01 - Šta je cloud?

Cloud je apstraktan koncept koji treba da zadovolji odgovarajuće celine. To je model koji treba da obezbedi pristup resursima (bile to aplikacije, dokumenti, hardver ili nešto drugo) korisniku u svakom trenutku. Cloud možemo smatrati i kao operativnim sistemom za data centre, upravlja resursima i definiše životni ciklus aplikacije.

Pet osnovnih karakteristika cloud-a

1. **On-demand self-service**
   Omogućava pristup resursima na cloud-u kad god su zahtevani. Veoma brzi odgovori bez uplitanja ljudskih resursa. Obično se pristupa preko nekog portala ili kontrolnog panela.
2. **Broad network access**
   Omogućava pristup svakom resursu na cloud-u sa bilo koje tačke.
3. **Resource pooling**
   Sami definišemo koliko želimo resursa - npr. Dropbox pored inicijalne besplatne verzije ima u ponudi i resource pool-ove tj. predefinisane pakete sa više prostora, ili Office365 u kojem definišemo koje servise želimo da koristimo.
4. **Rapid elasticity**
   Resursi trebaju da budu prilagodljivi našim potrebama kao korisniku, da mogu u trenutku kojem su nam potrebni budu dostupni, a kada nam više ne trebaju da ih jednostavno vratimo provajderu. Primer : Office365 aplikacije, iznajmljivanje filma preko D3.
5. **Measured service**
   Način naplaćivanja servisa. Dropbox npr. meri kapacitet tj. naplaćuje po kapacitetu.

Tri servis modela cloud-a

Servise u oblaku možemo da upotrevljavamo na tri načina - kao infrastrukturu, platformu ili softver.

1. **Infrastructure as a service (IAAS)**
   Podrazumeva iznajmljivanje računarskih resursa kao što su procesor, memorija, disk i operativni sistemi plaćeni u zavisnosti od toga koliko su upotrebljivani. Ovde se radi o resursima kao komponentama servera, pa infrastruktura uključuje i operativni sistem.
2. **Platform as a service (PAAS)**
   Uz infrastrukturne resurse uključuje i platformu za razvoj aplikacija. Mi smo vlasnik operativnog sistema i sve unutar njega mi radimo.
3. **Software as a service (SAAS)**
   Najam gotovih aplikacija. Obično dobijamo samo kredencijale (korisničko ime i lozinku) sa kojima se prijavljujemo na odgovarajući sajt i dobijamo sve aplikacije koje smo zakupili. Mi smo vlasnik krajnje aplikacije i ne vodimo računa o onome što se ispod dešava (npr. na kojoj infrastrukturi se to vodi, u kojem operativnom sistemu se izvršava, da li je dovoljno zaštićeno i sl.).

Četiri razvojna modela cloud-a

1. **Private cloud**
   Kompanija koristi arhitekturu i pokreće cloud servere unutar svog data centra.
2. **Community cloud**
   Model koji predstavlja kombinaciju private i public cloud-a koji koristi tematska grupa korisnika tipa cloud medicinskih institucija, fakulteta... Primer - na osnovu našeg ID-a zdravstvene kartice možemo iz bilo kog doma zdravlja da imamo podatke o istorijatu našeg zdravlja. Privatni cloud se povezuje sa infrastrukturom public cloud-a, čime public cloud faktički postaje ekstenzija privatnog kako bi se formirao jedan cloud.
3. **Public cloud**
   Model u kojem treće lice dostavlja resurse generalnoj javnosti preko interneta. Kompanije ne moraju da prave i održavaju cloud server u svojim prostorijama.
4. **Hybrid cloud**
   Nalik community cloud-u, osim što ne mora da bude neka tematska grupa. Kombinuje javne i privatne cloud resurse kako bi nam pomogao u poslovanju. Na primer, upotreba public cloud-a za skladištenje podataka i primena privatnog cloud-a za pokretanje proizvodnje.

Data centar se sastoji od nekoliko ključnih komponenti :

- Neka mreža (npr. pristupna, backend, ethernet...)
- Computer node-ovi (server, mašine koje obavljaju neke osnovne IO operacije vezane za aplikacije i servise koji se vrte tu)
- Storage komponenta na kojoj se skladište podaci.

Pasivna komponenta predstavlja skladište u koje stavljamo sirove komponente koje će aplikacije kasnije koristiti. Na primer, prilikom boot-ovanja sa mreže, ceo IMG fajl se nalazi na skladištu i određena hardverska komponenta prilikom pokretanja određene aplikacije povlači ceo taj IMG i obradi podatke koji su joj portebni. Kada završi sa njima vraća taj kompletan IMG u centralnu lokaciju za skladištenje.

Zašto koristiti cloud?

- **Ekonomija velikih brojeva**
  Veliki dobavljači nabavljaju servere mnogo jeftinije nego što mi možemo.
- **“Pay as you go” model**
  Za dodatne resurse ne moramo da kupujemo nove resurse već ih iznajmimo od provajdera. Ako nam ne trebaju postojeći resursi možemo da otkažemo njihovu upotrebu i ne plaćamo za njih.
- **Niska početna cena**
  Nemamo početna ulaganja i dugoročne ugovore.
- **Visoka dostupnost**
  Naše aplikacije rade 24/7/365.

02 - Data Center - High Level Design

Osnovne komponente data centra :

- Ethernet (frontend) mreža
- Serverska platforma
- Storage (backend) mreža
- Storage platforma

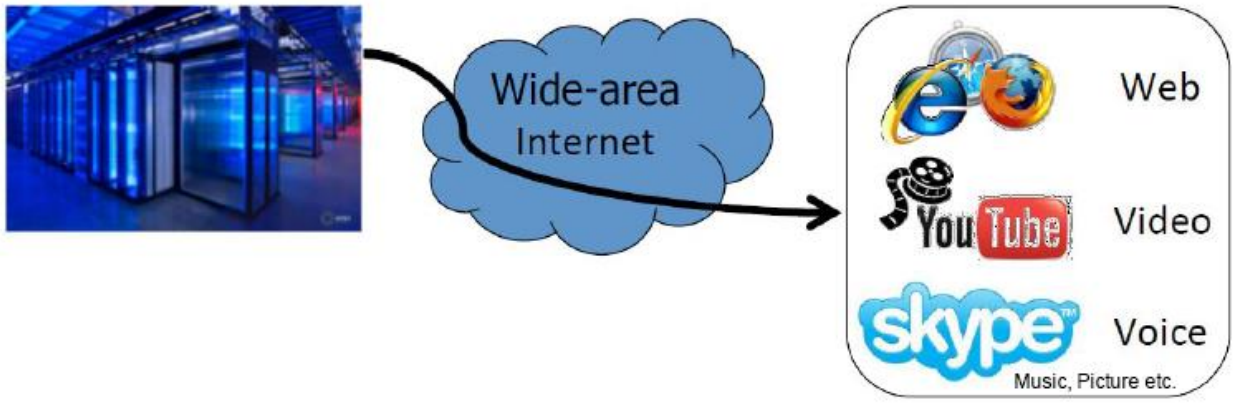
Osnovne podele tipova podataka u data centru :

- Produkcijski podaci - Production data
- Backup / Archive podaci

Osnovne komponente zaštite podataka u data centru :

- Lokalna i udaljena zaštita produkcijskih podataka
- Lokalna i udaljena zaštita backup / archive podataka

Frontend mreža obuhvata vezu između data centra i korisnika tj. web-a preko Wide Area Internet-a.



Backend mreža obuhvata vezu između server resursa i centralizovanog storage dela gde se podaci čuvaju.

Virtualizacija omogućava povezivanje više različitih hardverskih uređaja u kojima ćemo resurse naše aplikacije držati kao jedinstvenu celinu. Između tih hardvera stavljamo neki virtualizacioni kanal npr. između dva računara, i šta god se instalira na prvom radiće i na drugom, npr. nešto malo radi na jednom računaru, malo na drugom. Virtualizacija omogućava dinamičku relokaciju komponenti (utilization) i 24/7 dostupnost resursa unutar jednog data centra.

RAID - Redundant Array of Independent Disks

- **RAID 0** - Files are striped across discs, no redundant info, any disk failure results in data loss.
- **RAID 1/0** - Mirrored disks, data is written to two places, on failure just use surviving disk.
- **RAID 5** - Like data, distribute parity over all disks. Supports 1 disc failure (5 HDDs used).
- **RAID 6** - Level 5 with an extra parity (extra HDD). Can tolerate two failures.

03 - Cloud Protocols

Protokol je forma po kojoj se komunicira na nekom resursu. Skup pravila koje obe strane moraju ispoštovati kako bi se odvila komunikacija. Postoje lokalni protokoli (u okviru samog uređaja) koji su skoro istovremeni i remote tj. mrežni protokoli koji se mere u ms.

HTTP Cookie je tekstualna datoteka koja se čuva u veb-pregledaču dok korisnik pregleda neki veb-sajt. Kada korisnik u budućnosti pregleda taj isti sajt, sajt može dohvatiti podatke koji su sačuvani u kolačiću kako bi bio obavešten o prethodnoj korisničkoj aktivnosti nalik podacima i vremenu prijave, koje su stranice posećene i sl.

HTTP protkol se koristi za isporuku sadržaja preko web-a. HTTP je klijent server protokol u kojem klijent započinje komunikaciju. Nalazi se na aplikativnom sloju i zasniva se na TCP/IP protokolu.

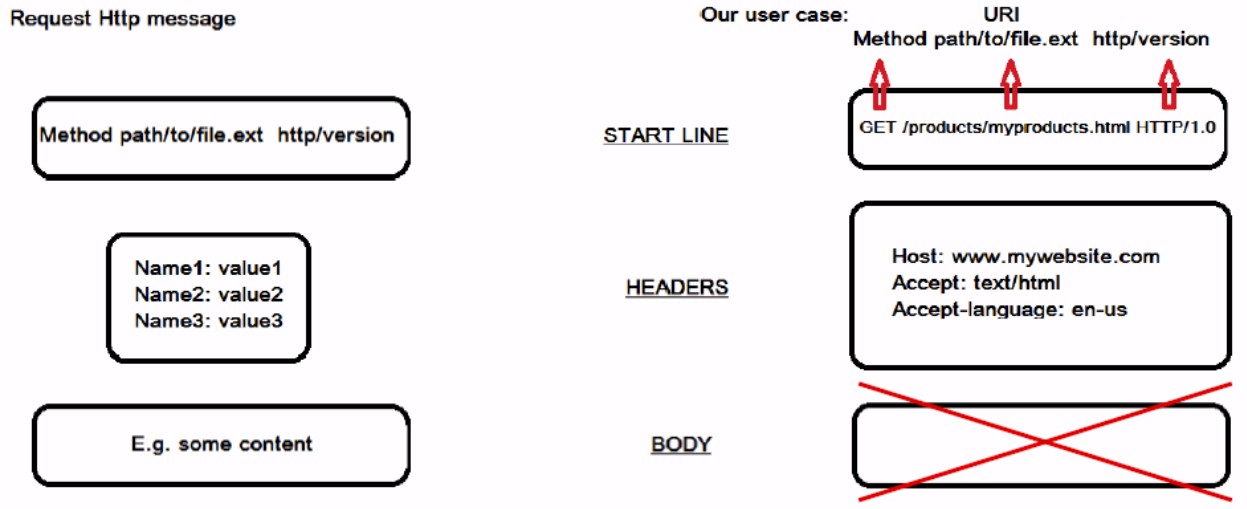
- **HTTP je protokol bez konekcije (connectionless protocol)**
  Nakon slanja zahteva, klijent se diskonektuje sa servera, i onda kada je odgovor spreman server ponovo uspostavlja vezu i dostavlja odgovor (response).
- **HTTP može da dostavi bilo kakav tip podatka**
  Sve dok oba uređaja u komunikaciji su sposobni da ga pročitaju
- **HTTP je protokol bez stanja (stateless)**
  Klijent i server se znaju međusobno samo za vreme trenutnog zahteva. Ukoliko se on zatvori, a dva uređaja žele da se povežu ponovo, oni će morati da obezbede informacije jedan drugom ispočetka, i veza će se odvijati kao ona prva.

Tipična HTTP poruka se sastoji iz tri dela :

1. **Start line** (metode zahteva, resurs)
2. **Headers** (sadrže informacije (meta-podatke) napisane u običnom tekstu)
   Language, Character set, Content type, Cookies...
3. **Body** (opcionalan)

Podaci u tri dela HTTP poruke će se razlikovati u zavisnosti da li se radi o **zahtevu** ili **odgovoru**.

Request - HTTP zahtev

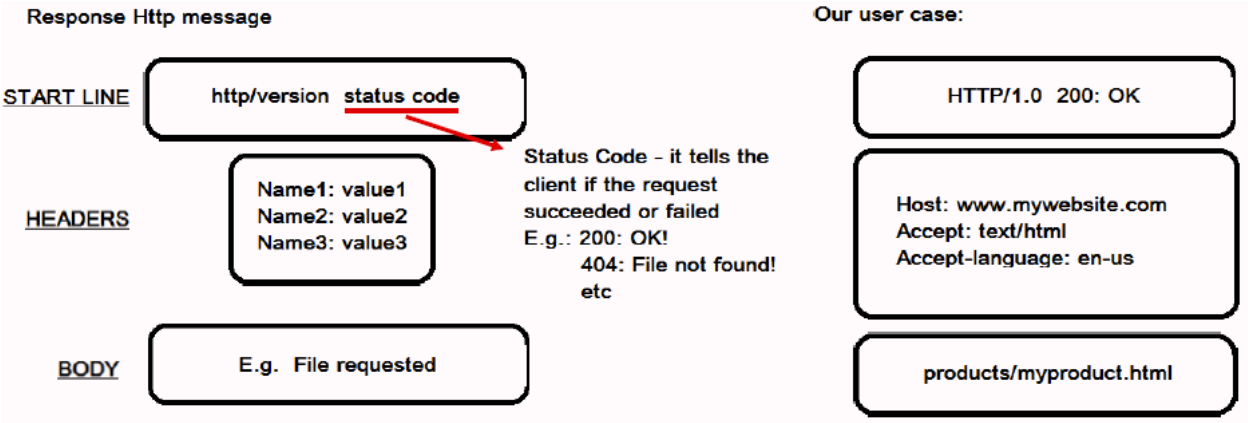


Metod govori serveru šta da uradi :

- **GET** - server šalje nove podatke.
- **POST**- server skladišti podatke u bazu podataka.
- **PUT** - server skladišti podatak.
- **DELETE** - govori serveru da ukloni podatak.

Razlika između POST i PUT je ta što se POST koristi za izmenu i obnavaljanje (modify and update) resursa, dok se PUT koristi za stvaranje ili prekopisanje (create or overwrite).

Response - HTTP odgovor



Statusni kodovi

100 - Informacija

200 - OK

300 - Redirekcija

400 - Klijentska greška

500 - Serverska greška

04 - Cloud bezbednost

Cloud computing prikuplja sve resurse i podatke na jednom mestu - centralizacija omogućava efikasnost upravljanja velikim brojem usluga koje koristi ogroman broj korisnika.

Kompanije imaju velike količine podataka koje se ne smeju iznositi van kompanije tipa finansijskih izveštaja, novih proizvoda i sl. Isto tako krajnji korisnici ne žele da drugi saznaju previše o njima (porodica, broj telefona), kao ni neke njihove važne informacije (brojevi kreditnih kartica npr.) Curenje podataka može dovesti do ekonomskog gubitka ili sudskog spora.

Bezbednost u Cloud-u je stepen zaštite od opasnosti koji se fokusira na hardver mehanizme, softversku ranjivost i sakrivanje informacija - maliciozni napadači žele da ukradu podatke ili unište sistem. Evolucija bezbednosti se može podeliti na tri celine :

Bezbednosne tehinke u Cloud-u osiguravaju osnovni mehanizam zaštite i dele se na sledeće delove :
- **Autorizacija** definiše pravo pristupa resursima i odbija zahtev nepoznatog korisnika.
- **Šifrovanje** *(encryption)* čini info. nečitljivim za svakoga osim onih koji poseduju odg. ključeve za dešifrovanje.
- **Izvor neprekidnog napajanja** *(UPS - Uninterrupted Power Supply).*
- **Backup podataka / servera** sprečava gubitak podataka i prekid rada servera logičkih grešaka.
- **Disaster recovery rešenja** - zaštita podataka na udaljenim lokacijama usled pr. katastrofa *(zemljotres)*.

Bezbedno upravljanje u Cloud-u - izvršenje jedne ili više politike bezbednosti :
- **Politika upravljanja pristupima** *(access control policy)* vrši autorizaciju grupe korisnika da bi izvršili skup operacija nad resursima.
- **Neka vrsta industrijskih smernica** za obuku i učenje zaposlenih o računarskoj tj. IT bezbednosti.
- **Planovi reagovanja na incidente** *(incident response plans)* su procedure delovanja u vanrednim okolnostima.

Cyber security predstavlja zaštitu sajber sredstava i kritičnih podataka.
- **Intrusion Prevention System (IPS)** - prate i beleže informacije o mreži i sistemske aktivnosti za maliciozne aktivnosti.
- **Social engineering** - manipulacija ljudima u obavljaju kriminalnih radnji i odavanja informacija.

Bezbednosne kontrole štite sve slabosti sistema i smanjuju efekat napada.
- **Kontrole za odvraćanje** *(Deterrent controls)* - cilj smanjenje napada na cloud, obaveštavaju potencijalne napadače da će biti po njih štetnih posledica.
- **Preventivne kontrole** *(Preventive controls)* - eleminišu ranjivosti, npr. snažna autentifikacija korisnika oblaka.
- **Kontrole otkrivanja** *(Detective controls)* -detektuju i reaguju na incidente, u slučaju napada signaliziraju preventivne ili korektivne kontrole kako bi rešile problem.
- **Korektivne kontrole** *(Corrective controls)* - ograničavaju štetu, stupaju na snagu tokom ili nakon incidenta, npr. vraćanje sigurosnih kopija sistema u cilju njegove rekonstrukcije.

Bezbednost u oblaku se grupiše na **Security and privacy** i **Data security**.

Security and privacy- sigurnost i privatnost u oblaku.
- Identity management - upravljanje identitetom. Svako preduzeće ima svoj sistem identifikovanja za kontrolu pristupa informacijama i resursima, cloud provajderi ili integrišu taj sistem ili koriste svoj.
- **Physical security** - fizička sigurnost gde cloud provajderi fizički obezbeđuju IT hardver od neovl. pristupa.
- **Personnel security** - sigurnost osoblja, npr. sigurnosni pregledi regruta, programi obuke...
- **Privacy** - privatnost, svi kritični podaci su maskirani ili šifrovani i samo ovlašćeni korisnici imaju pristup podacima u celosti.

Data security - bezbednost informacija u Cloud-u, sredstva bezbednosti informacija za izbegavanja pristupa i upravljanja podataka bez autorizacije. Postoje tri osnovna principa bezbednosti informacija :
- Confidentiality - poverljivost podataka
Korisnik može pristupiti osetljivim informacijama samo kada za to dobije dozvolu. Podaci mogu biti odvojene u različite slojeve bezbednosti : normal > security > top secret.
- Integrity - integritet podataka
Podaci ne mogu biti izmenjeni bez detekcije promena, oni ostaju tačni i nepromenjeni u toku prenosa istih.
- Availability - dostupnost podataka
Korisnici mogu dobiti podatke kada su im potrebni bilo gde ili bilo kada.

Proboj (penetration) - prikupljanje javno dostupnih informacija, pokušaj nalaženja slabosti i prava pristupa.
Napad - krađanja/brisanje podataka i obaranje sistema.

Scenariji napada u Cloud sistemu :
- **Maliciozni napadi** - napadač se **krije na Internetu** i pokušava da nanese štetu - krađa informacija, šteta.
- **Namere hakerisanja** - napadač se **ne krije na Internetu** i pokušava da nanese štetu.
- **Zabava ili samodokazivanje** - napadač želi da se zabavi ili pokaže veštine - patriotski sajtovi npr.

Scenariji tehnike napada u Cloud sistemu :
- **Bruteforce** - nasilni upad, šifra je kao osnovni metod autentifikacije meta napada.
- **Phishing** - simuliranje sigurne Web lokacije da bi se od korisnika dobile poverljive informacije.
- **Sniffer** - skeniranje, presretanje paketa u saobraćaju; provajderi koriste SSL/TSL krip. protokole.
- **Denial-of-Service** - pokušaj da se računarski resurs / usluga učini nedostupnim, haker šalje mnogo zahteva na server tako da server ne može da odgovori pravim korisnicima. **DDoS** kada više sistema napadne.
- **Botnet** - hakeri koriste trojance i crve preko kojih upravljaju mnogim računarima, botnet je kolekcija kompromitovanih računara koji se koriste u maliciozne svrhe napada (spam i DoS na neki server).

05 - Cloud infrastructure - Physical layer

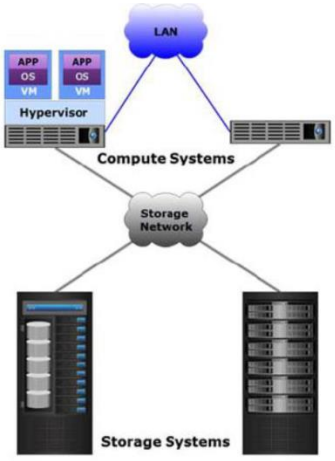
Fizički sloj cloud infrastrukture se sastoji od fizičkih *compute*, *storage* i *network* resursa.
- **Sistemi za obradu** pokreću softver provajdera i klijenata
- **Sistemi za skladištenje** skladište podatke aplikacija
- **Mrežni sistemi** međusobno povezuju sisteme za obradu, kao i sisteme za skladištenje.

Platforma za obradu (hardver, firmware i softver) pokreće provajderov i klijentov softver.
Dostavljaju se korisniku na dva načina :
- *Shared hosting* : više korisnika deli sisteme za obradu
- *Dedicated hosting* : svaki korisnik ima posebno namenjen sistem.

Provajderi obično koriste virtualizaciju i nude sisteme za obradu u obliku virtualnih mašina.
Platforme za obradu se dele na *Tower, Rack-mounted* i *Blade* *(ploča sa osn. komp.)* *compute system*.
Platforma za obradu : procesor, RAM, ROM, matična ploča, čipset, softver.

Sistem za skladištenje služi za čuvanje i dostavljanje elektronskih podataka. Provajderi koriste virtualizaciju kako bi napravili *storage pools* koje korisnici dele.
Sistem za skladištenje : magnetni diskovi, SSD, magnetne trake, optički diskovi (CD, DVD...)

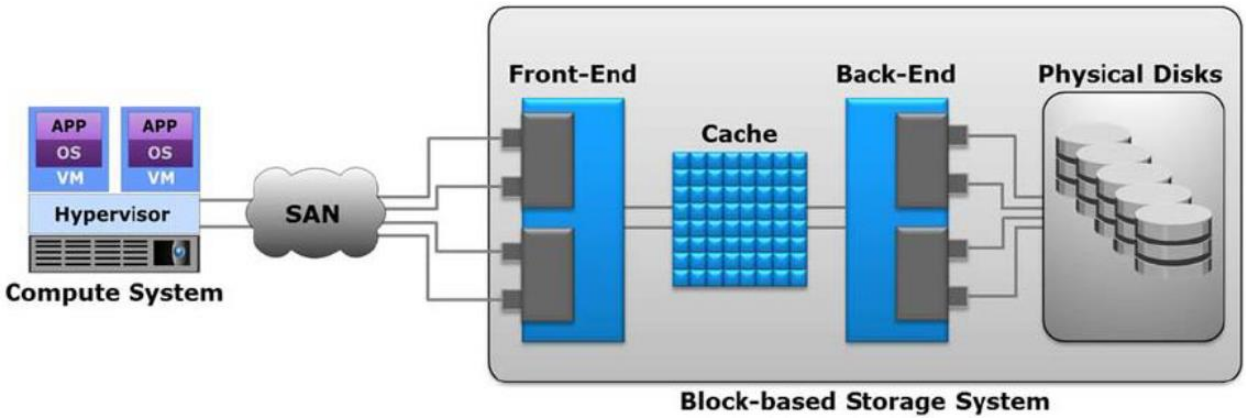
RAID - tehnologija skladištenja gde su podaci napisani u blokovima koji se prostiru na više diskova koji zajedno čine jednu RAID grupu.



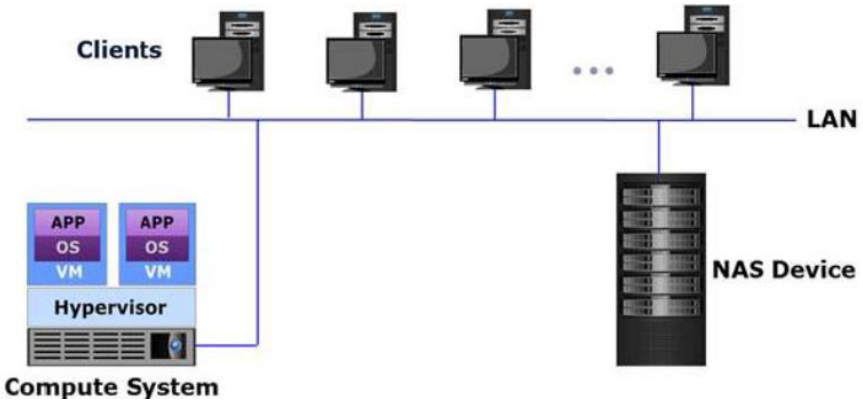
RAID 0	• Striped set with no fault tolerance
RAID 1	• Disk mirroring
RAID 1+0	• Nested RAID (striping and mirroring)
RAID 3	• Striped set with parallel access and a dedicated parity disk
RAID 5	• Striped set with independent disk access and distributed parity
RAID 6	• Striped set with independent disk access and dual distributed parity

Arhitektura sistema za skladištenje se deli po načinu pristupa podacima.
- Block-based, File-based, Object-based, Unified.

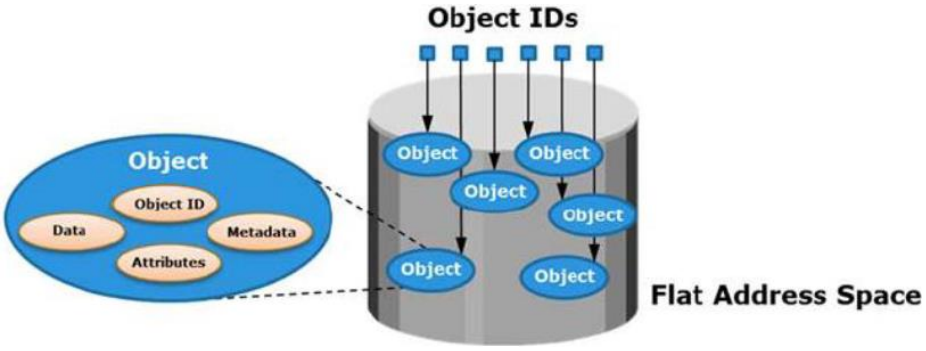
Block-based omogućava pravljenje i dodeljivanje volumena sistemima za obradu. Sistemi za obradu detektuju volumene kao lokalne diskove na kojima mogu biti pravljenji odg. file sistemi.

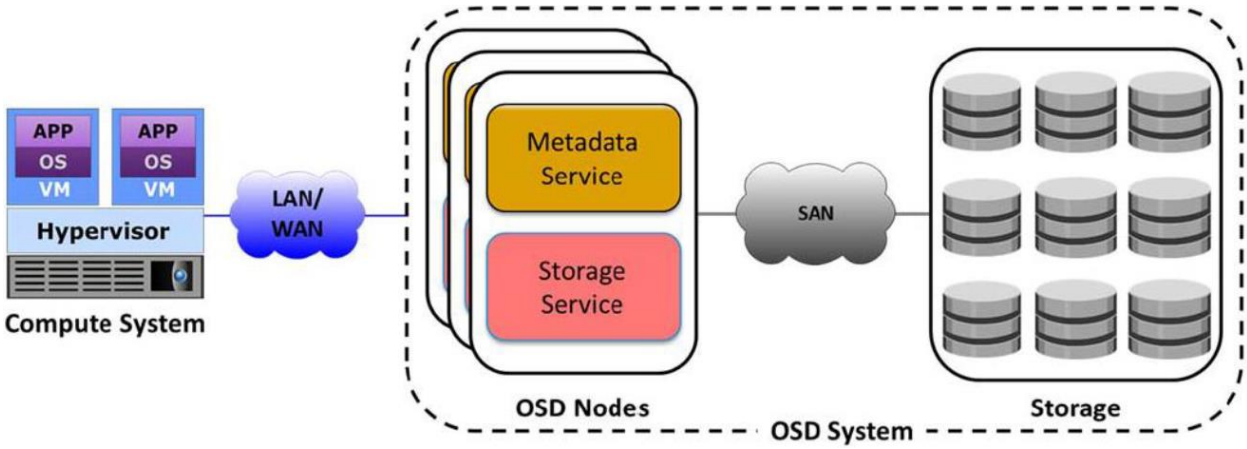


File-based sistem za skladištenje ima posvećen fajl server visokih performansi sa skladištem *(poznatiji kao **N**etwork-**A**ttached-**S**torage)*. Omogućava klijentima razmenu podataka preko IP mreže.

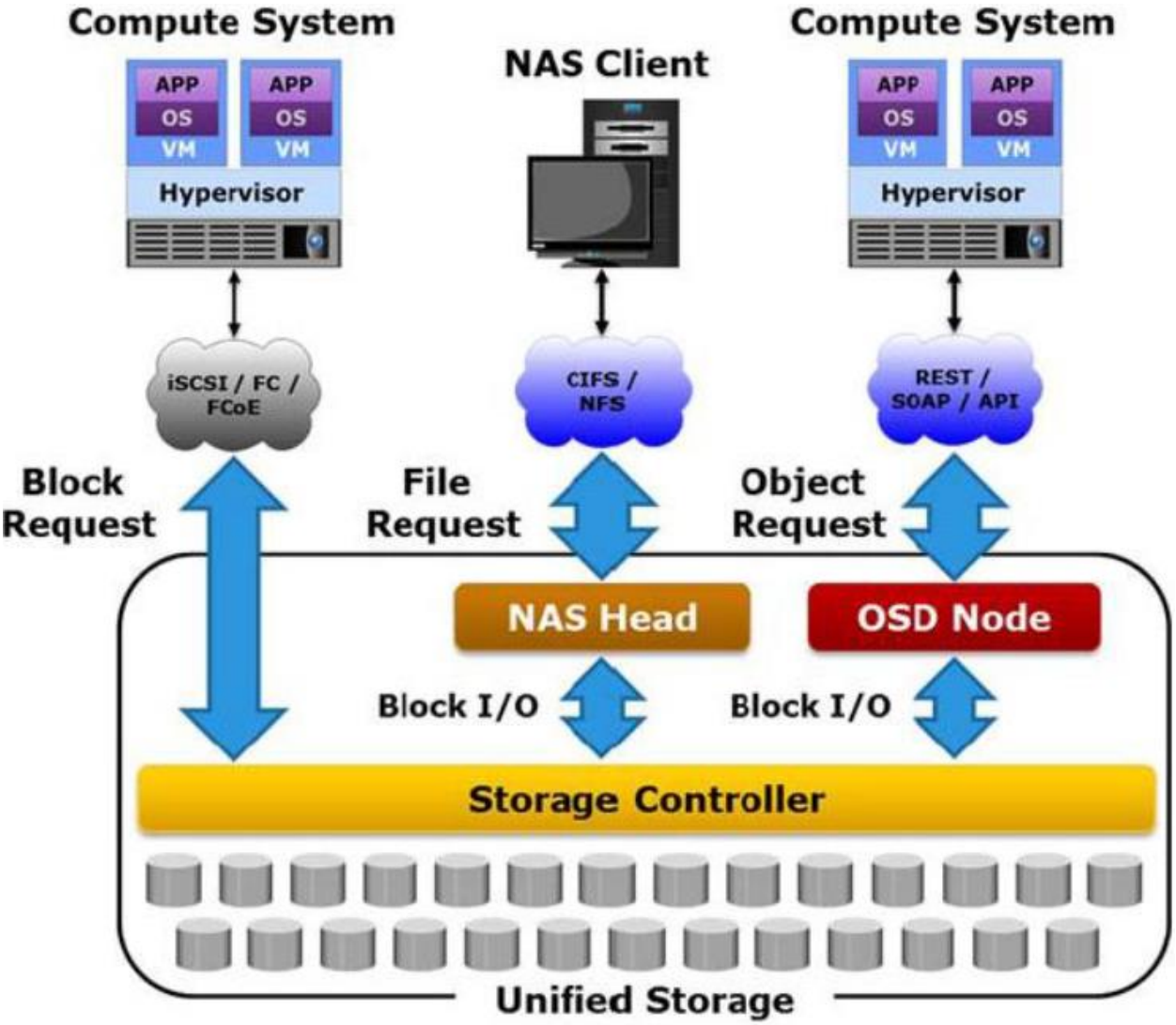


Object-based sistem skladišti podatke u obliku objekata na osnovu njihovog sadržaja i atributa. Objekti sadrže korisničke podatke, relevantne metapodatke i korisnički-definisane atribute. Jedinstveno se identifikuju preko njihovog ID-a.





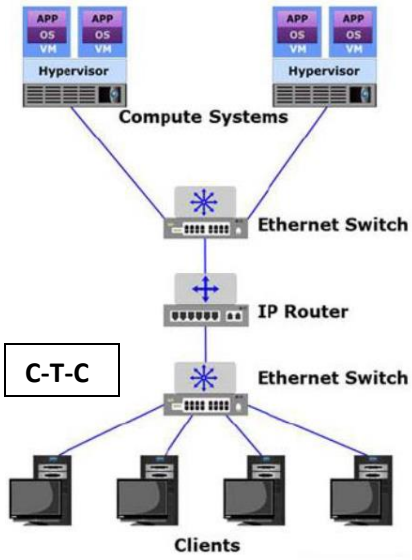
Unified sistem za skladištenje *(unified storage system)*



Na osnovu čvorova povezanih pomoću mreže, komunikacija preko mrežnog sistema se deli na :

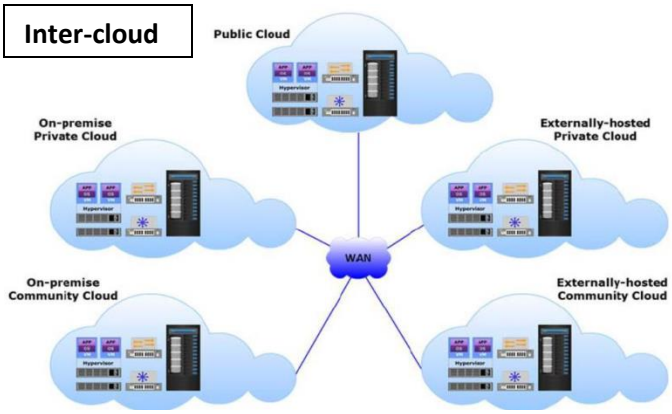
- **Compute-to-compute communication**

Fizičko povezivanje sistema za obradu, koristi IP zasnovane protokole kroz mrežne uređaje.



C-T-C

Inter-cloud



- Compute-to-storage communication

Storage Area Network (SAN) je mreža koja međupovezuju sisteme za skladištenje sa sistemima za obradu, omogućavajući sistemima za obradu pristup kao i deljenje podataka. SAN se dele na :

1. **FC SAN** - Koristi *Fibre Channel (FC) protokol* za prenos podataka, naredbi i stanja između sistema.

** Bukvalno samo oblak između compute systems i storage systems (videti jednu stranu kod FCIP)*

2. **IP SAN** - Koristi *Internet Protokol (IP)* za prenos saobraćaja. Dva glavna protokola su **iSCSI** i **FCIP**.

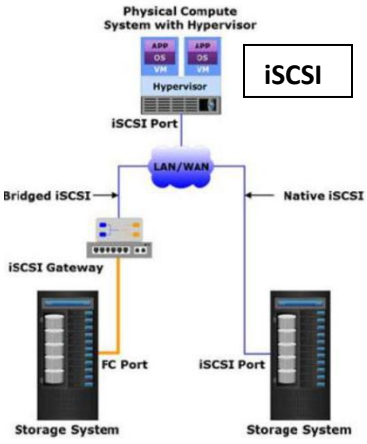
- **iSCSI** enkapsulira SCSI podatke u IP pakete koji se šalju preko IP-zasnovane mreže. *(slika levo)*
- **FCIP** enkapsulira FC frejmove u IP pakete koji se šalju između FC SAN preko IP-zasnovane mreže kroz FCIP tunel.

** Enkapsulira FC u IP, šalje IP kroz gateway, deenkapsulira FC iz IP-a. (slika sredina)*

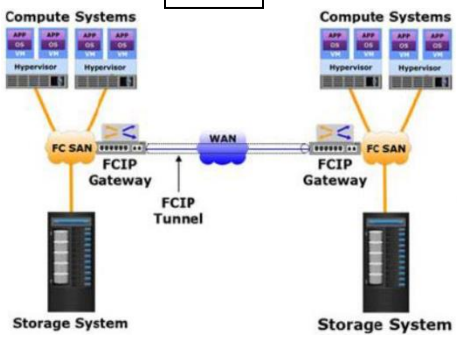
3. **FCoE SAN** - Ethernet mreža koja koristi FCoE protkol da prenese FC podatke kroz običan Ethernet saobraćaj.

** FcoE enkapsulira FC frejmove u Ethernet frejmove. c-t-c i FC storage saobraćaj se šalju preko istih mrežnih uređaja.*

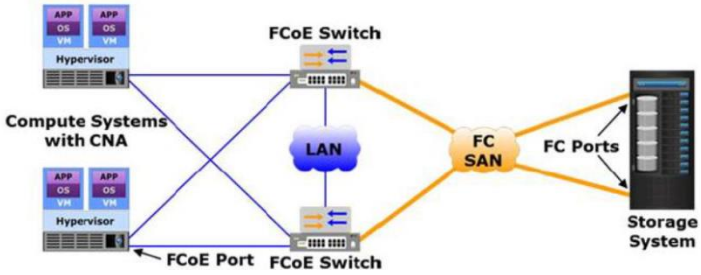
iSCSI



FCIP

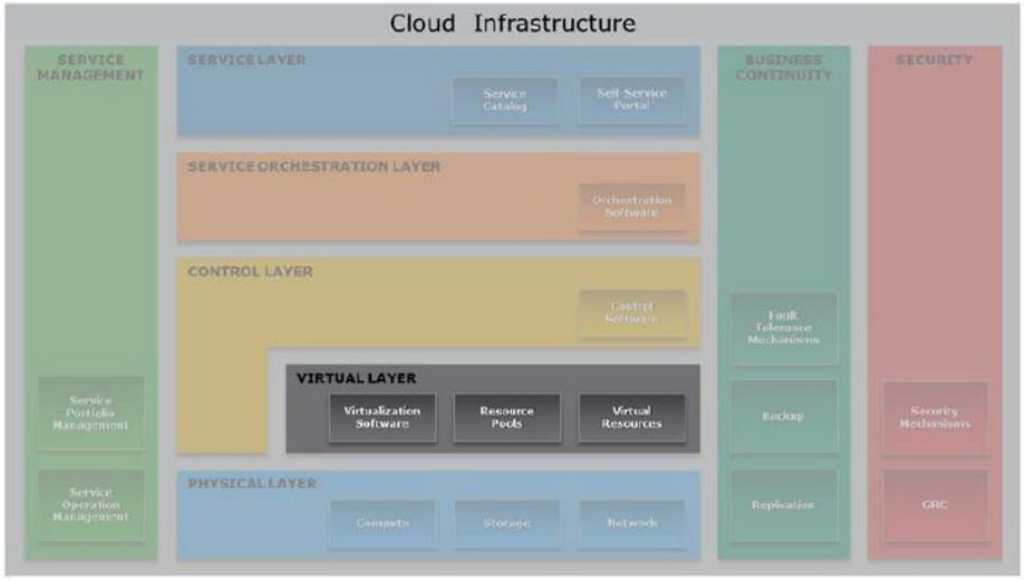


FCoE



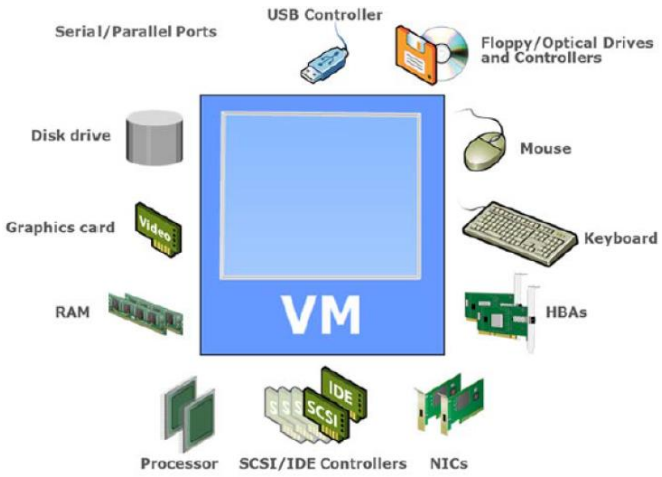
- Inter-cloud Communication - komunikacija između više oblaka preko WAN mreže.

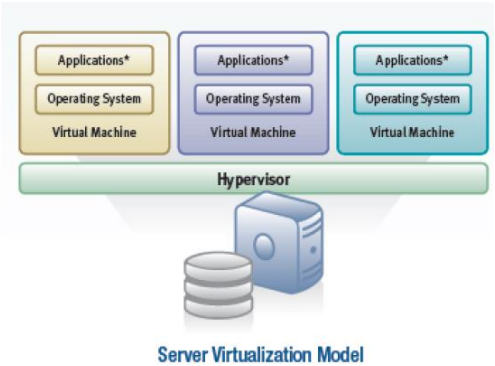
06 - Cloud infrastructure - Virtual layer



Virtualizacija označava logičku apstrakciju fizičkih resursa tipa obrade, mreže i skladišta koja omogućava jednom hardverskom resursu podršku više istovremenih instanci sistema ili mogućnost više hardverskih resursa da podržavaju jednu instancu sistema. Omogućava da resurs izgleda veće ili manje nego što zaista jeste.

Hypervisor je softver instaliran na sistemu za obradu *(compute system)*koji omogućava istovremeno pokretanje više operativnih sistema. On mapira virtuelni hardver na fizičkom hardveru.





Virtuelna mašina je logički sistem za obradu kreirana od strane hypervisor-a i instalirana na fizičkom sistemu za obradu. Sastoji se od virtuelnog hardvera i pokreće OS i aplikacije. **Virtuelna mreža** omogućava Ethernet povezivost i komunikaciju između VM unutar sistema za obradu. **ESXi** je **VMware** *(virtualization software)* koji vrši apstrakciju procesora, memorije, skladišta i mrežnih resursa u više VM.