

CC:

- **Päť entít** – konzument, poskytovateľ, auditor, sprostredkovateľ, prenos
- **Päť základných charakteristík** – samoobslužnosť, vysoká dostupnosť, zdieľanie prostriedkov, elasticita, meraná služba
- **Tri modely poskytovania služieb** – PaaS, IaaS, SaaS

konzument - Osoba alebo organizácia, ktorá udržiava vzťah a využíva služby Cloud poskytovateľa, vyberá zo služieb poskytovateľa a dáva požiadavky na konkrétnu službu ktorú následne využíva

poskytovateľ - Osoba alebo organizácia zodpovedná za dostupnosť služby pre záujemcov, vytvára a riadi výpočtovú infraštruktúru potrebnú pre doručenie a poskytovanie služieb cez internet konzumentom

auditor - Entita, ktorá môže vykonať nezávislú kontrolu služby za účelom objektívneho hodnotenia. Audity sa vykonávajú, aby sa overila zhoda so štandardmi. Kontrola sa môže týkať bezpečnosti, zachovania súkromia, výkonu a pod.

spostredkovateľ - Entita, ktorá riadi používanie, výkon a doručovanie služieb a dohaduje vzťah medzi konzumentom a poskytovateľom. Sprostredkovateľ poskytuje služby v troch kategóriách:

- **Sprostredkovanie služby** - zlepšuje danú službu tým, že vylepšuje jej niektoré vlastnosti a poskytuje k nim pridanú hodnotu pre konzumenta. Môže ísť o riadenie prístupu k službám, vylepšenie bezpečnosti, hodnotenie výkonu atď.
- **Spájanie služieb** - kombinuje a spája viaceré služby do jednej alebo viacerých nových služieb. Poskytuje zlúčenie dát a zaručuje ich bezpečný prechod medzi konzumentmi a viacerými poskytovateľmi.
- **Arbitráž služieb** - podobné spájaniu služieb. Sprostredkovateľ má možnosť vybrať služby od rôznych poskytovateľov. Takto je napr. možné vybrať z viacerých rovnakých služieb tú najlepšiu podľa známky hodnotenia.

prenos - Medzičlánok, ktorý poskytuje konektivitu a prenos služieb medzi konzumentom a poskytovateľom cez sieť, telekomunikačné zariadenia a iné

Samoobslužná interakcia na požiadanie: konzumentovi môže byť automaticky poskytnutá výpočtová sila, ktorú potrebuje bez ľudskej interakcie s poskytovateľom služby.

Vysoká dostupnosť siete: prostriedky sú prístupné cez sieť a dá sa k nim pristupovať z rôznych štandardných zariadení ako je napr. PC, mobilné telefóny a tablety.

Zdieľanie prostriedkov: výpočtová sila poskytovateľa je zdieľaná medzi viacerých konzumentov. Fyzické a virtuálne prostriedky sú dynamicky pridelené a odoberané podľa ich požiadaviek. Takto konzument nepozná presné miesto, kde sa jemu pridelené prostriedky nachádzajú (pri zovšeobecnení sa lokalita dá zúžiť napr. na štát alebo dátové centrum). Príkladom takýchto prostriedkov sú úložný priestor, CPU, pamäť a šírka pásma siete.

Rýchla elasticita: prostriedky sú elasticky pridelované a odoberané, v niektorých prípadoch automaticky, aby sa rýchlo prispôbili odpovedajúcim požiadavkám. Pre konzumenta sa tak prostriedky javia ako neobmedzené, ktoré môže využívať v hocijakom množstve, v hocijakom čase.

Meraná služba: Cloud systém automaticky kontroluje a optimalizuje prostriedky, tak že implementuje meranie v niektorej úrovni abstrakcie, potrebnej pre daný druh monitorovania (napr. úložný priestor alebo aktívne používateľské účty). Využitie prostriedkov môže byť monitorované, kontrolované a zhrnuté vo výstupoch, čím poskytuje transparentnosť pre poskytovateľa aj pre konzumenta danej služby.

SaaS:

- Službou pre konzumenta sú aplikácie prístupné cez internet, sprostredkované poskytovateľom

Konzumenti:

- Organizácie, ktoré poskytujú pre zamestnancov prístup k typickým kancelárskym aplikáciám (tabuľkový procesor, email a pod.)
- Koncoví používatelia, ktorí priamo používajú poskytovaný softvér
- Administrátori aplikácií, ktorí ich konfigurujú pre koncových zákazníkov
- Obchodná činnosť, zdieľanie súborov(kalendárov, obrázkov, ...), tabuľkové procesory, mail
- jednoduchý, efektívne využ. licencií, centralizovaná správa a dáta, úspora financií, zodpovednosť za správu preberá poskytovateľ

PaaS:

- Službou pre konzumenta je možnosť umiestniť vlastný softvér do prostredia cloud alebo možnosť využiť programovacie jazyky, knižnice a nástroje poskytnuté poskytovateľom

Konzumenti:

- Vývojári, tester, programátori, administrátori, end-users
- výhody zhodné so SaaS, + konzument oslobodený od povinnosti výberu inštalácie, údržby a ovládania komponentov platformy

IaaS:

- Službou pre konzumenta je poskytnutie výpočtovej sily, úložného priestoru, siete a ostatných základných prostriedkov tak, aby mohol umiestniť a spustiť ľubovoľný softvér v systéme cloud (vrátane operačného systému a aplikácií)

Konzumenti:

- Systémoví administrátori
- Plná kontrola nad VM, Flexibilný a efektívny prenájom výpočtovej sily, Prenositelnosť a interoperabilita so staršími aplikáciami

Modely implementácie:

Privátny cloud - cloud infraštruktúra je dostupná jedine pre jednu organizáciu pozostávajúcu z viacerých zákazníkov. Môže byť vlastnený a riadený organizáciou, treťou stranou alebo ich kombináciou. Existujú v prevedení s lokálnou aj vzdialenou správou.

Komunitný cloud - cloud infraštruktúra je dostupná jedine pre zákazníkov komunity organizácií, ktoré zdieľajú záujmy. Môže byť vlastnený a riadený jednou alebo viacerými organizáciami komunity, treťou stranou alebo ich kombináciou. Existujú v prevedení s lokálnou aj vzdialenou správou..

Verejný cloud - cloud infraštruktúra je pre použitie verejnosťou. Môže byť vlastnený a riadený podnikom, akademickou alebo vládnu organizáciou alebo ich kombináciou.

Hybridný cloud - cloud infraštruktúra pozostávajúca z dvoch alebo viacerých odlišných infraštruktúr (privátny, komunitný alebo verejný cloud), ktoré ostávajú jedinečné, ale sú spolu spojené štandardizovanou alebo proprietárnou technológiou, ktorá umožňuje kompatibilitu dát a aplikácií. Rozdiel medzi *lokálnou* a *vzdialenou správou* je významný. Obe variácie majú inú výkonnosť, spoľahlivosť a bezpečnosť.

OpenStack:

- založené NASA a RackSpace
- OpenSource pod verziou Apache 2.0
- TOP užívatelia CERN, AT&T, VW, Walmart, ...
- Aktualizácia každých 6 mesiacov.
- poskytuje všetky modely implementácie a poskytovania služieb
- má rôzne komponenty (moduly) – Nova, Swift, Cinder, Ceph, Neutron, Horizon, Keystone, Glance, Ceilometer, Heat, Trove, ...
- každý komponent ma vlastné demony a procesy

Výpočet - Nova

- Hlavný riadiaci komponent systému Cloud
- Najkomplikovanejší
- Spravuje výpočtovú silu
- Spravuje VM
- Nevyžaduje proprietárne systémové ani hardvérové požiadavky

Úložisko objektov - Swift

- Úložisko objektov
- Objekty ukladá a získava cez REST API
- Kopírovanie medzi viacerými HDD
- V prípade poruchy obnova dát
- Môže byť použitý pre zálohovanie a archivovanie
- Kompatibilné s AWS S3 API

Dátové úložisko - Cinder

- Poskytuje trvalé dátové úložisko pre VM
- Spravuje vytváranie, pripájanie a odpájanie blokov dát (v spolupráci s Nova)
- Možnosť vytvoriť snapshot VM

Dátové úložisko - Ceph

- Poskytuje trvalé aj objektové (dočasné) dátové úložisko pre VM
- Jednotné, škálovateľné a distribuované riešenie dátového úložiska

Sieť - Neutron

- Neutron slúži na manažment a spravovanie sietí v rámci systému OpenStack
- je najnovšou verziou sieťového manažmentu. Riadi sieť komunikáciu a je nezávislý od ostatných OpenStack služieb. Môže slúžiť napr. pre Load balancing, Firewalling, Namespaces a VPN siete

Typy sieťovej prevádzky:

- **Manažment** - Predstavuje riadiacu sieťovú komunikáciu medzi jednotlivými komponentami architektúry OpenStack.
- **API** - Sieťová prevádzka, ktorá je určená pre komunikáciu jednotlivých služieb OpenStack architektúry.
- **Internet** - Umožňuje prístup do verejnej siete, prostredníctvom Neutron smerovačov.
- **Guest** - Táto sieť je vyhradená pre komunikáciu virtuálnych zariadení zákazníkov.

Typy sietí:

- **Local** - Je lokálna sieť na danom výpočtovom uzle.
- **Flat** - Je „neznačkováaná“ sieť.
- **VLAN** - Je „značkováaná“ sieť.
- **VXLAN/GRE** - Je typ siete, ktorá je vytvorená nad infraštruktúrou poskytovateľa.

Webové rozhranie - Horizon

- Rozhranie pre administráciu a používanie systému
- Prístup k zdrojom CC
- Možnosť využívať služby v systéme OpenStack

Autentifikácia a autorizácia (Keystone)

- Centrálny bod s uloženými prístupmi používateľov k službám
- Funguje ako bežný autentifikačný a autorizačný systém
- Prihlasovanie: meno-heslo, token, AWS log-in
- Poskytuje zoznam všetkých implementovaných služieb
- Vytváranie prístupových práv, používateľov, pridelovanie zdrojov

Služba obrazov - Glance

- Ukladanie a načítanie OS images
- OpenStack ich využíva pri tvorbe VM
- Vytváranie snapshots - rýchla záloha

- Podporované formáty: raw, machine/AMI, VHD, VDI, qcow2, VMDK alebo OVF

Meranie - Ceilometer

- Ceilometer monitoruje a meria cloud za účelom spoplatnenia, merania, rozšíriteľnosti a zbierania štatistík

Orchestrácia - Heat

- Nástroj pre automatizáciu, manažment a administráciu prostredí
- Spracováva orchestračné skripty (JSON/YAML)
- Vytvorenie „stack“ prostredia

Databázové služby - Trove

- Trove poskytuje rozširovateľnú a spoľahlivú funkciu *databáza ako služba* pre relačné aj nerelačné databázy

OpenStack uzly:

kontrolér – centrálny, riadiaci a najdôležitejší prvok systému. Riadi všetky komponenty systému

sieťový uzol – riadi sieťovú prevádzku v systéme a pridáva sieťové funkcie

výpočtový uzol – výpočtový výkon pre systém. Mal by mať podporu HW virtualizácie.

OpenStack ďalej definuje ďalšie uzly pre pokročilé funkcie: uzol dátového úložiska a uzol objektového úložiska.

Zóny dostupnosti

- Rozdelenie CN (Compute Nodes) do logických skupín
- Volí sa pri vytváraní VM
- Štandardne sú všetky v jednej zóne

Zlučovanie CN

- Rozdelenie CN do logických skupín pre load balancing
- Zlučovať je možné aj v rámci zón

Flavor

- Konfigurácia výpočtovej sily pre VM
- Zadáva sa pri vytváraní VM
- Pozostáva z Id, Meno, Počet vCPU, RAM, Root disk, Krátkodobý disk, Swap.

Úložisko

Krátkodobý (ephemeral) disk:

- Existuje len počas života VM a vytrvá aj počas jej vypnutia a reštartu,
- Každá inštancia má aspoň jeden krátkodobý disk,
- Jeho veľkosť je definovaná daným flavor-om.

Trvalý (persistent) disk:

- Trvalý virtualizovaný blok disku. Jeho veľkosť určuje administrátor.
- Môže byť pridelený práve jednej inštancii v jednom čase, ale môže sa odpojiť a pripojiť k inej, s tým, že sa na ňom zachovávajú dáta (funguje podobne ako USB).
- Vyt. sa vo formáte RAW, bez partícií a súborového systému (po pridelení ich treba formátovať).

Ostatné pojmy systému OpenStack

- **Používateľ (user)** - je to digitálna reprezentácia osoby, systému alebo služby, ktorá využíva iné služby systému OpenStack. Používatelia majú pre prístup k zdrojom pridelený login alebo token.
- **Prihlasovacie údaje (credentials)** - dáta, ktoré potvrdzujú identitu používateľa (meno - heslo, token atď.).
- **Autentifikácia** - proces potvrdenia identity používateľa. Po overení prihlasovacích údajov, prideli OpenStack používateľovi autentifikačný token, ktorým sa bude preukazovať pri ďalších požiadavkách.
- **Token** - alfanumerický reťazec pre prístup k OpenStack zdrojom. Môže byť odobratý a je časovo obmedzený.
- **Projekt (tenant)** - spôsob ako zlúčiť alebo izolovať OpenStack zdroje. Môžu označovať zákazníka, účet, organizáciu alebo projekt. Administrátor takto dokáže napr. vyhradiť určitý výpočtový výkon konkrétnemu zákazníkovi.
- **Služba** - nova, glance, swift atď. Poskytujú jeden alebo viacero koncových bodov, na ktoré môžu používatelia pristupovať a tak vykonávať rôzne operácie.
- **Koncový bod** - sieťovo prístupná adresa, na ktorej sa nachádza služba (väčšinou URL).
- **Rola** - definovaná množina práv a privilégií pre konkrétnu množinu operácií. Token, ktorý je pridelený používateľovi obsahuje zoznam jemu pridelených rolí. Služba, ktorú požaduje tak vie určiť, k akým zdrojom má daný používateľ prístup.
- Nova využíva svoju službu *nova-scheduler*, aby našla CN, ktorá vyhovuje požiadavke
- Všetky CN ju pravidelne informujú o svojom stave, dostupných zdrojoch a HW možnostiach
- V základnej konfigurácii musí CN spĺňať nasledovné:
 - nachádza sa v požadovanej zóne,
 - má dostatok dostupnej RAM (RAM filter),
 - je schopný vyhovieť požiadavkám (výpočtový filter)

DevStack

- Vlastný IaaS Cloud behom niekoľkých minút
- Nainštaluje a nakonfiguruje: Keystone, Glance, Nova, Cinder, Neutron, Horizon

Orchestrácia:

- Jeden z najsilnejších nástrojov CC, tento pojem zahŕňa automatizáciu, vytváranie VM a manažment fyzických a virtuálnych zdrojov
- Pre konfiguračné súbory sa používajú serializačné/značkovacie jazyky (napr. YAML, JSON)

YAML:

- serializačný jazyk, začiatok súboru začína s ---, poznámky začínajú znakom #, na odsadenie používa medzery, nikdy nie „Tab“ (resp. je potrebné nastaviť, aby sa po stlačení klávesy „Tab“ vložili medzery – najlepšie 4, namiesto „tab“ znaku), escape character je znak ‘\’
- zoznamy sa definujú:
 - jeden záznam v riadku začínajúci pomlčkou (-)
 - viacero záznamov v riadku definovaných v [] oddelených čiarkou (,)

- definícia atribútov cez dvojbodku (*attribute:value*), reťazce môžu byť v úvodzovkách, ale nemusia, definícia bloku dát - | alebo >

JSON:

- nepoužíva odsadenia, nemá znak pre poznámky, zoznamy sa definujú v [] kde sú prvky oddelené čiarkami, definícia atribútov cez dvojbodku (*attribute:value*)

HOT Orchestrácia:

- Skripty pre komponent Heat vo formáte JSON alebo YAML, pre vytváranie prostredie možnosť definovať rôzne parametre, vytvorené prostredie = stack
- **Základné časti**
 - Povinná hlavička
 - Vstupné parametre (string, number, boolean, JSON-Map, list)
 - Definícia zdrojov
 - Výstupy

Sieťová virtualizácia

Network Virtualisation (NV):

- Umožňuje vytvoriť virtuálnu sieťovú infraštruktúru s využitím virtuálnych sieťových zariadení alebo inštancií.
- Izolované prostredia (multi-tenancy).
- VLAN, VXLAN, GRE (NVGRE), STT.

Technológia VXLAN:

- Virtual eXtensible Local Area Network.
- Jedna z najpoužívanejších technológií pre identifikovanie a oddelenie prevádzky jednotlivých zákazníkov CC.
- Umožňuje prenášať izolované virtuálne L2 siete cez L3 infraštruktúru poskytovateľa prostredníctvom zabalenia rámcov do VXLAN paketov.
- Virtuálna sieť sa vo VXLAN terminológii nazýva segment.
- Každý segment je identifikovaný 24 bitovým identifikačným číslom VNI.
- Celý pôvodný L2 ethernet rámec (okrem jeho zabezpečovacej sumy) je zabaľovaný do VXLAN paketu ako UDP dátová časť.
- Zabaľovanie a rozbaľovanie rámca zabezpečuje rozhranie, ktoré sa nazýva VXLAN „ukončovací bod“ (*Tunnel Endpoint - VTEP*).
- Skladá sa z dvoch logických častí, ktoré sa nazývajú uplink a downlink.

Technológia (NVGRE) GRE

- Network Virtualisation using Generic Routing Protocol.
- Spodných 24 bitov GRE hlavičky je určených pre identifikátor zákazníčkovej siete (tzv. *Tenant Network Identifier - TNI*).

Technológia STT

- Stateless Transport Tunneling.
- Na rozdiel od technológií VxLAN a NVGRE, STT technológia používa 64 bitové context ID.
- Hlavičky protokolu STT vyzerajú ako TCP hlavičky, vďaka čomu je možné využiť hardvérovú technológiu TSO - TCP Segmentation Offload.

Network Functions Virtualisation

- Nahrádza súčasné fyzické sieťové zariadenia softvérovými sieťovými zariadeniami a funkciami.
- Inštancia s virtuálnou sieťovou funkciou.

Hlavné ciele NFV

- Inovácia súčasných služieb prostredníctvom softvérového vývoja a nasadenia sieťových funkcií.
- Automatizácia sieťových funkcií prostredníctvom softvéru.
- Zníženie nákladov na nadobudnutie (CapEx - Capital Expense) a prevádzku (OpEx - Operating Expense) sieťových funkcií.

Výhody NFV

- Zníženie spotreby elektrickej energie a celkovej ceny zariadení.
- Viaceré prostredia pre testovacie a produkčné účely v rámci rovnakej infraštruktúry.
- Poskytovanie služieb viacerým zákazníkom bez nutnosti zapojenia nového hardvéru.

Príklady implementácie NFV

- Prepínacie zariadenia: BNG, CG-NAT, smerovače
- Mobilné sieťové zariadenia: HLR/HSS, MME, SGSN
- Bežné domáce smerovače a prepínače
- Technológie pre tunelovanie: IPSec/SSL, VPN
- Aplikačné servery: Cache Servers, Load Balancers, Application Accelerators

NFV v Cloud Computing

- Jadro CC tvoria virtualizačné techniky ako hardvérová virtualizácia s využitím hypervisor-ov, virtuálnych prepínačov a smerovačov (vSwitch a vRouter).
- Kľúčovým elementom v NFV a CC je používanie výkonných fyzických zariadení.

Modely poskytovania NFV

- Network Functions Virtualisation Infrastructure as a Service (NFVlaaS).
- Virtual Network Function as a Service (VNFaaS).
- Virtual Network Platform as a Service (VNPaaS).

Model NFVI ako služba (NFVlaaS)

- Je služba poskytujúca prostredie, v ktorom môžu byť spustené rôzne sieťové virtuálne zariadenia a funkcie.
- NFVI sa dá prirovnať svojou podstatou k IaaS.
- Fyzické umiestnenie infraštruktúry nie je pre poskytovanie CC služieb podstatné.
- Rozšírenie portfólia ponúkaných služieb poskytovateľa ako aj integrácia s inými prostrediami.
- Zlepšenie dostupnosti služieb zákazníkovi.
- Nutnosť vyhovieť geografickým obmedzeniam pre citlivé dáta.

Model VNF ako služba (VNFaaS)

- SaaS je porovnateľný s VNFaaS, v ktorej aplikácia je VNF inštancia poskytovateľa a spoločnosť je zákazník, ktorý používa jej služby.
- Zákazník nemá prístup ku konfigurácii NFV infraštruktúry alebo VNF inštancii.
- Zákazník VNFaaS nemusí investovať vlastné prostriedky do ďalších sieťových služieb.
- SaaS je porovnateľný s VNFaaS, v ktorej aplikácia je VNF inštancia poskytovateľa a spoločnosť je zákazník, ktorý používa jej služby.
- Zákazník nemá prístup ku konfigurácii NFV infraštruktúry alebo VNF inštancii.

- Zákazník VNFaaS nemusí investovať vlastné prostriedky do ďalších sieťových služieb.
- Zdieľanie dostupných zdrojov.
- Centralizovaný manažment.
- Zjednotenie ponúkaných sieťových služieb.

Model VNP ako služba (VNPaaS)

- Služba v ktorej poskytovateľ ponúka zákazníkovi nástroje alebo VNF funkcie pre vybudovanie vlastnej virtuálnej siete a zariadení.
- Zákazníci používajú šablóny preddefinované poskytovateľom a rôzne nástroje pre automatizáciu.
- Poskytnutie nástrojov pre vytváranie a spravovanie zákazníkových VNF inštancií.
- Prístup do rozhrania (API).
- Monitorovanie používania zdrojov.

SDN:

- Technológia, ktorá predstavuje nový spôsob návrhu, implementácie a manažmentu súčasných sietí v rámci ktorého oddeluje riadiacu a dátovú časť siete.
- SDN kontrolér, Southbound Application Program Interface (SAPI) a Northbound API (NAPI) rozhrania
- **SDN kontrolér** je hlavný riadiaci prvok siete.
- **SouthBound API** je rozhranie pre komunikáciu medzi SDN kontrolérom a prepínačmi alebo smerovačmi.
- **Northbound API** je rozhranie pre komunikáciu medzi SDN kontrolérom a službami (aplikáciami) nad danou sieťou.

Vlastnosti:

- Znižovanie nákladov bez nutnosti použitia drahých Application Specific Integrated Circuit (ASIC) hardvérových modulov.
- Programovateľnosť siete a sieťových zariadení.
- Efektívna automatizácia a optimalizácia.
- Rýchle spúšťanie aplikácií, služieb a infraštruktúry podľa aktuálnych potrieb.
- Schopnosť vytvárať nové typy aplikácií, služieb a modelov.