



**UNIVERZITET SINGIDUNUM**

# **Implementacija sigurnog datacentra za potrebe sistemskih i web servisa**

**Mentor:**

**Prof. dr. Mladen Veinović**

**Student:**

**Marko Živanović**



Beograd, 2015

**Sažetak:** U ovom radu predmet razmatranja biće metode projektovanja datacentara za potrebe sistemskih servisa. U prvom delu rada razmatraće se opšti zahtevi koji jedan savremen datacentar mora da ispuni. Zatim biće prezentovane metode i rešenja koja se koriste u razvijenim zemljama, podela posla unutar datacentra, metode zaštite servisa i podataka. Na kraju rada biće predložen metod projektovanja i opisan kompletan proces implementacije datacentra. Biće obuhvaćen i scenario oporavka centra na sekundarnoj lokaciji. Zbog osetljivosti podataka u radu nećemo otkrivati tačnu lokaciju datacentra i kompaniju. Kompaniju ćemo nazvati „West“, datacentar na primarnoj lokaciji „scPrime“ i datacentar na sekundarnoj lokaciji „scBackup“

**Ključne reči:** datacentar, metode projektovanja, bezbednost datacentara, oporavak datacentra na sekundarnoj lokaciji.

## **Implementation of secure datacentra for system and web services**

**Abstract:** In this paper, subject of discussion will be datacenter design methods for purpose of system and web services. First part we will discuss about general design goals and demands for modern datacenters. After that we will review implemented solution for datacenter in developed countries, datacenter internal organization, security measures for services and data. Lastly, datacenter design will be suggested method for and complete implementation process will be reviewed. Disaster recovery scenario will be reviewed also. Due to sensibility of data in this paper real names for company and datacenter locations will not be used. Company will be called „West“, datacenter primary location scPrime and secondary location scBackup.

**Keywords:** datacenter, design methods, datacenter security, disaster recovery scenario.

## SADRŽAJ

|                                                           |           |
|-----------------------------------------------------------|-----------|
| <b>1. Uvod .....</b>                                      | <b>3</b>  |
| <b>2. Metodologija naučnog istraživanja .....</b>         | <b>5</b>  |
| 2.1 Uvodne napomene .....                                 | 5         |
| 2.2 Predmet istraživanja .....                            | 5         |
| 2.3 Cilj istraživanja .....                               | 5         |
| 2.4 Istraživačke hipoteze .....                           | 5         |
| 2.5 Metodi istraživanja i tok istraživačkog procesa ..... | 6         |
| <b>3. Primeri datacentra .....</b>                        | <b>7</b>  |
| 3.1 Vojni datacentri .....                                | 7         |
| 3.1.1 SAD .....                                           | 7         |
| 3.1.2 Letonija .....                                      | 8         |
| 3.1.3 Velika Britanija .....                              | 10        |
| 3.2 Poslovni datacentri .....                             | 10        |
| 3.2.1 Google .....                                        | 11        |
| 3.2.2 Microsoft .....                                     | 13        |
| <b>4. Elementi datacentra .....</b>                       | <b>16</b> |
| 4.1 Lokacija .....                                        | 17        |
| 4.2 Računari za obradu podataka .....                     | 18        |
| 4.3 Računari za skladištenje podataka .....               | 19        |
| 4.4 Računarsko-telekomunikacioni segment .....            | 20        |
| 4.5 Modul neprekidnog napajanja .....                     | 21        |
| <b>5. Projektovanje datacentra .....</b>                  | <b>23</b> |
| 5.1 Projektni zahtevi .....                               | 23        |
| 5.2 Analiza postojećeg stanja .....                       | 26        |
| 5.3 Dodatni zahtevi .....                                 | 27        |

|                                                                        |           |
|------------------------------------------------------------------------|-----------|
| 5.4 Faze .....                                                         | 29        |
| 5.4.1 Faza 1: Dokaz koncepta .....                                     | 29        |
| 5.4.2 Faza 2: Proširenje kapaciteta .....                              | 29        |
| 5.4.3 Faza 3: Potpuna realizacija primarne lokacije .....              | 29        |
| 5.4.4 Faza 4: Realizacija sekundarne lokacije .....                    | 29        |
| <b>6. Implementacija .....</b>                                         | <b>30</b> |
| 6.1 Faza 1: Dokaz koncepata .....                                      | 30        |
| 6.1.1 Povezivanje komponenti u funkcionalnu celinu .....               | 31        |
| 6.1.2 Instalacija i konfigurisanje storidž sistema .....               | 33        |
| 6.1.3 Instalacija menadžment servera za virtuelnu infrastrukturu ..... | 33        |
| 6.1.4 Testiranje uspostavljene konfiguracije .....                     | 34        |
| 6.2 Faza 2: Proširenje kapaciteta .....                                | 35        |
| 6.3 Faza 3: Potpuna realizacija primarne lokacije .....                | 38        |
| 6.3.1 Adaptacija Primarne Lokacije .....                               | 39        |
| 6.3.2 Računari za obradu podataka .....                                | 41        |
| 6.3.3 Računari za skladištenje podataka .....                          | 42        |
| 6.3.4 Računarsko-telekomunikacioni modul .....                         | 45        |
| 6.3.5 Modul neprekidnog napajanja .....                                | 47        |
| 6.4 Faza 4: Realizacija sekundarne lokacije .....                      | 47        |
| 6.5 Backup rešenje .....                                               | 49        |
| 6.5.1 Symantec NetBackup .....                                         | 49        |
| 6.5.2 Quantum backup uređaji za backup na diskove .....                | 51        |
| <b>7. Bezbednost .....</b>                                             | <b>52</b> |
| 7.1 Infrastruktura za zaštitu .....                                    | 54        |
| 7.2 Praktična implementacija .....                                     | 57        |
| <b>8. Zaključak .....</b>                                              | <b>60</b> |
| <b>9. Literatura .....</b>                                             | <b>61</b> |
| <b>10. Spisak Slika .....</b>                                          | <b>62</b> |

## 1. Uvod

Savremeni trendovi i razvoj tehnologija, kao i sve veća integracija Interneta u različite životne i poslovne procese, iznose i zahtev za iznalaženjem adekvatnih rešenja i mehanizama zaštite i organizaciju podataka. Ti procesi podrazumevaju širok spektar aktivnosti, stvaranje, razmenu i čuvanje velikih količina podataka, kontrolisanje pristupa njima i uspostavljanje neprekidnosti u radu sistemskih servisa.

Razvoj informacionih tehnologija i hardware-a, omogućio je obradu velikih količina podataka i kreiranje skupova podataka podesnih za prezentovanje krajnjem korisniku. Svi podaci moraju biti negde uskladišteni i dostupni za obradu. Jako često se dešava da je jedan skup podataka potreban za više proračuna u potpuno različitim naučnim oblastima.

Datacentri se mogu uopšteno definisati kao računarski sistemi koji omogućavaju skladištenje, obradu i prezentovanje podataka. Pri razmatranju datacentra treba imati u vidu da njihovu efikasnost i pouzdanost ne određuju samo računari već i ljudi koji njime upravljaju. Ako govorimo o Internetu možemo smatrati da su datacentri hard disk i procesor Interneta dok bi sistemske servise mogli smatrati matičnom pločom Interneta.

Zbog navedenog, a i drugih prednosti, datacentri imaju zapaženu ulogu, kada se radi o pitanjima bezbednosti, pouzdanosti ili neprekidnosti rada aplikacija i servisa. Datacentri takođe imaju i čitav niz mana, koje su predmet istraživanja i razvoja, kako bi se one otklonile. Sa jedne strane omogućavaju prihvatanje velikih količina podataka i time ubrzavaju obradu istih, dok sa druge strane predstavljaju tzv. „Tačku otkaza“ (*eng Single point of failure*). Raznim malicioznim postupcima može se ugroziti podaci i učiniti ih dostupnim trećim licima koja nemaju pravo na njihovo korišćenje. Zbog velike količine podataka na jednom mestu maliciozni korisnici predstavljaju veliku pretnju.

U prvom delu ovog rada, razmatraće se opšti zahtevi koji jedan savremen data centar mora da ispuni. Datacentri se rangiraju po stepenu pouzdanosti pa samim tim i zahtevi se bitno razlikuju od nivoa do nivoa. Takođe razmatraće se načini realizacije opštih zahteva.

U drugom delu rada, razmatraće se bezbednosni problemi funkcionisanja datacentara kao i metode projektovanja. Pregled postojećih rešenja u razvijenim zemljama biće obrađen u ovom delu rada.

U posljednjem delu, predložiće se metoda projektovanja datacentra i biće objašnjen celokupan proces implementacije na konkretnom primeru. Predmet sagledavanje biće kompletan razvoj datacentra, od ideje do puštanja u rad.

## 2. Metodologija naučnog istraživanja

### 2.1 Uvodne napomene

U ovom istraživanju obuhvaćeni su datacentri, sa razmatranjem metoda projektovanja, implementacije za potrebe sistemskih i web servisa, u cilju rešavanja različitih bezbednosnih problema, pri čemu se mora uzeti u obzir i njihovo bezbedno funkcionisanje, odnosno, sagledati izazovi sa kojima se susreću i tehnike njihovog rešavanja.

### 2.2 Predmet istraživanja

Predmet ovog istraživanja su metode projektovanja datacentara, njihova bezbednost i primena za potrebe sistemskih i web servisa. Obuhvaćeni su pojmovi datacentra, sistemskih servisa, web, metodologije projektovanja biometrijskih sistema sa njihovim prednostima i manama,. Takođe, obuhvaćene su metodologije stepenovanja pouzdanosti datacentra i njihova podesnost za čuvanje pojedinih vrsta podataka.

### 2.3 Cilj istraživanja

**Naučni cilj:** Istraživanje, definisanje i analiza optimalne metoda za projektovanje datacentra kao i načini realizacije kompletnog datacentra od ideje do puštanja u rad.

**Društveni ciljevi:** Obezbeđivanje adekvatnog informisanja svih koji razmatraju implementaciju datacentra u svom preduzeću.

### 2.4 Istraživačke hipoteze

**Opšta hipoteza:** Savremeno društvo se suočava sa nizom problema u oblastima čuvanja, obrade i prezentacije podataka. Jedno od mogućih rešenja je i implementacija datacentra. Zbog svojih karakteristika, i brojnih prednosti, datacentri imaju veliki potencijal za primenu u svim oblastima informacionih tehnologija (IT) i shodno tome, predstavljaju oblast istraživanja od velikog značaja. U ovom radu fokus će biti primena u oblasti sistemskih i web servisa. Datacentri su sami potencijalna meta napada, i bitno je imati u vidu njihove bezbednosne probleme pri razmatranju njihove implementacije.

**Posebna/radna hipoteza:** Datacentri predstavljaju potencijalno rešenje za organizaciju i skadištenje podataka kao i više bezbednosnih problema, među kojima je i tkz DoS napad, ali moraju se imati u vidu i njihove mane.

## **2.5 Metodi istraživanja i tok istraživačkog procesa**

Pri izradi ovog rada korišćene su osnovne naučne metode deskripcije, indukcije, dedukcije, analize, sinteze i generalizacije.

Metoda deskripcije je korišćenja pri objašnjavanju osnovnih pojmova i sistema funkcionisanja.

U teorijskim segmentima su primenjene metode indukcije, dedukcije i analize, a u izvođenju zaključaka metode sinteze i generalizacije.

### 3. Primeri datacentra

Ne postoji univerzalna metoda projektovanja datacentra. Namena datacentra u mnogome određuje njegove parametre pa tako i način projektovanja. Tokom istraživanja izdvojile su se dve namene kod kojih se bitno razlikuju metode projektovanja i to su: vojni datacentri i poslovni datacentri. Ključna razlika je da kod vojnih datacentara vrsta podataka koju će čuvati i obrađivati je unapred poznata dok poslovni datacentri se kreiraju tako da budu fleksibilni i sposobni da prihvate bilo koji tip podatka.

#### 3.1 Vojni datacentri

Kod vojnih datacentara stepen razvoja u ovoj oblasti je jako različit. Zemlje zapadne Evrope i Severne Amerike koje raspolažu velikim vojnim budžetima imaju visok stepen razvoja na ovom polju i gotove sve su uspostavile svoj privatni oblak koji je fizički dislociran na par lokacija, obično u centralnim delovima zemlje. Ovakav pristup sa jedne strane optimizuje komunikacione resurse, a sa druge znatno otežava uništenje, što je osnovni cilj kako bi se usporio ili onemogućio lanac komandovanja.

Zemlje istočne Evrope i Latinske Amerike ne raspolažu imponantnim vojnim budžetima, stoga stepen razvoja datacentara je na jako niskom nivou. Uglavnom postoje specijalizovani sistemi za prenos određenog tipa informacija (poput prenosa podataka o cilju kod rada PVO), koji su zastareli, ali i dalje funkcionalni. Ove zemlje zavise od stranih donacija i ukoliko se neka donacija realizuje, nivo razvoja se znatno unapredi. Primer takvih zemalja jeste Bugarska, koja je, zahvaljujući donacijama, uspostavila nekoliko datacentara na svojoj teritoriji i instalirala integrisani sistem za upravljanje vojnim resursima, koji je takođe bio deo donacije.

##### 3.1.1 SAD

Prvi datacentar u oružanim snagama je uspostavljen 1974. Iskustva iz rata u Vijetnamu pokazala su da postoji potreba za centralizovanom obradom podataka. Takođe u tom periodu ukinuto je dobrovoljno služenje vojske i pojavila se potreba za uspostavom jedinstvenog informacionog sistema koji bi vodio računa o ljudstvu i njihovim zaduženjima.

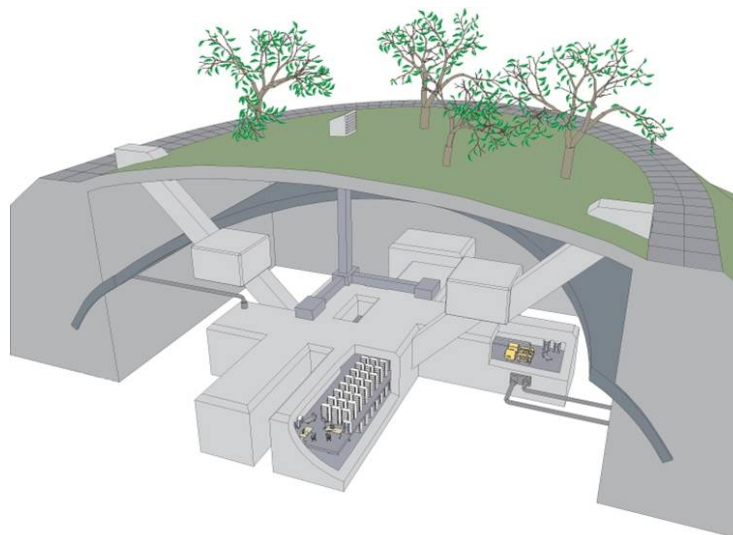
Danas SAD raspolažu velikim brojem datacentara. Gotovo svaki vid vojske ima zasebnu infrastrukturu i rešenja iz ove oblasti. Trenutno je aktuelan projekat vojnog privatnog oblaka verzija 2 (APV2). Ovaj projekat treba da konsoliduje sve postojeće resurse i učini ih dostupnim svim pripadnicima oružanih snaga SAD bez obzira na vid ili trenutnu lokaciju. Ovaj projekat realizuju civilne institucije, što je u skladu sa novom parolom „Ne moraš posedovati sistem da bi ga kontrolisao“. Ovakvim pristupom se postižu znatne uštede, jer sve što je potrebno da bi se pristupilo podacima je Internet konekcija. Glavna ideja je da postoji centralizovano mesto za obradu i prezentaciju podataka, a to je privatni oblak dostupan preko Interneta. U jedinicama postoje samo manji i mobilni centri koji prevashodno služe za dostavljanje podataka privatnom oblaku. Mobilni centri mogu da vrše i inicijalnu obradu podataka, kako bi podatke transformisali u oblik koji privatni oblak razume. Ovakvim pristupom se postiže da su svi važni podaci van jedinice, i to u privatnom oblaku. Sve sakupljene informacije su odmah dostupne svim jedinicama. Zaposedanjem nekog od mobilnih centra, neprijatelj ne bi došao do bitnih podataka, jer su sve informacije u privatnom oblaku, a ne na lokalnim serverima.

Ovaj pristup je jako dobar, ali i jako skup. Zahteva visoku tehničku opremljenost jedinica i satelitske Internet linkove, jer se lokacije jedinica ne mogu predvideti, pa se samim tim ne može ni Internet konekcija unapred obezbediti u zoni dejstva jedinice.

Jako mali broj armija u svetu ima preduslove za implementaciju ovakvog rešenja.

### **3.1.2 Letonija**

Letonija je bivša republika SSSR i u doba hladnog rata istureno rezervno komandno mesto se nalazilo na njenoj teritoriji. S obzirom na svoju namenu, ova lokacija se nalazi u podzemnom bunkeru. Podzemni bunker se nalazi u blizini glavnog grada Letonije, Rige. Lociran je 9 metra iznad nivoa mora, ali i 12 metra ispod zemlje što ga čini otpornim na plavljenje i elektromagnetno ometanje.



Slika 1. Šema datacentra „Grizinkaln“ Riga, Letonija

Ideja da se ova lokacija iskoristi za datacentar je sasvim opravdana, bez obzira na inicijalnu namenu lokacije. Dobar deo opremanja lokacije je već odrađen. Postoje otvori za ventilaciju, telekomunikaciona i naponska kanalizacija kao i višestruki ulazi i izlazi za evakuaciju. S obzirom da je bunker građen 50-tih godina prošlog veka, korišćeni su veliki bakarni kablovi pa su telekomunikacione cevi jako prostrane. Prostom zamenom bakarnih kablova optičkim kablovima koji su višestruko tanji, lako se dolazi do velikog unapređenja u kapacitetu linkova.

Naponska mreža je rešena putem postojećeg priključka na javnu naponsku mrežu. Dodata su po 2 dizel-generatora za sistem klimatizacije i sistem servera. Naponske mreže za klimatizaciju i serversku infrastrukturu su u potpunosti odvojene. Svi sistemi za klimatizaciju, prečišćavanje vode i vazduha su već postojali, pa su samo tehnološki unapređeni.

Ovakav pristup omogućava da se malim ulaganjima uspostavi datacentar sa odličnim uslovima za rad servera i ljudi. Ukoliko je namena ovog datacentra isključivo vojna, nedostatak ovakvog pristupa je tajnost. Lokacije bunkera u doba hladnog rata javno su dostupne, kao i njihove šeme. Pored toga, bunker su projektovani prema naoružanju iz doba kada su građeni, tako da njihova zaštita i tajnost nisu prepreka modernom naoružanju.

### **3.1.3 Velika Britanija**

Ovaj model uspostave datacentra je zasnovan na civilnim centrima za obradu i skladištenje podataka. Ogromna veličina podataka se prikuplja, obrađuje i prezentuje u mirnodopskim uslovima i na sopstvenoj teritoriji. Uzimajući ove činjenice u obzir, sasvim je opravdan sistem uspostave koji se zasniva na zakupu postojećih resursa od domaćih kompanija. Tako se uspostavljaju datacentri na zahtev, dok se troškovi održavanja svode isključivo na zakup servera shodno potrebama. Tajnost podataka se obezbeđuje putem kriptovanja informacija na nivou operativnog sistema, tj. rada sa diskovima (kompanija E-Safe nudi takva rešenja). Ovim se postižu znatne uštede i koriste se mrežna i serverska infrastruktura onoliko koliko je potrebno.

Za potrebe jedinica koje operišu u ratnim uslovima uspostavljaju se mobilni datacentri i koriste se kontejneri poznatih proizvođača poput HP, Dell, IBM. Mobilni datacentri mogu se instalirati i u bivšim atomskim skloništima, jer zahtevaju samo naponski i mrežni priključak da bi radili.

Ovaj pristup se koriste nekoliko članica NATO-a, poput Finske, Švedske, Velike Britanije i drugih. Ovaj pristup obezbeđuje jako brzu uspostavu, ali sa druge strane jako zahtevan u tehničkom smislu. Za njegovu realizaciju potrebni su linkovi velikog kapaciteta ka natprovajderu i kripto-zaštitni uređaji koji rade na velikim brzinama (većim od 1GB/s). Takođe, postoji problem uvezivanja mobilnih datacentara i stacionarnih u jedinstvenu mrežu, koji zahteva dobre komunikacione linkove na svim lokacijama mobilnih datacentara, a oni se gotovo uvek nalaze u zoni ratnih dejstava. Ovakve komunikacione linkove mogu imati samo bogatije zemlje ili one sa sopstvenom mrežom satelita.

### **3.2 Poslovni datacentri**

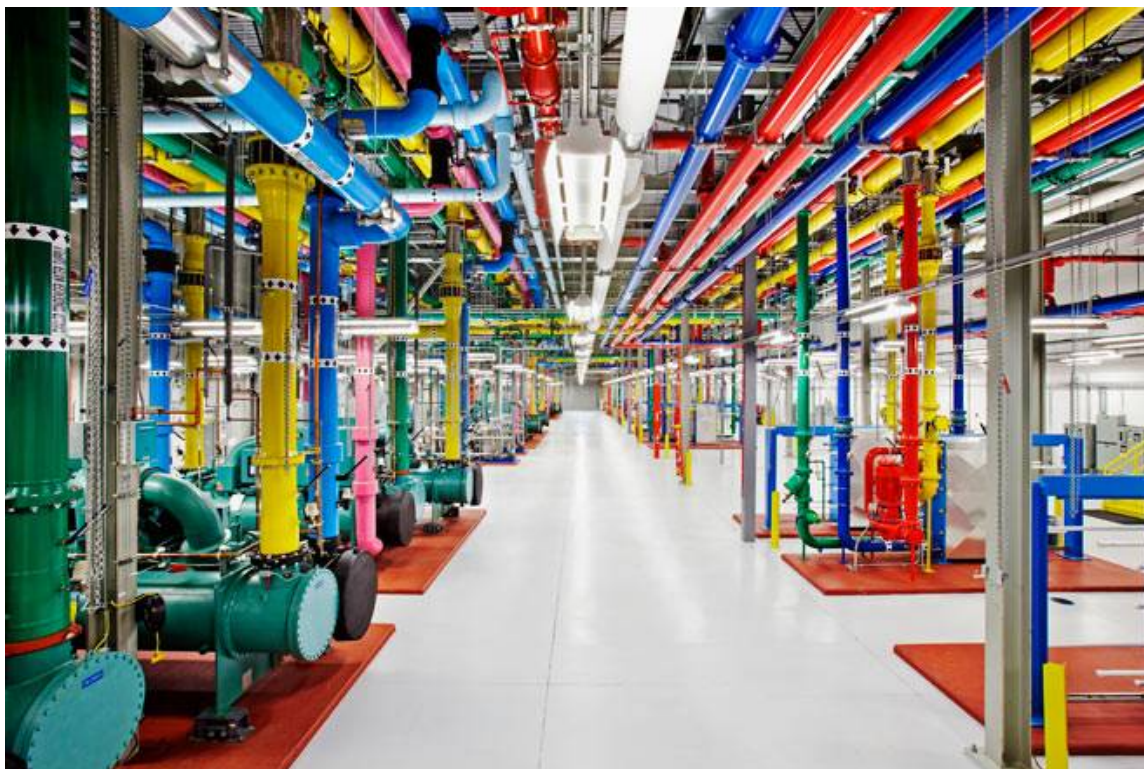
Kod poslovnih datacentara nije poznato sa kojim podacima će se raditi kao ni količine podataka. Zbog ovog stabilnost je jako važna. Microsoftov datacentar u Sietlu je u početku imao samo 10 rekova a danas je jedan od „Azure“ centra. Prilikom uspostave datacentra ovog tipa ekonomičnost je najvažnija što veća isplativost to je veći i datacentar. Poslovni datacentri su uglavnom locirani u zemljama u kojima je zakup telekomunikacionih kapaciteta povoljniji ili pak u zemljama gde su potrebe za hlađenjem manje (Švedska, Norveška, Kanada...). Energetske uštede su cilj svakog dizajna. Danas datacentri troše 1,5% električne energije.

### 3.2.1 Google

Google je najpopularni i najveći svetski pretraživač Interneta. Postoji oko 16 godina i gotovo od početka svog postojanja je lider među pretraživačima Interneta. Posедуje pregršt javno dostupnih servisa poput pretrage, video snimaka-youtube, google dokumenata i mnoge druge. Svaki od njih zahteva što je moguće brži odgovor na korisnički zahtev, bilo da je to rezultat pretrage ili prva scena nekog videa.

U početku je google iznajmljivao servere i od telekom kompanija i to je bilo dovoljno dobro, ali sa porastom broja korisnika i brzina odziva se smanjivala. Kada je dostigla 3,5 sekunde korisnici su polako počeli da se vraćaju drugim pretraživačima uprkos odličnom algoritmu pretrage.

Problem sporog odziva je zahtevao uspostavu datacentra. Google je ovaj problem shvatio ozbiljno i unajmio je Ursa Hölzla da dizajnira datacentar infrastrukturu. Hölzle je brzo došao do zaključka da jedan datacentar nije rešenje već mreža datacentara. Obzirom da je ovakva mreža jako skupa, morao biti inovativan kako bi smanjio troškove. Google je napravio prvi datacentar sa kompletno vodenim hlađenjem. Do tad koristili su se klima uređaji koji troše puno električne energije i samim tim datacentri nisu bili energetske efikasni. Google je osmislio sistem hlađenja u kome se toplota servera prenosi na vodu koja se postepeno odvodi u zasebne rezervoare u kojima se hladi i ponovo vraća u sistem hlađenja.



Slika 2. Postrojenje za hlađenje vode. Datacentar Daglas

Sledeća inovacija je ostvarena na polju umrežavanja datacentra. Svaki datacentar ima neki google servis koji opslužuje all ne retko korisnik traži 2 i više servisa odjednom. U ovoj situaciji brzina interkonekcija između datacentara dolazi do izražaja a ona je najveća google'ova snaga. Google se trudi da ima maksimalno brze interkonekcije, jedino ograničenje su fizička svojstva provodnika odnosno kabla.

Kupovina youtube servisa google-u je zadala novi zadatak koji je isti stručnjak rešio. Koliko god interkonekcije bile brze, datacentar je udaljen od lokacije korisnika hiljadama kilometara što bitno utiče na brzinu odziva. Uspostava datacentar u svakoj zemlji je skupa i ne isplativa. Rešenje je uspostava manjih datacentara na lokacijama telekom kompanija. Ti mali datacentri predstavljaju svojevrsan keš za google servise tako najpopularniji video snimci, dokumenta, lokacije su uvek u kešu tj „blizu“ korisnika samim tim i brzina odziva je velika.

Danas ove ideje predstavljaju fundamentalna znanja u projektovanju datacentara i serverske infrastrukture uopšte, ali google možemo smatrati pionirom modernih datacentra.



Slika 3. Serverska soba. Datacentar Council Bluffs

### 3.2.2 Microsoft

Za Microsoft proces pirkupljanja i obrade podataka započinje 1989 sa pojavom prve verzije sql baze podataka. Sam microsoft, iako najveća softverska kuća u svetu, je dugo slovio samo za porizvođača operativnog sistema i office paketa. Sa pojavom kompanije google i njenog velikog prodora u IT svet, microsoft je uvideo svoju grešku i pokušao da brzo reši problem akvizicijom ne tako male kompanije kao što je yahoo. Ta akvizicija nikada nije realizovana i microsoft je bio primoran da započne razvoj sopstvene tehnologije za rad sa datacentrima.

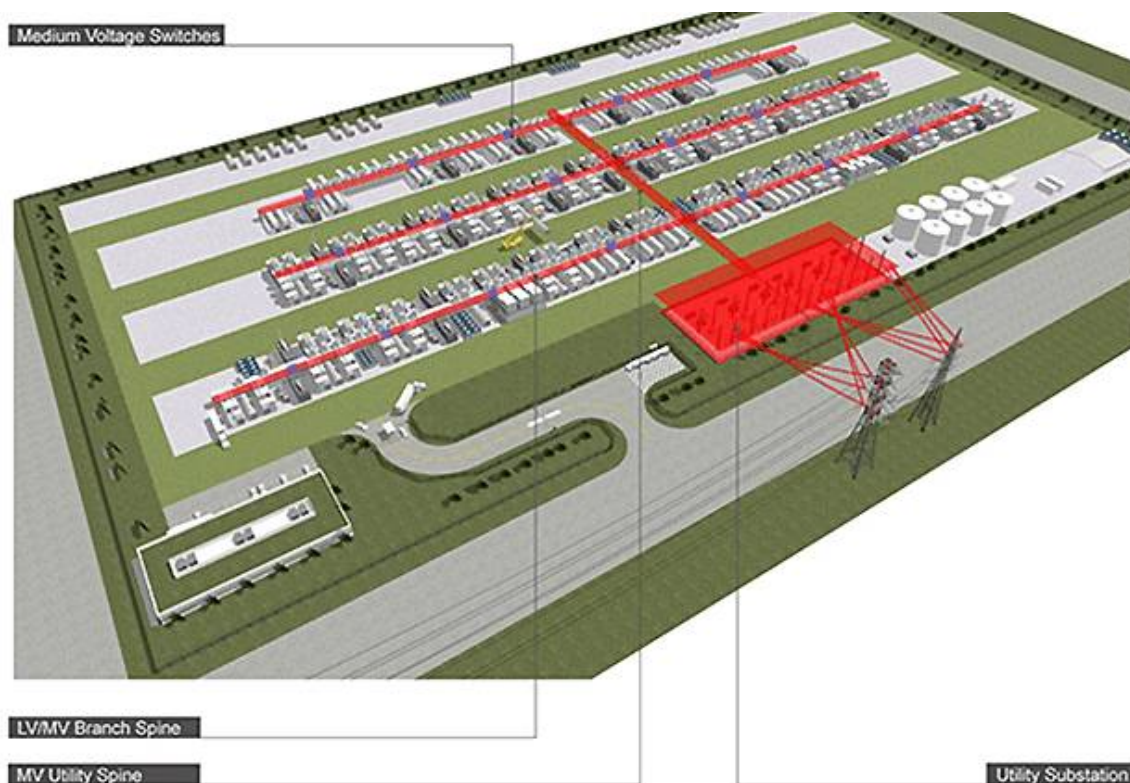
Fokus je uvek bio isti: ostvariti što veći kapacitet za obradu i skladištenje podataka sa što manjim utroškom energije. Razvoj virtuelizacije i Interneta uslovio je da sve više korisnika ne želi da pravi svoje datacentre već želi da ih dobije na zahtev i u skladu sa svojim trenutnim potrebama. Da bi odgovorio svim zahtevima tržišta microsoft je razvio i patentirao sopstveni mehanizam uspostave skalabilnih datacentara. Datacentar koji „raste“ po zahtevu korisnika sastoji se iz modula. Sa povećanjem broja i obima zahteva korisnika raste i broj modula. Microsoft modul za uspostavu data centra se naziva ITPACK.

ITPACK sadrži do 8 rek oramana. U postolju se nalazi protiv tegovi i priključci za električno napajanje, vodeno hlađenje (opciono pošto je prvenstveno projektovan za vazdušno hlađenje). Svaki modul ima zasebnu jedinicu za napajanje i nadzor. Ventilatori na vrhovima a filteri na vratima rek oraman obezbeđuju sistem vazdušnog hlađenja. Hladan vazduh se uvlači sa prednje strane i pomoću ventilatora izbacuje na drugu stranu. Ovde se koristi princip hladnog i toplog toka vazduha. Lokacije gde se moduli instaliraju treba da obezbedi samo sistem napajanja modula i prodor hladnog vazduha.



Slika 4. Microsoft modul IT PACK

Ovom metodom projektovanja datacentara ostvaruje se ušteda vode od približno 90% i približno 30% energije. Danas svaki Microsoft datacentar prati ovaj dizajn.



Slika 5. Šema Microsoft datacentara.

Ovom arhitekturom postiže se i ušteda u broju radnih inženjer sati jer timovi koji projektuju i optimizuju sadržaj ITPAC modula i lokacije mogu da rade potpuno nezavisno jedni od drugih. Ovo je jako važna ušteda imajući u vidu činjenicu da je Microsoft danas kompanija koja najviše ulaže u razvoj datacentara ali je i najveći zakupac datacentar kapaciteta kod drugih kompanija.

#### 4. Elementi datacentra

U Dosadašnjim primerima i razmatranjima dizajna datacentara, mogu se prepoznati određeni segmenti koji je zajednički bez obzira na namenu datacentra. Nakon definisanja projektnih zadataka i inicijalnog kapaciteta, svaki segment se može zasebno i jednovremeno projektovati. Segmenti datacentra:

- Lokacija,
- Računari za obradu podataka,
- Računari za skladištenje podataka,
- Računarsko-telekomunikacioni modul i
- Modul neprekidnog napajanja.

U radu svakog datacentra najbitnije je sačuvati podatke, bez obzira na očekivane ili neočekivane okolnosti. Pored redundanse unutar jedne lokacije (u vidu rezervnih servera, svičeva, jedinica za skladištenje podataka), treba obezbediti i redundansu na nivou lokacija. Ukoliko dođe do otkaza rada cele lokacije (npr. usled otkaza kompletnog sistema napajanja) šta se dešava sa podacima? Ukoliko ne postoji rezervna (redundantna) lokacija - svi podaci su izgubljeni.

Kako bi se prevazišao ovaj problem, uvode se redundantne lokacije za svaku lokaciju. Obično se, zbog količine podataka, ne kopiraju svi podaci između lokacija unutar jednog datacentra, već samo određeni skup podataka koji je označen kao prioritetan. Redundantna lokacija, da bi ispunila važeće standarde, mora biti minimalno udaljena 50 milja (80,46 km).

U narednih poglavljima svaki segment biće detaljnije objašnjen.

## 4.1 Lokacija

Segment lokacija predstavlja sve činioce koje se vezuju za samu lokaciju. Lokacija može biti i 20 metara ispod zemlje, ili mobilni metalni kontejner, ali uslove koje treba da obezbedi su isti. Na planiranoj lokaciji mora biti obezbeđeno:

- Klimatizacija,
- Redundantno osnovno napajanje,
- Ventilacija,
- Odvojene prostorije za opremu i ljudstvo,
- Naponska kanalizacija,
- Telekomunikaciona kanalizacija,
- Sanitarni uslovi za boravak ljudstva,
- Višestruki izlazi za evakuaciju.

Klimatizacija je osnovna briga lokacije. Način na koji se implementira sistem klimatizacije u mnogome diktira konačan energetska bilans datacentra i cenu uspostave datacentra. Zbog ušteda u energiji, poželjne lokacije datacentra su one u kojima je priroda rešila dobar deo ovog problema putem niskih spoljnih temperatura (Hamina, Finland (google), Luleå, Sweden (Facebook)), ili jakih vetrova i jeftinije energije (Chicago USA (Microsoft)).

Datacentri su veliki potrošači električne energije i zahtevaju da se dovod električne energije vrši sa minimum dva nezavisna pravca po mogućstvu od dve različite kompanije. Ovaj zahtev je jako teško ispoštovati u gradovima jer uspostava visoko naposke mreže nije moguća u naselejnim sredinama. Takođe ukoliko bi jedan datacentar bio lokaciran u centru grada, svi građevinski radovi bi bili znatno skuplji zbog potrebnih dozvola a i širenje datacentra bilo bi ograničeno na zemljište koje je unapred kupljeno.

Zbog svih navedenih činjenica veći datacentri su uvek locirani u slabo naseljenim sredinama koje su infrastrukturno opremljene za te potrebe. Obzirom da eventualni troškovi postavljanja komunikacionih kablova predstavlja približno 5% od ukupnih troškova segmenta lokacije, izmeštanje datacentra van naseljene zone se smatra dobrim rešenjem.

Okvirno pravilo za proračun troškova je da troškovi uspostave infrastrukture na odabranoj lokaciji čine 50% svih troškova za uspostavu datacentra.

#### **4.2 Računari za obradu podataka**

Ukoliko bi ceo datacentar posmatrali kao jedan veliki računar, ovaj segment bi imao ulogu radne memorije, procesora i ulazno-izlaznih komponenti (audio karta, grafička karta, mikrofoni...). Ovaj rad se bavi datacentrima za potreba sistemskih servisa gde ne postoji realna potreba za većom obradom podataka ali to ne znači da je ovaj segment manje važan. Ukoliko bi zadatak datacentra bio keširanje video zahteva (youtube) ili online obrada audio-video zapisa, ovaj segment bi imao dominantnu ulogu.

Uobičajena praksa je da se ovaj segment implementira putem Blade sistema servera zbog lakšeg upravljanja rezursima. Takođe ovaj sistem omogućava laku nadogradnju sistema sa novim serverima jer se sve mrežne instalacije vezuju za šasiju blade sistema.



Slika 6. Blade sistem servera

### 4.3 Računari za skladištenje podataka

Ako je primarni cilj datacentra da obradi podatke i sačuva rezultate obrade, ovaj segment datacentra je najbitniji. Svi ostali segmenti služe za njegov neprekidan rad i priliv podataka za skladištenje. Dizajn ovog segmenta bitno ne određuje cenu samoga datacentra ali u mnogome određuje njegove performanse. Ovaj segment se implementira u vidu RAID nizova u kojima je moguće oporaviti niz čak i ukoliko nekoliko diskova jednovremeno otkaže. Vodeći proizvođači opreme za ovaj segment su: EMC, NetApp, Hitachi, IBM. Svaki od njih je razvio sopstenu tehnologiju sistema za skladištenje podataka a neke od njih ćemo objasniti u narednim poglavljima.



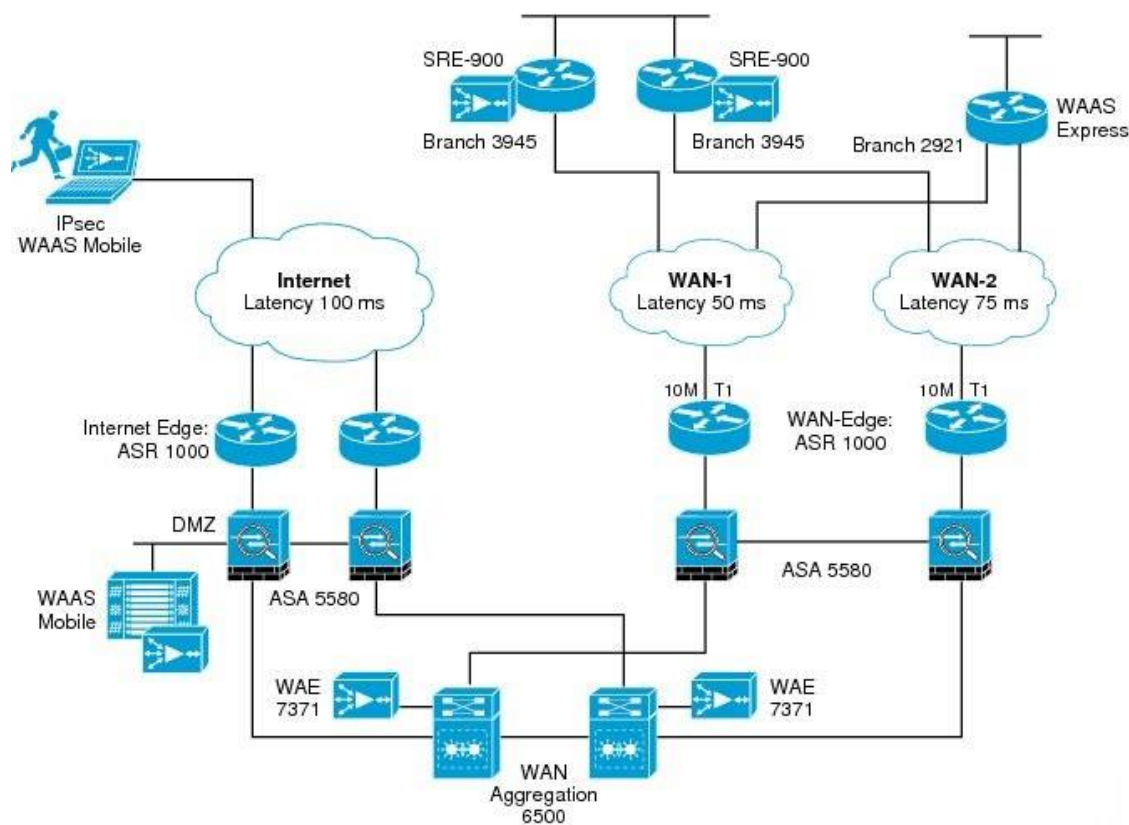
Slika 7. Sistem za skladištenje podataka.

#### 4.4 Računarsko-telekomunikacioni segment

Računarsko-telekomunikacioni segment u mnogome zavisi od ostalih modula. Sa porastom broja uređaja raste i kompleksnost ovog segmenta. Namena ovog segmenta je da sve segmente poveže u jedinstvenu i funkcionalnu celinu, stoga mora biti redundantan i otporan na prekide u komunikaciji.

Računarsko-telekomunikacioni segment čini datacentar dostupnim svojim korisnicima i predstavlja most između datacentra i spoljne mreže (npr Internet). Ovakva pozicija nameće

još jedan jako važan zadatak ovog segmenta a to je bezbednost kako podataka datacentra tako i samih korisnika datacetra. Softverski napadi na datacentre mogu biti toliko sofisticirani da budu otkriveni tek posle nekoliko meseci. Zato se dizajnu ovog segmenta poklanja velika pažnja.



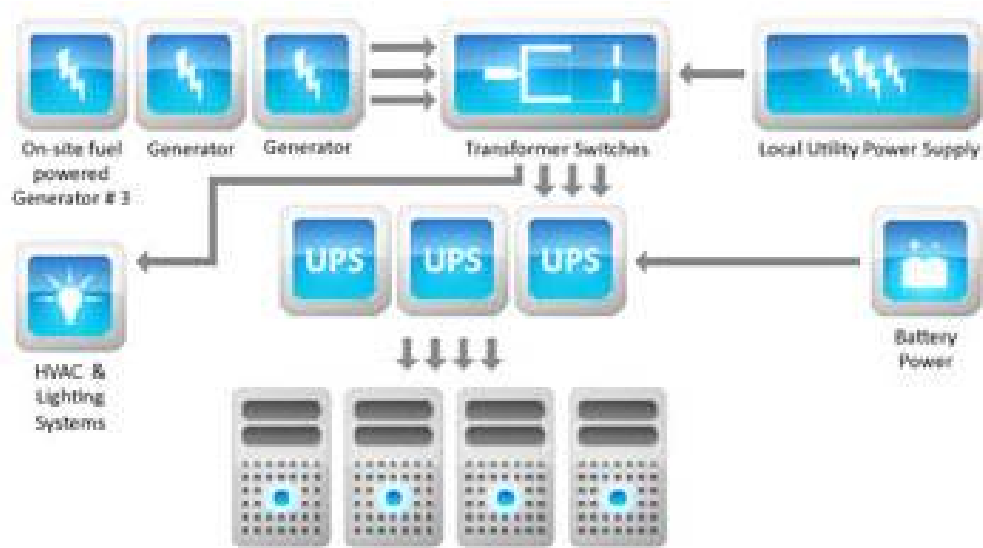
Slika 8. Predlog dizajna datacentra mreže kompanije CISCO

## 4.5 Modul neprekidnog napajanja

Modul neprekidnog napajanja sprečava gubitak podataka usled prekida u napajanju električnom energijom. Neprekidnost se može obezbediti putem baterijskih jedinica ili agregata. Potreban nivo, odnosno trajanje napajanje posle prekida u napajanju električnom energijom zavisi od važnosti datacentra odnosno nekog njegovog modula.

Sistem napaja je jedan od faktora pouzdanosti datacentra i jedan od bitnih faktora koji utiču na konačnu cenu uspostave datacentra. Ustaljena implementacija sistema napajanje je kroz

primarni, sekundarni i tercijalni sistem napajanja. Primarni sistem je obični neki jeftiniji izvor poput vetro parka za potrebe datacentra u Čikagu, ili primarna energetska kompanija sa kojom postoji povoljan ugovor. Sekundarni sistem se zasniva na standardnoj električnoj instalaciji kojom se doprema energija od sekundarnog dobavljača. Tercijalni izvor obično predstavlja dizel agregati.



Slika 9. Primer šeme napajanja datacentra

## 5. Projektovanje datacentra

U ovom delu moramo početi sa iznošenjem konkretnih zahteva koje datacentar mora da ispuni. Zahtevi moraju da obuhvataju svih 5 segmenata kako bi bio moguć jednovremeni rad timova.

Zbog osetljivosti podataka u daljem tekstu nećemo otkrivati tačnu lokaciju datacentra i kompaniju. Za potrebe rada, kompaniju ćemo nazvati „West“, datacentar na primarnoj lokaciji „scPrime“ i datacentar na sekundarnoj lokaciji „scBackup“

### 5.1 Projektni zahtevi

West kompanija ima približno 30.000 zaposlenih. 30.000 zaposlenih koriste približno 30.000 računara u kancelariji (desktop ili laptop) i bar još 15.000 ili 50% njih koriste bar jedan dodatni uređaj koji se vezuje na mrežu. Dakle naš datacentar ima približno 45.000 korisnika.

Radno vreme u West kompaniji je 8 sati ali se period rada razlikuje. Možemo reći da se početak kreće od 7-9 pa do 15-17 časova. Dakle naš period opterećenja je od 7-17 časova. Ono što želimo je da van ovih sati naš scPrime ne radi sa punim kapacitetom jer bi on bio opterećen oko 5%. Nepotrebne resurse treba ugasiti i time uštedeti energiju.

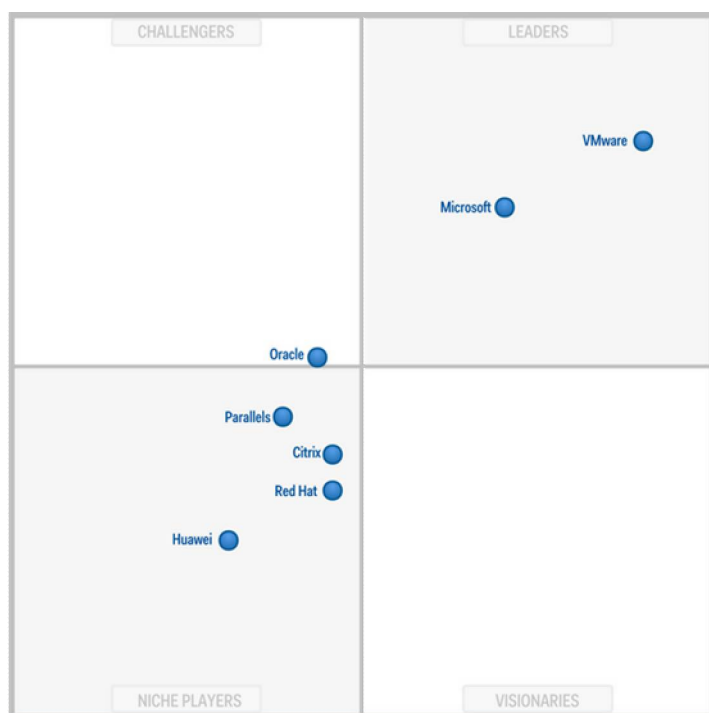
Obzirom da su ulaganja u klimatizaciju i adaptiranje najveća, treba odmah predvideti faze realizacije. Infrastruktura same lokacije zavisi i od broja uređaja koje treba rashladiti. U svakoj fazi treba rešiti tretnunte potrebe kompanije. Kako rastu zahtevi kompanije tako raste i kapacitet datacentara. Za svaku potencijalnu lokaciju datacentra potrebno je uraditi idejni projekat sa proračunom sredstava. U ovom radu nećemo se baviti idejnim projektom jer on uglavnom obuhvata građevinske i energetske proračune.

Pored već navedenih scPrime treba da ispuni i sledeće zahteve:

- U potpunosti usaglašen sa idejnim projektom datacentra,
- Opisati potrebne telekomunikacione infrastrukture (broj svičeva, minimalan kapacitet linkova),
- Opisati energetske potrebe i dati plan dogradnje postojećih kapaciteta ako za to ima potrebe,
- Razraditi uspostavu rezervne lokacije koja je u potpunosti redundantna. U slučaju otkaza primarne lokacije rezervna mora da se aktivira automatski,
- Osnovu projekta čine: tehnologija virtuelizacije, softver VMware Site Recovery Manager, vSphere Cluster. Svaka tehnologija mora biti nezavisno objašnjena, a potom i način njenog uvođenja u predloženi koncept,
- Realizacija projekta mora biti podeljena po fazama. Za svaku fazu definisati potrebe, sa cenom koštanja realizacije,
- Plan opremanja hardverom i softverom za realizaciju svake faze projekta,
- Projekat mora da sadrži minimalan broj ljudstva sa definisanim pojedinačnim ulogama, neophodnom stručnom spremom, kao i predlog organizacije njihovog rada,
- Prva faza mora biti uspostava testnog okruženja kojim se dokazuje valjanost koncepta predloženog samim projektom. Minimalan kapacitet skladišta u ovoj fazi je 5 TB,
- Uspostava rezervne lokacije mora biti predviđena u poslednjoj fazi projekta,

- Ciljni kapacitet datacentra je 100 TB, što treba uzeti kao osnov za proračune,
- Minimalna pouzdanost mora biti 99,99% dok je 99,999% preferirana dostupnost (ukoliko ne zahteva znatno veća finansijska ulaganja).
- Za potrebe uspostavljanja veza između scPrime i scBackup (rezervna lokacija) dati procenu kapaciteta veza, tip veze, kao i procenu kašnjenja.

Danas postoje više kompanija koje nude svoja rešenja za virtuelizaciju. VMware platforma je odabrana jer je ta kompanija pionir na ovom polju i uvek je bila na vrhu sa tehnologijom koja postavlja standarde u pomenutoj oblasti. Još jedan razlog u prilog ovoj odluci je podatak da West kompanija ima već ljudstvo koje je završilo specijalističke vmware kurseve, te postoji dobra baza znanja iz ove oblasti.



Slika 10. Grather magični kvadranti na polju virtuelizacije

## 5.2 Analiza postojećeg stanja

Kompanija West je već radila na uspostavi datacentra ali neorganizovano i pokušavajući da reši samo trenutne probleme. Deo infrastrukture je postavljen ali nije povezan na odgovarajući način. Treba uzeti u obzir da nije moguće dalje širenje prostorije i da su energetske kapaciteti na izmaku.

Ostala zapažanja:

- U prostoriji koja je predviđena za adaptaciju datacentra, smeštena su 4 ormana sa IT opremom (zadržavaju se dva postojeća ormana, dva se izbacuju).
- Prostorija ima dupli pod i plafon spuštene tipa Armstrong.
- Pregradni zidovi su montažni i nisu protivpožarno zaštićeni.
- Spoljašnji zid, orjentisan ka jugozapadu, ima parapet 67cm, ostali deo je zastakljen.
- Visina prostorije je 3,7 m (od duplog poda do spuštenog plafona). Visina duplog poda je 0,5 m, visina spuštanja plafona 0,5 m.
- Električna instalacija u okviru prostorije sa opremom IT je vođena u duplom podu i u kanalicama po zidu.
- Sva oprema se napaja iz utičnica montiranih na zid.
- Svi potrošači u prostoriji sa opremom IT u sebi napajaju se iz istog razvodnog ormana RO-1, smeštenog u hodniku, ispred prostorije.
- Iz razvodnog ormana RO-1 se pored potrošača u prostoriji sa IT-opremom, napajaju i okolne kancelarije sa oko 15 - tak radnih mesta.

- Trafostanica 10/0.4kV, 630kVA (TS1) je smeštena nedaleko od zgrade datacentra ali u okviru istog kompleksa.
- Pored mrežnog napajanja, postoji i agregatsko napajanje - SDMO
- V630, 630KVA/500KW.
- Iz trafo stanice TS1 (i agregata) napajaju se i potrošači u susednoj zgradi (kancelarije sa oko 530 radnih mesta).
- Postoji još jedna trafostanica (TS2). Od trafostanice TS2 do razvodnog ormana RO-1 položen je kabl koji nije u funkciji (nije povezan).
- U prostoriji postoji oprema za klimatizaciju: dva split sistema, jedna prozorska i jedna mono blok jedinica, kao i dva grejna tela - radijatori sa 24 članka.
- U prostoriji su instalirani javljači požara, ali nema instalacije za gašenje požara.

Postojeća serverska infrastruktura je delimično virtuelizovana i postoji jedan virtuelni klaster sa 3 host-a koji nije u eksploataciji već u je test režimu rada.

### 5.3 Dodatni zahtevi

Uzimajući u obzir anлізу postojećeg stanja dolazimo do dodatnih zahteva za uspostavu datacentra:

- Izabrati virtuelnu platformu koja odgovara postavljenom nivou funkcionalnosti i koja obezbeđuje traženi nivo raspoloživosti i otpornosti na otkaze,
- Virtuelna platforma mora da bude skalabilna i da obezbeđuje jednostavno proširenje kapaciteta servisa i volumena storidža od bar 1:20 u odnosu na početne

- zahteve, s tima da ne zahteva prevremenu i neekonomičnu nabavku i rezervaciju fizičkih resursa,
- Izabrati storidž platformu koja raspolaže pouzdanošću traženog nivoa i pri tome obezbeđuje efikasno i ekonomično upravljanje diskovnim prostorom,
  - Obezbediti mogućnost udaljenog kopiranja podataka da bi se sprečilo njihovo uništenje – namerno, kao posledica katastrofe ili kardinalne ljudske greške,
  - Rešenje napraviti tako da bude potpuno redundantno u svim svojim hardverskim elementima i otporno na otkaz bilo koje pojedinačne komponente,
  - Obezbediti potpunu zaštitu podataka primenom bekap rešenja koje obezbeđuje lokalnu, udaljenu kopiju i oporavak na bilo kojoj sekundarnoj lokaciji scBackup
  - Obezbediti automatski oporavak u slučaju otkaza celokupnog hosta/servera i/ili jednog storidž kontrolera,
  - Obezbediti pokretanje automatske procedure oporavka celog datacentra u slučaju katastrofe na zahtev administratora sistema, kao i testiranje i dokumentovanje procedure oporavka na zahtev,
  - Fiksno i ekonomično korišćenje linkova između udaljenih lokacija,
  - Obezbediti jednostavnu i pouzdanu integraciju u postojeću mrežnu infrastrukturu kompanije West,
  - Obezbediti potpunu kontrolu administrativnog pristupa infrastrukturi, kao i registrovanje svih značajnih događaja u dnevnicima (logovima),
  - Obezbediti alat za nadzor infrastrukture i detekciju grešaka/kvarova,
  - Planirati obuku i obučiti stručno osoblje kompanije West za korišćenje instalirane infrastrukture,
  - Obezbediti da u prvoj fazi realizacije projekta koncept funkcionisanja datacentra bude uspešno potvrđen u svim navedenim elementima,
  - Omogućiti implementaciju novih tehnologija, pre svega „cloud computing“ rešenja, na već izgrađenoj virtuelnoj platformi, i time obezbediti potpunu hardversku

nezavisnost aplikativnih servisa i podataka, njihovu enkapsulaciju i zaštitu, kao i potpunu mobilnost u okviru postojeće infrastrukture.

## **5.4 Faze**

Kako bi sprečili utrošak značajnih finansijskih sredstva u eventualno nefunkcionalni datacentar, treba isprojektovati i samu podeli na faze.

### **5.4.1 Faza 1: Dokaz koncepta**

U ovoj fazi se na postojeći klaster dodaje sistem za skladištenje podataka kapaciteta 5TB. Cilj ove faze je i da se ispitaju performanse samog sistema za skladištenje i odaberu uređaji koji će se koristiti na primarnoj lokaciji.

### **5.4.2 Faza 2: Proširenje kapaciteta**

U ovoj fazi planirano je proširenje kapaciteta za 100% tj na 10TB i to bez gašenja sistema. Obzirom da već postoji određena redundansa na polju hardware, u ovoj fazi vršimo i testiranje otkaza diskova i ponašanje sistema za skladištenje.

### **5.4.3 Faza 3: Potpuna realizacija primarne lokacije**

Nakon svih testova odabrani su uređaji i možemo vršiti potpunu implementaciju svih segmenata datacentra. Uređaji koji su se koristi za dokazivanje koncepta se prebacuju na sekundarnu lokaciju kako bi se nakon uspostave primarne lokacije izvršile sve pripreme za implementaciju sekundarne lokacije.

### **5.4.4 Faza 4: Realizacija sekundarne lokacije**

Realizacijom ove faze dobijamo potpuno redundantan i pouzdan datacentar visoke dostupnosti. Treba napomenuti da se ne kopiraju svi podaci sa scPrime na scBackup već samo oni koji su označeni kao prioritetni, približno 33%.

## 6. Implementacija

Implementacija prati projekat pa samim tim biće podeljena u iste 4 faze. U narednim poglavljima svaka faza biće detaljno objašnjena.

### 6.1 Faza 1: Dokaz koncepta

Ova faza je na prvi pogled trivijalna u tehničkom smislu. Potrebno je povezati dva servera i jedan sistem za skladištenje u funkcionalnu celinu i proveriti performanse. Međutim ova faza je mnogo više. U ovako malom okruženju možemo instalirati sve što je potrebno za datacentar bilo koje veličine i kapaciteta za obradu i skladištenje podataka.

Hardversko-softverske komponente koji su potrebne za ovu fazu realizacije:

| Rb | Nazi komponente         | Količina | Namena                                                                                                         |
|----|-------------------------|----------|----------------------------------------------------------------------------------------------------------------|
| 1  | IBM H Šasija            | 1        | Obezbeđuje jedinstveno napajanje, povezivanje i menadžment za sve servere u šasiji                             |
| 2  | IBM H 22                | 2        | Blejd server – host za virtuelnu infratukturu                                                                  |
| 3  | Storage NetApp FAS 3210 | 1        | Storidž sistem – skladište podataka na diskovima koje je zajedničko za sve hostove u virtuelnoj infrastrukturi |
| 4  | ESXi 5 licence          | 1        | Licence za VMware hipervizor – ključna komponenta virtuelne infrastrukture                                     |

Računarsko-telekomunikaciona oprema koji je potreban za ovu fazu realizacije:

| Rb | Nazi komponente       | Količina | Namena                                                                                                                                                                        |
|----|-----------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | CISCO Catalzst        | 1        | Ključni svič (komutator) koji<br>virtuelnu infrastrukturu<br>povezuje sa ostatkom lokalne<br>mreže (korisnicima) i koji<br>obezbeđuje rutiranje između<br>različitih VLAN-ova |
| 2  | Brocade 300 FC switch |          | SAN svič koji povezuje hostove<br>virtuelne infrastrukture i<br>storidž podsistem(e)                                                                                          |

Sva oprema i licence su bile dostupne u trenutku realizacije ove faze sa izuzetkom sistema za skladištenje podataka (u daljem tekstu storidž). Jedan od ciljeva ove faze implementacije je dokaz funkcionanosti predloženog harveskog rešenja za storidž.

#### **6.1.1 Povezivanje komponenti u funkcionalnu celinu**

IBM H blejd šasija je montirana u orman za montažu opreme u gornjoj polovini ormana, tako da je na vrhu ormana ostavljeno bar 6 jedinica za mrežnu opremu, a na dnu ormana

6 jedinica za besprekidno napajanje i iznad njega počevši od polovine ormana nadole za

montažu storidž sistema. Ostavljen je prostor od bar 8 jedinica za proširenje storidža u drugoj fazi projekta.

Napajanja u blejd šasiji su vezana na različite letve za napajanje i različite napojne grane prema uređajima za besprekidno napajanje. Instaliran je i upravljački modul blejd šasije na predviđenu lokaciju u šasiji. U šasiju su montirani moduli za povezivanje u LAN i SAN mreže i dodati blejd serveri u šasiju s leva na desno.

Aktivna mrežna oprema (CISCO Catalyst 3750) je montirana u gornjem delu ormana (kako je navedeno). Ključna namena ovog sviča je da poveže svičeve i upravljački modul iz blejd šasije, u jedinstvenu celinu kao i da spoji uspostavljeno okruženje sa ostakom mreže.

Bitno je naglastiti da ovaj svič takođe vrši izolaciju saobraćaja putem VLAN-ova (virtuelnih lokalnih mreža) i to na: upravljačku mrežu, interkonekcije virtuelnog klastera i korisnička mreža putem koje se pristupa servisima u virtuelnom okruženju.

Lokalna mreža je konfigurisana na sledeći način:

- Vezu blejd server – interni svič konfigurisan kao „trunk“ tako da može da propusti sve VLAN mreže koje su u upotrebi na scPrime,
- Isto tako konfigurisati i Cisco 3750,
- Međusobne veze VLAN-ova rutirati za podmreže za koje je potrebna međusobna vidljivost,
- Lokalnu mrežu segmentirati na tri segmenta: upravljačka mreža (izolovana od spoljnih korisnika), mreža za interkonekcije hipervizora (za potrebe vMotion i Storage vMotion migracija) i korisnička mreža (aplikativni servisi),
- Podešeni svi parametri mrežne hipervizora (adrese, maske, mrežni prolaz),
- Podešen virtuelni svič na hipervizoru i kreirane upravljačke, intekonektivne i korisničke port grupe,
- Podešene port grupe prema šemi VLAN-ova koji se koriste u scPrime tj indentično kao na Cisco 3750.

### **6.1.2 Instalacija i konfigurisanje storidž sistema**

Prvi korak je montiranje storidž sistema u orman i povezivanje portova za menadžment storidža sa svičevima za lokalnu mrežu. Putem direktnog pristupa na konzolu storidž sistema podešene su menadžment adrese na storidž kontrolerima. Nakon ovih podešavanja administrativni portal storidža je dostupan.

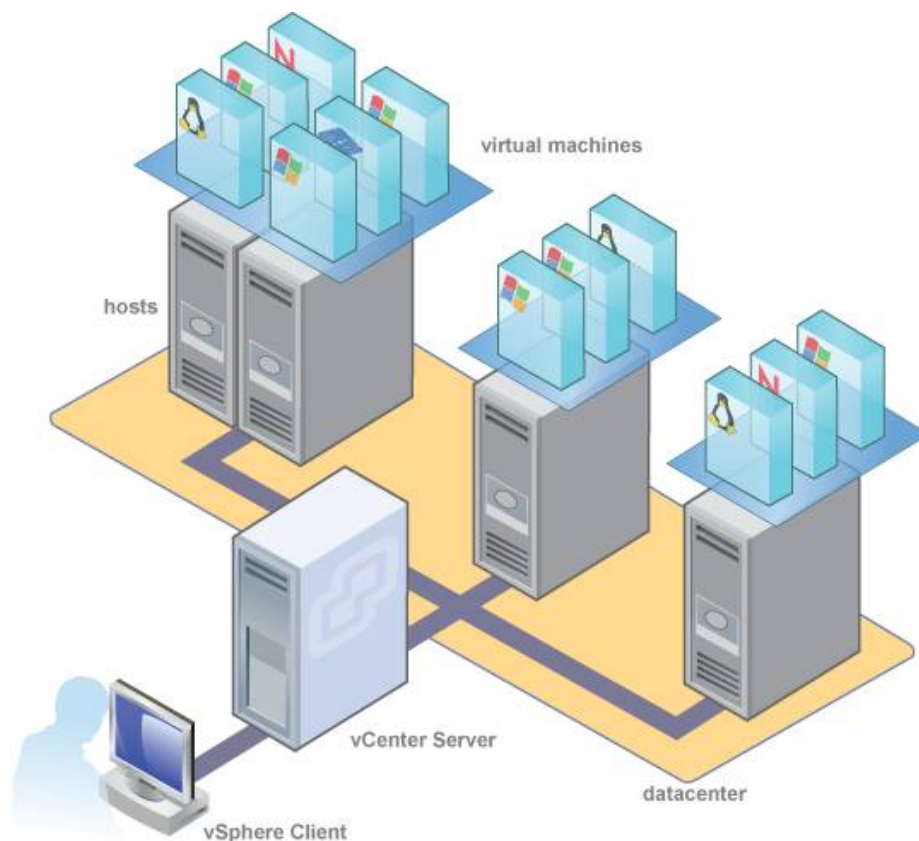
Prvo se podešava protokol pristupa a u ovom slučaju to je fiber Chanel (FC). Prvo je kreiran test volumen veličine 500 GB na storidž sistemu. Potom se storidž povezuje na svičeve i proverava novouspostavljena konektivnost. Za povezivanje se koriste isključivo monomodni optički kablovi.

Obzirom da je sada storidž sistem povezan na mrežu, potrebno je još uspostaviti vezu sa virtuelnim serverima (u daljem tekstu hostovi). Takođe na FC sviču treba konfigurisati dualne putanje do hostova.

Nakon ove konfiguracije sistem je potpuno funkcionalan i možemo početi sa instaliranjem virtuelnih servera.

### **6.1.3 Instalacija menadžment servera za virtuelnu infrastrukturu**

Iako je novouspostavljeni sistem (virtuelni klaster) funkcionalan i dalje nije omogućeno jedinstveno upravljanje resursima virtuelnog klastera. Ovu ulogu vrši vCenter, VMware alatom koji je u stanju da upravlja svim resursima virtuelnog klastera bez obzira na njegovu veličinu. Ovaj alat se instalira u okviru Windows 2008 Standard 64-bit virtuelne mašine i pristupa mu se putem još jednog VMware alata a to je vClient. Sam Vcentar zateva MS SQL server za svoj nesmetan rad, SQL server može ali ne mora biti na istom mašini kao i vCentar ali se smatra dobrom praksom ako su vCentar i SQL server razvojeni na dve različite mašine.



Slika 11. Arhitektura VMware sistema za upravljanje virtuelnim okruženjem

#### 6.1.4 Testiranje uspostavljene konfiguracije

Obzirom da su sve komponentne predviđene za fazu1 intalirane, preosaje da se izvrši testiranje sistema. Za potrebe testa korišćenje su Virtuelne mašine sa operativnim sistemima windows XP, windows 7 i wondows 2008. Takođe kreiran je dodatni volumen na storidžu (LUN). Operacije koje su testirane su: migracija sa hosta na host bez promene volumena, migracija sa promenom volumena, fault tolerant opcija VMware-a.

VMotion je proces migracije unutar VMware virtuelnig klastera tokom kojeg se virtuelna mašina izmešta na drugi host i/ili na drugi volumen.

Fault Tolerant je VMware funkcionalnost koja podrazumeva da se jedna virtualna mašina izvršava na 2 hosta. Na jednom je primarna kopija dok se sekundarna kopija samo ažurira. Ukoliko primarna kopija odnosno njen host postane nedostupan, sekundarna kopija postaje primarna i virtualna mašina nastavlja sa radom. Virtualna mašina koja ima ovu opciju aktivnu, zauzima resurse na oba hosta.

Na svim testovima uspostavljeno okruženje je pokazalo odlične rezultate. Tokom migracije nije bilo zastoja u radu servisa. U slučaju fault tolerant testa, samo „4 ping“ su bila izgubljena u opravku virtualne mašine.

Treba napomenuti da je tokom ove faze vršeno testiranje i storidža proizvođača IBM i ACER. Obzirom da sistemski servisi ne predstavljaju veliko opterećenje za hard diskove, jedna druga VMware tehnologija je korišćena za izbor proizvođača storidža a to je vDesktop. Virtualizacija desktopova predstavlja veliko opterećenje za hard diskove storidža pa samim tim je odličan test. Na ovom testu ACER R700 proizvod se pokazao potpuno neupotrebljiv i preglasan. IBM Storewise serije 3000 pokazao je dobre performanse i izuzetno je lak za instalaciju i konfigurisanje ali je u pogledu performansi pokazao 50% slabiji rezultat od NetApp-a. Na NetApp storidž vreme restarta windows XP mašine je oko 55 sekundi dok na IBM približno 90 sekundi. Zbog ovog testa razmatran je samo NetApp storidž.

Ovim testiranjem je prva faza projekta u potpunosti završena. Zbog odličnih rezultata na testu možemo smatrati da je koncept uspešan i da možemo krenuti u dalju realizaciju.

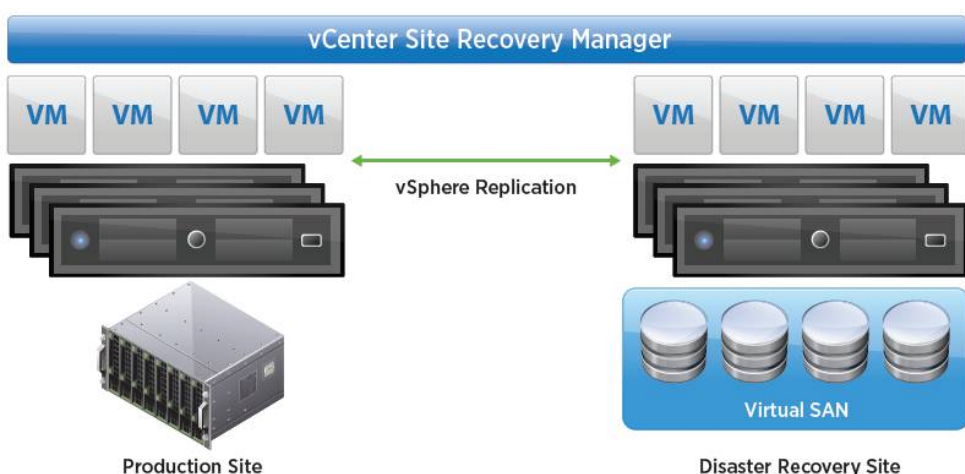
## **6.2 Faza 2: Proširenje kapaciteta**

U ovoj fazi realizujemo nekoliko bitnih koraka. Kapacitet za skladištenje podataka se povećava sa 5TB na 10TB što je inicijalni kapacitet sekundarne lokacije. Proširenje je realizovano dodavanjem novog kućišta sa diskovima koristeći postojeći FC kontroler. Celokupno proširenje se realizuje bez gašenja sistema.

Još jedan zadatak ove faze implementacije je i testiranje tehnologije oporavka od katastrofa (Disaster Recovery Scenario). Obzirom na tajnost podataka kojima kompanija West raspolaže, nije bilo moguće angažovanje spoljnih savetnika i izrada kompletnog plana implementacije, dosta tehnologija je usvajano tokom procesa implementacije. VMware tehnologija repliciranja virtuelnih mašina na 2 lokacije je jedna od njih.

Svo testiranje je realizovano u istoj prostoriji, bez instaliranja uređaja na planiranoj sekundarnoj lokaciji. Novouspostavljeni sistem od 10TB je imao ulogu primarne lokacije dok je stari sistem (server HP DL580 kapacitet 2,2TB) imao ulogu sekundarne lokacije.

VMware vCenter Site Recovery Manager (SRM) je alat koji objedinjuje nekoliko VMware tehnologija u jedinstveni sistem. Njegova glavna odlika je nezavisnost od hardverskih komponenti jer se replicacija vrši između virtuelnog hipervizora na lokaciji A i virtuelnog hipervizora na lokaciji B. Ukoliko bi se replicacija odvijala između uređaja za skladištenje podataka, proces replicacije između 2 uređaja različitih proizvođača ne bi bio moguć.



Slika 12. VMware Arhitektura sistema za oporavak od katastrofa

Obzirom da se replikacija radi na nivou hipervizora, jedinica replikacije je virtuelna mašina. Procena je da sve virtualne mašine neće zauzeti više od 10TB, stoga faza 2 predstavlja i podešavanje sistema za buduću sekundarnu lokaciju. Obzirom da SRM poseduje mogućnosti testiranja scenarija bez zaustavljanja servera na primarnoj lokaciji, testiranje oporavka sistema je realizovano bez uticaja na rad produkcionih servisa. Svi rezultati su bili pozitivni i jedina nepoznanica u ovom sistemu je telekomunikacioni kapacitet interkonekcija između primarne i sekundarne lokacije.

Za replikaciju podataka između scPrime i scBackup (između dva hipervizorska storidž sistema) neophodno je uspostaviti komunikacionu vezu baziranu na TCP/IP protokolu. Storidž sistemi koji su planirani za implementaciju raspolažu softverom za replikaciju koji koristi navedeni protokol. Za replikaciju na rastojanjima većim od 100 km koristi se asinhroni režim kopiranja podataka, jer je kašnjenje na linku veće od 2ms što se smatra gornjom granicom za sinhronu replikaciju. Pored toga, sinhrona replikacija je nepodesna jer dodatno smanjuje raspoloživost (zbog toga što treba uračunati i raspoloživost linkova i storidža na sekundarnoj strani).

Procena je da dnevna izmena podatka na primarnoj lokaciji iznose manje od 1 GB dnevno. U prvoj fazi i znatno manje (oko 200 MB). Ako se pretpostavi da se promene stvaraju u toku radnog vremena, dakle 8 sati dnevno, proizilazi da je obim promena najviše 125 MB na sat, ili  $125 * 8 = 1000$  Mb/h. Preračunato, to iznosi  $1000/3600 = 0,28$  Mb/s ili 280 Kb/s. Dakle, sama replikacija ne zahteva značajan mrežni protok. Ako uračunamo i replikaciju bekap podataka (koji su prethodno komprimovani i deduplikovani) ova vrednost će se uvećati ne više od 25% (zbog kompresije i deduplikacije podataka). Ukoliko se pojave vršna opterećenja u kojima je obim promena znatno veći od 125 MB sat, mehanizam asinhronu replikacije će odložiti blokove koji se repliciraju na lokalni log volumen i na taj način smanjiti zasićenje linka. Bez obzira što ovo nije mnogo verovatno, ova funkcionalnost asinhronu replikacije obezbeđuje dodatnu zaštitu od preopterećenja spoljnih puteva i mogla bi biti od interesa kod uspostavljanja novih datacentra.

U ovom radu smo naveli primere datacentara u kojima su interkonekcije 40GB i više, dok je pračun u ovom radu u Kb/s. Ukoliko koristimo kriptografske metode zaštite na prvom sloju OSI modela brzine od 40GB nam nisu dostupne jer ne postoje kripto uređaji sposobni da rade na toj brzini. Kod ovako zaštićenih interkonekcija brzine se meri u MB/s pa je minimalizacija telekomunikacionih kapaciteta od vitalnog značaja.

### **6.3 Faza 3: Potpuna realizacija primarne lokacije**

U ovom koraku vršimo kompletnu uspostavu primarne lokacije datacentra, scPrime. Prvi korak u realizacije ove faze je adaptacija lokacije koja će biti detaljno opisana u narednom poglavlju rada. Sledeći korak je realizacija preostalih 4 segmenta koji će biti opisanani u zasebnim poglavljima.

VMware virtuelizaciona tehnologija je lepak koji spaja sve komponente u funkcionalnu sredinu. Ova tehnologija je trenutno najnaprednija, najfunkcionalnija i najpouzdanija virtuelna platforma na tržištu (prema gartneru Slika 10). VMware vSphere platforma daleko odskoče i u pogledu funkcionalne kompletnosti i parametara vezanih za sposobnost pouzdanog izvršenja postavljenih zadataka. Pri tome ima tržišno učešće u domenu standardne serverske infrastrukture (H86-64) od preko 70% i preko 150.000 instalacija u svetu, od koji su mnoge vezane za datacentre.

Cilj u pogledu racionalnog korišćenja resursa je da se postigne iskorišćenje CPU i memorije hostova u granicama od 60 – 80%. Prekoračenje gornje granice dopušteno je u kratkotrajnim intervalima vršnog opterećenja. Ukoliko bi u dužem vremenskom intervalu iskorišćenje CPU-a bilo iznad 90% može se očekivati značajan rast vremena odziva (“response time”), tj. pad performansi aplikacija iz perspektive krajnjeg korisnika.

Treba imati u vidu i činjenicu da je VMware ESX host sposoban da obradi preko 300,000 IOPS (!), što znači da hipervizor u praktičnim primenama ne može biti usko grlo u pogledu obrade ulaza/izlaza.

Sve gore navedene karakteristike opredeljuju VMware virtualizacionu tehnologiju kao odličnu podlogu za usposavu datacentara.

### **6.3.1 Adaptacija Primarne Lokacije**

Predviđeno je da se postojeća prostorija sa unutrašnje strane oblaže vatrootpornim gips

kartonskim pločama, vatrootpornosti 30min. Montažni pregradni zidovi ka susednim kancelarijama se na delu između stubova demontiraju i montiraju se novi montažni pregradni zidovi sa vatrootpornim gips kartonskim pločama. Na zidove ka hodniku i susednoj kancelariji montiraju se protivpožarna vrata. Plafon se demontira i montira se novi, tipa Armstrong, Rigips Casoprano ili sl. vatrootpornosti 30min. Dupli pod se demontira i postavlja se novi, antistatik dupli pod, nosivosti veće od 1300 kg/m<sup>2</sup>. Sve obloge zidova od gips kartonskih ploča su završno obrađene gletovanjem i bojene disperzivnom belom bojom u dva sloja. Na terasi, iznad prostorije datacentra, montira se čelični nosač za smeštaj spoljnih kondenzatorskih jedinica klima uređaja.

Neophodno je obezbediti da se iz postojećeg razvodnog ormana napaja samo oprema datacentra, tj. iz razvodnog ormana treba izmestiti svu ostalu instalaciju koja se ne odnosi na datacentar – napajanje okolnih kancelarija sa oko 15-tak radnih mesta. Postojeći kabl koji je položen od TS2 do TO-M/II treba proveriti i ponovo staviti u funkciju, kako bi se obezbedilo dvostrano napajanje datacentra. Ova instalacija treba da omogući priključenje novog dizel agregata (opciono) koji bi bio instaliran samo za potrebe datacentra. U okviru prostorije datacentra svu električnu instalaciju treba demontirati i voditi novu instalaciju

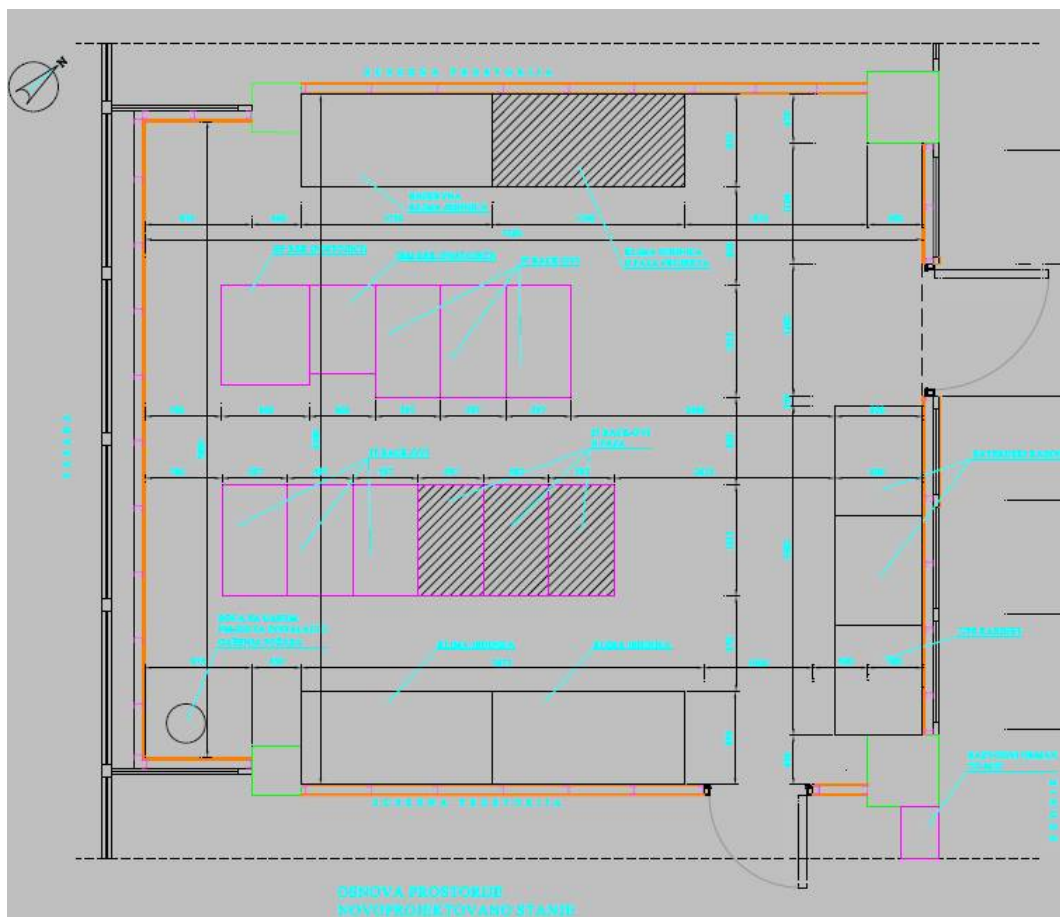
u kanalima u duplom podu. Potrebno je proveriti vrednost otpornosti uzemljivača i efikasnost instalacije gromobranske zaštite.

U prostoriji budućeg datacentra postojeća oprema za klimatizaciju se demontira, jer ne zadovoljava, kako po projektovanom kapacitetu, tako i po nameni, jer nije predviđena za primenu u datacentrima. Prodori demontiranog freonskog cevovoda se zapušavaju materijalizacijom zida. Kako bi se sprečio uticaj Sunca koji bi povećao dobitke toplote, predviđeno je postavljanje gips kartonskog zida ispred zastakljenih površina. Uređaji koji su predviđeni za klimatizaciju su slobodnostojeći, sa podnim izduvavanjem kroz rešetke za ubacivanje vazduha u duplom podu, koje bi se rasporedile prema dispoziciji IT opreme.

Spoljašnje kondezatorske jedinice bi se smestile iznad prostorije. Predviđena konfiguracija uređaja za klimatizaciju je N+1 (N radnih+1 rezervni).

U prvoj fazi projekta bi se montirala 3 uređaja. Emerson M35UA+HCE58 (2 radna+1 rezervni), a u drugoj fazi još jedan uređaj. Emerson M35UA+HCE58, što bi činilo konačnu konfiguraciju od 3 radna+1 rezervni.

U prostoriji budućeg datacentra predviđena je instalacija stabilnog sistema za gašenje požara gasom FM-200, koja podrazumeva bocu od 120 l sa 105 kg gasa, cevovod i 6 mlaznica.



Slika 13. Šema adaptacije lokacije za potrebe primarnog datacentra scPrime.

### 6.3.2 Računari za obradu podataka

Serverska infrastruktura (VI platforma) je zasnovana na IBM serverskoj platformi, konkretno, blade serverima sa po 2 šestojezgarna procesora familije Intel Xeon X5600 i 96GB memorije (IBM BladeCenter HS22). U funkciju su dve IBM BladeCenter H blade šasije sa inicijalno dva servera i sa mogućnošću proširenja (u skladu sa potrebama) na 28 servera iste ili slične konfiguracije kao osnove za virtuelnu infrastrukturu primarnog data centra. Za pristup SAN i LAN infrastrukturi koristi po jedan dvoportni CNA adapter po serveru, koji bi se mapirao na Cisco Nexus 4000I module u blade šasiji preko kojih bi se ostvarilo povezivanje sa jezgrom LAN/SAN mreže, na način opisan u Poglavlju 6.3.4.

ESXi hipervizor je instaliran na SSD diskovima hostova, čime su obezbeđene visoke performanse hosta i brz restart u slučaju potrebe. Takođe, SSD disk bi se mogao koristiti za implementaciju “host cache” funkcionalnosti vSphere 5, čime bi se omogućilo skladištenje („swap“) memorije virtuelnih mašina na deljeni prostor na lokalnom SSD disku hosta u slučaju preopterećenja fizičke memorije hosta. Kapacitet diskova nije kritičan, pošto sam ESXi ne zahteva više od 10 GB slobodnog prostora.

Serverska infrastruktura zajedno sa storidž sistemom, opisanom u sledećem odeljku, na primarnoj lokaciji angažuje najviše 15 KW snage.

### **6.3.3 Računari za skladištenje podataka**

Kao rešenje za storidž infrastrukturu, odabrana je NetApp storidž platforma. Poslednja generacija NetApp storidž sistema donosi pravu unifikaciju storidž protokola, pa jedan sistem sadrži agregirane sve opcije prezentacije storidž sistema (FC, ISCSI, FCoE, CIFS, NFS.). Nova NetApp FAS3200 serija nudi širok obim storidž funkcionalnosti koje omogućava softverski paket instaliran na kontrolerima – Data ONTAP Essentials. Pored osnovnih funkcionalnosti, prilikom nabavke uređaja obezbeđene su i SnapMirror licence za replikaciju i FlexClone licence za “writeable snapshot”, za potrebe automatskog oporavka virtuelne infrastrukture u slučaju katastrofe korišćenjem VMware Site Recovery Manager rešenja. Tokom instalacija više od 100.000 sistema ove klase utvrđen je nivo pouzdanosti koji je u skladu sa projektnim zadatkom, tj. više od 99,999%

NetApp storidž arhitektura implementira visoko performantni RAID6 nivo zaštite koji kombinuje prednosti RAID10 i RAID6. Ova NetApp implementacija RAID6 zaštite naziva se RAID-DP. RAID-DP je toliko brz da NetApp u svojim benchmark testovima koristi upravo RAID-DP a ne RAID10.

|             | RAID 5 | RAID 6 | RAID 10 | RAID-DP |
|-------------|--------|--------|---------|---------|
| Cost        | Low    | Low    | High    | Low     |
| Performance | Low    | Low    | High    | High    |
| Resiliency  | Low    | High   | Med     | High    |

Slika 14. Uporedni prikaz RAID konfiguracija

Storidž sistem na primarnoj lokaciji je NetApp FAS3240 sledećih karakteristika:

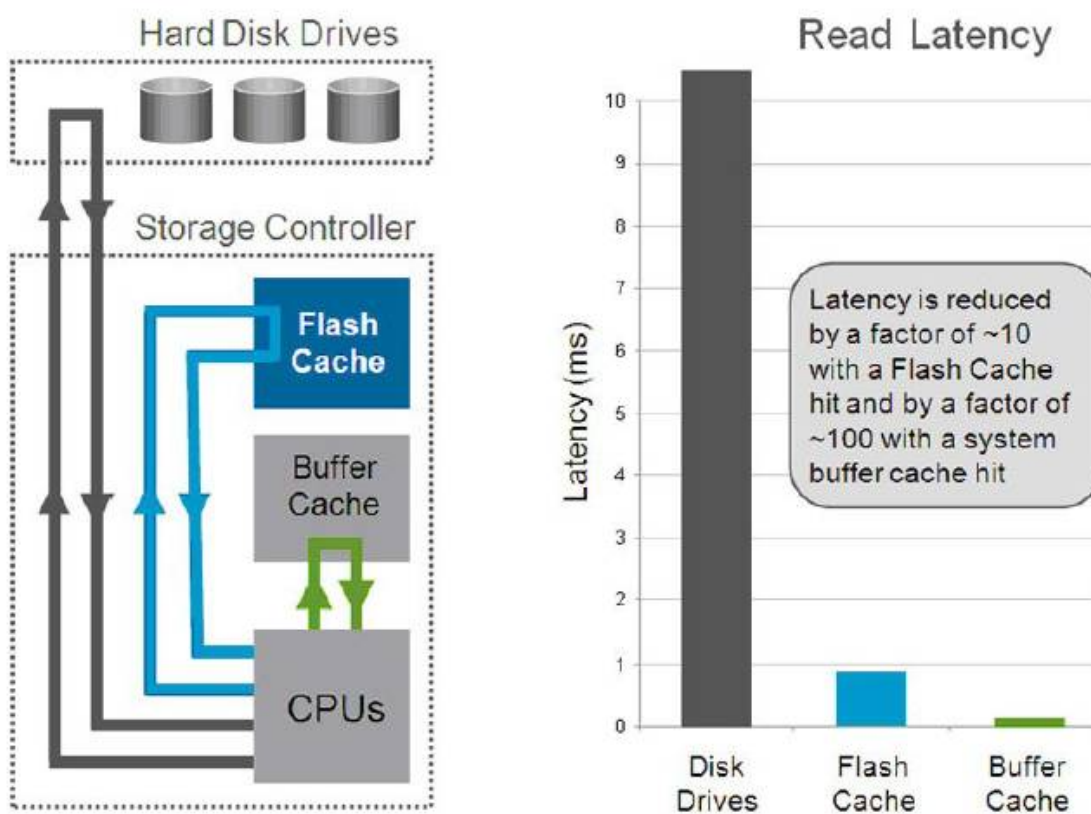
|                             |                                                |
|-----------------------------|------------------------------------------------|
| Maksimalni sirovi kapacitet | 1200TB                                         |
| Korisni kapacit             | 100TB                                          |
| Maksimalan broj diskova     | 600                                            |
| Broj diskova                | 4 x 24 x 450GB SAS 15K +<br>4 x 24 x 1 TB SATA |
| Memorija                    | 16GB                                           |
| Podrška za protokole        |                                                |

Tabela 1. Karakteristike storidža primarne lokacije

Planirana je nadogradnju NetApp sistema na primarnoj lokaciji sa još nekoliko funkcionalnosti kojima se poboljšavaju performanse samog sistema i višestruko povećava

otpornost na otkaze. Da bi se potpuno eliminisale pojave poput sporog starta servisa (povećano opterećenje storidž sistema u slučaju istovremenog starta većeg broja virtuelnih mašina) i postigle performanse poredive sa SSD diskovima, predlaže se nadogradnja storidž sistema na primarnoj lokaciji sa dva FlashCache modula od po 512GB flash memorije.

Ove kartice omogućavaju keširanje korisničkih i meta podataka na flash memoriji i mogu redukovati kašnjenje u pristupu podacima i do 10 puta u poređenju sa čitanjem sa diskova. Flash Cache moduli su posebno efektivni kod procesa čitanja nasumičnih setova podataka, kao što su baze podataka.



Slika 15. Keširanje zahteva na NetApp storidžu

NetApp za storidž replikaciju između dva sajta koristi SnapMirror tehnologiju, koja funkcioniše preko TCP/IP. SnapMirror za prenos blokova između storidž-a koristi NetApp Snapshot tehnologiju da bi replicirao samo promenjene blokove, kao i kompresiju čime se

dodatno smanjuje vreme potrebno za replikaciju i bolje koristi link između dve lokacije. SnapMirror podržava tri moguće implementacije replikacije - sinhrona, semi-sinhrona i asinhrona i omogućava da se za različite LUN-ove definišu različiti tipovi i nivoi replikacije.

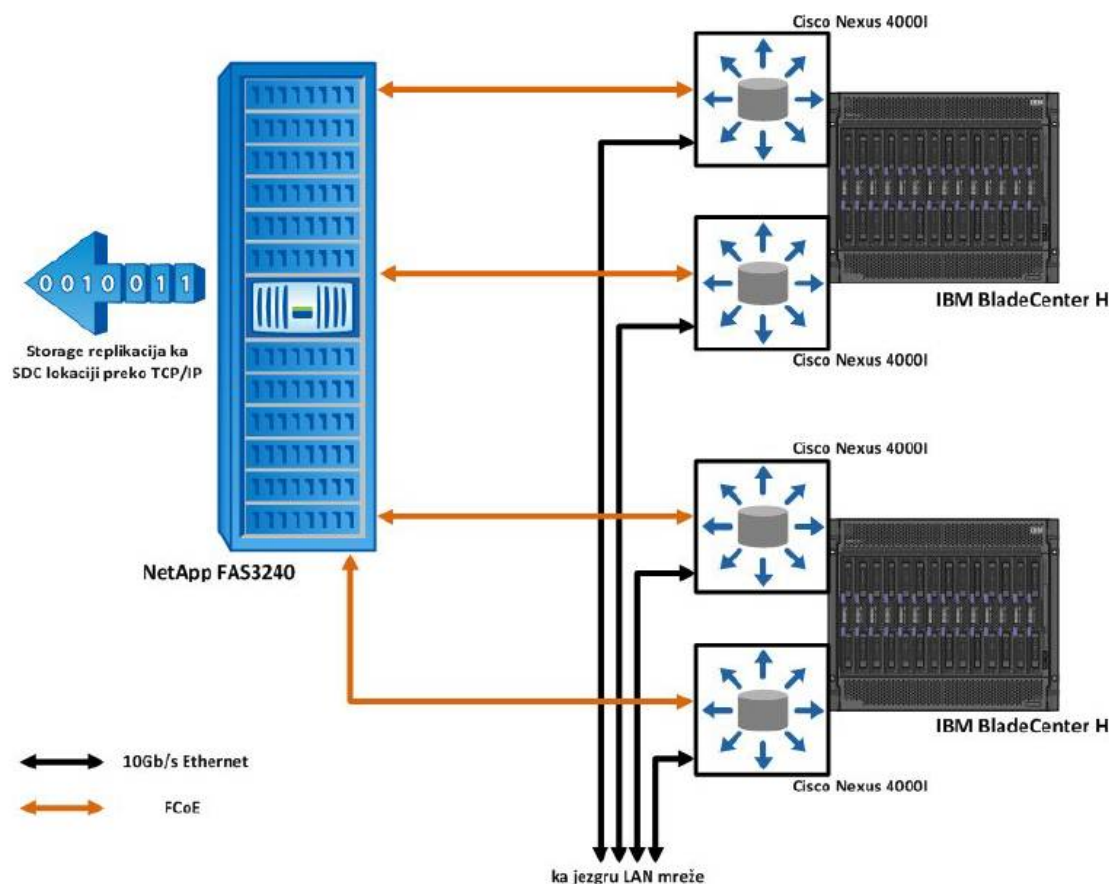
Ne preporučuje se korišćenje sinhronog moda replikacije zato što su benefiti takvog moda replikacije mali, a u zavisnosti od propusnosti linka između lokacija mogući su i problemi u svakodnevnom radu. Takođe, sinhroni mod replikacije ne obezbeđuje konzistentnost podataka na aplikativnom nivou, kako kod NetApp-a tako i kod bilo kog drugog storidž proizvođača. Replikacija između sajtova je asinhrona.

| Otkaz/Događaj              | Metod zaštite                   |
|----------------------------|---------------------------------|
| Otkaz jednog diska         | RAID4, RAID5, RAID6             |
| Otkaz dva diska            | RAID6                           |
| Otkaz napajanja i hlađenja | Redundantne komponente storidža |
| Otkaz storidž procesora    | Redundantne komponente storidža |

Tabela 2. Pregled mogućih vanrednih događaja na NetApp sistemima za skladištenje

#### 6.3.4 Računarsko-telekomunikacioni modul

Rešenje za jezgro SAN mreže na primarnoj lokaciji je Cisco Nexus 4000I blade module. Cisco Nexus 4000I svičevi poseduju 10 Gb Ethernet portove sa podrškom za IEEE Data Center Bridging (DCB) i Fibre Channel over Ethernet (FCoE) tehnologije, preko kojih bi se vršilo povezivanje virtuelizacionih hostova i NetApp storidž sistema (Slika 15), kao i povezivanje virtuelizacionih hostova sa jezgrom LAN mreže.



Slika 16. Arhitektura SAN mreže na primarnoj lokaciji

Dizajn SAN mreže ima za cilj ostvarivanje visoke skalabilnosti, kao i uključivanje novih LAN/SAN tehnologija (10-40 Gb Ethernet, FCoE) koje će dugoročno predstavljati osnovu razvoja datacentar infrastrukture. Rešenje omogućava konsolidaciju serverske LAN i SAN infrastrukture u jezgru primarnog datacentra, rezultujući uštedama na operativnom planu i olakšanom administracijom i održavanju u odnosu na kombinovanu Ethernet i FC SAN infrastrukturu. Kako bi se postigla 10GB/s Ethernet konektivnost ka serverskoj infrastrukturi, za povezivanje uplink-ova Cisco Nexus svičeva potrebno je obezbediti četiri 10GB/s Ethernet porta u jezgru LAN mreže odnosno interkonekciju ka ostatku mreže.

### **6.3.5 Modul neprekidnog napajanja**

U prostoriji datacentra je predviđena instalacija modularnih UPS uređaja Rittal Rimatrix5 (UPS modul 40kW), u konfiguraciji N+1 (N radnih+1 rezervni), sa baterijama koje pokrivaju autonomnost rada od 10 min. Instalacija se sastoji od jednog UPS kabineta i dva baterijska kabineta. Ovo je dovoljno za inicijalnu konfiguraciju datacentra. Planirano je da ovaj modul raste sa dodavanjem nove opreme.

I faza – inicijalna konfiguracija datacentra:

- 1 UPS kabinet sa 4kom x UPS modula od 40kW (3 radna+1 rezervni)
- 2 Baterijska kabineta sa 200 akumulatorskih baterija 28Ah

II faza:

- 1 UPS kabinet sa 5kom x UPS modula od 40kW (4 radna+1 rezervni)
- 2 Baterijska kabineta sa 250 akumulatorskih baterija 28Ah

Realizacija II faze realizacije modula neprekidnog napajanja može otpočeti tek po demontaži postojećeg napojnog kabla, položenog od trafo stanice do razvodnog ormana i montaže novog kabla, većeg preseka (150mm<sup>2</sup>).

### **6.4 Faza 4: Realizacija sekundarne lokacije**

Oprema za sekundarnu lokaciju scBackup je preuzeta iz faze 2. Na sekundarnoj lokaciji nema produkcionog opterećenja već je primarni zadatak oporavak u slučaju “pada” scPrime. Obzirom da nema većih produkcionih potreba nema potrebe ni za adaptacijom prostora kao u slučaju scPrime.

Konektivnost sa scPrime datacentrom je realizovana putem postojeće internet mreže. Brzina interkonekcije je 8Mbps u slučaju kriptovanja saobraćaja ili 10Gbs bez kripto zaštite.

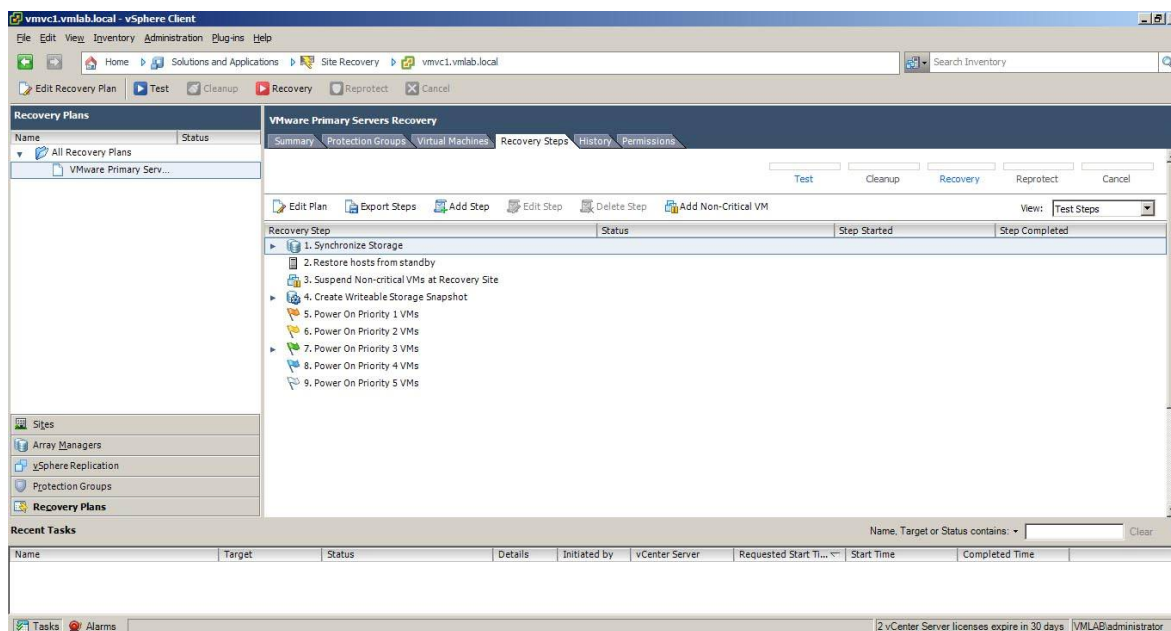
Realizacija ove faze omogućava implementaciju replikacije i instaliranje VMware Site Recovery Manager (SRM). Ova komponenta omogućava:

- Izradu planova zaštite produkcionih servisa na sekundarnoj strani
- Testiranje planova zaštite
- Plansko preseljenje sa primarne lokacije na sekundarnu na zahtev korisnika
- Aktiviranje servisa na sekundarnoj lokaciji u slučaju prekida rada (katastrofe) produkcionog sajta
- Potvrta u prvobitno stanje (“failback”)
- Dokumentovanje svih navedenih aktivnosti
- SRM zahteva uspostavljenje VMware virtuelne infrastrukture na primarnoj i sekundarnoj lokaciji (dve infrastrukture upravljane odvojenim vCenter instancama), storidž infrastrukture i replikaciju izabranih volumena na storidžu.

Plan oporavka servisa se propisuje odgovarajućim dokumentom („DR plan“), koji definiše listu servisa sa prioritetima, međusobnu zavisnost servisa, kao i redosled njihovog aktiviranja. Plan se može testirati sa proizvoljnom učestanošću (više puta mesečno, kvartalno, ...) i svaki test je detaljno dokumentovan, tj. ostaju zapisi o svim izvedenim koracima oporavka servisa i njihovim rezultatima.

Aktiviranje DR plana u slučaju katastrofe se započinje na zahtev administrator sistema i teče potpuno automatski. Korisnik sve svoje produkcione servise može na sekundarnoj strani oporaviti u zadatom vremenu oporavka (obično manje od 4 sata). SRM softver se

licencira po broju servisa koji se štite. Procenjujemo da broj štićenih servisa neće preći 100.



Slika 17. Primer plana oporavka

## 6.5 Bekap rešenje

### 6.5.1 Symantec NetBackup

Kao rešenje za bekap odabran je Symantec NetBackup. Ovo rešenje od svih trenutno dostupnih Enterprise bekap rešenja na tržištu pruža najveći nivo integracije sa VMware infrastrukturom, jednostavno se licencira (tzv. Front End TB licence - prema količini podataka koja se bekapuje) i predstavlja ukupno vodeće rešenje za bekap na tržištu (26% tržišnog učešća). Najveća prednost ovog rešenja u odnosu na druge bekap proizvode je potpuno automatizovan oporavak bekap sistema u slučaju katastrofe.

Upravljanje NetBackup-om se vrši preko NetBackup OpsCenter-a, web interfejsa koji omogućava centralizovano upravljanje, nadzor i izveštavanje za sve NetBackup sisteme i bekap infrastructure. NetBackup poseduje široku podršku i agente za rasprostranjene aplikacije i servise (MS SQL, Exchange, AD, MySQL itd.), kao i napredne bekap/restore funkcionalnosti, među kojima i:

- oporavak SQL baze podataka primenom samo onih transakcija izvršenih pre zadatog vremena,
- on-line bekap Exchange servera uz mogućnost oporavka na nivou baze, poštanskog sandučeta ili pojedinačnih poruka iz bekapa u jednom prolazu,
- granularni oporavak elemenata AD baze sa svim atributima,
- mogućnost upravljanja arhiviranjem na trakama,
- oporavak na „golom“ hardveru - funkcionalnosti sa podrškom za mrežno podizanje sistema i privremenu instalaciju OS-a koje garantuju brzi kompletan oporavak sistema,
- funkcionalnost sintetičkih bekap-a: kreiranja punog („full“) bekapa na osnovu poslednjeg punog bekapa i kasnijih inkrementalnih bekap-a („incremental forever“).

Symantec NetBackup sadrži tesnu integraciju sa VMware vSphere platformom. Korišćenje VMware Changed Block Tracking tehnologije omogućava kreiranje vrlo brzog i prostorno efikasnog bekapa, pošto je nakon inicijalnog bekap-a virtuelne mašine svaki sledeći bekap inkrementalan i tada se bekapuju samo promenjeni blokovi. NetBackup poseduje tzv. inteligentnu polisu za virtuelnu infrastrukturu, koja između ostalog omogućava automatsko otkrivanje i zaštitu virtuelnih mašina, definisanje bekap polisa na osnovu vCenter objekata (foldera, pulova resursa i sl.), kao i balansiranje paralelnih bekap virtuelnih mašina na osnovu trenutnog opterećenja virtuelizacionih hostova. NetBackup nudi i mogućnost granularnog oporavka fajlova sa virtuelnih diskova bez obzira na tip bekapa (puni, diferencijalni i sl.) i bez potrebe za ponovnim kreiranjem diska virtuelne mašine, dok je najavljena i funkcionalnost bekapa virtuelnih mašina u jednom prolazu, koja bi omogućila da se iz bekapa diska virtuelne mašine izvrši oporavak pojedinačnih elemenata podržanih aplikacija (npr. SQL baze, Exchange poštanskih sandučića i sl.).

Virtuelne mašine na kojima se nalaze aplikacije sa transakcionim logovanjem (npr. Exchange, SQL Server) bekapuju se preko NetBackup agenata instaliranih na njima i

tehnologije vStorage API za zaštitu podataka, dok bi se backup ostalih produkcionih virtuelnih mašina vršio samo korišćenjem vStorage API tehnologije. Za testne i razvojne mašine koje je potrebno backupovati ali ne i dugoročnije čuvati i oporavljati posle katastrofe, predlaže se da se backup vrši pomoću VMware Data Recovery alata koji je sastavni deo predloženih VMware licenci.

Predložena arhitektura backup sistema se sastoji od dve nezavisne backup infrastrukture na primarnoj i sekundarnoj lokaciji, koje su međusobno povezane i “svesne” jedna druge na nivou backup sistema. Pored backup podataka na sekundarnoj lokaciji bi se takođe replicirao NetBackup katalog (baza), koji bi se koristio za automatski oporavak celokupnog backup sistema na sekundarnoj lokaciji u slučaju katastrofe.

### **6.5.2 Quantum backup uređaji za backup na diskove**

Kao odredište za backup podataka bili bi korišćeni uređaji za “disk-na-disk-na-traku” (D2D2T) backup Quantum DXi 6702 (po jedan na svakoj lokaciji). Ovi uređaji bi zamenili trake kao medijum za backup. Na sekundarnoj lokaciji bi bila instalirana i biblioteka traka koja bi bila povezana na D2D2T uređaj i koja bi služila za kopiranje podataka radi arhiviranja na nekoj trećoj (udaljenoj) lokaciji.

Quantum DXi uređaji obezbeđuju vrlo visoku propusnu moć backupa (preko 3 TB/h), kompresiju i deduplikaciju sadržaja. Deduplikacijom se volumen ponovljenih backupa smanjuje preko 20 puta (manje od 5%), a skladištenje se vrši na diskovima koji su zaštićeni vezivanjem u RAID 6 grupe. Kapacitet DXi 6702 uređaja za backup na svakoj lokaciji je isti i iznosi 8 TB korisnog prostora, sa mogućnošću proširenja na 80 TB. Uz pretpostavku da je koeficijent deduplikacije oko 20 puta, ukupan volumen backupovanih podataka iznosi preko 1 PB. DXi 6702 na PDC se replicira na isti uređaj na sekundarnu lokaciju preko IP veze.

Replikacija je vrlo efikasna jer se radi posle deduplikacije. Takođe, replikacija podataka (tok podataka) je kriptovana.

## 7. Bezbednost

Bezbednost je od ključnog značaja za svaki datacentar. Iako se bezbednosne polise I uređaji instaliraju kao poslednje faza pre puštanja u rad, svest od bezbednosti mora biti pristutna tokom realizacije svake faze projekta.

Osnovna namena datacenta je skladištenje većih količina podataka na jednoj lokaciji. Logično je da takva lokacija postane meta malicioznog delovanja (napada). Hakeri danas raspolažu mnoštvom alata koji automatizovano kreiraju napade na datacentar infrastrukturu ili pak samo testiraju ranjivosti kako bi se kreirali sofisticirani napadi koje nije lako okriti.

Kada govorimo o bezbednosti datacentara ovo su osnovni pojmovi:

- Pretnje (eng Threats): Događaji koji mogu izazvati štetu nad podacima ili računarsko telekomunikacionom infrastrukturom datacentra,
- Ranjivost (eng Vulnerability): Mane u bezbednostim polisama ili resursima datacentra koje mogu dovesti do ostvarivanja nekih od pretnji,
- Napad (eng Attack): Praktično ostvarenje neke od pretnji.

Neke od pretnji su:

- Distribuirani napad na određeni servis sa ciljem pada njegovih performansi (eng DDoS),
- Odliv poverljivih podataka,
- Krađa ili izmena podataka,

- Neovlašćena upotreba računarskih resursa,
- Krađa identiteta.

Velika većina ranjivosti datacentara su u sledećim oblastima:

- Implementacija: Softverske komponente, nepotpuno testiranje aplikacija i mrežnih protokola,
- Konfiguracija: Nepotpuno konfigurisanje, korišćenje podrazumevanih opcija ili čak lozinki,
- Projektovanje: Loš dizajn bezbednosnih polisa, nepostojanje redundatnosti u sistemu bezbednosti.

Glavni uzroci ovih problema:

- Korišćenje zastarelih softverskih alata,
- Korišćenje default opcija sistema.

Uobičajeni napadi:

- Skeniranje: Aktivnost u kojoj napadač sagledava protokole u upotrebi i javno dostupne portove,
- Distribuirani napad na određeni servis sa ciljem pada njegovih performansi (eng DDoS). Primeri ovog napada su: SYN flood ( TCP ) , Smurf attack (ICMP), Ping of Death (ICMP). Primer alata koji se koriste za distribuirane napade su: Trinoo, Tribe Flood Network (TFN), Stacheldraht.
- Virusi i Crvi: U oba slučaja radi se o malicioznom kodu specifične namene. Razlika je u tome što virusi zahtevaju neki vid interakcije sa korisnikom prilikom razmnožavanja dok crvima interakcija nije potrebna. Neki popularnih crva su: CodeRed, Nidma, SQL Slammer.

## 7.1 Infrastruktura za zaštitu

Osnovna namena ovih uređaja je da spoje dve mreže ali i da kontrolišu saobraćaj između njih. Ovi uređaji se nazivaju zaštitni zidovi ali ne retko se koristi i naziv u originalu Firewall (eng). U daljem tekstu biće korišćen originalni naziv.

Firewall su sofisticirani filteri koji odvajaju određene segmente lokalne mreže i po potrebi povezuju na „spoljni“ sve putem javnih IP adresa. Neki od tipova ovih uređaja su:

- Firewall uređaji za filtriranje paketa,
- Firewall uređaji za proksiranje saobraćaja,
- Firewall uređaji za ispitivanje sesija,
- Hibridni firewall uređaji.

Jedan od komponenti firewall-a (može biti i nezavisni harverski uređaj) je Intrusion prevention system (IDS). Zadatak ove komponente je skeniranje saobraćaja u realnom vremenu i detekcija malicionznih aktivnosti koje se odvijaju. Komponente ovog sistem su:

- Senzori, softverki agenti intalirani na određenim delovima mreže sa zadatkom da analiziraju saobraćaj, optrećenje uređaja i detektuju malicionzne aktivnosti,
- Upravljački modul, skuplja podatke dobijene od senzora i po potrebi alarmira adminstratore. Kompletan konfiguracija sistema se vrši putem ovog modula

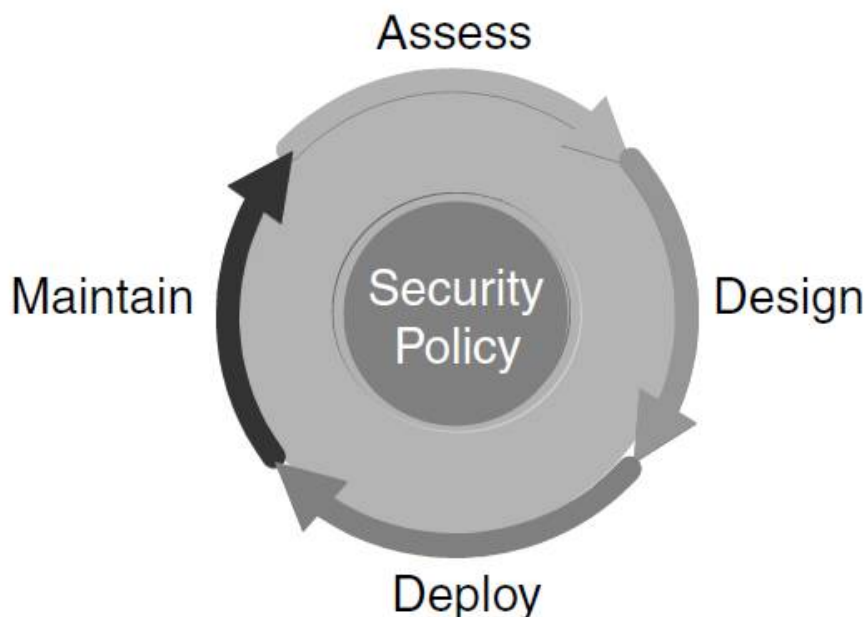
Ukoliko IDS segment detektuje neku malicioznu aktivnost neki od mogućih odgovora su:

- IP session Login, logovanje kompletne sesije sa što više detalja,
- TCP resets, slanje TCP reset paketa ka napadaču u cilju zaustavljanja TCP sesije,
- Blokiranje, IDS može inicirati dinamičko kreiranje polise na ruterima ili svičevima sa ciljem zabrane malicioznog saobraćaja.

Kroz analizu saobraćaja dolazimo do polisa koje treba primeniti na firewall uređaje. Srećom veliki deo analiza je već odrađen od strane bezbednosnih kompanija tako da je na administratorima da prate “dobru praksu” konfigurisanja uređaja koju propisuju njihovi proizvođači.

Dobra praksa je dovoljna za inicijalno podešavanje uređaja. Svaki datacentar ima svoje specifičnosti pa se zato moraju definisati i zasebne polise. Treba napomenuti da su polise “živa” stvar i da zahtevaju redovnu evaluaciju i održavanje. Tipičan životni ciklus polisa je:

- Procena,
- Dizajn,
- Primena,
- Održavanje.



Slika 18. Životni ciklus bezbednosne polise

- Procena (eng. Assessment), proces testiranja i verifikovanja ranjivosti sistema kroz procedure procene rizika,
- Dizajn (eng. Design), proces kreiranja polise i testinje njenog pozitivnog uticaja na novootkrivenu ranjivost,
- Primenna (eng. Deployment), početak primene polise na uređajima,
- Održavanje (eng. Maintenance), proces praćenja saobraćaja i realnog uticaja nove polise na bezbednost datacentra.

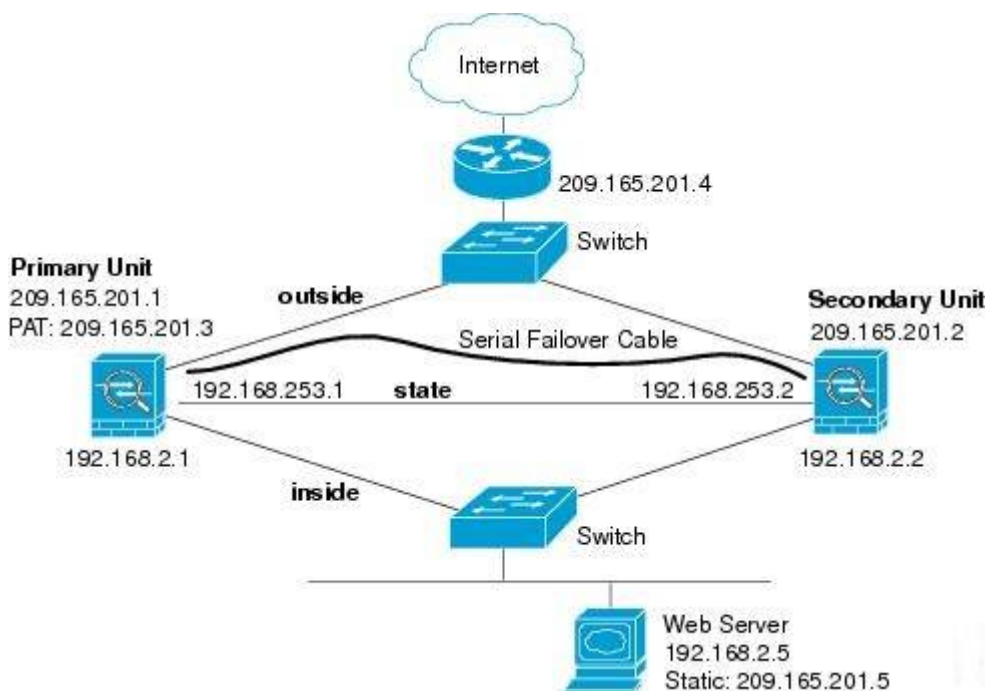
Proces procene i analize rizika (iz kojeg se rađaju nove polise) je izuzetno komplikovan i neretko obilan posao ali u svim većim datacentrima predstavlja dnevni zadatak. U njima postoje posebno obučeni inženjeri čiji je jedini zadatak analiza logova sa raznih uređaja i procena rizika.

## 7.2 Praktična implementacija

Datacentar opisan u ovom radu je obezbeđen putem firewall uređaja CISCO ASA 5525-X. Ovaj uređaj je u stanju da prihvati 30.000 TCP sesija, ukupan protok 2Gbs od tog 600Mbs za IDS. Obzirom da je Internet interkonekcija datacentra oko 1Gbs ovaj uređaj u potpunosti zadovoljava trenutne potrebe.

Firewall se sastoji od dva CISCO 5525-x uređaja koji su povezani u Active-Stand by režimu. Ukoliko primarna ASA prestane sa radom sekundarna ASA preuzima kompletnu konfiguraciju i krajnji korisnici nisu svesni pada primarne ASA-e.

Konfiguracija opreme je podeljena na administatore mrežnih uređaja i administratore server i servisa. Ova organizacija je jako važna jer omogućava primenu takozvanog duplog ključa kod konfiguracije sistema i “objavljivanja” servisa. Nijedan server nema javnu IP adresu već se isključivo koristi NAT/PAT za prevođenje privatnih adresa i portova u javne. Ukoliko se uspostavlja novi server sa servisima koji treba da budu javno dostupni potrebno je da administrator serverske infrastructure instalira server, postavi mrežne kartice u odgovarajuće VLAN-ove tj mreže i dodeli privatne adrese. Potom administrator mrežne infrastructure objavljuje ove privatne adrese tj servise putem NAT/PAT. Gotovo je nemoguće da se neki server ili servis slučajno učini dostupnim na Internetu.



Slika 19. Mrežna arhitektura pri konekciji datacentra na Internet

Sistem dvostrukog ključa je nastao kao rezultat više napada na mrežne i računarske resurse datacentra a koje su krivi sami administratori. U narednim pasusima biće navedeni neki od primera.

Prilikom testiranja jednog od firewall rešenja uočeni su jako slabi rezultati gotovo da zaštita mreže nije postojala. Takođe sve polise su periodične bile brisane, a optrećenje servera u test mreži je raslo. Nakon nekoliko sati pretrage utvrđeno je da je ostavljena podrazumevana šifra za logovanje na firewall uređaj pa malicionzni korisnik nije imao problema sa pristupom.

Stručno usavršavanje administratora je svakako poželjno naročito na polju bezbednosti. Jedan od administratora je pisao rad na temu tkz. Bot mreža. To su mreže koje koriste grupe zaraženih računara za lansiranje distribuiranih napada. Administrator je namerno inficirao jedan server u testnom delu mreže radi pribavljanja logova. Nakon pribavljanja logova administrator je ostavio podignut server i napustio je svoje radno mesto. Sledeći administrator u smeni je primetio ogroman upload i zagušenje linka. Prva pomisao je bio

DdoS napad ali izvor napada je bio server sa interne mreže datacentra dakle sam datacentar je bio napadač. Problem je rešen za 2h ali u tom periodu deo web servisa nije bio vidljiv usled pada uplaod perfomansi Internet konekcije. Ovaj „napad“ bi se teže realizovao u sistemu duplog ključa jer je potrebno i da mrežni administrator zaboravi da isključi NAT-ovanje i da administrator servisa zaboravi da isključi server.

NTP (Network Time Protocol) je u upotrebi još od 1985. Tačno vreme je jako važno za uporednu analizu logova te je UDP port 123 koji ovaj protokol koristiti gotovo uvek otvoren u podrazumevanim konfiguracijama uređaja. Jedan od većih (po kapacitetu) DDoS napada desio se u junu 2014. Napad je koristio upravo ovu ranjivost. Do tada gotovo svi napadi su bili fokusirani na web server i na neki od sajtova koji se hostuju u datacentru. Ovo je bio prvi napad ovog tipa. Obzirom da je port uvek otvoren prošao je sve polise i napad učinio uspešnim. Servisi nisu bili dostupni približno 3h. Nakon ovog napada sve podrazumevane konfiguracije su izmenjene i ova slabost je uklonjena.

Indentičan napad je pokušao oktobra 2014 posle prekida fudbalske utakmice Srbija Albanija. Napada je trajao 8 minuta a servisi delimično (Internet konekcija je bila 75% zauzeta, 25% je bilo dostupno korisnicima) nisu bili dostupni 4 minuta. Ovaj slučaj najbolje odslikava značaj ispravnog konfigurisanja uređaja.

## 8. Zaključak

Datacentri predstavljaju prirodnu evoluciju lokalnih korporativnih mreža. Rastom broja poslovnih procesa koji se automatizuju, korporativne mreže su dobijale sve veći broj servera. Sledeća odluka koju korporativni menadžment mora da donese je da li će uspostavljati sopstvenih datacenter ili će jednostavno zakupiti resurse u skladu sa sopstvenim potrebama. Obe varijante imaju svoje prednosti i mane. Ovaj rad je fokusiran na uspostavu korporativnog datacentra, bez obzira na veličinu kompanije.

Kada se pomene pojam projektovanja datacentara, uvek je prva pomisao na implementaciju velikih kompanija poput Google-a ili Microsoft-a. Ovaj rad predlaže iterativno-inkrementalnu metodu projektovanja i implementacije. Koraci u projektovanju i implementaciji datacentra, predloženi u ovom radu, mogu se primeniti na datacentar bilo koje veličine.

Razvoj infrastrukture treba biti usaglašen sa realnim potrebama kompanije jer je jedino tako isplativ. Nakon adaptiranja lokacije, najskuplja stvar u datacentru je prostor na sistemu za skladištenje. Optimlna popunjenost sistema za skladištenje je između 50% i 75%. Ispod ovog nivoa system se smatra ne isplativim jer hardverska oprema danas brzo tehnološki zastareva i već posle 6 meseci uređaji gube oko 30% inicijlane vrednosti. Popunjenost preko 75% smatra se kritičnom i zahteva hitnu reakciju.

Menadžment neretko nema razumevanja za ove naizgled radikalne poteze. Virtuelizacija na kojoj se zasniva velika većina datacentara danas, je relativno nova tehnologija, naročito za menadžere izvan oblasti informacionih tehnologija. Zato se u ovom radu kao prvi korak navodi dokaz koncepta. Jedan od ciljeva ovog koraka je i praktična demonstracija sa ciljem da se i menadžment uveri u mogućnosti tehnologije koju projekat implementira.

Nadogradnja predloženog modela projektovanja i same implementacije datacentra moguća je u domenu unificiranog pristupa resursima. Tehnologija virtuelizacije omogućava automatizovano kreiranje datacentra za potrebe drugih korisnika nad dodeljenim skupom resursa. VMware-ova implementacija se naziva vCloud Director. Ovaj alat omogućava inventarisanje svih dostupnih resursa i njihovo organizovanje u funkcionalnu celinu. Korisnik može da uspostavi svoj “mali” datacenter samo kliktanjem mišem i sa jako malo tehničkog znanja. Korisnici su najčešće interni(iz iste kompanije), pa se ovakva organizacija i pristup resursima naziva privatni oblak(eng Cloud) .

## 9. Literatura

- [1] Adrian, M. C., Eric, S. C., & Phillip, Z. X. (2014). A Reconfigurable Fabric for Accelerating Large-Scale Datacenter Services. IEEE
- [2] Edmund, B. N, Jeremy, E, & Jinliang, F. (2013). Flat Datacenter Storage. University of Texas at Austin.
- [3] Albert, G., James R, H., & David, A. M. (2009). VL2: A Scalable and Flexible Data Center Network. SIGCOMM'09 Barcelona, Spain.
- [4] Dennis A, Michael R. M., & Philip M.W. (2010). Energy Proportional Datacenter Networks, ISCA'10 , Saint-Malo, France.
- [5] <http://www.eia.gov/>
- [6] Brad N, & Noemi G.(2010). IDC Enterprise Storage white paper,
- [7] Neil R., Implementing Energy Efficient Data Centers, APC(2014)
- [8] Alexander L. & Amin V., A Scalable, Commodity Data Center Network Architecture, SIGCOMM'08 (2008)
- [9] Torben K, & Dennis B. How Data Center Infrastructure Management Software Improves Planning and Cuts Operational Costs, Schneider Electric (2014)
- [10] Kevin N, Data Center Infrastructure Management, SIGCOMM'11 (2011)
- [11] Shesha K. & Shaji A, Intel IT's Data Center Strategy, Intel (2014)
- [12] Suzanne N, & Neil R, Data Center Projects: Growth Model, Schneider Electric (2011)
- [13] Theophilus B. & Aditya A, Network Traffic Characteristics of Data Centers in the Wild, IMC'10 (2010)
- [14] William B The Internet Data Center Build v. Buy Decision, DPI (2014)
- [15] <http://www.datacenterjournal.com>
- [16] Ram K. Behavioral Security threat Detection Strategies for Data Center switches and Routers, Brocade Communications (2014)

## 10. Spisak Slika

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Slika 1 Šema datacentra „Grizinkaln“ Riga, Letonija.....                       | 10 |
| Slika 2 Postrojenje za hlađenje vode. Datacentar Daglas.....                   | 11 |
| Slika 3 Serverska soba. Datacentar Council Bluffs .....                        | 13 |
| Slika 4 Microsoft modul IT PACK.....                                           | 13 |
| Slika 5 Šema Microsoft datacentara.....                                        | 15 |
| Slika 6 Blade sistem servera.....                                              | 19 |
| Slika 7 Sistem za skladištenje podataka.....                                   | 20 |
| Slika 8 Predlog dizajna datacentra mreže kompanije CISCO.....                  | 21 |
| Slika 9 Primer šeme napajanja datacentra.....                                  | 22 |
| Slika 10 Grather magični kvadranti na polju virtuelizacije.....                | 25 |
| Slika 11 Arhitektura VMware sistema za upravljanje virtuelnim okruženjem.....  | 34 |
| Slika 12 VMware Arhitektura sistema za oporavak od katastrofa.....             | 36 |
| Slika 13 Šema adaptacije lokacije za potrebe primarnog datacentra scPrime..... | 41 |
| Slika 14 Uporedni prikaz RAID konfiguracija.....                               | 43 |
| Slika 15 . Keširanje zahteva na NetApp storidžu.....                           | 44 |
| Slika 16 Arhitektura SAN mreže na primarnoj lokaciji.....                      | 46 |
| Slika 17 Primer plana oporavka.....                                            | 49 |
| Slika 18 Životni ciklus bezbednosne polise.....                                | 56 |
| Slika 19 Mrežna arhitektura pri konekciji datacentra na Internet.....          | 58 |