

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

STUDIJSKI PROGRAM

SAVREMENE INFORMACIONE TEHNOLOGIJE

**Implementacija Storage Area Network i VMware vSphere ESXi
u savremenim datacentrima
- MASTER RAD -**

Mentor:

prof. dr Mladen Veinović

Kandidat:

Filip Lukić

2012/410453

Beograd, 2014.

Sažetak

Uređaji za skladištenje podataka se smatraju temeljom na kome počiva čitav informacijski sistem i kao takvi moraju da prate ciljeve i poslovne modele ozbiljnih kompanija. U okruženjima gdje se radi sa velikim količinama podataka i gdje je njihova pouzdanost i brzina dostupnosti više nego neophodna, postavljanje samo više brzih uređaja nije dovoljno. Potrebne su nove tehnologije koje nam mogu omogućiti veću dostupnost mreže, dostupnost podataka i iskorištenost sistema, dosadašnje tehnologije nam to nisu omogućavale. SAN može uspješno da ispuni ovaj izazov.

SAN koncept za skladištenje podataka nudi mogućnost povezivanja jednog storidza sa više servera i sve to uz visoke performanse dostupnosti. Vezuje se sa serverima preko interne mreže koja ima visoku propusnu moć, može da podrži prenos velike količine podataka. Drugim riječima skladišteni prostor je izmješten i distribuira se kroz čitavu mrežu. SAN omogućava centralizaciju skladištenih uređaja i klaster servera, čime se omogućava lakša i jeftinija administracija. Ideja je da se stvori inteligentna SAN infrastruktura koja će zadovoljiti potrebe visoke dostupnosti i heterogenog pristupa informacijama. Mnoge vodeće IT kompanije kao što su: Microsoft, VMware, Cisco, IBM, uspješno razvijaju ovaj koncept skladištenja podataka preko mreže i integrišu ga u svoje proizvode. Ja ću se u ovom radu bazirati na VMware i IBM proizvode i pokušaću da objasnim kako se SAN konfiguriše na VMware ESX/ESXi.

Abstract

Data storage devices are considered to be the foundation on which rests the whole information system and as such as must follow the goals and business models serious companies. In environments where working with a large amount of data and where their reliability and speed of access to more than necessary, setting a more rapid device is not enough. Needed are new technologies that we can provide greater network availability, access data and system utilization, the technology we are not enabled. SAN can successfully meet this challenge.

SAN storage concept offers the possibility of connecting any storage with multiple servers and all with high-performance access. Is linked to the server from the internal network that has high bandwidth, can support the transmission of large amounts of data. In other words, storage space is relocated and is distributed throughout the network. SAN provides centralized device and stored cluster server, which makes it easier and cheaper administration. The idea is to create an intelligent SAN infrastructure that will meet the needs of high availability and heterogeneous access to information. Many leading IT companies such as Microsoft, VMware, Cisco, IBM, successfully developed the concept of data storage over the network and integrate it into your product. I'll be in the paper based on VMware and IBM products and try to explain how to configure the SAN to VMware ESX / ESXi.

Sadržaj

1	Uvod	7
1.1	Predmet istraživanja	7
1.2	Značaj	7
1.3	Cilj	8
1.4	Hipoteza	8
2	Mreža	12
2.1	Pojam mreže	12
2.2	Modeli interkonekcije	12
3	Skladišteni prostor - Storage	14
3.1	Osnove storage	14
3.2	Tehnologije za skladištenje podataka na serverima	20
3.2.1	Direktno povezani skladišteni prostor	20
3.2.2	Skladišni prostor povezan u mreže	21
3.2.3	SAN	22
4	Storage Area Network	22
4.1	Optički povezane SAN mreže	23
4.2	iSCSI SAN mreže	24
4.3	Fibre Channel protocol	25
4.4	Fibre Channel Addressing	26
4.5	World Wide Names	27
4.6	Fibre Channel servisi	27
4.7	Bezbednost Fibre Channel u Storage Area Network	29
5	Implementacija SAN pomoću VMware ESX/ESXi	30
5.1	Razumijevanje virtualizacije	31
5.1.1	Virtualizacija skladištenog prostora	34
6	Korištenje ESX/ESXi u Fibre Channel SAN	36
6.1	Storage area network u VMware	36
6.1.1	Multipathing i Path Failover	37
6.1.2	Prednosti koje pružaju SAN i ESX/ESXi	37
6.1.3	Migriranje virtuelne mašine u toku rada	38

6.2	Razumijevanje VMFS	39
6.3	Kako Virtuelna Mašina pristupa podacima na SAN-u	40
6.4	Redudanta na nivou hosta u ESX/ESXi klasteru	41
6.5	Konfiguracija LUN u ESX/ESXi.....	43
6.6	Kreiranje novog poola i mapiranje hosta.....	43
6.6.1	Kreiranje Pool	45
6.6.2	Mapiranje kreiranog Pool.....	46
6.7	Dodavanje Volumena od strane ESX/ESXi u klaster	46
7	SAN Storage Backup faktori	48
8	Zaključak	50
9	LITERATURA	52

Slike

Slika 1	Uporedne karakteristike virtuelnih softvera	10
Slika 2	Prikaz nivoa OSI i TCP-IP modela	13
Slika 3	Primjer ručnog kopiranja podataka	14
Slika 4	Primjer RAID 0.....	15
Slika 5	Primjer RAID 1 diskova	16
Slika 6	Primjer RAID 3.....	17
Slika 7	Primjer RAID 5.....	17
Slika 8	Primjer RAID 10.....	18
Slika 9	Primjer RAID 53.....	18
Slika 10	Primjer RAID 0+1.....	19
Slika 11	Mreža samo sa DAS rešenjem.....	21
Slika 12	Primjer povezivanja NAS uređaja sa mrežom.....	21
Slika 13	Prikaz jednostavne skladišne mreže (SAN – storage-area network).....	23
Slika 14	Virtualizovana VMware IT struktura	30
Slika 15	Virtualizacija u odnosu na tradicionalne servere	32
Slika 16	Prikaz virtuelnog SAN kontrolera	35
Slika 17	Prikaz storage monitoringa u vSphere web client	37
Slika 18	Prikaz kontrol panela za migriranje mašina.....	38
Slika 19	Prikaz ping-a web servera u toku migracije	39
Slika 20	Dijeljenje VMFS na više hostova	40
Slika 21	Primer dodavanja VMFS diska hostu.....	41
Slika 22	Prikaz redudante na nivou Hosta	42
Slika 23	Failover kod FC.....	43

Slika 24 Web interfejs storwize IBM V3700	44
Slika 25 Storidž sistem i MDisk	45
Slika 26 Mapiranje <i>Volume</i> na jednom od hostova	46
Slika 27 Dodavanje <i>Volume</i> na jednom od servera	47
Slika 28 Data Protect grafički prikaz.....	49

Tabele

Tabela 1 Fibre Channel Address struktura	26
Tabela 2 Portovi is servisi koji prolaze kroz <i>fabric</i>	28

1 Uvod

1.1 Predmet istraživanja

Ovaj rad ima za zadatak da bliže pojasni kako se skladište podaci u skladištenom prostoru (storage) i koje su to tehnologije koje se najčešće koriste za skladištenje podataka. Poseban osvrt u radu dat je Storage Area Network (SAN) skladištenom prostoru, kako funkcionuje, čemu služi, koje su njene mogućnosti (prednosti i mane), šta su novo donijele u odnosu na druge tehnologije za skladištenje podataka, koja je razlika između SAN (Storage Area Network) i drugih tehnologija za skladištenje podataka kao što su DAS i NAS *storage*.

U drugom dijelu rada je naveden primjer konfigurisanja u VMware ESXi koji se koristiti za konfigurisanje Fibre Channel SAN. U ovom istraživanju sam pokušao da ukažem na prednosti i mane koje nudi ovo rešenje. Virtualizacija svakim danom nalazi sve veću primjenu u informacionim tehnologijama, tako se i virtualizacija proširila sa virtuelnih mašina i servera na skladištenje podataka. Virtualizacija nam omogućava da maksimalno iskoristimo skladišteni prostor, u ovom radu ćemo pokazati kako se to može uraditi uz pomoć SAN i ESXi. VMware ESX/ESXi operativni sistem je kaorišćen da se pokaze kako se fizički serveri (Host) mogu povezati u isti *cluster* i kao takvi mogu funkcionisati kao jedan server, takođe je pokazano kao se povezuje SAN preko FC sa istim *cluster-om*. Dobijeni *cluster* funkcioniše kao jedna cjelina ili kao jedan veliki server na kome se nalazi veliki broj vrtuelnih mašina čija administracija i održavanje postaje jednostavnija. Istrživanjem su obuhvaćena i backup rešenja cistavog sistema i brzina oporavka ukoliko dođe do greške na sistemu.

1.2 Značaj

Značaj ovog istraživanja je da se prikaže kako je moguće praktično primjeniti *Storage Area Network* na realne *data* centre, nudi se predlog efikasnog uređenja malih i serednjih *data* centara. Prikazuje značaj novog načina povezivanja skladištenog prostora sa serverima.

Društveni značaj je u tome što korištenjem ovih tehnologija se povećava efikasnost rada vašeg *data* centra, od štednje električne energije do poboljšanja iskorištenja i dostupnosti resursa na kvalitetan način. Administracija u data-centru se značajno pojednostavljuje i automatizuje, što daje mogućnost smanjenja broja zaposlenih u IT sektoru. Mogućnost lakog testiranja je jedna veoma bitna stvar koja takođe u mnogome olakšava posao zaposlenim u IT sektoru.

1.3 Cilj

Cilj ovog istraživanja je sagledavanje problema uređenja skladištenja podataka i njegovo rešavanje na kvalitetan i dugoročan način. Ponuđeno rešenje nema ograničenja nadgradnje na broj jedinica skladištenog prostora i na udaljenost servera od skladištenog prostora, sto pomera granice mogućnosti u odnosu na dosadašnje skladištene prostore koje smo imali.

Društveni cilj je prikaz rešavanja problema na komercijalnim proizvodima koji imaju jako široku primenu kako u velikim i sredinjim *data* centrima, tako i u individualnim primjerima korištenja softvera za virtualizaciju.

1.4 Hipoteza

Sa sve većim razvojem informacionih tehnologija i oslanjanjem kako velikih organizacija tako i običnog čovjeka na računar i internet, potreba za skladištenjem podataka postala je sve veća i složenija. Bezbjedno skladištenje podataka danas postaje jako složen i zahtjevan posao. Posebno u vrijeme kada se teži da se sva administracija prevede u digitalan oblik, samim tim povećava se i osjetljivost podataka koji se koriste. Porastom obima i količine podataka javila se potreba za pronalaženjem kvalitetnijih rešenja za skladištenje podataka.

Ovaj rad ima za zadatak da pokaže kako se može unaprijediti čuvanje i dostupnost podataka u *data*-centrima korištenjem novih tehnologija kroz teorijski i praktičan primjer. Rad u svom prvom dijelu ukazuje objašnjenje pojmova koje je neophodno znati prije nego što se započne sa implementacijom ovog sistema. U drugom dijelu se pokazuje kako se na praktičan način uz pomoć VMware EXS/EXSi i Storage Area Network može napraviti moderan i moćan *data*-centar gdje je održavanje i administracija u mnogome automatizovana i pojednostavljena.

Tehnologije kao što su Storage Area Network(SAN), adapter magistrale računara (HBA-host bus adapter) i broj logičke jedinice (LUN – logical unit number) nekada su bili termini koji su se ticali isključivo profesionalaca koji se su bavili isključivo skladištenjem podataka. Poznavanje ovih tehnologija je bilo prilično daleko od potreba prosječnog Windows administratora. Međutim, napredovanjem tehnologije dolaskom novih tehnologija kao što su Windows servisi virtuelnih diskova (Virtual Disk service) i iSCSI, došao je i SAN i donio sa sobom razne benefite na u pogledu skladištenja podataka.

Danas da bi postali uspješan IT administrator u malim i srednjim *data*-centrima, morate dobro poznavati tehnologije skladištenja podataka. Pored osnovnih pojmova koje morate poznavati da bi konfigurisali skladišteni prostor, kao što su RAID nivoi, neophodno je da znate kako se koriste i konfiguriraju tehnologije kao što su DAS, NAS, SAN.

Prvi dio rada ima za zadatak da bliže pojašni pojam SAN mreža počev od osnovnih pojmova i da kaže šta su SAN mreže, koje su njene mogućnosti (prednosti i mane), šta je to novo što one donose i kako se mogu upotrijebiti u realnim uslovima.

U **drugom dijelu rada** je opisan proces integrisanja i konfigurisanja FC SAN sa ESX/ESXi u data-centar. Ideja je da se pokaže kako se storidž može pvezati sa serverima preko interne super brze mreže. Iako se nalazi na mreži i nije direktno povezan na serveru on može imati vrhunske performanse, iskorišćenost, dostupnost, pouzdanost i lako i jednostavno proširenje. Za primer implementacije ja sam koristio VMware ESX/ESXi, pokušao sam da opišem i druge funkcije koje ovaj VMware proizvod nudi.

Microsoft i Citrix imaju slične proizvode, koji takođe imaju dobre performanse. Microsoft sa svojom poslednjom verzijom Hyper-v nudi izuzetno dobre performanse, koje su značajno unaprijeđene u poslednjim verzijama. VMware i Hyper-v su skoro izjednačeni po pitanju performansi, ono o čemu treba voditi računa kada se radi o odabiru između ova dva proizvoda jesu licence. Kada je u pitanju *data*-centar sa više fizičkih servera i sa više CPU morate strogo voditi računa o licencama, jer se plaća licenca za svaki host posebno i za svaki CPU. Takođe licence važe i za mrežne adaptere i kontrolere zavisno od njihove podržane brzine. Postoje proizvodi kao što su XEN kompanije Citrix koji je besplatan i to ga čini konkurentim i interesantnim za mnoge IT administratore. Veoma je važno voditi računa o kompatibilnosti proizvoda sa proizvođačima IT opreme, Microsoft i VMware su kompatibilni sa većinom proizvođača IT opreme.

Pored kompanije IBM koja zajedno sa VMware prednjače u razvoju virtualizacije informacionih tehnologija, VMware takođe odlično sarađuje i sa Cisco-m, i pored toga što se čini da izgledaju kao najveći konkurenti, oni su zajedno uspjeli da razviju mrežni kontroler koji može da propusti dvjesto fizički različitih mreža kroz jedan adapter. Na slici 1 su prikazane uporedne karakteristike pomenutih proizvoda.

Karakteristike	VMware vSphere sa vCenter-om	Windows Server 2008 R2 sa Hyper-V sa SCVMM R2	Citrix XenServer sa Essentials Enterprise
Migracija virtulene mašine bez njenog isključenja tkz. "živa" migracija	✓	✓	✓
Oblik održavanja virtulene mašine tkz. "patching" servers bez njenog isključenja	✓	✗ Samo 1 "živa" migracija po hostu je moguća	✗ Samo 1 "živa" migracija po hostu je moguća)
Režim za održavanje sa dinamičkom raspodelom opterećenja	✓	✓	✓
"Živa" migracija grupe za skladištenje tkz. storidža	✓	✗	✗
Podrška za "Živu" migraciju sa jednog mrežnog protokola na drugi npr sa iSCSI na NFS ili Fibre channel i obrnuto	✓	✗	✗
(Konverzija iz jedne veličine do veličine diskova obezbeđenih u toku "žive" migracije grupe za skladištenje tkz. storidža)	✓	✗	✗

Slika 1 Uporedne karakteristike virtuelnih softvera

Neke od mogućnosti koje pružaju ESX/ESXi i SAN:

- Migracija virtulene mašine bez njenog isključenja je tkz. "živa" migracija
- Vise fizickih servera na kojem rade virtelne mašine je tkz. „Host“(Domacin)
- Režim za održavanje sa dinamičkom raspodelom opterećenja po „Hostovima“
- Migracija virtulene mašine sa jedne grupe za skladištenje (tkz.storidž grupa) na drugu bez njenog isključenja je tkz. **"Živa" migracija grupe za skladištenje**

ESX/ESXi zajedno sa FC SAN pruža visoke performase i udobnost korištenja sto ćete imati prilike da vidite u ovom radu. Takođe ESX/ESXi može fukcionisati i kada se koriste druge komponente, npr. ako finansije igraju značajunu ulogu u realizaciji projekta jako dobro

resenje mogu biti HBA SAS kontroleri gdje bi se serveri spajali direkno sa storidzom SAS kablovima.

2 Mreža

2.1 Pojam mreže

Računarske mreže, ili samo mreže kako ih često nazivamo, su skup računara i uređaja povezanih komunikacionim kanalima. Ovi kanali omogućavaju dijeljenje resursa, servisa, informacija u okviru njih. Iako se ova definicija može doživjeti kao jednostavna, razumijevanje načina na koji mreža radi može biti veoma konfuzno i komplikovano za ljude koji se ne bave informacionim tehnologijama (IT) ili za ljude koji tek kreću da se bave sa njima. Zato ću prvo pokušati da objasnim osnovne pojmove umrežavanja.

Da bi se izvršila uspješna komunikacija u bilo kom obliku, potreban nam je niz različitih pravila kako bi ta komunikacija bila uspješna. Za komunikaciju između ljudi kao jedan od osnovnih vidova za komunikaciju među ljudima zadužen je govor. Da bi se ispunio jedan od preduslova kako bi ljudi mogli da se sporazumiju potrebno je da imaju zajednički jezik. Kad dva čovjeka razgovaraju, oni ostvaruju komunikaciju preko jezika, ako govore istim jezikom mogu biti sigurni da sve što saopše jedan drugome mogu razumjeti. Da bi nesmetano komunicirali sa ljudima, mi koristimo jezik kao komunikacioni protokol, i zvuci i pisanje su komunikacioni medij.

Slično tome i računarska mreža treba skoro iste komponente kao naš ljudski primer, ali razlika je u tome što svi faktori moraju biti ispunjeni na neki način da se obezbedi efikasna komunikacije. Ovo se postiže upotrebom industrijskih standarda ili modela pomoću kojih se odvija komunikacija, i kompanije se pridržavaju tih standarda kako bi se osiguralo da se komunikacija odvija nesmetano ukoliko se koriste proizvodi različitih proizvođača.

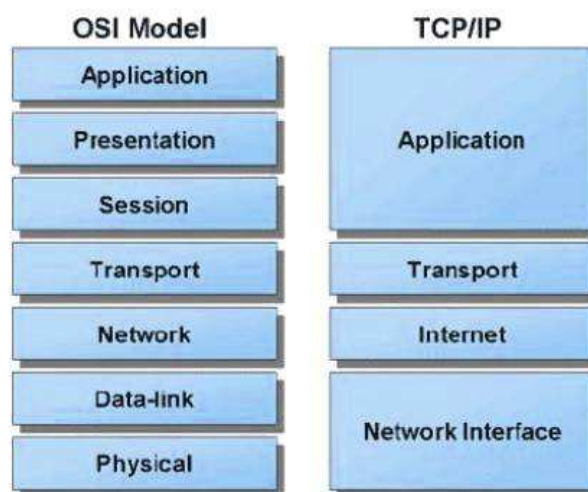
2.2 Modeli interkonekcije

Da bi komunikacija između dva korisnika bila uspješna, svaka informacija mora da prođe kroz standardizovane modele interkonekcije kako na jednoj tako i na drugoj strani. Najčešći standardi koji se koriste za povezivanje izvora i odredišta kod računarskih mreža, su otvoreni sistem interkonekcije modela (OSI¹), Ministarstvo odbrane (DoD), TCP / IP, i Fibre Channel. Svaki model ima svoje prednosti i mane, oni se primjenjuju zavisno od potreba sistema, gde ima maksimalnu korist u pogledu performansi, pouzdanosti, dostupnosti, trošk-korist, itd...

¹ http://en.wikipedia.org/wiki/OSI_model

Najviše primjenjivani model je TCP/IP model, ovaj model nije standardizovan od strane institucija za standardizaciju ali zbog svoje široke primjene postao je *de facto* standard. Nastanak TCP/IP modela je išao obrnutim redosledom od nastanka OSI modela, prvo su napravljeni protokoli, a model je u stvari bio opis postojećih protokola. TCP/IP skup protokola koji omogućava računarima različitih proizvođača koji rade pod različitim operativnim sistemima da međusobno komuniciraju. Razvila ga je 1960. godine DARPA² (Defense Advanced Research Project Agency) za mrežu za komuniciranje paketa. Kasnije je uključen Berkeley Software Distribution of UNIX. Od 1990. godine je način za povezivanje računara.

Na slici 3-1 su predstavljeni OSI Model i TCP/IP model a



Slika 2 Prikaz nivoa OSI i TCP-IP modela

² <http://en.wikipedia.org/wiki/DARPA>

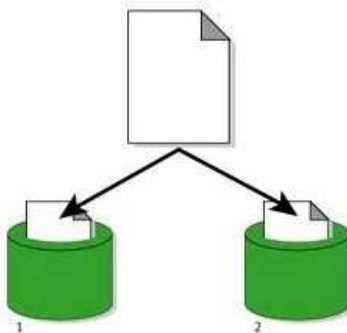
3 Skladišteni prostor - Storage

3.1 Osnove storage

Svi znamo da skladišteni prostor (*Storage*) koristimo da za skladištenje podataka u informacionim sistemima. *Storage* je sačinjen od hard diskova (HDD) na kojima se čuvaju podaci. Da bi razumjeli šta je *skladišteni prostor* i kako on funkcioniše, počecemo od *hard disk drive* (HDD). Zatim ćemo objasniti *storage* sisteme visokih performansi, otpornost na greške, visoka dostupnost, itd...

U zavisnosti od metoda korišćenja i tehnologije HDD postoje brži i sporiji diskovi. Evolucija HDD-a se razvija nevjerovatnom brzinom, sada možete uskladišti stotine gigabajta na jednom HDD, što nam omogućava da sve podatke koje smo ikada imali možemo sačuvati na jednom disku. Iako se čini da nam je ovaj pristup donosio samo prednosti do sada, postavimo sebi samo jedno pitanje šta će se desiti ako iz bilo kog razloga nismo u mogućnosti da pristupimo HDD na kom su nam važni podaci?

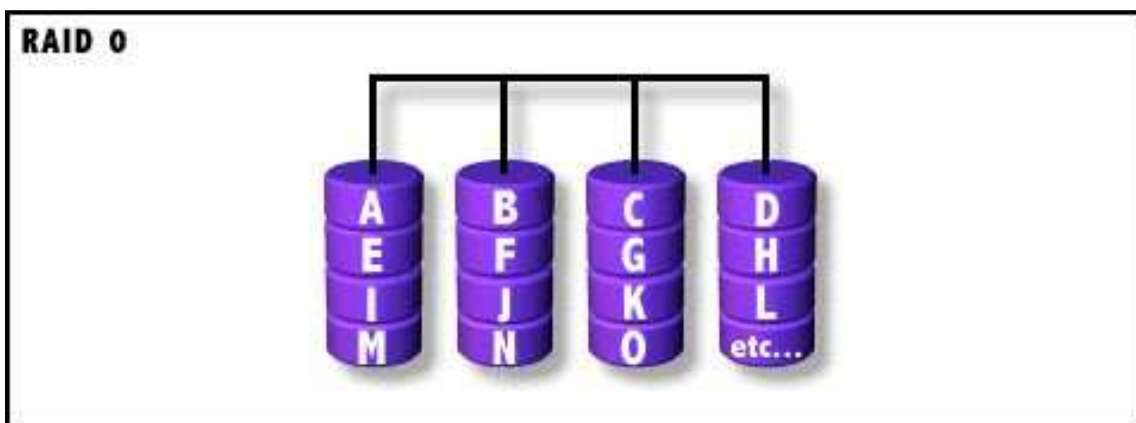
Da bi izbjegli ove neželjene posledice i probleme sa čuvanjem važnih informacijama, najsigurnije je da te informacije imamo na još nekom mjestu, kako bi bili sigurni da ako iz nekog razloga ne možemo pristupiti disku imamo alternativu. Jedno rešenje može biti sekundarni hard disk, gdje ručno možemo da iskopiramo naš primarni HDD na drugi (sekundarni) HDD kao što pokazuje slika 3. Kad napravimo ovu kopiju imaćemo utisak da će naši podaci biti bezbjedniji. Međutim koliko često treba da vodimo računa o tim kopijama, da svakodnevno vršimo dopune na sekundarnom disku. To nam predstavlja svakodnevno opterećenje i obavezu, da moramo kopirati i najmanju promjenu na oba diska da bi nam podaci bili osigurani.



Slika 3 Primjer ručnog kopiranja podataka

Rešenje ovog problema možemo naći u *Redundant Array of Independent Disks*³ (RAID) konceptu. Jasno nam je da je potrebno vršiti rezervnu kopiju svaki put kada se naprave promjene na disku, da bi informacije bile bezbjedne. I takođe nam je jasno da je to nemoguće ručno uraditi na pravi način, zato ćemo iskoristiti mogućnosti *RAID-ova* da sav taj proces sigurnosnog kopiranja on uradi za nas. Kako bi razumjeli kako treba podesiti diskove da backup može da se vrši automatski. *RAID controller* može vršiti održavanje sinhronizaciju i upravljanje svim upisima i čitanjima (input/output (I/O)) na diskovima u storidžu.

RAID 0 je takozvani *striped* režim rada za koji je potrebno najmanje dva diska. Podtaci se „cepaju” na delove (blokove) koji se snimaju na odvojene diskove. Na taj način se drastično ubrzava rad sa podacima, kako kod čitanja tako i kod upisa. Brzina rada je približno onoliko puta veća koliko diskova koristite. Naravno, što više diskova ima na jednom kontroleru, toliko i on ima više posla, pa zato ne možemo da govorimo o ubrzanju od tačno dva, tri ili četiri puta. Raspoloživ prostor predstavlja zbir veličine svih diskova povezanih u RAID. Ovaj nivo RAID-a se ne svrstava u „pravi” RAID zato što ne poseduje kontrolu grešaka, što mu je i glavni nedostatak. Zbog toga, otkazivanje jednog od diskova dovodi do gubitka svih podataka, a verovatnoća da se tako nešto desi je veća samim tim što je u upotrebi više diskova. Zato se RAID 0 ne koristi u uslovima u kojima je bitan integritet podataka, već samo tamo gde postoji potreba za velikim prostorom i brzinom.



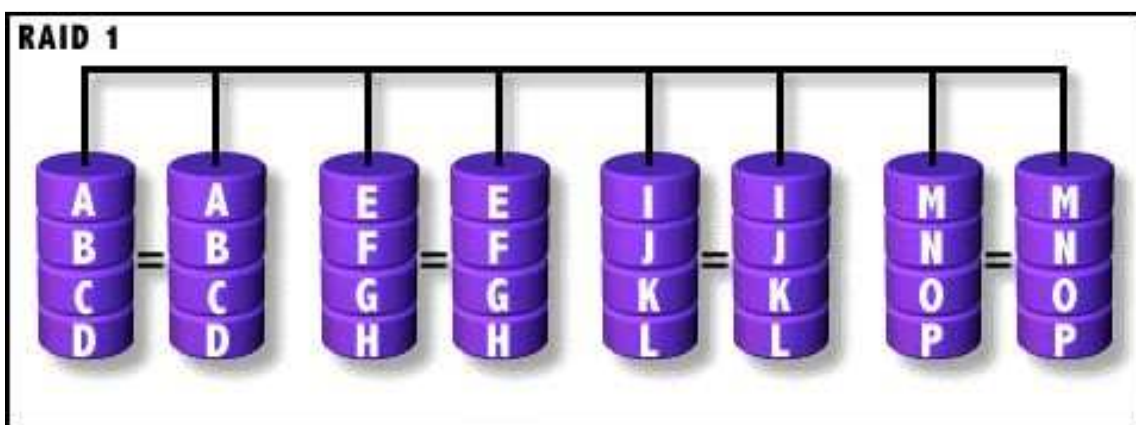
Slika 4 Primjer RAID 0

RAID 1 je tzv. *mirroring* i zahtijeva najmanje dva diska. Svaki disk ima svoje „ogledalo” na kom se presnimavaju svi podaci. Iz toga je jasno da je veličina prostora na dva diska, je u stvari, veličina jednog diska, a brzina snimanja je jednaka brzini upisa na dva disk. Kod čitanja se međutim postiže duplo veća brzina jer se podaci (odnosno njihovi delovi) istovremeno čitaju sa oba diska. Iako ovo na prvi pogled deluje neefikasno, ipak je jasno da je RAID-a 1 primena

³ <http://en.wikipedia.org/wiki/RAID>

u sredinama gde su podaci izuzetno važni jer u trenutku otkazivanja jednog hard diska postoji identična kopija podataka na drugom disku.

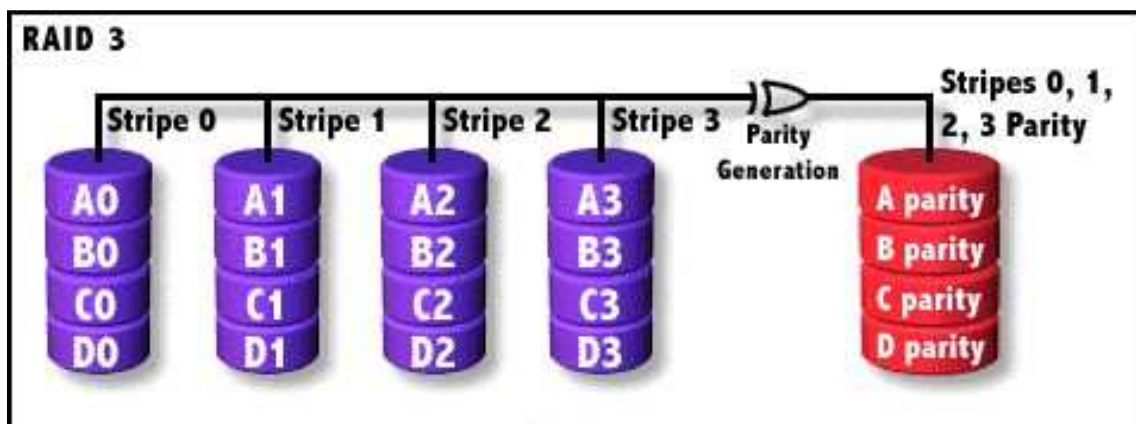
RAID 2 je jedan od nivoa RAID-a koji je ostao u domenu teorije. Podaci se dele po bitovima i zapisuju se na posebne diskove, ali se za svaki podatak izračunava i tzv. Hamingov kôd za korekciju grešaka koji se i sam deli na više diskova. Na taj način su moguće velike brzine čitanja i pisanja, a zahvaljujući kôdu, greške se „u letu” otkrivaju i ispravljaju. Za efikasan rad neophodna je i sinhronizacija diskova. Ovaj nivo RAID-a je izuzetno otporan na često javljanje grešaka i otkazivanje diskova, ali pošto se to kod savremenih diskova ne dešava često, zbog prevelike cene implementacije ovaj RAID ne nalazi praktičnu primenu u realnim uslovima.



Slika 5 Primjer RAID 1 diskova

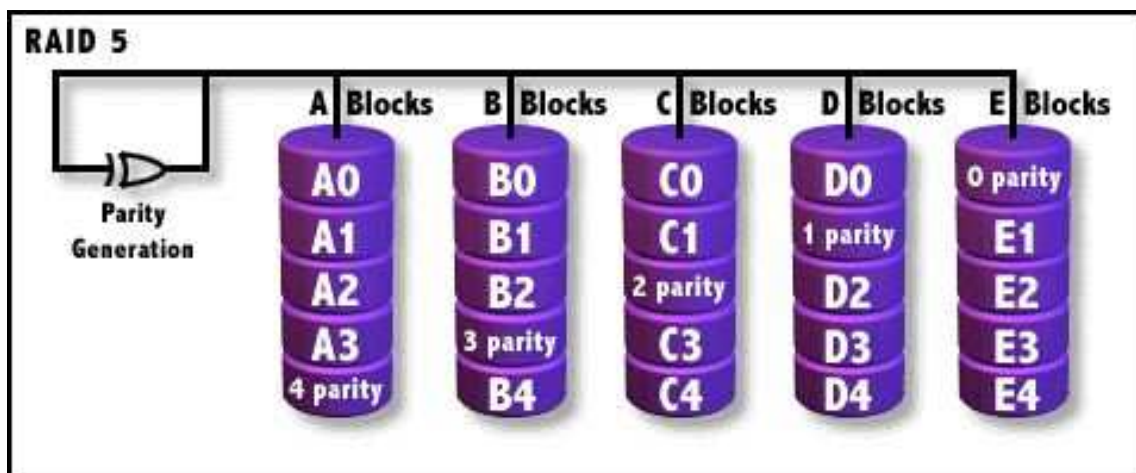
RAID 3 je sličan **RAID-u 2**, ali za razliku od njega ima mnogo češću primjenu u praksi. Za realizaciju RAID-a 3 potrebna su najmanje tri hard diska. Podaci se dijele i snimaju na odvojene diskove, ali se pri tom i izračunava parnost (parity) tih djelova koja se snima na poseban disk. Zbog toga se postižu velike brzine pisanja i čitanja, kao i detekcija i ispravljanje grešaka. Slobodan prostor predstavlja zbir veličina diskova na koje se snimaju podaci (bez diska za snimanje parnosti). RAID 3 je otporan na otkazivanje jednog od diskova, pri čemu se podaci rekonstruišu na osnovu parnosti i podataka sa ostalih, ispravnih diskova. Nedostatak je što kod istovremenog pristupa više korisnika usko grlo predstavlja disk na kojem je *parity*.

RAID 4 je veoma sličan **RAID-u 3** i zahteva isti broj diskova. Razlika je u tome što se podaci dijele na blokove koji se zapisuju na odvojene diskove, a njihova parnost se zapisuje na poseban disk. Usko grlo je i ovde disk na kojem je parnost, a RAID 4 je spor i pri upisu i prilično neefikasan kod obnove oštećenih podataka, tako da se u praksi jako rijetko koristi.



Slika 6 Primjer RAID 3

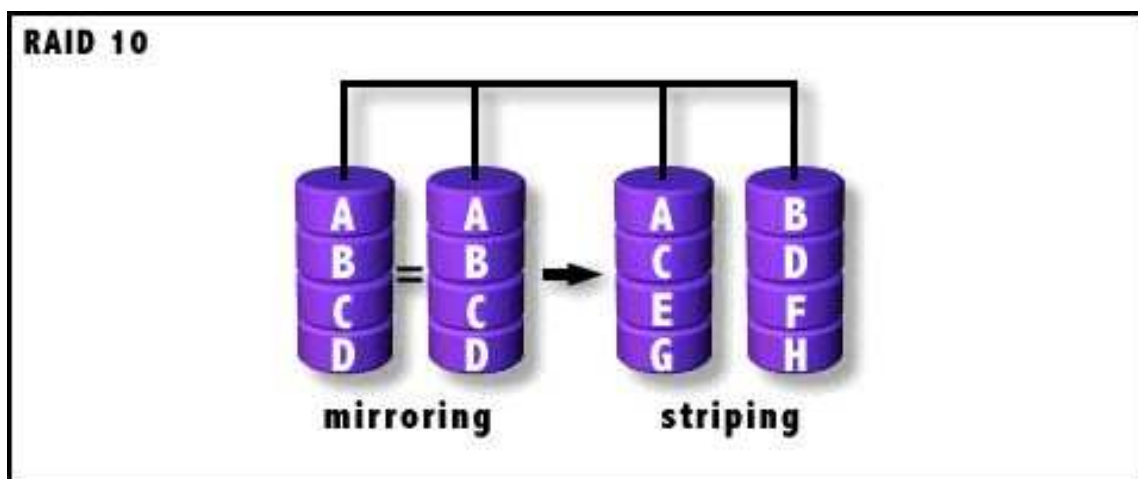
Umjesto njega, mnogo češće se koristi njemu sličan **RAID 5** koji također zahtijeva najmanje tri diska za implementaciju. Informacije se dijele na blokove i generišu se podaci o parnosti, ali ovde ne postoji poseban disk za parnost, već se ona upisuje redom na svaki disk koji je povezan u RAID 5. Na ovaj način se izbjegava usko grlo iz prethodna dva nivoa. Ovo je najprimjenljiviji RAID od svih RAID nivoa.



Slika 7 Primjer RAID 5

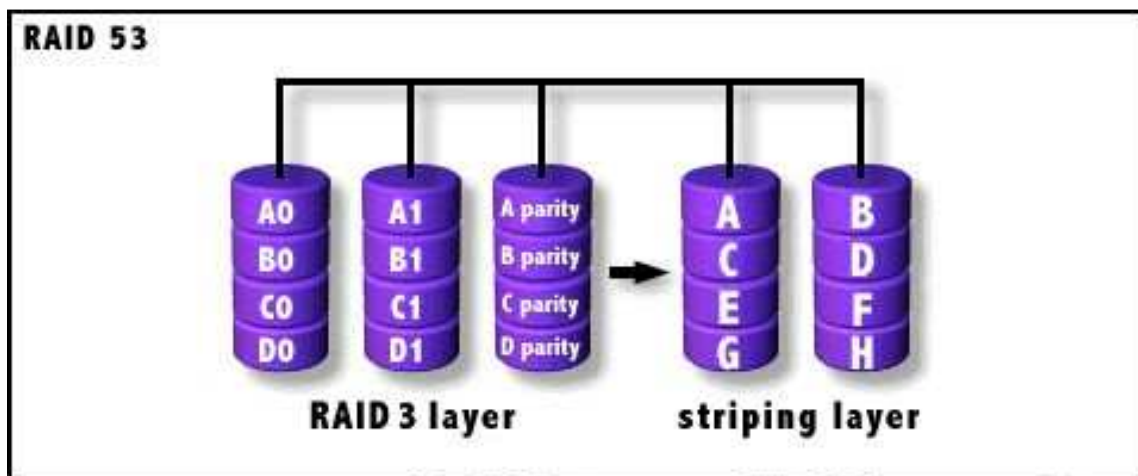
RAID 6 je proširenje **RAID-a 5** koje pruža dodatnu zaštitu od greške tako što se koristi tzv. dvodimenzionalna parnost. Pored već poznate parnosti blokova, izračunava se i parnost podataka po disku, a zatim se svaki od tih podataka zapisuje na drugi hard disk. Na ovaj način, RAID 6 može da izdrži istovremeno otkazivanje više diskova i zato se sreće jako često, u situacijama u kojima je integritet podataka veoma, veoma bitan.

RAID 7 je marketinški termin firme Storage Computer koji u stvari predstavlja RAID 4 sa keširanjem pisanja. Na taj način se postižu velike brzine upisa, ali isto tako postoji rizik od gubitka podataka iz keša u slučaju otkazivanja diska ili nestanka struje.



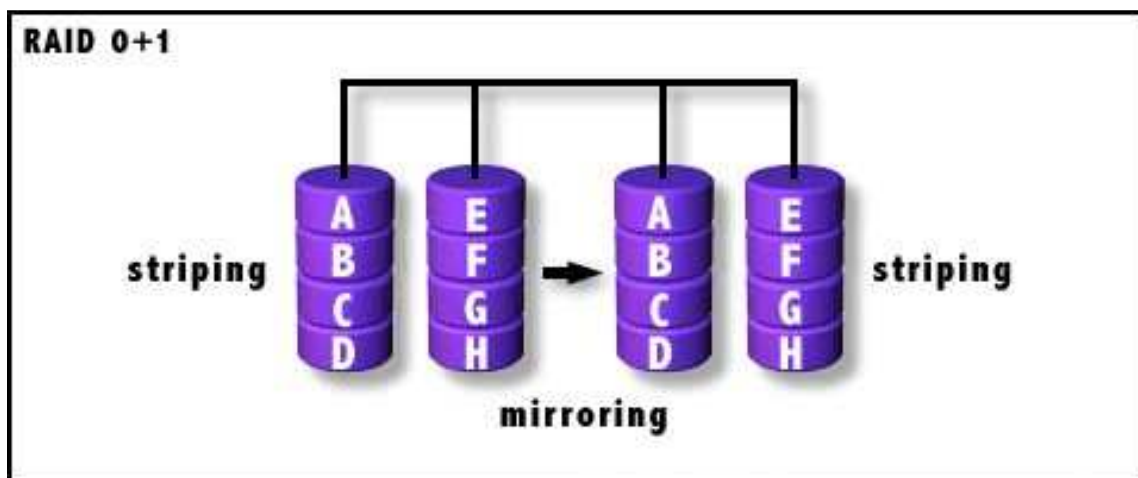
Slika 8 Primjer RAID 10

RAID 10 pruža dobre brzine uz veliku pouzdanost i zahteva najmanje četiri diska. U isto vreme se kombinuje *mirroring* i *striping* odnosno RAID 1 i RAID 0, pa otud i oznaka 10. Podaci se „cepaju” i snimaju na odvojene diskove, a svaki od tih diskova ima svoju kopiju. Jasno, glavni nedostatak ovog sistema jeste cijena, i iskorištenost resursa.



Slika 9 Primjer RAID 53

RAID 53 je, u stvari, kombinacija RAID-a 0 i RAID-a 3 i zahtjeva najmanje pet diskova. Ovaj nivo je organizovan kao RAID 0, s tim što segmenti nisu zasebni diskovi, već diskovi povezani u RAID3. Ovaj nivo RAID-a još je skuplji od prethodnog.



Slika 10 Primjer RAID 0+1

RAID 0+1 je veoma sličan RAID-u 10, s tim što se rasparčani podaci snimaju na RAID 0 granu, a u isto vreme se pravi kopija cele grane. Ako neki od diskova otkaže, ceo niz nastavlja da funkcioniše kao RAID 0 niz.

Stvarni savjet

J. C. Mackin

Mada ih ne možete praviti u Windowsu, RAID nivoi poznati kao RAID 0+1 i RAID 1+0 prilično se često koriste. RAID 0+1 (ili 01) predstavlja preslikavanje odsečaka (engl. *mirror of stripes*), u suštini dvostruku kopiju raspodeljenog volumena. Ova vrsta RAID volumena izrađuje se pravljenjem skupa RAID 0 volumena, a zatim njihovim preslikavanjem. RAID 1+0 (ili 10), sa druge strane, predstavlja raspodeljeno preslikavanje (engl. *stripe of mirrors*) u kome se podaci raspodeljuju u odsečke između više preslikanih volumena. Ovu vrstu RAID volumena izrađujete tako što prvo napravite niz preslikanih volumena, a zatim pravljenjem RAID 0 volumena duž tog preslikanog volumena.

Oba rešenja zauzimaju 50 posto diskova za otpornost na greške, a oba nude izuzetne performanse za čitanje i upisivanje. RAID 1+0, međutim, nudi veću vjerovatnoću za oporavak ukoliko više diskova otkaže. Imajte na umu da se ova dva RAID nivoa ne nazivaju uvijek isto. Neke kompanije (uključujući Microsoft) ponekad za RAID 01 i 10 koriste zajedničku oznaku 0+1. Ukoliko je potrebno da svoje zahtjeve nedvosmisleno prenesete isporučiocu opreme, bolje je da koristite izraze preslikavanje odsječaka (*mirror of stripes*) ili raspodijeljeno preslikavanje (*stripe of mirrors*).

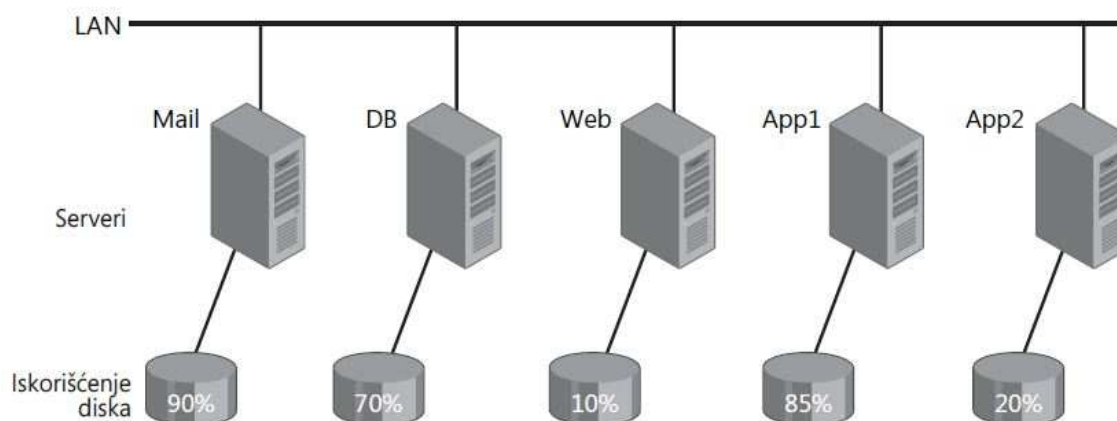
3.2 Tehnologije za skladištenje podataka na serverima

Uporedo sa porastom zahtjeva za sve većim skladišnim prostorom servera povećava se i broj novih tehnologija za skladištenje podataka. Tokom godina izbor za skladišni prostor servera širio se od jednostavnih direktno povezanih skladišnih prostora (DAS – direct-attached storage) preko skladišnih prostora povezanih u mreže (NAS – network-attached storage) do, najnovijih, optičkih povezanih (FC – Fibre Channel) i iSCSI SAN mreža.

3.2.1 Direktno povezani skladišteni prostor

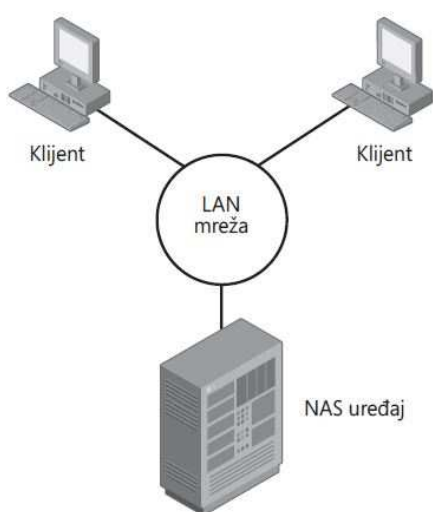
DAS je skladišni prostor povezan samo sa jednim serverom. Primer DAS rešenja je skup hard diskova unutar samog *storage* ili RAID diskova u posebnom kućištu koji su sa serverom povezani preko SCSI ili FC kontrolera. Osnovna osobina DAS skladištenja je da samo jednom serveru nudi brzo pristupanje podacima iz skladišnog prostora u blokovima, direktno preko interne ili eksterne magistrale. (Pristupanje u blokovima, za razliku od pristupanja po datotekama, znači da se podaci premeštaju u neformatiranim blokovima umesto u formatiranim datotekama.) DAS je poželjno rešenje za servere kojima su neophodne dobre performanse i kojima nije neophodan posebno veliki skladišni prostor. Na primer, DAS se često koristi za infrastrukturne servere kao što su DNS, WINS i DHCP serveri, kao i za kontrolere domena. Serveri datoteka i veb serveri takođe veoma dobro rade na serverima koji koriste DAS.

Najvažnije ograničenje DAS skladištenja jeste u tome da mu direktno može pristupati samo jedan server, što za posledicu ima nedovoljno efikasno upravljanje skladišnim prostorom. Na primer, na slici 11 prikazana je LAN mreža u kojoj su sva skladišta podataka direktno povezana sa serverima. Uprkos tome da Web i App2 serveri imaju višak skladišnog prostora, ne postoji jednostavan način da se ti resursi upotrebe za Mail ili App1 server kojima je potrebno više skladišnog prostora.



Slika 11 Mreža samo sa DAS rešenjem

3.2.2 Skladišni prostor povezan u mreže



Slika 12 Primjer povezivanja NAS uređaja sa mrežom

NAS je samostalan skladišni prostor kome drugi serveri i klijenti mogu lako da pristupe preko mreže. NAS uređaj ili aparat je posebno konfigurisan server kojeg pokreće operativni sistem posebno projektovan za rad sa datotekama. Osnovna prednost NAS skladištenja jeste u tome da se jednostavno ostvaruje i da klijentima i serverima na LAN mreži može da ponudi veliku količinu skladišnog prostora. Nedostatak NAS skladištenja jeste u tome da je, pošto serveri i klijenti pristupaju NAS uređaju preko LAN mreže umesto preko lokalne magistrale, pristupanje podacima sporije i da se zasniva na prenosu datoteka, a ne blokova podataka. Brzina rada NAS skladištenja je zbog toga skoro uvek manja od one kod DAS skladištenja. Zbog svojih osobina i ograničenja, NAS obično dobro pristaje serverima datoteka, veb serverima i drugim serverima kojima nije neophodan posebno brz pristup do podataka.

3.2.3 SAN

SAN (Storage-Area Network⁴) je mreža visokih performansi posebno predviđena za prenošenje blokova podataka između servera i podсистема skladišta podataka. Sa tačke gledišta operativnog sistema, SAN skladišni prostor izgleda kao da je instaliran na samom računaru ili serveru. Najvažnija karakteristika koja SAN mreže razlikuje od DAS skladištenja jeste u tome da skladišni prostor u SAN mrežama nije ograničen na jedan server već je, u stvari, dostupan proizvoljnom broju servera. (SAN skladišni prostor može se premeštati sa servera na server, ali izvan okruženja klasterovanog sistema datoteka, istovremeno može da mu pristupa više servera.)

➤ SAN u odnosu na DAS

Mada su DAS brzine prenosa podataka obično veće od onih u SAN mrežama, razlika u performansama između DAS i SAN tehnologija neprestano se smanjuje. Uprkos prednosti u brzini magistrale koju nudi DAS, SAN mreže se još uvek smatraju poželjnijim rešenjem zato što pogodnost zajedničkog skladišnog prostora koju nude SAN mreže nadoknađuje nedostatak nešto sporije brzine pristupa.

4 Storage Area Network

SAN mreža sačinjena je od posebnih uređaja, uključujući HBA adaptere na matičnim serverima, komutatore koji pomažu preusmjeravanju saobraćaja pri skladištenju podataka, podсистeme diskova za skladištenje podataka i trake za memorisanje podataka. Ovi hardverski uređaji koji povezuju servere i skladišta podataka u SAN mrežu nazivaju se struktura (engl. fabric) SAN mreže. Svi ovi uređaji povezuju se optičkim ili bakarnim kablovima. Pošto se povežu u strukturu, raspoloživi skladišni prostor deli se na virtuelne particije koje se nazivaju broj logičke jedinice (LUN⁵ – logical unit number), koji serveru potom izgledaju kao lokalni diskovi.

SAN mreže su namijenjene centralizaciji resursa za skladištenje podataka pri čemu nema ograničenja u pogledu rastojanja i mogućnosti za povezivanje koja postavlja DAS⁶ skladištenje. Na primjer, arhitektura paralelne SCSI⁷ magistrale ograničava DAS na 16 uređaja (računajući i kontroler) do najvećeg rastojanja od 25 metara. SAN mreža sa optičkim vezama

⁴ Mikro knjiga

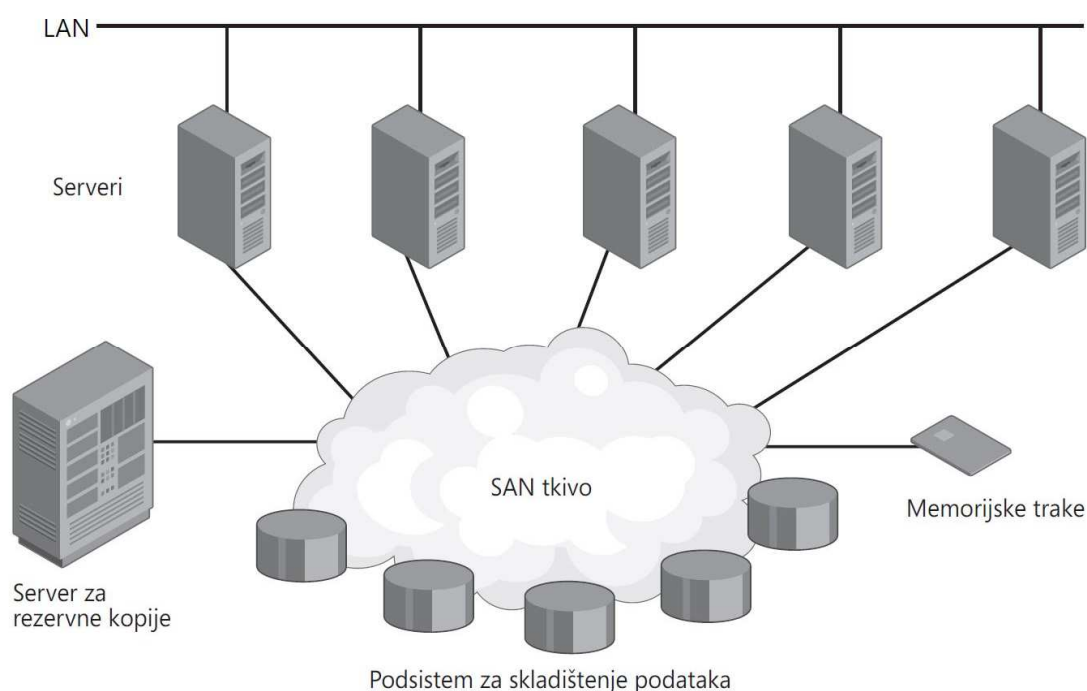
⁵ http://en.wikipedia.org/wiki/Logical_unit_number

⁶ http://www.webopedia.com/TERM/D/direct_attached_storage.html

⁷ <http://en.wikipedia.org/wiki/SCSI>

(FC SAN – Fibre Channel SAN) pomjera ograničenja udaljenosti na 10 km ili više i omogućava da se praktično neograničen broj uređaja poveže u mrežu. Ove prednosti omogućavaju da SAN mreže izdvoje skladištenje podataka iz pojedinačnih servera i da skupe neograničen skladišni prostor u mrežu gdje taj skladišni prostor može da se deli.

SAN mreže su dobro rešenje za servere kojima je neophodan brz pristup velikim količinama podataka (posebno podacima u blokovima). U ovakve servere spadaju serveri za elektronsku poštu, serveri za pravljenje rezervnih kopija, serveri za prenos multimedijalnog sadržaja uživo, serveri za aplikacije i serveri baza podataka. Korišćenje SAN mreža takođe omogućava efikasno umnožavanje (replikaciju) podataka na veća rastojanja, što se obično koristi kao deo rešenja za oporavak od pada sistema (DR – disaster recovery).



Slika 13 Prikaz jednostavne skladišne mreže (SAN – storage-area network)

SAN mreže se obično javljaju u dvije podvrste: sa optičkim kablovima (Fibre Channel) i iSCSI.

4.1 Optički povezane SAN mreže

Optička veza (FC – Fibre Channel) nudi visoke performanse za ulaz/izlaz (I/O – input/output) blokovima podataka do uređaja za skladištenje podataka. Zasnovan na serijskom SCSI

interfejsu, FC je najstarija i najšire prihvaćena tehnologija za međusobno povezivanje unutar SAN mreža. Za razliku od paralelnih SCSI uređaja, FC uređaji ne moraju da čekaju (ili da se nadmeću) za deljenu magistralu. Umesto toga, FC koristi posebne komutatore za istovremeno prenošenje informacija između više servera i uređaja za skladištenje podataka.

Najveća prednost FC povezivanja je u tome da je to najšire prihvaćena SAN tehnologija i da je, bar do nedavno, nudila najbolje performanse. Nedostatak FC tehnologije su troškovi opreme i složenost primene. Komponente optički povezane mreže obuhvataju HBA adaptore servera, kablove i komutatore. Sve ove komponente posebno su napravljene za FC povezivanje, pri čemu svaki isporučilac nudi sopstveno rešenje, relativno su skupe i zahtevaju posebnu stručnost.

4.2 iSCSI SAN mreže

Internet SCSI (iSCSI⁸) je industrijski standard razvijen da bi se omogućio prenos blokova SCSI preko Ethernet mreže korišćenjem TCP/IP protokola. Serveri sa iSCSI uređajima komuniciraju preko lokalno instaliranog softverskog agenta poznatog kao iSCSI inicijator (engl. iSCSI initiator). iSCSI inicijator šalje zahteve i prima odgovore od iSCSI mete (engl. iSCSI target), što može da bude ili krajnji uređaj za skladištenje podataka ili posredni uređaj kao što je komutator (switch). Struktura iSCSI mreže takođe obuhvata jedan ili više iSNS (Internet Storage Name Service) servera koji, po mnogo čemu sličan DNS serverima na LAN mreži, obezbeđuju pronalaženje i podjelu na oblasti SAN resursa.

Oslanjajući se na TCP/IP protokol, iSCSI SAN mreže koriste pogodnost da su umreženi uređaj i znanja o njima prilično rašireni, što je činjenica koja iSCSI SAN mreže čini uopšteno govoreći jednostavnijim i jeftinijim za primenu u odnosu na FC SAN mreže.

Pored niže cijene i znatno lakše primjene, ostale prednosti iSCSI u odnosu na FC su:

- Mogućnost povezivanja na veća rastojanja Organizacije koje imaju sjedišta na više mjesta mogu da imaju čitav niz „SAN ostrva” koja trenutno ograničenje za FC povezivanje od 10 km ne može da premosti. (Postoje novi načini za povećanje mogućnosti povezivanja optičkim vezama do nekoliko stotina kilometara, ali su ove metode i skupe i složene za primenu.) Sa druge strane, iSCSI može da poveže SAN

⁸ <http://en.wikipedia.org/wiki/ISCSI>

mreže u izdvojenim predstavništvima korišćenjem već postojećih gradskih mreža (MAN – metropolitan area network) i regionalnih mreža (WAN – wide-area networks).

- U FC protokol nijesu ugrađene nikakve bezbjednosne mjere. Umjesto toga, bezbjednost se prvenstveno ostvaruje ograničavanjem fizičkog pristupa SAN mreži. Za razliku od FC protokola, Microsoftovo rešenje iSCSI protokola obezbjeđuje bezbjednost uređajima na mreži korišćenjem CHAP (Challenge Handshake Authentication Protocol) protokola za provjeru autentičnosti i bezbjednosna pravila IP protokola (IPSec – Internet Protocol security) za šifrovanje. Pošto ove metode za bezbjednu komunikaciju već postoje u Windows mrežama, mogu se odmah proširiti sa LAN mreža na SAN mreže.

Osnovni nedostatak iSCSI SAN mreže je u tome da, osim ako nije napravljena namjenskim (i skupim) 10 GB Ethernet kablovima i komutatorima, I/O prenos iSCSI mreže sporiji je od onog koju SAN mreža zasnovana na FC vezama može da ponudi. A, ukoliko se ipak odlučite da koristite 10 GB opremu za iSCSI SAN mrežu umjesto uobičajenog gigabajtnog Ethernet, visoka cijena takvog 10 GB rešenja potrla bi prednost u ceni iSCSI u odnosu na FC mreže.

4.3 Fibre Channel protocol

Povezivanje SAN preko Fibre Channel⁹ nudi veoma vleike prefomanse čitanja i upisa, jako često se primjenjuje u *data-centrima* gdje udaljenost od servera ni mnogo velika i u sisitemima koji su izolovani. Bilo je i do sada riječi o Fibre Chennel protokolu u radu ali sad ćemo detaljnije približiti Fibre Channel i mogućnosti koje on nudi, napomenućemo njegove vrline i mane.

Fibre Chennel protokol je definisan kao grupa IP i OSI protokola. Sada ćemo napravaviti kratak opis slojeva FC:

FC-0: Physical Ovaj nivo je definisan za sve fizičke specifikacije u protokolu: konekcije, kablovi za prenos, prijem, signal, itd... Treba napomenuti da je Fibre Chennel gledano iz perspektive ovog nivoa seriski protokol.

FC-1 Encoding: Fibre Channel protokol šifruje 8-bit karaktere u 10-bit karakteru za potrebe efikasnog prenosa.

⁹ <https://cs.uwaterloo.ca/cscf/research/cerasblade/documents/Docs/25P2509.pdf>

FC-2 Framing and Signaling: Ovo je sloj gdje su prenosni protokoli specifični. On sadrži strukturu prenosa, frame definicije, procedure, itd...

FC-3 Extended Link Services: Ovaj sloj uključuje neke usluge koje se koriste od strane FC uređaja za dobijanje i pružanje informacija FC mrežnoj infrastrukturi, kao i samim FC uređajima.

FC-4: Upper Level Protocols (ULP): Ovo je sloj definisan kao viši nivo protokola mapira sa Fibre Channel, definiše mapiranje, itd... Ovo je sloj gdje je FCP definisan (SCSI preko Fiber Channel).

Navešću neke od topologija u kojima se Fibre Channel obično implementira:

- Point-to-point topologija: to je topologija gdje su sa obje strane FC portovi, direktno povezani jedan na drugi. TX konektor jednog čvora je direktno povezan na RX konektor udaljenog čvora, što dovodi da jedan kabal povezuje oba čvora.
- Arbitrated-loop-topologija: svi čvorovi su povezani na jedan medijum, koji fizički dijeli sa svim ostalim FC portove.
- Switched topologija: ovo je topologija koja je slična IP mreži sa svičevima, gdje su HBA konektovani na storage uređaj ili kontroler preko kog uređajima omogućava simultani (istovremeni) saobraćaj do svih prortova. Svaka grupa međusobno povezanih switch-eva naziva se fabric (struktura) i definiše se jedinstvenim imenom, zonom i adresom prostora u Fibre Channel mreži.
- Public loop topologija: to je jedna nadgledana petlja koja je povezana sa *fabric*, gdje uređaji u petlji mogu pristupati onim drugim u istom *fabric*-u.

U daljem radu ćemo analizirati samo Switch Topology.

4.4 Fibre Channel Addressing

U kontekstu strukture Fibre Channel adresa na FC portu je 24-bit broj koji identifikuje FC uređaj povezan na nju. Switch-evi koriste ove adrese kao indeks u internoj *routing* tabeli, kako bi usmjerili saobraćaj najkraćim putem sa jednog uređaja na drugi uređaj.

Tabela 1 Fibre Channel Address struktura¹⁰

2	2	2	2	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

¹⁰ SANS Institute InfoSec Reading Room

3	2	1	0	9	8	7	6	5	4	3	2	1	0																
Domain_ID								Area_ID								Port_ID													
Address Identifier																													

- *Domain ID* je broj koji identifikuje jedan ili više switch u samoj *domain* strukturi. Obično *domain id* je broj *switch-a* unutar strukture, ali ako ima više od jedan, oni bi trebalo da budu direktno spojeni preko direktno povezanog linka koji se zove *Inter Switch Link (ISL)*.
- *Area ID* identifikuje *Nx_Port* koji je konektovan na *switch*. Ako uređaj konektovan na *switch* nije *Nx_port*, onda ovaj broj identifikuje cijelu javnu petlju (public loop).
- *Port_ID* identifikuje jedan *Nx_Port* ili AL-PA (Arbitrated Loop Physical Address) na konektovanom uređaju na *Public Loop* na strukturnom portu.

Neke od identifikacija ne mogu biti korišćene zato što su rezervisane da omoguće pristup nekim od servisa.

4.5 World Wide Names

Da bi se identifikovao uređaj (čvor ili port) konektovan na Fibre Channel infrastrukturu, uređaj mora imati statičku adresu ili "Ime" koje je jedinstveno za taj uređaj i to ime se zove World Wide Name (WWN). Jedno ime se veže za FC čvor i jedano za svaki FC port u čvoru. WWN mora biti konfigurisan kao statički na uređaju, ovaj koncept je sličan MAC adresama kod Ethernet uređaja.

WWN struktura je 64-bit, obično se predstavlja u 8 parova kao heksadecimalan broj HH:HH:HH:HH:HH:HH:HH:HH. On ima posebnu strukturu koja otkriva informacije o uređaju.

4.6 Fibre Channel servizi

Fiber Channel strukture pružaju niz usluga svojim klijentima (FC čvorovima), što im omogućava da komuniciraju sa storage mrežom i razmjenjuju informacije kao dvije različite strane, da razmjenjuju parametre veze, konfiguracije ili promjene topologije. Ovi servisi

moгу pristupati logovanjem na portove koje nose Well Known Address (WKA). WKA su lični karakteri porta koji su rezervisani za upotrebu unutar srtukture.

Sledeća tabela prokazuje posebne portove i servise koje fabric omogućava kroz nju:

Tabela 2 Portovi is servisi koji prolaze kroz *fabric*

Adresa	Opis
FF FC 01h do FF FC Efh	Rezervisano za Domain Controllers
FF FF F0h	N_Port Controller (see FC-LS)
FF FF F1h do FF FF F3h	Rezervisano
FF FF F4h	Event Service (see FC-GS-5)
FF FF F5h	Mulicastt Server
FF FF F6h	Clock Synchronization Service
FF FF F7h	Security Key Distribution Service
FF FF F8h	Alias Server
FF FF F9h	Quality of Service Facilitator – Class 4 (QoSF)
FF FF Fah	Management Service
FF FF FBh	Time Service
FF FF FCh	Directory Service
FF FF FDh	Fabric Controller

FF FF FFh	Broadcast Alias_ID
-----------	--------------------

Svaki od ovih servisa mogu imati jedan ili više pod-servisa. Nisu svi servisi dostupni čitavoj strukturi. To zavisi od proizvođača switch koji je implementiran u strukturu, obično proizvođači switch daju informacije o servisima dostupnim samo na njihovim proizvodima.

4.7 Bezbijednost Fibre Channel u Storage Area Network

Kada se razmatraju mogući napadi na Fibre Channel, prva stvar koju treba učiniti, napraviti scenario pod kojim bi taj napad bio moguć i izvodljiv u realnim uslovima.

Kada se govori o bezbijednosti Fibre Channel¹¹ najčešća greška koja se dešava jeste pretpostavljanje da je Fibre Channel bezbjedan samo zato što se nalazi u server sobi i što je izolovan, tako da se nemože niko direktno priključiti na Fibre Channel mrežu. Iako je u suštini možda to tačno, ovaj argument je nedovoljan da bi bili sigurni da su naši podaci bezbjedni. Obično ozbiljna preduzeća i organizacije vode računa o bezbijednosti i zaštiti server sobe, jako mali broj ljudi ima direktan pristup server sobi i veoma je teško kompromitovati podatke. Ali postoje mnogi serveri koji su u fazi razvoja i testiranja koji takodje imaju pristup SAN mreži. Tu se može lako napraviti propust, jer je uobičajeno da veliki broj ljudi ima naloge na ovakvim serverima, koji često i ne pripadaju matičnoj kompaniji, to često mogu biti izvođači radova, razvoji inženjeri, itd... Obično bezbijednost ovakvih testnih servera ili servera u razvoju nije jaka često se dešava da root/administrator nalog lozinka bude jednostavno „root“ i mnogi drugi parametri budu podešeni na početn default parametre koji su javno dostupni.

Da bi napadač ugrozio sistem njegova polazna tačka, je vjerovatno da prvo preko neprivilegovanih korisnika pređe na privilegovane korisnike sa administratorskim pravima. Ovaj scenario se dosta koristi kod korisnika koji koriste SAN. Veoma često razvojni i test serveri ne samo da imaju pristup SAN-u nego imaju pristup i istim nizovima diskova koji se koriste za proizvodne servere. Kada napadač dobije administratorski/root pristup, u zavisnosti od napada koji želi da izvrši, potrebno je da uradi nešto od sledećeg:

- Mora koristiti alate koji podržavaju isti OS i HBA drivere.
- Ručno mijenjanje konfiguracije HBA kako bi izvršila WWN Spoofing.

¹¹ Fibre Channel Storage Area Networks: An Analysis
From A Security Perspective
Copyright

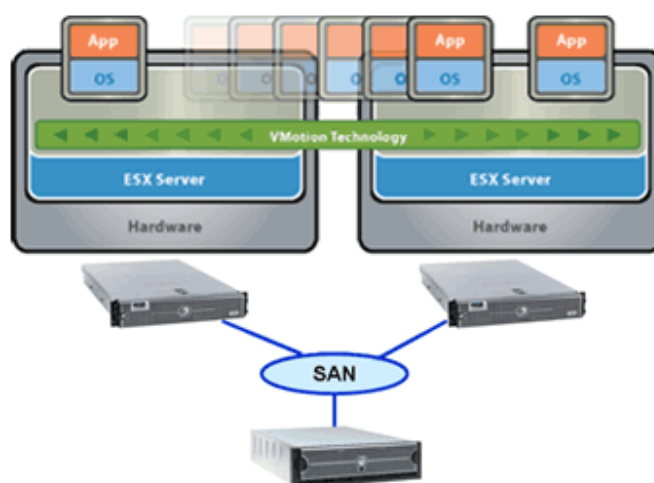
- U nekim slučajevima je potrebno instalirati drugu verziju HBA FC drajvera i na taj način izvesti napad. U ovom slučaju se mogu koristiti Linux OS jer je kod ovih operativnih sistema driver code obično dostupan i moguće ga je mijenjati.

Ovi primjeri napada na SAN ne mogu se smatrati svakidašnjima napadima koje može svako da pokuša. Ovo su primjeri veoma ozboljnih napada gdje je osnovini cilj napadača da ukrade, pokvari ili uništi informaciono jezgro neke firme. Napadač koji vrši ovakve napade, planira napad dugo i svjestan je posledica koje može načiniti. Organizacije koje su potencijalne mete ovakvih napada svaki pokušaj napada trebaju jako ozbiljno da shvataju.

5 Implementacija SAN pomoću VMware ESX/ESXi

U ovom dijelu rada više ću se bazirati na konfiguraciju konkretnog primjera gdje ću koristiti VMware ESXi OS na serverima a konfiguracija će se izvoditi kroz VMware vCentar.

ESX/ESXi arhitektura omogućava administratorima da dijele hardverske resurse na više izolovanih jedinica koje se nazivaju virtuelne mašine



ESX/ESXi se sastoji od više komponenti, glavne komponente ESX/ESXi sistema su **sloju Virtualizacije, Hardverske interfejs komponente i Korisnički interfejs**.

Sloj Vrtualizacije omogućava idealizovano virtuelno-hardversko okruženja koja se oslanja na fizičke resurse sistema. Ovaj sloj uključuje **Virtual Machine Monitor (VMM)** koji je odgovaran za virtualizaciju i **VMkernel**. **VMkernel** upravlja svim fizičkim resursima, radnom memorijom, fizičkim procesorima, skladištenim prostorom i mrežnim kontrolerima. Virtuelni sloj raspoređuje operativne sisteme virtuelnih mašina i servise na konzoli ako rade na ESX *hostu*. Virtualizacioni nivo govori operativnom sistemu kako treba da pristupa fizičkim uređajima, zbog toga Vmkernel mora imati sve drajvere firickih uređaja kako bi omogućio pristup ka njima.

Slika 14 Virtualizovana Vmware IT struktura

Hardverske komponente komuniciraju sa virtuelnim mašinama kao sto su *CPU* i *HDD* koristeći hardverske interfejs komponente. Ove komponente omogućavaju drajverima da omoguće komunikaciju hardverskim servisima, dok krije hardverske razlike iz drugih dijelova sistema.

Korisnički interfejs omogućava administratorima da kroz grafičko ili *command line* okruženje pristupaju hostovima ili virtuelnim mašinama i konfiguriraju ih. Administrator ESX/ESXi hostovima može pristupiti preko VMware *vSphere Client* koji je grafičko okruženje i instalira se na racunaru administratora kao aplikacija. **vSphere¹²Client** ima i svoj *web* interfejs, gdje administrator može pristupiti hostovima preko *browser-a*. Virtuelnom centru se može pristupiti i preko *command line* korićenjem nekih od softvera za tu namjenu npr. Putty.

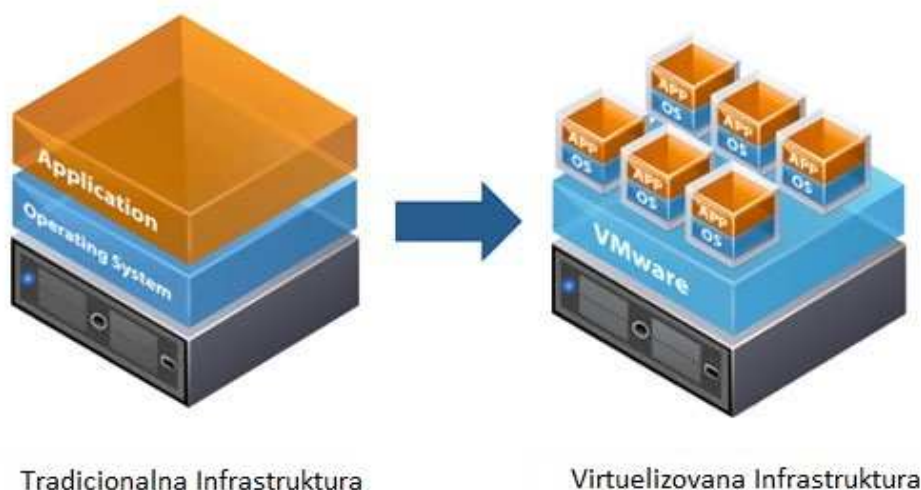
5.1 Razumijevanje virtualizacije

Šta je Virtuelizacija?

Virtuelizacija je kompjutersko kreiranje virtuelne verzije nečega što inače postoji kao "stvarno", a najčešće su to serveri, operativni sistemi, skladišteni prostor (sistem za skladištenje podataka, hard disk) ili mrežni resursi.

¹² http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2FPDF%2Fic_pdf.html

Virtuelizacija šematski prikazano



Slika 15 Virtualizacija u odnosu na tradicionalne servere

- Nekome ko se prvi put susreće sa terminom virtuelizacije, najjednostavniji primjer za bolje razumijevanje ove tehnologije biće: podela hard diska na tzv. particije. Dakle, postoji jedan fizički uređaj za skladištenje podataka, ali ga uz pomoć programa podelimo na dva ili više dela i onda ih OS posmatra kao zasebne uređaje. Slično tako na jednom kompjuteru možete npr. napraviti više virtuelnih kompjutera (zvanih virtuelne mašine) koji će obavljati zadatke i ponašati se isto kao da imate više fizički odvojenih kompjutera. Prednosti i mogućnosti takvog okruženja možete pretpostaviti. Neke od prednosti virtualizacije su:
- **Konsolidacija servera** – Pomoću virtuelizacije možete konsolidovati više operativnih sistema na jedan *hardware*. Praksa je pokazala da se stepen konsolidacije kreće od 5:1 do 15:1 za serverske operativne sisteme. Na ovaj način se postižu velike uštede u kapitalnim troškovima (nabavka servera, UPS uređaja, klimatizera, mrežnih svičeva itd.) i u operativnim troškovima (potrošnja električne energije, jednostavnija administracija itd).
- **Testiranje i razvoj software-skih sistema** – Jednostavnost u instaliranju operativnih sistema, pravljenja identičnih kopija i kreiranje *snapshot*-ova (*point-in-time* kopija) virtualizaciju čine idealnom platformom za razvoj i testiranje *software*-skih rešenja.

- **Kontinuitet servisa** – Virtualizovani operativni sistem je u stvari skup nekoliko fajlova. Migracija operativnog sistema sa jedne *hardware*-ske platforme na drugu se radi prostim kopiranjem fajlova. Ovaj način manipulacije operativnim sistemima i aplikacijama unutar operativnih sistema značajno pojednostavljuje rešenja za kontinuitet servisa kao što su sistemi visoke dostupnosti i sistemi za oporavak od katastrofa.

Postoje nekoliko glavnih polja u IT industriji gdje se virtualizacija najviše primjenjuje i u kojima najviše napreduje i najviše dolazi do izražaja:

- Virtualizacija servera¹³ - Korišćenjem **virtuelizacije servera**, moguće je pokretati više različitih operativnih sistema istovremeno i to na jednom fizičkom serveru (kompjuteru). Statistike pokazuju da se mnogi serveri koji ne koriste virtualizaciju koriste samo 15% svojih kapaciteta. Virtualizacijom se postiže 80% veća iskorišćenost.
- Virtualizacija sistema za skladištenje podataka (storage) - **Virtuelizacija sistema za skladištenje (storage-a)** je udruživanje više fizički odvojenih sistema za skladištenje u jedan virtuelni mrežni uređaj za skladištenje podataka, kojim se može upravljati centralno. Virtuelizovani "hardovi" mogu ponuditi veće performanse i efikasnije korišćenje prostora u odnosu na fizičke uređaje, takođe će i smanjiti potrebu za kupovinu novih uređaja. Administratori u ovom slučaju svoj posao pravljenja rezervne kopije, arhiviranje, oporavak (recovery) itd. rade jednostavnije i za mnogo manje vremena.
- Virtualizacija kompjuterskih mreža - **Virtuelna mreža** je potpuna reprodukcija fizičke kompjuterske mreže, ali u obliku softvera i kao takva nudi iste karakteristike i bezbednost kao i fizička, čak i više od toga. I kod njih su, samo logički ne i fizički, prisutni portovi, switchevi, routeri, firewallovi, load balanseri itd. Sa tim da takve mreže imaju mogućnost većeg stepena automatizacije procesa, monitoringa i sl.
- Virtualizacija desktopa/aplikacija - **Virtuelizacija desktopa i/ili aplikacija** donosi mnogo fleksibilniju, efikasniju kao i sigurniju isporuku navednih usluga. Tradicionalno, svaki korisnik ima svoj "desktop" na kojem radi, čuva podatke itd...postoji i potreba za održavanjem svakog pojedinačnog desktopa (radne stanice, kompjutera), eventualnim popravkama, instaliranjem novih verzija i "zakrpa" OS-a i aplikacija... što dodatno oduzima vreme, napore, novac kako poslodavcu tako i zaposlenima u IT. Takođe postoji i mogućenost nenamerne kompromitacije podataka usled kvara,

¹³ <http://veljko.info/sta-je-virtuelizacija-i-koje-su-njene-prednosti/>

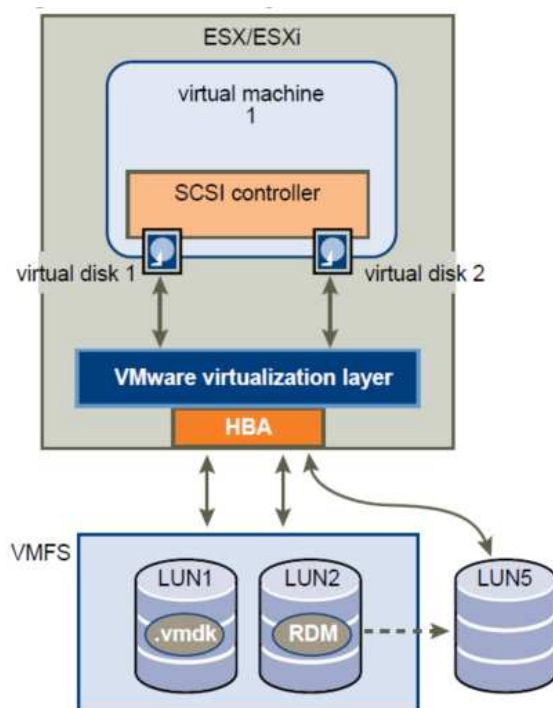
požara, poplave, krađe, itd. Virtuelni *desktop* ili program se zapravo nalazi u datacentru i može biti isporučen korisniku na zahtev. **Bilo kada i bilo gde**. Korisnik ne mora da odlazi u kancelariju da bi imao pristup "*desktop-u*", jednostavno svom virtuelnom *desktop-u* može pristupiti putem svog tableta, smartphonea ili kućnog *desktop-a*.

Najpoznatiji hypervizori trenutno su:

- [VMware](#) - vSphere, vCenter, vPlayer
- [Microsoft](#) - Hyper-V
- [Citrix](#) - XenServer, XenDesktop
- [Oracle VM](#) - Server, VirtualBox
- [Parallels](#) - (za "Mac")

5.1.1 Virtualizacija skladištenog prostora

ESX/ESXi pruža virtualizaciju skladištenog prostora, koji predstavlja fizičko skladištenje virtuelnih mašina na storidžu. ESX/ESXi mašine koriste virtuelne diskove za skladištenje svojih operativnih sistema i drugih dokumenata koji su neophodni za rad. Virtuelni disk predstavlja jedan veliki fail, koji se lako može kopirati i pemeštati, manipulaisati sa njim na mnoge druge načine. Virtuelnoj mašini možete dodjeljivati više virtuelnih diskova, ona će ih sve vidjeti kao da su to njeni fizički diskovi. Da bi pristupala virtuelnim diskovima virtuelna mašina koristi virtuelni SCSI kontrolere. Ovi kontroleri uključuju BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS i VMware Paravirtual. Sa tačke gledišta virtuelne mašine, VM vidi svaki disk kao da je povezan direktno fizički na SCSI kontroler i vidi ga kao svo fizički disk. Bez obzira da li pristupa stvarnom fizičkom disku ili pristupa preko SCSI, iSCSI network ili Fibre Channel adaptera, VM ga vidi kao svoj disk i svervisi se izvršavaju kao da je fizički disk *host-a*.



Slika 16 Prikaz virtuelnog SAN kontrolera

Kada planirate da konfigurisanje neki novog *storage* uređaja i stavite ga u rad. Morate mnogo voditi računa o tome šta su to preporuke proizvođača¹⁴, da **pool-ove** i druge opcije koje konfigurirate na *storage* radite u skladu sa preporukama. Kada ste kreirali određeni *pool* dodijelite ga određenom RAID-u, zatim ga mapirate u određenom hostu ili klasteru i dodijelite mu LUN-ove. Takođe treba voditi računa da pristupate vSphere samo preko jednog servisa ili web ili klijent aplikacije, to je i preporuka proizvođača.

¹⁴ http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2FPDF%2Fic_pdf.html

6 Korištenje ESX/ESXi u Fibre Channel SAN

Kada je potrebno da podesite ESX/ESXi hostove da koriste FC SAN potrebno je poznavanje i razumijevanje niza drugih informacija o ESX/ESXi i SAN nizovima. U prvom dijelu smo govorili o Fibre Channel i mogućnostima koje pruža o njegovim vlinama i mana, u ovom drugom dijelu rada baziraćemo se samo na njegovu implementaciju kod ESXi i SAN.

6.1 Storage area network u VMware

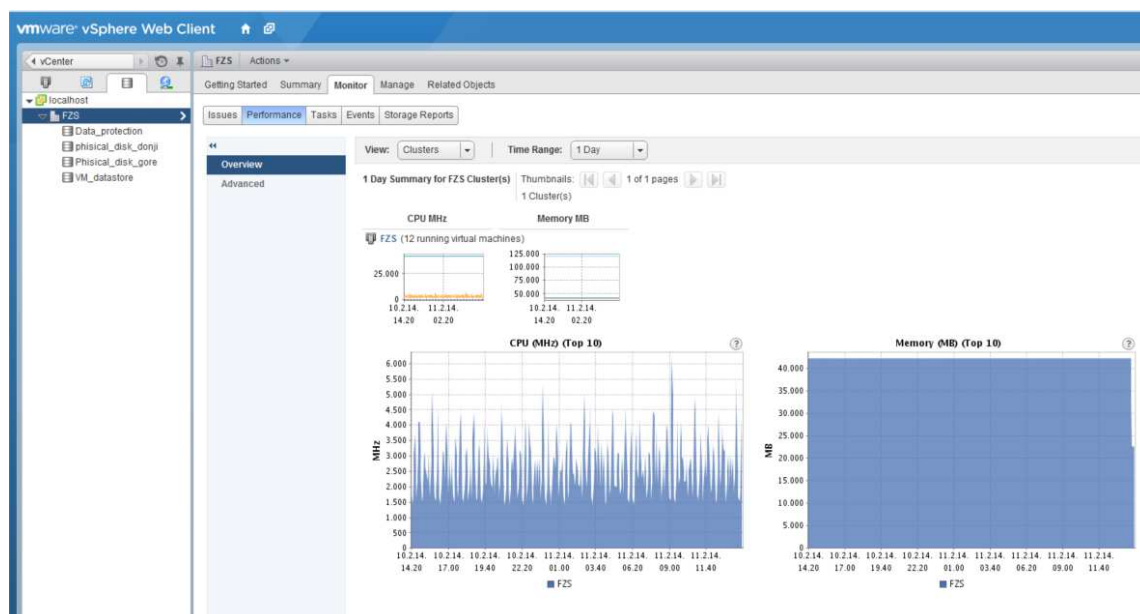
Ako ste neko ko ima iskustva sa ESX/ESXi i planirate da vaš sistem konfigurirate tako da hostovi ESX/ESXi rade preko SAN, potrebno je da se bolje upoznate kako se SAN i ESXi vide međusobno i kako komuniciraju. O tome kako SAN funkcionise i o konceptu SAN, detaljnije sam pisao u prvom dijelu rada, takođe jako dosta informacija se može naći na **Internetu**. Ova tehnologija se svakodnevno mijenja i napreduje, tako da ako se pripremate da prvi put konfigurirate SAN pogledajte internet dokumentaciju vodećih kompanija u IT industriji (IBM, Cisco, VMware, Microsoft).

Storage Area Network je specijalizovana mreža visokih performansi za prenošenje blokova podataka koji povezuje server ili *host* u klasteru sa *storage-om* visokih performansi. Komponente kao što su **HBA**¹⁵ *host bus adapter* koji se ugrađuje na serveru, HBA se veže na switch koji pomaže *storage-u* da usmjerava saobraćaj, kablovi *storage* i diskovi za *storage* predstavljaju komponente SAN-a. Da bi ste prenijeli saobraćaj od servera do diljene memorije na *storage-u*, SAN koristi *Fibre Channel* protokol sa komandama SCSI koji se nalaze u FC okvirima. Da bi ste ograničili pristup servera na *storage-u*, kako bi razdvojili saobraćaj između servera, SAN omogućava zoniranje gdje serveri vide samo ono što je u okviru njihove zone. Zone se kreiraju za svaku grupu servera koje pristupaju zajedničkoj grupi LUN-ova na *storage*. Zone mogu da se vežu za HBA adapter sa kojim su povezani sa serverom, one nisu vidljive spolja, vidljive su samo za uređaje iznutra. Zone su slične LUN maskama, koje se koriste za održavanje ko može da pristupa LUN-ovima.

Za pristup i konfiguraciju skladištenom prostoru koristimo VMware vSphere to je klijentska aplikacija koju instaliramo na računaru i koristimo je za pristup data centru. Ova aplikacija se koristi za pristup ESX/ESXi hostovima i kad se ne radi o konfiguraciji skladištenog prostora. Glavna konfiguracija **clastera** se radi iz **vcenar** konzole, njoj se može pristupati na dva načina,

¹⁵ <http://www.redbooks.ibm.com/technotes/tips0776.pdf>

preko **vSphere** aplikacije koju instalirate na svom računaru i preko **web client vSphere** kome pristupamo preko browsera.



Slika 17 Prikaz storage monitoringa u vSphere web client

6.1.1 Multipathing i Path Failover

Kada SAN koristi *multipathing* tehniku, to znači da ESX/ESXi koristi više od jednog servera u istom klasteru. Klaster ESX/ESXi čine dva ili više servera koji se konfiguriraju da rade kao jedan server. Multipathing omogućava da dva fizička servera koriste iste LUN-ove na storidžu. Ako se dogodi da veza servera i storage-a padne, SAN će preusmjeriti saobraćaj preko drugog kontrolera i to se naziva *path failover*.

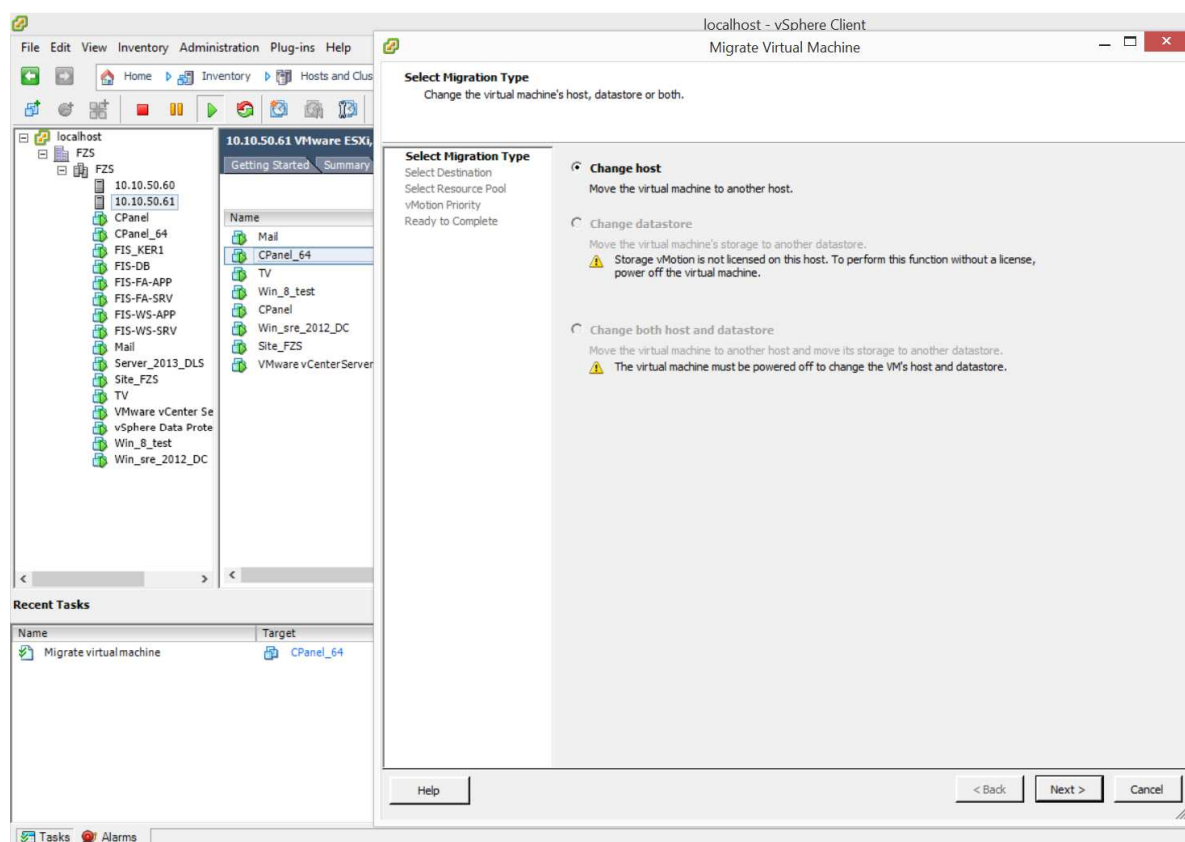
6.1.2 Prednosti koje pružaju SAN i ESX/ESXi

Održavanje virtuelnih mašina je mnogo pojednostavljeno ako koristite *storage area network*. ESX/ESXi koroz opciju vMotion i vCenter omogućavaju da se virtualna mašina migrira na drugi server bez gašenja ukoliko skladišteni disk smještena na SAN-u. vCenter koristi to što su virtuelne mašine centralizovane i samo mijenja *host*, kroz vMotion može se omogućiti **load balacing** bez prekida rada virtuelne mašine. Ako koristite ESX/ESXi koji u klasteru ima više

hostova (servera) koji imaju više virtuelnih mašina, često će vam se desiti da vam zahvali prostora na *storage*-u. Ako koristite SAN rešenje, vaš problem se može vrlo jednostavno riješiti dodavanjem novog *storage-a* na koji ćete kasnije migrirati mašine i sve bez prekida rada virtuelne mašine. Takođe može na „bezbolan“ način izvršiti rekonfiguraciju LUN-ova ukoliko ste dali nekom LUN-u preveliki prostor ili je došlo do greške pri konfigurisanju. Ukoliko je projektujete sistem koji će imati **Disaster recovery** ESX/ESXi i SAN su jedne od vemo dobrih rešenja jer su veoma laki za administraciju i u tim uslovima i jeftini za povezivanje sa udaljenom lokacijom ukoliko nisu potrebne velike brzine linkova.

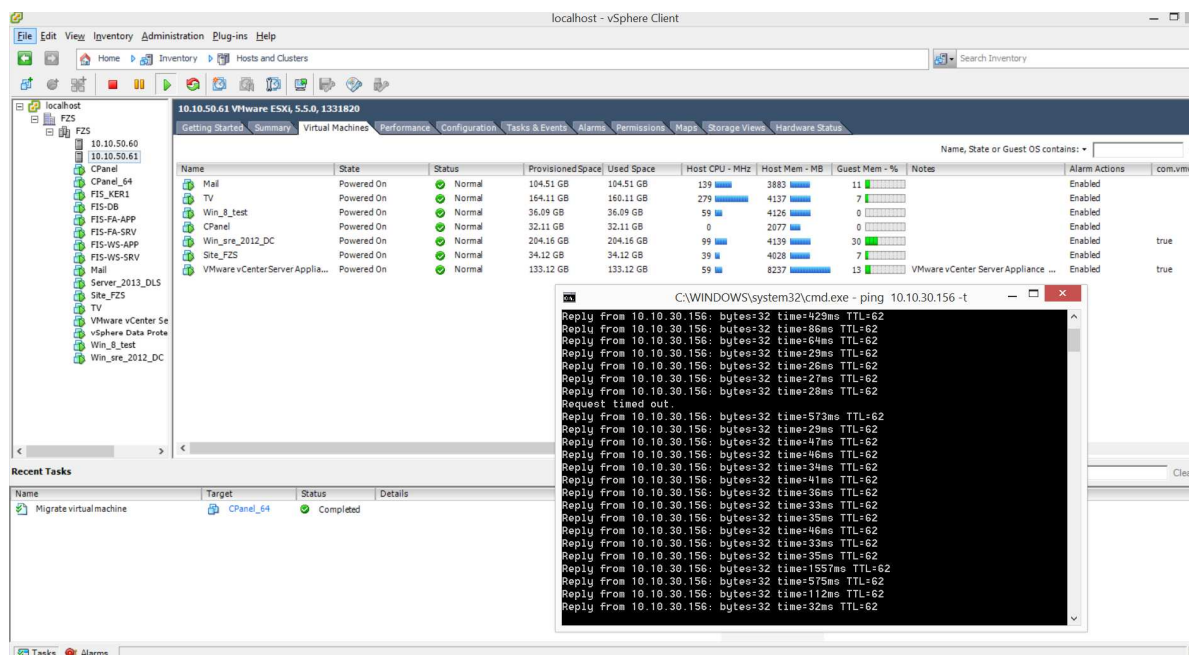
6.1.3 Migriranje virtuelne mašine u toku rada

Jedna veoma značajna mogućnost koju nudi ESX/ESXi jeste mogućnost migriranja virtuelne mašine “na živo” na drugi fizički server. Veoma je značajno napomenuti da je vrijeme migriranja prilično kratko. Ako koristimo **ping** da pratimo dostupnost mašine u toku migriranja možemo vidjeti da je mašina skoro čitavo vrijeme dostupna i da propadnu svega nekoliko **ICMP** paketa.



Slika 18 Prikaz kontrol panela za migriranje mašina

Na slici ispod možemo vidjeti **cmd** prozor koji pokazuje ping-ovanje virtualne mašine u trenutku njenog migriranja. Virtualna mašina je web server koji na sebi ima sajt koji je u produkciji i možemo vidjeti da je prilikom pingovanja propao samo jedan paket a trajanje migracije je trajalo manje od 30 sekundi. Što pokazuje da se na sajtu nisu mogle osjetiti nikakve promjene.



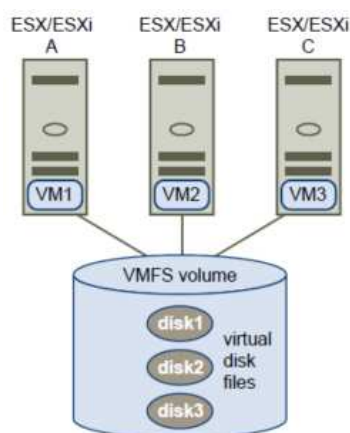
Slika 19 Prikaz ping-a web servera u toku migracije

6.2 Razumijevanje VMFS

Za čuvanje virtuelnih diskova ESX/ESXi koristi *storage*, pri tom on skriva podatke o skladištenom prostoru virtualnoj mašini i prikazuje ga najčešće u Virtual Machine File System (VMFS)¹⁶ formatu. To je **file system** format visokih performansi koji je namijenjen za čuvanje podataka virtualne mašine. VMFS može raditi sa više virtuelnih mašina. Ako se vaš VMFS fail nalazi na SAN-u onda ga ESX/ESXi hostovi vrlo lako mogu vidjeti i dodijeliti virtuelnim mašinama koje se produkuju na njima. Veoma je značajno da jedan VMFS fail se može nalaziti na više fizičkih uređaja, što znači da ukoliko se desi da nam zahvali prostor možemo dodati novi storidž i proširiti VMFS. ESX/ESXi sa više *Host-ova* istovremeno može pristupiti istom VMFS.

¹⁶ http://en.wikipedia.org/wiki/VMware_VMFS

Kada *Host-ovi* dijele zajednički *Volumen* teško je odrediti koji je pristupni period kojem host-u zbog različitosti aplikacija koje se izvršavaju. Zbog toga VMware preporučuje miksovanje mašina na hostovima kako bi se postigla ravnotežra na svim nivoima u isto vrijeme.



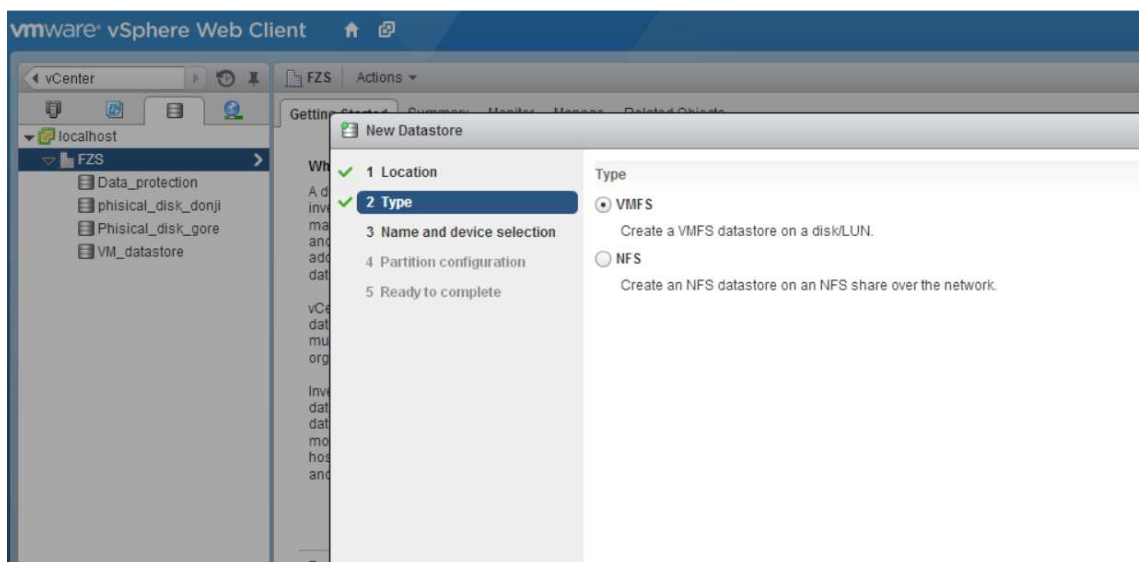
Slika 20 Dijeljenje VMFS na više hostova

6.3 Kako Virtuelna Mašina pristupa podacima na SAN-u

ESX/ESXi zapisuje podatke o virtuelnoj mašini na u fajlu VMFS koji je smješten na SAN-u. Procesi komuniciranja VM sa SAN-om opisani su u sledećim stavkama:

- 1) Kada operativni sistem (OS) koji se nalazi na virtuelnoj mšini hoće da komunicira sa diskom koji se nalazi na storidžu, on izdaje naređenja SCSI controleru, koji kod ESX/ESXi virtualizovan, on dalje komunicira sa VMFS failom koji se nalazi na storidžu.
- 2) Upravljački programi operativnog sistem virtuelne mašine komuniciraju sa virtuelnim SCSI kontrolerom.
- 3) Virtuelni SCSI kontroler prosleđuje komandu do VMkernel.
- 4) VMkernel obavlja sledeće zadatke.
 - a. Pronalazi fajl u VMFS koji odgovara virtuelnom disk mašine.
 - b. Mapira blokova podataka na virtuelnim diskovima sa odgovarajućem blokovima na fizičkom uređaju.
 - c. Šalje izmijenjen zahtjev I/O od VMkernel do fizičkog HBA.
- 5) Fizički HBA obavlja sledeće zadatke.
 - Paketi za I/O salju zahtjeve u skladu sa pravilima FC protokola.
 - Prenosi zahteve za SAN.

- 6) U zavisnosti od toga koji port HBA koristi za povezivanje na *fabric*, SAN *switch* dobija zahteve i usmjerava ga na uređaj za skladištenje na koji host želi da pristupi.

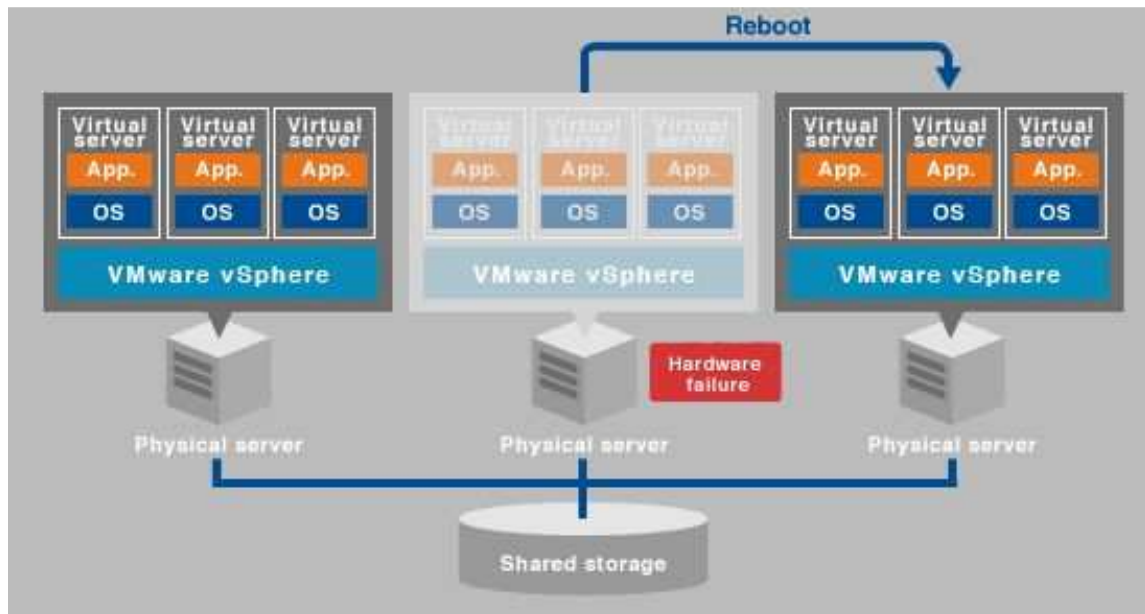


Slika 21 Primer dodavanja VMFS diska hostu

Ako su hostovi u klasteru kao što je slučaj na slici, dovoljno ga je mapirati na samo jednom Hostu *pool* automatski postaje vidljiv i na drugim hostovima u klasteru.

6.4 Redudanta na nivou hosta u ESX/ESXi klasteru

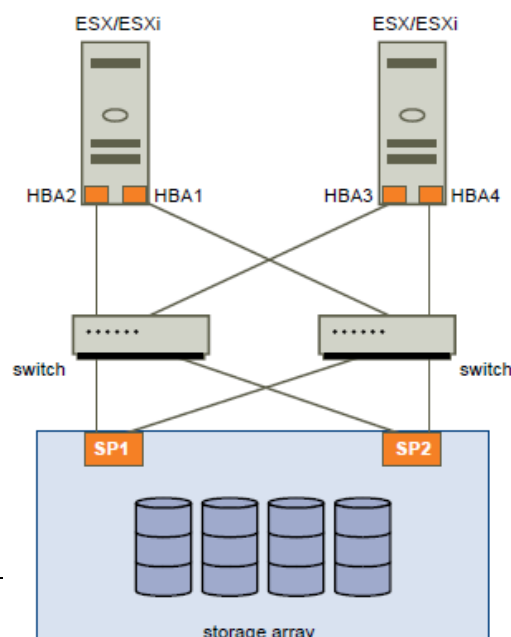
Kada ste krenuli u projektovanje informacionog sistema, prva stvar o kojoj se vodi mnogo računa jeste da sistem ima redudante. Da bi sistem bio dostupan 24h, 365 dana u godini mora imati redudantu na nivou svih komponenti koje učestvuju u radu i od vitalnog su značaja za rad sistema. Potrebno je imati redudante na nivou napajanja svih komponenti, redudante veza na nivou switcheva i routera, itd... Ako ste se izabrali VMware za izgradnju virtuelnog **data centra** sa ESX/ESXi imate mogućnost da kreirate klastere i u klastere fizičke serevere (host-ove). Kada su hostovi povezani oni rade kao jedan servere ukoliko se desi da jedan od servera „padne“ vCenter će automatski pobrinuti da prebaciti sve mašine koje su na serveru na druge servere koji su u klasteru.



Slika 22 Prikaz redundante na nivou Hosta

Ovo su jako značajne mogućnosti i dosta jednostavne za korištenje kada se dobro konfigurišu, ono što mana ovog rešenja jesu licence, koje su vjemoma restriktive i skupe, svaka automatika i udobnost se skupo naplaćuje.

SAN multipathing konfiguracija koja uglavnom pruža jednu ili više switch-eva u SAN i jedan ili više storidza za skladištenje podataka. Na slici 23 prikazano je više fizičkih veza sa svakim serverom i sa uređajem za skladištenje podataka. Na primer, ako HBA1 ili veza između HBA1 i FC *switch* padne, HBA2 preuzima i obezbeđuje vezu između servera i *switch*. Proces preuzimanja jedne HBA na drugi se naziva **HBA Failover**.



Slika 23 Failover kod FC

6.5 Konfiguracija LUN u ESX/ESXi

Kada konfigurišete LUN-ove morate imati plan kako želite da podesite storidž u onosu na VMFS. Kada treba da donesete odluku kako LUN-ovi treba da izgledaju imajte na umu sledeće stvari:

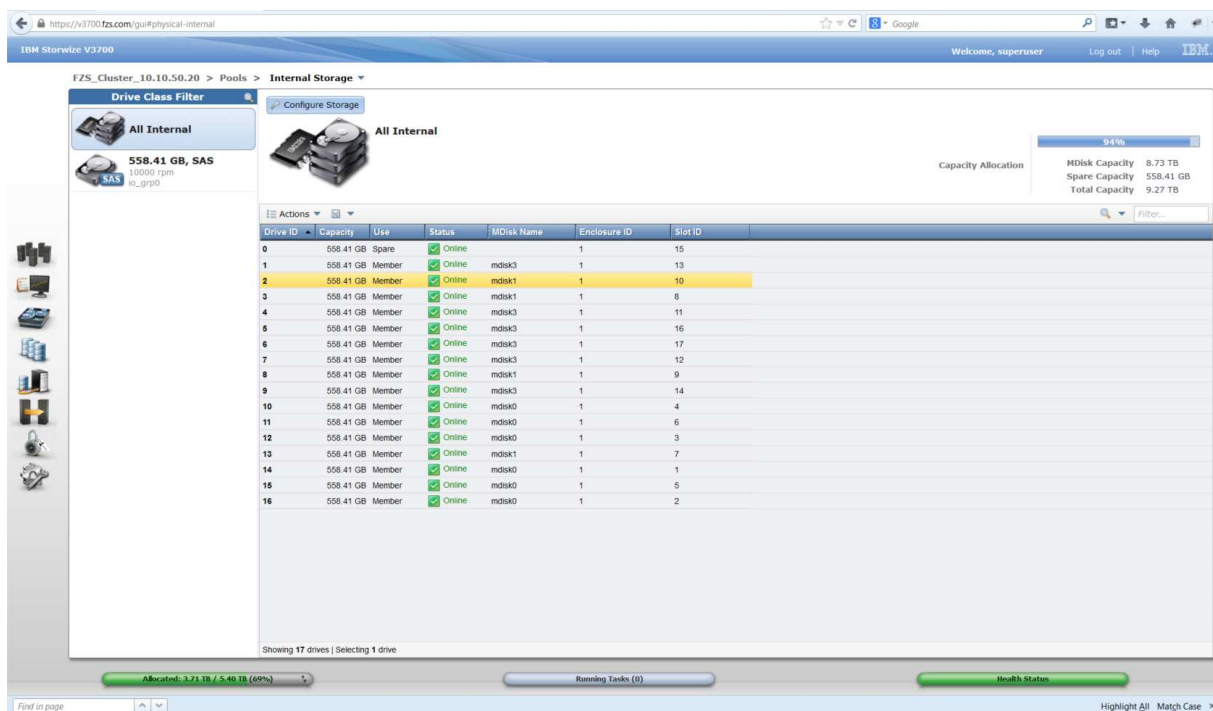
- Svaki LUN treba da bude u odgovarajućem RAID nivou i storidž treba da bude podešen shodno potrebama OS ili aplikacije koja se izvršava na toj virtuelnoj mašini,
- Dobro je da LUN ima samo jedan VMFS,
- Ako imate više **VM** koje pristupaju istom VMFS, vodite računa o dodjeljivanju prioriteta mašinam koji pristupaju diskovima.

Ako hoćete manje ili veće LUN-ove držite se sledećih savjeta:

- Kod većih LUN imate veću fleksibilnost kod kreiranje VM ne morate voditi računa o veličini virtuelnog diska,
- Kod većih LUN imate prostora za pravljenje više snapshots,
- Manji LUN-ovi su lakši za upravljanje.

6.6 Kreiranje novog poola i mapiranje hosta

U ovom dijelu je dat realan primjer konfigurisanja storidža u realim uslovima, storidž se veže na dva fizička servera preko SAN-a. Uređaj na kome je rađena konfiguracija je storwize IBM V3700.



Slika 24 Web interfejs storwize IBM V3700

Ovaj storidž u ovoj konfiguraciji u sebi sadrži 17 diskova iste brzine i kapaciteta, naravno jedan disk je **Spare**. Ovo je početni dio konfiguracije gdje treba primijeniti pravila konfigurisanja koja su objašnjena u prvom dijelu rada, a tiče se odabira RAID, koja je namjena diskova, itd... Ono o čemu treba voditi računa jeste da *Pool* koji su u različitim RAID trebalo bi da budu i u različitim **MDISK**¹⁷. MDISK ili upravljač disk je logička jedinica za fizički skladišteni prostor. MDISK nisu vidljivi za Host sistemima. MDisk se može sastojati od više fizičkih diskova koji su predstavljeni kao jedan logičan disk na mrežno skladištenje potataka (SAN). MDisk uvijek omogućava potrebne blokove fizičkom storidžu, čak kad nema jedan na jedan disk na korespondenciju sa fizičkim diskom. Svaki MDisk je podijeljen prema vrsti kojoj pripada (veličina, brzina,...). Kada se disk dodaje u *Pool* veličina diska mjeri u koji će MDisk biti dodijeljen zavisno od atributa storidža.

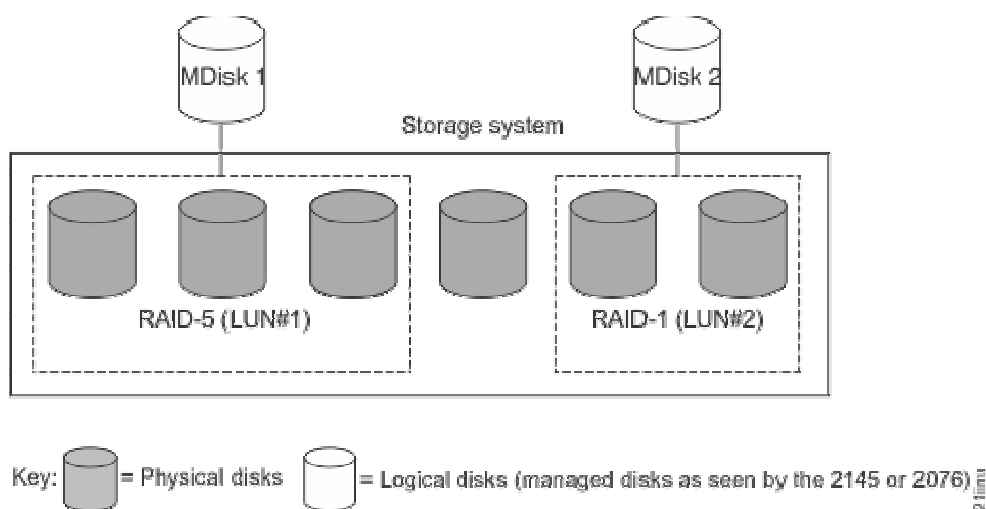
Pristupni režimi:

Pristupni režim određuje kako grupisani sistem koristi MDisk. Sledeća lista opisuje tipove mogućih režima pristupa:

17

http://pic.dhe.ibm.com/infocenter/svc/ic/index.jsp?topic=%2Fcom.ibm.storage.svc.console.641.doc%2Fsvc_mdisksovr_1bchav.html

- **Unmanaged** - Disk se ne koristi u sistemu
- **Managed** – MDisk je dodijeljen *pool*-u u skladištenom prostoru i omogućava korišćenje produženog volumena
- **Image** - MDisk je dodijeljen direktno *volumenu* sa mampiranjem jedan na jedan
- **Array** - MDisk predstavlja skup diskova u RAID-u za interni storidž



Slika 25 Storiđž sistem i MDisk

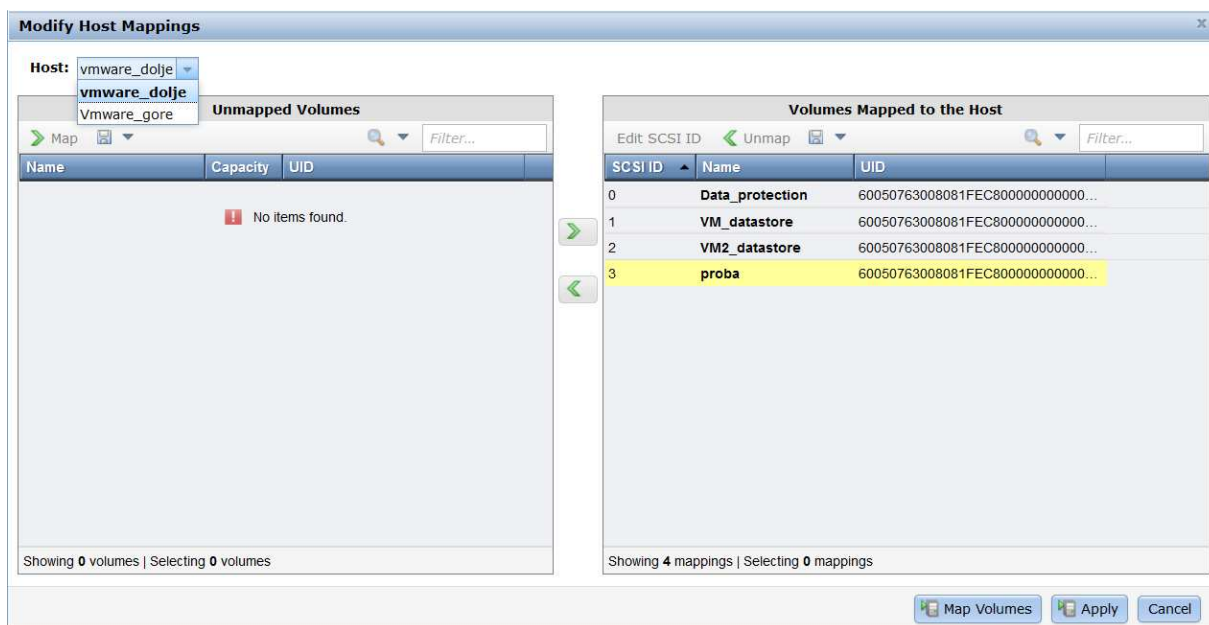
6.6.1 Kreiranje Pool

Kod kreiranja *Pool*-a biramo u kom RAID-u će se *Pool* nalaziti i biramo da diskovi budu u istom MDisk. Na konkretnom primeru kreirana su dva *Pool*-a, jedan je u RAID5, drugi je u RAID10. U prvom dijelu rada bilo je dosta priče o tome kako se koriste RAID-ovi i njihove karakteristike. *Pool* koji se nalazi u RAID5 se koristi za backup, razlog zašto je odabran RAID5 jeste zato što za rezervne kopije brzina upisa i čitanja nije od presudnog značaja, a RAID 5 ne zauzima mnogo resursa i iskorišćenost je velika. Za *Pool* koji se koristi za produkciju na kome će biti virtualne mašine odabrao sam RAID10, on zauzima duplo više memorije od one koju možete da koristite ali nudi dobre performase što je jako značajno kada je osjetljivost podataka velika.

Sledeće korak je kreiranje *Volume*, ono o čemu ovdje treba voditi računa da se *volumes* kreiraju sa strane storidža a ne sa strane VMware, ako se kreiraju i sa jedne i sa druge strane može doći do greške i to nije dobra praksa.

6.6.2 Mapiranje kreiranog Pool

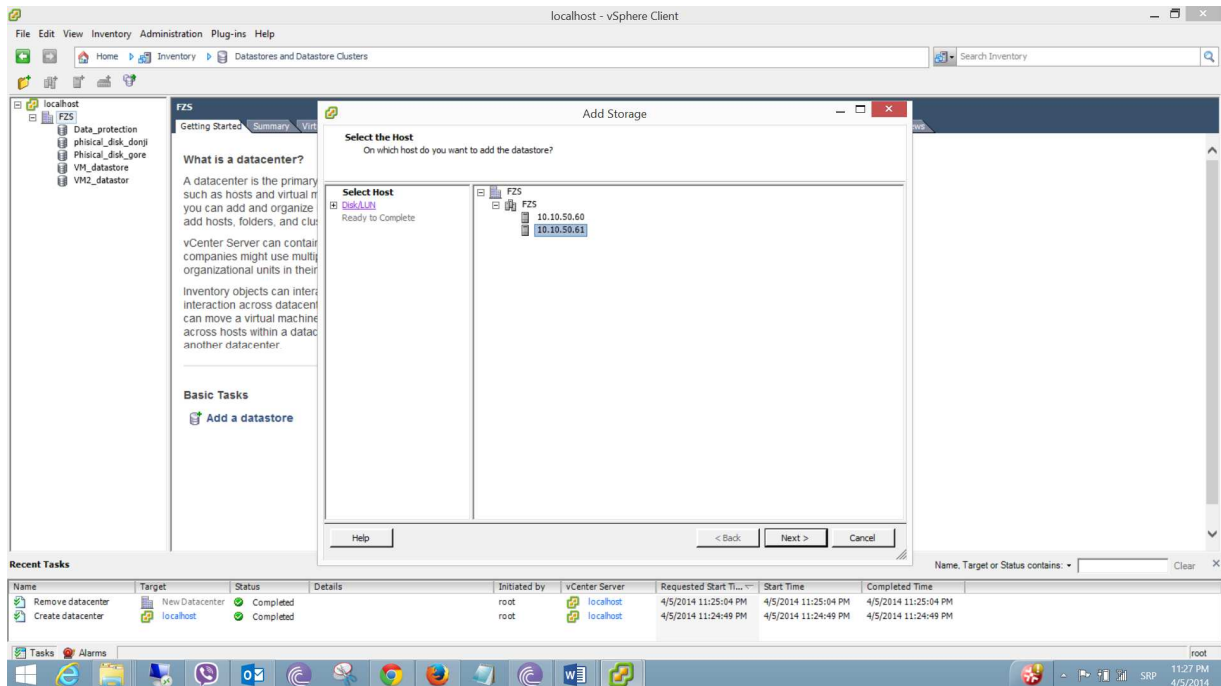
Prvo treba dodati *Host-ove* i portove koji su povezni. To radimo zbog toga jer je potrebno da storidž zna za svaki host u SAN-u i da zna za svaki link do SAN-a, jer ukoliko dodje do greške storidž saobraćaj se može prenijeti preko drugog linka. Kada smo uspješno dodali Host-ove sledeći korak je da dodamo *volume* na *host* kako bi se mogao vidjeti od strane ESX/ESXi. Slika ispod nam pokazuje kako se to može uraditi. Isti postupak mapiranja treba ponoviti i za sve druge fizičke servere (host) koji se nalaze u klasteru.



Slika 26 Mapiranje *Volume* na jednom od hostova

6.7 Dodavanje Volumena od strane ESX/ESXi u klaster

Dodavanje se vrši preko **vCentra**, dodavanje se može uraditi preko web klijenta i preko **vShere** aplikacije, bolja je praksa uraditi to preko **vShere**. Sve što je potrebno je pokrenuti dodavanje **datastore** na jednom od host-ova. Kada LUN dodamo na jednom od host-ova on se automatski može vidjeti na svim host-ovima koji se nalaze u klasteru. Na slici ispod možete vidjeti primer dodavanja LUN-a u klaster.



Slika 27 Dodavanje Volume na jednom od servera

7 SAN Storage Backup faktori

U SAN okruženju, backup ima dva cilja. Prvi cilj je da arhivira *online* podatke na *offline* medi. Ovaj proces se ponavlja periodično sa svim *online* podacima po vremenskom rasporedu. Drugi cilj je da se omogući pristup *offline* podacima ukoliko je neophodno oporaviti oštećene podatke. Na primjeru oporavka (recovery) baze, ona često zahtijeva pronalaženje arhiviranih fajlova koji nisu trenutno online.

Zakazivanje rezervne kopije zavisi od više faktora:

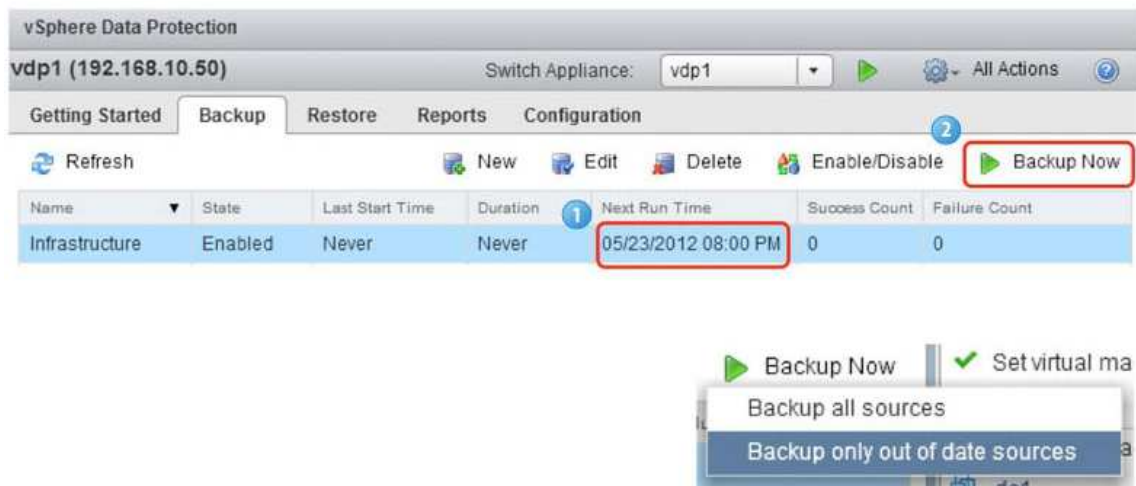
- Identifikacija kritičnih aplikacija koje zahtijevaju češći backup u okviru datog vremenskog perioda.
- Rezervna kopija i vrijeme za koje se rezervna kopija izvrši. Proverite koliko je potrebno vremena da se vaša rezervna kopija izvrši, koliko treba čekati da se pokrene poslednja kopija.
- Ako se koristi ponavljanje sinhronizacije potrebno je imati veću propusnu moć na linku sa primarnim i sekundarnim propusnim uređajima.
- Generalni uticaj na SAN okruženje i performanse (dok se izvršava bekapovanje) i druge aplikacije
- Vremensko zakazivanja *backup-a* (ukoliko je *backup* zakazan u vrijeme kad je produkcija izvršava mnoštvo zahtjeva može doći do usporavanja sistema)
- Vrijeme zakazivanja svih rezervnih kopija u *datacenter*
- Vreme potrebno da se napravi pojedinačna rezervna kopija
- Dostupnost resursa za arhiviranje, obično je to *offline* mediji

Bitna stvar je kada dizajnirate strategiju backup-a da vodite računa o backup-u svake aplikacije, neophodno je da tačno znate vrijeme za koje će svaka od aplikacija da pokrene svoju rezervnu kopiju. Na primer, ako backup ima mnogo kopija i vrijeme za recovery je mnogo dugo, onda je potrebno ispitati raspored backup-ova i optimizovati ga. Ako određena aplikacija zahtijeva *recovery* u određenom vremenskom roku, *backup* proces treba da obezbijedi svojim rasporedom da se ovaj proces izvede nesmetano. Brz oporavak može zahtijevati upotrebu online *backup-a* ukoliko je pristup *offline* medija spor.

VMware u je razvio servis **vSphere Data Protect**¹⁸ koji je namijenjen da bude pojednostavljeni backup virtuelnih mašina. Ovaj servis je veoma jednostavan za korištenje i veoma koristan, on

¹⁸ <http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vmware-data-protection-administration-guide-51.pdf>

dolazi u vidu virtuelne mašine koja se implementira u vCentar, lako se pokreće i koristi. Veoma je zahvalan za pravljenje rezervnih kopija virtuelnih mašina, možete birati koja VM se bekapuje i u koje vrijeme, *Data Protect* u zadano vrijeme odradi backup na živo bez gašenja mašine što je veoma značajno.



Slika 28 Data Protect grafički prikaz

8 Zaključak

Kao što smo vidjeli konfiguracija SAN klastera je veoma složena, da bi se kvalitetno konfigurisao skladišteni klaster potrebno je poznavati više tehnologije i razumjeti načine na koji oni funkcionišu, da bi mogli da odabremo na pravi način za konfigurisanje skladištenog prostora shodno našim potrebama i potrebama organizacije. Vidjeli smo sta je *storage* kako ga možemo povezivati sa serverima i kako možemo podešavati diskove da bi dobili otpornost na greške.

Poseban osvrt u radu je posvećen SAN tehnologijama. SAN nam omogućava mnogo toga u pogledu mogućnosti i iskorištenja prostora. Vidjeli smo da je Storage Area Network je mreža visokih performansi namijenjena za prenos blokova podataka. Pokazao sam koji su načini povezivanja *storage* sa serverima preko SAN-a i koje su razlike prednosti i mane tih povezivanja. U Storage Are Network se može povezati neograničen broj *storage* uređaja i servera. Sto predstavlja veliki napredak u odnosu na DAS gdje postoje ograničenja broja *storage* uređaja koji se mogu povezati. Napredak nam donosi i u pogledu udaljenosti *storage* i servera. Do sad DAS nam je nudio mogućnost udaljenosti od servera svega nekoliko metara, sad nam SAN nudi povezivanje uređaja bez ograničenja, to nam omogućava iSCSI SAN. SAN se može povezivati preko FC koji nudi visoke prefomanse (I/O) prenosa blokova podataka i mogućnost udaljavanja do 10km od servera (Postoje novi načini za povećanje mogućnosti povezivanja optičkim vezama do nekoliko stotina kilometara, ali su ove metode i skupe i složene za primenu) sto ga čini podređenim u odnosu na iSCSI SAN koji može da poveže SAN mreže u izdvojenim predstavništvima korišćenjem već postojećih gradskih mreža (MAN – metropolitan area network) i regionalnih mreža (WAN – wide-area networks).

SAN mreža nam daju velike benefite u pogledu iskorištenja prostora, jer omogućava iskorištenje maksimalnog kapaciteta diskova na skladištenom prostoru, sto je bio problem kod DAS tehnologije. Takođe SAN tehnologija je donijela benefite u pogledu brzine prenosa blokova podataka kroz svoju mrežu, sto je problem kod NAS tehnologije. Jer je NAS tehnologijama zasnova na LAN mreži i cijela komunikacija sa *storage* se obavlja preko lokane magistrale, pristupanje podacima je sporije i zasniva se na prenuosu podataka, a ne prenosu blokova podataka kao kod SAN-a.

Mana SAN-a je, sto je veoma skupa tehnologija, mnogo zavisi i od toga na koji način se implementira i koje funkcionalnosti se očekuju. Pored toga što je skupa za implementaciju, skupa je i za održavanje. Istrazivanja koja su sprovele neke od veklikih svjetskih kompanija koje koriste SAN, govore da su se ne malo povećali troškovi održavanja skladištenog prostora.

Bezbijednost podataka može biti još jedan problem, pogotovu ako se koriste FC veze, sto sam opisao u radu.

Tehnologije koje smo koristili za implementaciju konkretnog informacionog sistema odnose se na veće data centre, one organizacije koje su spremne da izdvoje veću količinu novca za opremu i za mnoge licence koje su neophodne za puštanje u produkciju navedenih proizvoda. Praksa je pokazala da je ESX/ESXi dobro rešenje za administriranje *data-centra*, da ima mnogo opcija i mogućnosti, lako je i jednostavno održavanja. Mada ovakvo uređenje IT infrastrukture je namijenjeno visoko platežnim organizacijama. Da bi sistem imao smisla moraju se koristiti najmanje dva servera istih ili sličnih performansi i storage mora biti vezan sa pouzdanom vezom velike propuste moći, to nam protvrđuje navode da ova konfiguracija mnogo košta.

ESX/ESXi omogućava da usled *pada* jednog servera, drugi server sam aktivira sve virtuelne mašine na sebi i to sve može da uradi toliko brzo da krajnji korisnik ne osjeti baš nikakvu promjenu ako u tom trenutku pristupa serveru. Ali loša vijest je ta da se ova mogućnost od strane VMware dodatno naplaćuje i to jako mnogo. Jeftinija opcija je da ESX/ESXi sam prebaci mašine na drugi host ali morate čekati da se VM na drugom serveru ponovo podignu, sto je isto prihvatljivo sobzirom da dobijete servis u produkciji u roku od par minuta. Ova opcija se dodatno plaća ali je mnogo pristupačnija od prve.

Posebno morate voditi računa za koje mogućnosti imate licencu i kada vam licence ističu, VMware vam dozvoljava da u probnoj verziji možete konfigurisati sve, ali ako nemate licencu za određene funkcije, kada aktivirate sistem on vam obriše podešavanja za koja niste imali licencu, sto vas može neprijatno iznenaditi ako ste konfigurisali čitavu virtuelnu mrežu, ili mapirali storage a nemate licencu za taj link koji koristite, itd...

Zaključak je da što veći sistem imate to korištenje FC SAN i ESX/ESXi sve više ima smisla upotrebljavati ga. Mogućnosti koje pružaju mnogo olakšavaju rad administratora, jer pružaju mnogo prostora za manipulaciju, sto znači da administratori mogu brzo i lako rešavati novonastale probleme i testirati nove mogućnosti, što ga čini omiljenim među administratorima.

9 LITERATURA

- [1] IBM - Introduction to Storage Area Networks and System Networking -
<http://www.redbooks.ibm.com/>
- [2] Mikro knjiga - Konfigurisanje skladišnog prostora i klastera servera
- [3] SANS Institute InfoSec Reading Room - Fibre Channel Storage Area Networks: An Analysis From A Security Perspective
- [4] Cisco – Storage Area Networking Protocols and Architecture -
<http://www.cisco.com/networkers/nw04/presos/tech/docs/OPT-2T01.pdf>
- [5] Storage Area Network Implementation on an Educational Institute Network Computer Networking and Communication
- [6] HP P4000 LeftHand SAN Solutions with VMware vSphere Best Practices
- [7] Exam Ref 70-417, J.C. Mackin, Microsoft Press
- [8] www.wikipedia.org
- [9] www.webopedia.com
- [10] www.cs.uwaterloo.ca
- [11] http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2FPDF%2Fic_pdf.html
- [12] <http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-installation-setup-guide.pdf>
- [13] <http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vmware-data-protection-administration-guide-51.pdf>
- [14] http://www.vmware.com/pdf/vsphere4/r41/vsp_41_san_cfg.pdf
- [15] http://pic.dhe.ibm.com/infocenter/svc/ic/index.jsp?topic=%2Fcom.ibm.storage.svc.console.641.doc%2Fsvc_mdiskovr_1bchav.html

[16] http://pic.dhe.ibm.com/infocenter/storwize/v3700_ic/index.jsp