup_fs.sh -d /backup -H servepc
/root/Scripts/backup_fs.sh -d /backup -H serv01app
/root/Scripts/backup_fs.sh -d /backup -H serv02app
/root/Scripts/backup_fs.sh -d /backup -H serv03app
exit
```

Kod skripte /root/Scripts/backup_fs.sh koja se poziva iz skripte date u kodu P.1 dat je u kodu P.2.

Kod P.2: *Kod skripte /root/Scripts/backup_fs.sh*

```
#!/bin/bash

############################################################
usage="Usage:
        ./backup_fs.sh [-H <hostname>] [-d <backup_dir> [-i <ignore_FS>]
                        [-f <fs_to_backup>] [-h]

        ### OPTIONAL PARAMETERS ###
        -H      : Hostname (IP adresse or DNS name), default is localhost
        -d      : Backup directory, default is /backup
        -i      : FS to ignore, default is /tmp, /software, /mnt/iso, /backup.
                  In case of multiple FSs to ignore, syntax should be [ -i
\"/FS1|/FS2|/FS3\" ]
        -f      : Specific FS to backup, default is all
                  In case of multiple FSs to back up, syntax should be [ -f
\"/FS1|/FS2|/FS3\" ]
        -h      : Help (print command usage, and quit)

# Written By: Vladana Mrdak
# Created: 27/12/2013
# Description: Perform backup of entire Linux box using rsync
# Tested successfully on Red Hat Enterprise Linux and Centos
# Version: 3.0 (updated 1/07/2014)
"

# Get Options and check parameters
while getopts "H:d:i:f:h" option;
do
        case $option in
                H) HOST=$OPTARG;;
                d) BACKUP_DIR=$OPTARG;;
                i) IGNORE_FS=$OPTARG;;
                f) FS_TO_BACK=$OPTARG;;
                h) echo -e "$usage"
                   exit;;
        esac
done
```

```
# Check if the host is remote or localhost, and get the list of filesystems
if [[ -z "$HOST" || $HOST == `hostname` ]]
  then
     export HOST=`hostname`
     DF_LIST=`df -P | grep -viE "tmp|software|iso|:"`
  else
     DF_LIST=`ssh root@${HOST} df -P | grep -viE "tmp|software|iso|:"`
fi

# Create backup directory if not existant or specified
if [ -z "$BACKUP_DIR" ]
    then
       export BACKUP_DIR=/backup
fi
DF_LIST=`echo "$DF_LIST"| grep -v "$BACKUP_DIR"`

# Create a list of FSs to backup
if [ -z "$IGNORE_FS" ]
  then
  if [ -z "$FS_TO_BACK" ]
     then
        DF_LIST=`echo "$DF_LIST" | tail -n +2`
     else
        DF_LIST=`echo "$DF_LIST" | grep -E "$FS_TO_BACK"`
  fi
  elif [ "$IGNORE_FS" == "/" ]
  then
     DF_LIST=`echo -e "$DF_LIST" | tail -n +3`
  else
     DF_LIST=`echo -e "$DF_LIST" | tail -n +2 | grep -vE "$IGNORE_FS"`
fi

LIST_FS=`echo "$DF_LIST" | awk '{print $6;}'`
COUNT_FS=`echo "$LIST_FS" | wc -l`
SPACE_FS=`echo "$DF_LIST" | awk '{print $3;}' |awk '{ sum+=$1} END {print sum}'`

if [ ! $COUNT_FS -eq $COUNT_FS ]
  then
     echo -e "List of FSs is not well supplied"
     exit
fi

export BCK_DIR=${BACKUP_DIR}/${HOST}/FS/
if [ ! -d ${BCK_DIR} ]; then
        mkdir -p ${BCK_DIR}
fi

export DIR_NUM=`cd ${BCK_DIR};ls -l | grep 201 | wc -l`
export OLDEST_DIR=`cd ${BCK_DIR};ls | sort | head -n 1`
export TODAY=`date +%Y%m%d`
if [ -f `cd ${BCK_DIR}; ls | grep ${TODAY}` ]; then
        if [ ${DIR_NUM} -ge 3 ]; then
             mv ${BCK_DIR}/${OLDEST_DIR} ${BCK_DIR}/${TODAY}
             else
             mkdir -p ${BCK_DIR}/${TODAY}
        fi
fi

# Check if there is enough space on specified backup device
SPACE_AVAIL=`df -P | grep $BACKUP_DIR | awk '{print $4}'`

if [ ! $(($SPACE_AVAIL-$SPACE_FS)) -gt 10 ]
   then
        echo -e "There is not enough space to perform backup"
        exit
```

```
fi

# Rsync function that backs up one FS on Linux box
rsync_fs()
{
if [ -z "$1" ]
  then
    echo -e "No argument supplied"
    exit
elif [ "$1" == "/" ]
  then
     LOG="root"
  else
     LOG=${1#?}
fi

if [ "$2" == `hostname` ]
  then
     EXIST_FS=`df -P| grep $1 | awk '{print $6;}' | head -n 1`
     export FS=$1
  else
     EXIST_FS=`ssh root@${HOST} df -P | awk '{print \$6;}' | grep \$1 | head -n 1`
     export FS=root@${HOST}:$1
fi

if [ "${EXIST_FS}" != "$1" ]
   then
        echo -e "$1 FS does not exist"
        exit
   else

export BCK_DIR=${BACKUP_DIR}/${HOST}/FS
export EXP_DIR=${BCK_DIR}/`date +%Y%m%d`
mkdir -p ${EXP_DIR}
export EXP_LOG=${EXP_DIR}/${LOG}.log
echo -e `date` > ${EXP_LOG}
if [ "$1" == "/" ]
   then
       /usr/bin/rsync -avzx --progress --delete --
exclude={/dev,/sys,/media,/proc,/lost+found} --inplace --ignore-errors --blocking-io -
-numeric-ids --timeout=1500 ${FS} ${EXP_DIR} >> ${EXP_LOG} 2>&1
echo -e ${EXP_LOG}
   else
       /usr/bin/rsync -avzx --progress --delete --exclude={/lost+found} --inplace --
ignore-errors --blocking-io --numeric-ids --timeout=1500 ${FS} ${EXP_DIR} >>
${EXP_LOG} 2>&1
echo 2
fi
wait # until the background compress job ends
echo `date`  >> ${EXP_LOG}
fi
}

for CURRENT_FS in $LIST_FS
do
        rsync_fs $CURRENT_FS $HOST
done;

exit
```

Prilog 5

Prilog 5 sadrži medijum u vidu CD-ROMa na kom se nalazi sistem skripti u Linux formatu koji obavlja proces kreiranja klonova Oracle baza podataka. Kod je inicijalno razvila Ayelet Avramov na operativnom sistemu HP-UX i dala na korišćenje i modifikaciju autoru ovog rada.