AZURE: analiza strukture oblaka i primjer uporabe

Pauro, Kristijan

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Pula / Sveučilište Jurja Dobrile u Puli**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:137:685762

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-05-04**

Repository / Repozitorij:

Digital Repository Juraj Dobrila University of Pula

Sveučilište Jurja Dobrile u Puli
Fakultet informatike

KRISTIJAN PAURO

AZURE (RAČUNALSTVO U OBLAKU) INFRASTRUKTURA KAO USLUGA: Primjer korištenja Microsoft Azure unutar tvrtke Cenosco

Diplomski rad

Pula, 2021.

Sveučilište Jurja Dobrile u Puli
Fakultet informatike

KRISTIJAN PAURO

AZURE (RAČUNALSTVO U OBLAKU) INFRASTRUKTURA KAO USLUGA: Primjer korištenja Microsoft Azure unutar tvrtke Cenosco

Diplomski rad

JMBAG: 0145017083, izvanredni student
Studijski smjer: Informatika

Predmet: Računalne mreže

Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija

Mentor: Mario Radovan

Pula, travanj 2021.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Kristijan Pauro, kandidat za magistra informatike ovime izjavljujem da je ovaj Diplomski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Diplomskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, 2021. godine

IZJAVA

o korištenju autorskog djela

Ja, Kristijan Pauro dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom „Azure (računalstvo u oblaku) infrastruktura kao usluga: Primjer korištenja Microsoft Azure unutar tvrtke Cenosco“, koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

Sadržaj

1. Uvod 1
2. Računalstvo u oblaku 2
2.1. Povijest računarstva u oblaku 2
2.2. Definiranje računarstva u oblaku 4
2.3. Prednosti računarstva u oblaku 5
2.4. Modeli usluga računarstva u oblaku 8
2.5. Infrastruktura kao servis (IaaS) 12
3. Microsoft Azure 16
3.1. Komponente platforme Microsoft Azure 16
3.2. Windows Azure 17
3.2.1. Compute 17
3.2.2. Storage 18
3.2.3. Fabric Controler 19
3.2.4. Content delivery network (CDN) 19
3.2.5. Connect 19
3.3. SQL Azure 20
3.3.1. SQL Azure Database 20
3.3.2. SQL Azure Reporting 21
3.3.3. SQL Azure Data Sync 22
3.4 Azure App Fabric 23
3.5 Windows Azure Marketplace 24
4. Azure virtualna mreža 25
4.1. Prikaz VPN enkapsulacije kroz TCP/IP slojeve 27
4.2. EdgeRuter Site-to-Site VPN spajanje udaljenih lokacija 29
4.3. VPN mogućnosti spajanja na Azure mrežnu infrastrukturu 30
4.3.1. Point-to-site VPN 30
4.3.2. Site-to-site VPN 31
4.3.3. ExpressRoute konekcija 33

4.4. Stvaranje Site-to-site konekcije 35
4.5. Stvaranje virtualnog Hub-a za Site-to-Site 36
4.5. Azure Site-to-Site VPN Cenosco 42
5. Primjeri korištenja i upravljanja infrastrukturom Microsoft Azure 51
5.1 Grupa resursa u Azure okolini 54
5.2 Azure Load balancers 54
5.3 Primjer Cenosco skripte za izradu web stranica 55
6. Opis tvrtke Cenosco 57
7. Zaključak 64
Literatura 65
Popis slika 68
Sažetak 70
Summary 72

1. Uvod

Računarstvo u oblaku (*eng. Cloud computing* = *Cloud*) je u stalnom porastu i naveden je kao jedan od deset strateških tehnoloških trendova IT (*eng. Information Technology*) industrije. Računarstvo u oblaku u svom osnovnom obliku nam nudi poslužiteljsku infrastrukturu (poslužitelj željenih karakteristika), platformu (razvojna platforma za razvijanje aplikacija) i softver (aplikacija). Za pristup navedenim oblicima računarstva u oblaku jedini preduvjet je pristup Internetu. Poduzeće nema potrebu za velikim ulaganjima u vlastiti podatkovni centar, zapošljavanje novog kadra koji će isti održavati u funkciji i plaćati dodatne troškove struje za napajanje i hlađenje jednog podatkovnog centra. Veliki adut računarstva u oblaku je visoka dostupnost servisa (bez prekida u radu) i pristup servisima izvan lokalne podatkovne mreže.
Računarstvo u oblaku pruža modernu alternativu tradicionalnom lokalnom centru podataka. Javni dobavljač oblaka u potpunosti je odgovoran za kupnju i održavanje hardvera i pruža širok spektar usluga platforme koje se može koristiti.

IaaS- infrastruktura kao usluga (*eng. Infrastructure-as-a-Service)* javlja se kao idealno rješenje u mnogim poslovnim slučajevima. Potražnja za računalnim resursima je izrazito promjenjiva što znači da tijekom vremena javljaju i vršna opterećenja dijelova infrastrukture, ali postoje i razdoblja kod kojih se potražnja za tim dijelovima topi. Isto tako, korištenje ove usluge vrlo je pogodno kada se radi o novim poslovnim sustavima (Startup) koji nemaju novaca za visoka ulaganja u hardver. Također, i u poslovnim sustavima čije se poslovanje vrlo brzo razvija i širi proširenje i nadogradnja hardvera postaju usko grlo. Nadalje, ulaganje u Iaas je vrlo dobro i u situacijama kada se na menadžment vrši pritisak da se smanje troškovi kapitalnog ulaganja kako bi se cjelokupna politika troškova usmjerila u operativna ulaganja. Na kraju, IaaS nudi rješenje temeljem kojeg poslovni ili privatni korisnici ne moraju kupovati hardver, mrežnu opremu, odnosno cjelokupnu infrastrukturu jer im je ona dostupna u iznajmljenoj usluzi. Svaka od tih usluga jest sastavni model računalnog oblaka, međutim, pristup tim uslugama ovisi o modelu oblaka prema kriteriju primjene.

2. Računalstvo u oblaku

Računalstvo u oblaku predstavlja revolucionarni koncept koji nudi pristup osobnim podacima i aplikacijama s bilo kojeg uređaja u bilo koje vrijeme, potrebna je samo internetska veza. Osobni podaci i aplikacije nisu fizički smješteni na računalu već se nalaze u oblaku što za prednost daje svojim korisnicima brži i jednostavniji pristup i uporabu podataka.

2.1. Povijest računarstva u oblaku

Veliki broj ljudi pretpostavlja da se oblačno računarstvo počelo razvijati u 21. stoljeću, no to nije točno.
Postupna evolucija oblačnog računarstva započela je još 1950. godine kada su postojala velika mainframe računala. Korisnici su takvim računalima pristupali preko terminala, no zbog velike cijene takvih računala nije bilo komercijalnog uspjeha. Isto tako korisnici u to vrijeme nisu zahtijevali veliku količinu pohrane podataka niti snažnu procesorsku moć.

Razvoju oblačnog računarstva značajno je pridonio koncept virtualnih strojeva eng. *virtual machines* pomoću kojih je bilo moguće istovremeno pokrenuti više operacijskih sustava na nekoj hardverskoj platformi.[1] Pomoću virtualnih strojeva računalna infrastruktura poput memorije, procesora, mreže, tvrdog diska itd. mogla je biti isporučena svakom korisniku putem mreže. Ukratko virtualizacija je softver koji omogućuje isporuku dio računalne infrastrukture korisniku. Osim virtualizacije hardvera moguća je virtualizacija softvera (npr. softver za elektroničku poštu) i prostora za pohranu (npr. online pohrana podataka poput Dropbox-a). Napredak telekomunikacija jedan je od ključnih čimbenika u razvoju oblačnog računarstva. U početku telekomunikacijske kompanije nudile su point-to-point podatkovne veze. Razvojem virtualnih privatnih mreža usluge prijenosa podataka bile su jeftinije i kvalitetnije. Pojavom VPN-a (eng. *virtual private network)* nije bilo potrebno graditi

[1] Destefani Neto M, A brief history of cloud computing. 2014., Dostupno na: http://thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/, (pristupljeno 18.ožujka 2021.).

fizičku infrastrukturu kojom bi se omogućilo da više korisnika ima pristup mreži nego su telekomunikacijske tvrtke bile u mogućnosti pružiti zajednički pristup istoj fizičkoj infrastrukturi.[2] Ideju globalne mreže računala predstavio je J.C.R. Licklider čija je vizija bila da svatko na svijetu ima pristup podacima i programima iz bilo kojeg mjesta. Licklider je radio na razvoju ARPANET (*eng. Advanced Research Projects Agency Network)* sustava koji je bio razvijen prije današnjeg interneta. Također sa svojim suradnicima predstavio je računalo koje je imalo obradu podataka u realnom vremenu te je time značajno pridonio i drugim računalnim disciplinama.[3] Navedena postignuća značajno su utjecala na razvoj oblačnog računarstva.

John McCarthy bio je američki računalni znanstvenik koji je poznat kao otac umjetne inteligencije. Godine 1960. došao je na ideju o globalnoj mreži računala koja bi korisnicima omogućila da dijele podatke povezivanjem na središnje računalo. Samim time to bi smanjilo cijenu korištenja računala. Takva inovacija u ono vrijeme predstavljala je značajan doprinos razvoju interneta i bila je prethodnik oblačnog računarstva. Također imao je ideju o prodaji i kupovanju putem globalne mreže računala što danas predstavlja e-commerce.[4] Njegova izjava na jednoj konferenciji da svaki korisnik treba platiti računalne resurse koje zapravo koristi i da svaki korisnik ima pravo na neograničene računalne resurse u ono vrijeme bila je ravna znanstvenoj fantastici. Danas oblačno računarstvo upravo teži tome. Tijekom 1960. godina razvio je koncept računala pod nazivom *time-sharing* koji je omogućavao korisnicima da koriste jedno središnje računalo istovremeno. Smatrao je da se računalni resursi ne prodaju kao proizvodi već kao usluga, što predstavlja još jednu sastavnicu oblačnog računarstva. U svom daljem znanstvenom radu McCarthy se posvetio mnogo više umjetnoj inteligenciji nego oblačnom računarstvu. Za svoj rad dobio je Turingovu nagradu koja se dodjeljuje samo najuspješnijim znanstvenicima na području računarske znanosti i smatra se ekvivalentom Nobelove na grade za to područje.[5]

[2] Ibidem
[3] Craig D, Cloud computing history. 2014., Dostupno na: http://constructioninformer.com/2010/08/14/cloud-computing-history/, (pristupljeno 18.ožujka 2021.).
[4] Childs M, McCarthy J, Computer scientist known as the father of AI. 2011., Dostupno na: http://www.independent.co.uk/news/obituaries/john-mccarthy-computer-scientist-known-as-the-father-of-ai-6255307.html, (pristupljeno 18.ožujka 2021.).
[5] Ibidem

2.2. Definiranje računarstva u oblaku

Računalstvo u oblaku (eng. *Cloud computing*) je brzo rastući oblik računalstva koji se temelji na pružanju računalnih resursa i usluga putem udaljene veze odnosno interneta. Panian (2013.) navodi kako je Cloud, prema definiciji Nacionalnog instituta za standarde i tehnologiju (NIST) „model obrade podataka koji omogućuje sveprisutan i jednostavan pristup skupu djeljivih računalnih resursa poput računalnih mreža, poslužiteljskih računala, medija za pohranu podataka, aplikacija i usluga koje je moguće konfigurirati i stavljati na raspolaganje korisnicima uz njihov minimalan osobni angažman ili uz najmanju moguću interakciju s pružateljem tih resursa.“[6] Kratko rečeno, svrha i ideja oblak tehnologije zasniva se na tome da su svi podaci koji su potrebni korisniku budu tom istom korisniku dostupni u bilo kojem trenutku uz prisustvo Interneta. To je usluga koja nudi neograničene količine svih resursa onda kada je to korisniku potrebno.

Termin oblačno računarstvo odnosi se na pohranu i pristup podacima te programima na neki odabrani vanjski servis kojemu pristupamo preko interneta. Termin oblak ili eng. *cloud* predstavlja kompleksan spoj više fizičkih poslužitelja u jednu grupu koja se naziva *cluster.*[7] Više takvih grupa najčešće se nalaze na različitim lokacijama. Isto tako oblak je često korištena metafora za internet gdje je internet predstavljen u raznim dijagramima.

Za korisnika takvog sustava nije važno znati koliko se poslužitelja nalazi u grupi ili koja je točna lokacija poslužitelja, za njega je bitno da dobi traženu uslugu. Za profesionalnog informatičara oblačno računarstvo omogućava da se razvojni inženjeri i programeri usredotoče na implementaciju poslovne logike te na taj način više ne moraju implementirati infrastrukturu niti instalirati potrebne aplikacije.[8] Sistemski inženjeri u takvom načinu rada usredotočeni su na održavanje platformi na kojima se

[6] Panian Ž. (2013). Elektroničko poslovanje druge generacije. Zagreb: Ekonomski fakultet Zagreb.
[7] Bronzin T, „Cloud Computing“ ili programska rješenja u oblacima, 2009., Dostupno na: http://pogledkrozprozor.wordpress.com/2009/08/29/%E2%80%9Ecloud-computing%E2%80%9C-ili-programska-rjesenja-u-oblacima/, (pristupljeno 18.ožujka 2021.).
[8] Bronzin T, „Cloud Computing“ ili programska rješenja u oblacima, 2009., Dostupno na: http://pogledkrozprozor.wordpress.com/2009/08/29/%E2%80%9Ecloud-computing%E2%80%9C-ili-programska-rjesenja-u-oblacima/, (pristupljeno 18.ožujka 2021.).

izvodi oblačno računarstvo. Važno je napomenuti da korisnik plaća onoliko računalnih resursa koliko doista koristi i da ne vodi brigu oko nabavke hardvera te instalacije i održavanja softvera.

Bitna stavka vezana uz oblačno računarstvo svakako stalna dostupnost podataka, naravno preduvjet za to je stalna internet veza. Oblačno računarstvo često je jeftinije od vlastite infrastrukture. Tvrtka više ne mora planirati kapitalna ulaganja u IT infrastrukturu, ne mora zapošljavati IT stručnjake za održavanje hardvera i softvera. Već u tim aspektima mogu se predvidjeti značajne uštede u poslovanju. U oblačnom računarstvu resursi su najčešće neograničeni, dok kod vlastite infrastrukture to nije slučaj. Prednost neograničenih resursa u oblačnom računarstvu izuzetno je bitna jer na taj način kada tvrtki zatreba više računalnih resursa ona ih unajmi, a otpusti kada potreba za istima nestane. Ukoliko bi tvrtka imala vlastitu infrastrukturu ona bi često ostala neiskorištena. Termin oblak datira još od samog početka stvaranja interneta. Godine 1960. američki stručnjak za računalnu inteligenciju John McCarthy predvidio je brojne navedene prednosti oblačnog računarstva.[9] Još i danas oblačno računarstvo je u neprekidnom razvoju, a najviše napora u razvoj ulažu tvrtke koje se bave pružanjem usluga u oblaku.

2.3. Prednosti računarstva u oblaku

Kako bi se internetski servis mogao smatrati oblak servisom, on mora imati sljedeće karakteristike:[10]

- Samostalan rad dostupan na zahtjev
- Pristup sa širokopojasne mreže
- Nezavisnost resursa od lokacije
- Brza elastičnost
- Mjerena usluga.

[9] Ibidem
[10] Krutz R, Vines R. (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, Indiana: Wiley Publishing

Prednosti koje nam donosi novi poslovni model oblačnog računarstva iz gledišta korisnika su sljedeće:[11]

- Niža cijena programske podrške: plaća se usluga, tj. plaća se ono što se trenutno koristi. Time se izbjegavaju velika ulaganja u nabavku programske opreme i infrastrukture.
- Korisniku je uvijek dostupna zadnja verzija programske podrške koju ažurira tvrtka kod koje se plaća najam usluge
- Aplikacije i podatci dostupni su sa svake lokacije gdje korisnik ima pristup internetu
- Značajno manji troškovi održavanja softvera (nije potrebno kupovati licence za korištenje softvera) i hardvera (nije potrebno kupovati novi hardver jer se plaća najam postojećeg), cijena najma može biti fiksna ili varijabilna što se definira ugovorom
- Sigurnost podataka – kod korištenja usluga oblačnog računarstva mogućnost gubitka podataka jako je mala. Tvrtke koje pružaju takve usluge najčešće nude sigurnosnu kopiju podataka, antivirusnu zaštitu i druge mehanizme koji sprečavaju gubitak ili krađu podataka.[12]

S druge strane prednosti oblačnog računarstva iz gledišta profesionalnih informatičara su sljedeće:[13]

- Isto kao što je za korisnika prednost dostupnost aplikacije tako je to ujedno i prednost za profesionalnog informatičara jer samim time održavanje aplikacije je lakše i brže.
- Skalabilnost aplikacija odnosi se na mogućnost posluživanja velikog broja korisnika. Cloud Computing platforme omogućavaju iskorištavanje velikog broja poslužitelja i računskih centara na različitim mjestima.

[11] Bronzin T, „Cloud Computing“ ili programska rješenja u oblacima, 2009., Dostupno na: http://pogledkrozprozor.wordpress.com/2009/08/29/%E2%80%9Ecloud-computing%E2%80%9C-ili-programska-rjesenja-u-oblacima/, (pristupljeno 18.ožujka 2021.).
[12] Conlon D, Cloud computing & small business-security pros and cons. 2011., Dostupno na: www.trendmicro.com/cloud-content/us_pdfs/security-intelligence/sb_cloud-computing_small_business-pros-and-cons.pdf, (pristupljeno 18.ožujka 2021.).
[13] Bronzin T, „Cloud Computing“ ili programska rješenja u oblacima, 2009., Dostupno na: http://pogledkrozprozor.wordpress.com/2009/08/29/%E2%80%9Ecloud-computing%E2%80%9C-ili-programska-rjesenja-u-oblacima/, (pristupljeno 18.ožujka 2021.).

Za profesionalnog informatičara i tvrtke koje se bave oblačnim računarstvom ova karakteristika je bitna jer ona omogućuje korisniku da plaća ono što zapravo koristi, što smanjuje cijenu usluge.

- Fleksibilnost u mijenjaju i prilagodbi aplikacija – aplikacija se može prilagoditi jednoj grupi korisnika iz jednog mjesta
- Kontroliran korisnički pristup – korisničkom administracijom jednostavno je ograničiti pristup, brisanje i izmjene podataka.

Do sada su navedene prednosti novog poslovnog modela oblačnog računarstva, no postoje i nedostaci.

U početku navedeni su nedostaci koji se javljaju za korisnika:[14]

- Problem dostupnosti – uslugu nije moguće koristiti ako je internetska veza slaba ili u prekidu
- Problem sigurnosti – pružatelj usluge može zloupotrijebiti naše povjerenje te može manipulirati podacima, dokumentima pa i samom bazom podataka. Također nije isključena mogućnost prisluškivanja komunikacije između nas kao korisnika usluge i naše klijentske tvrtke.
- Problem ovisnosti o jednom pružatelju programske podrške, tj. usluga. Još uvijek nisu razvijeni standardi o zapisu podataka i njihovoj razmjeni između različitih platformi.
- Vrijeme odgovora može biti relativno dugo ukoliko se oblak nalazi na udaljenom poslužitelju, što nije dobro za aplikacije koje zahtijevaju obradu podataka u realnom vremenu

[14] Bronzin T, „Cloud Computing“ ili programska rješenja u oblacima, 2009., Dostupno na: http://pogledkrozprozor.wordpress.com/2009/08/29/%E2%80%9Ecloud-computing%E2%80%9C-ili-programska-rjesenja-u-oblacima/, (pristupljeno 18.ožujka 2021.).

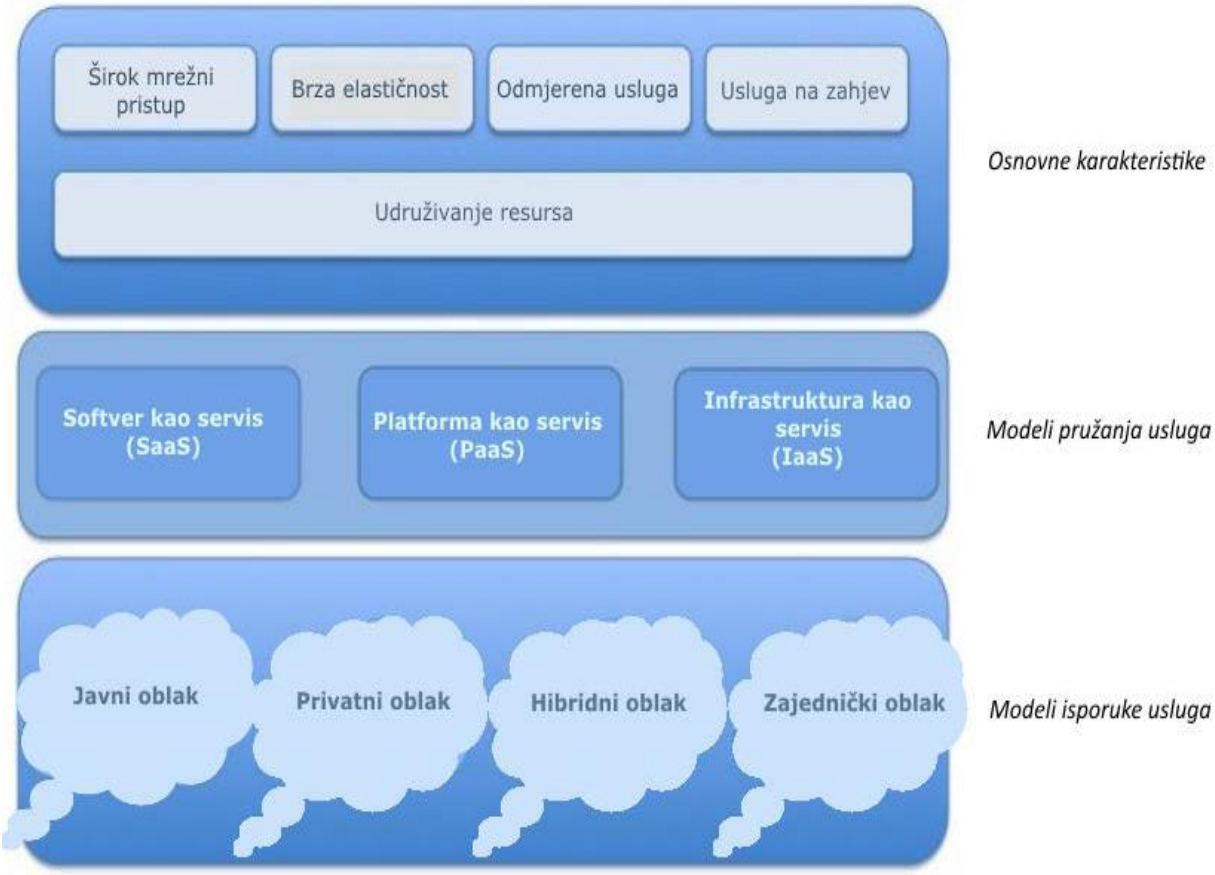
Također postoje i nedostaci za profesionalne informatičare koji nude takav poslovni model:[15]

- Mora se usvojiti nov način razvoja aplikacija. Različit je pristup kod projektiranja arhitekture aplikacije kada se tvrtka odluči koristiti usluge oblačnog računarstva. Isto tako primjerice arhitektura aplikacije se može razlikovati ovisno o samom davatelju usluge (nije ista arhitektura ukoliko se odluči za Microsoftove ili Amazon usluge)
- Ne postoje standardi za povezivanje, premještanje, programsku podršku aplikacija i podataka različitih davatelja usluga oblačnog računarstva

2.4. Modeli usluga računarstva u oblaku

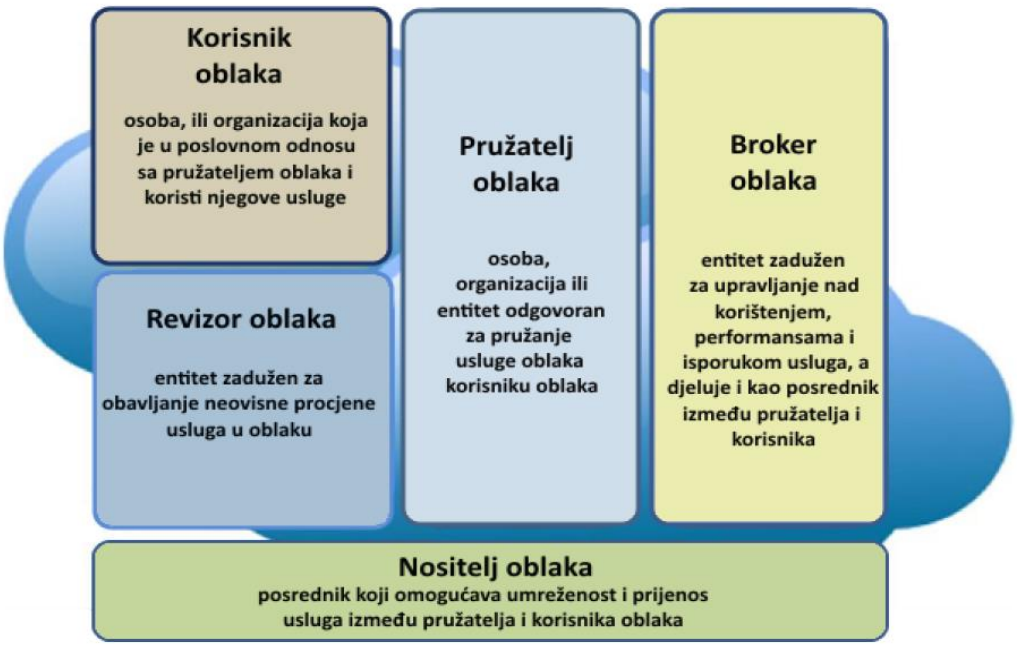
Računalstvo u oblaku relativno je širok pojam i obuhvaća infrastrukture različitog obujma sa različitim vrstama korisnika i načinima upravljanja. Definirano je kroz nekoliko modela pružanja usluga i implementacije, kao i nekoliko ključnih karakteristika. Američka vladina organizacija pod imenom Nacionalni institut standarda i tehnologija (*eng. National Institute of Standards and Technology - NIST*) bavi se definiranjem različitih standarda korištenih u tehnologiji, pa je tako, između ostaloga, definirala i računalstvo u oblaku. Prema NIST-u (2013), model računalstva u oblaku promovira dostupnost prije svega, te se sastoji od pet ključnih karakteristika, tri modela pružanja usluga i četiri modela implementacije (slika 2).

[15] Ibidem



Slika 1. - Model računalstva u oblaku prema NIST-u (Prema: Cloud Security Alliance,2011:13)

U pružanju usluga računalstva u oblaku sudjeluje i nekoliko različitih entiteta, koji su isto tako definirani od strane NIST-a, slika 3 prikazuje te entitete.



Slika 2. - Entiteti računalstva u oblaku (Prema: NIST, 2013:23)

NIST definira pet entiteta, korisnik oblaka (*eng. cloud consumer*), pružatelj oblaka (*eng. cloud provider*), revizor oblaka (eng. *cloud auditor*), broker oblaka (eng. *cloud broker*) i nositelj oblaka (*eng. cloud carrier*).[16] Svaki od ovih entiteta na neki način sudjeluje u uslugama računalstva u oblaku. Korisnik oblaka koristi usluge od pružatelja usluge oblaka u skladu sa ugovorom. Pružatelj usluge je odgovoran za dostupnost i kvalitetu usluge, također u skladu sa ugovorom o razini usluge. Nositelj u oblaku je entitet koji djeluje kao posrednik između pružatelja i korisnika, a zadaća mu je omogućiti umreženost i prijenos usluga u oblaku. Broker je zadužen za obavljanje nadzora i upravljanje nad korištenjem, performansama i isporukom usluga u oblaku, kao i za pregovaranje odnosa između korisnika i pružatelja usluge. Revizor je entitet čija zadaća je obavljanje nezavisne procjene usluga u oblaku, njihovih performansi kao i sigurnosti usluga. Struktura modela pružanja usluga u oblaku sastoji se od tri osnovna modela te je on podijeljen na softver kao servis (*eng. Software-as-a-Service - SaaS*), platformu kao servis (*eng. Platform-as-a-Service - PaaS*) i infrastrukturu kao servis (*eng. Infrastructure-as-a-Service – IaaS*).[17]

Infrastruktura kao servis isporučuje računalne resurse i mogućnost pohrane, a temelji se na virtualizaciji.[18] Softver kao servis predstavlja model isporuke softvera, gdje korisnik koristi aplikacije kojima pristupa preko web preglednika. Platforma kao servis pruža različite razvojne alate uz pomoć kojih korisnik može razvijati vlastite servise.

SaaS model korisniku pruža mogućnost korištenja aplikacija koje su dostupne unutar oblak infrastrukture. Najčešće je pristup do aplikacija realiziran putem običnog web preglednika, dok korisnik nema pristup infrastrukturi koja podržava aplikacije. Za korisnika, najvažnija je aplikacija i pristup njoj i njezinim mogućnostima, dok je čitava infrastruktura na kojoj počivaju aplikacije briga pružatelja usluge. Jedina interakcija korisnika sa pozadinskom infrastrukturom je u slučaju ako korisnik želi prilagoditi aplikaciju, odnosno konfigurirati određene postavke. Drugim riječima softver kao servis je tehnološka platforma koja omogućava korištenje aplikacija putem interneta u obliku usluge, koja se koristi i plaća prema potrebi, umjesto da se one kupuju kao zasebne

[16] National Institute of Standards and Technology NIST. 2013., NIST Cloud Computing Standards Roadmap. Dostupno na: http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf, (pristupljeno 20.ožujka 2021.).
[17] Ibidem
[18] Shah J, Patel K, Patel H. Security Issues in Cloud Computing. International Journal of Engineering and Innovative Technology (IJEIT). 2013., Dostupno na: http://ijeit.com/vol%202/Issue%2010/IJEIT1412201304_14.pdf, (pristupljeno 20.ožujka 2021.).

aplikacije namijenjene instalaciji na lokalnim računalima, čime se uvelike smanjuju troškovi jer se izbjegava kupnja, instalacija i kasnije održavanje softvera na lokalnim računalima.[19] Korisnik ne mora ulagati dodatne financijske resurse u različite programske pakete i licence, potreban mu je samo pristup do aplikacije. Najjednostavniji primjeri SaaS platforme su Google Docs, koji nudi obradu dokumenata i DropBox koji nudi pohranu podataka i dokumenata. Prednosti koje SaaS model pruža korisniku zasigurno su direktna mogućnost upotrebe, zatim činjenica kako je pružatelj usluge stalno u koraku sa tehnologijom i neovisno o platformi za koju je aplikacija namijenjena, pružatelj osigurava da ta aplikacija radi na različitim platformama. Danas je najčešća upotreba SaaS usluga u obliku korištenja raznih e-mail servisa, web konferencija, online antivirusnih rješenja, aplikacija namijenjenih za zabavu te aplikacija namijenjenih vođenju projekata.[20]

PaaS model korisniku pruža uslugu razvojne okoline u kojoj korisnik može izgraditi vlastite aplikacije koristeći programske alate koje podržava pružatelj usluge. PaaS model se koristi kod izrade različitih aplikacija, web i mobilnih, koristeći već konfigurirane komponente koje nudi i održava pružatelj usluge. Kao i kod SaaS modela, korisnik nema pristup pozadinskoj infrastrukturi, uključujući serverima, operacijskom sustavu i pohrani podataka. PaaS model pruža uslugu koja omogućuje upravljanje cjelokupnim životnim ciklusom razvoja aplikacija, od dizajna i razvoja pa do testiranja i implementiranja.[21] Neki od pružatelja PaaS usluga su EngineYard koji nudi platformu za razvoj web aplikacija, Google App Engine koji nudi programske jezike Java, Python, Go i PHP, Windows Azure koji nudi razvoj u .NET tehnologijama itd.

IaaS model korisniku kao uslugu daje na korištenje cjelokupnu računalnu infrastrukturu, odnosno virtualnu platformu. Osnovna namjena IaaS modela je pružanje korisnicima računalne resurse kao što su poslužitelji, mrežne komponente i

[19] Padhy RP, Patra MR, Sataphy SC. Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2011., Dostupno na: http://ijcsits.org/papers/Vol1no22011/13vol1no2.pdf, (pristupljeno 20.ožujka 2021.).
[20] Sathiyapriya K, Malathi D, Vijaya Kumar K, Nagadevi S. A Study on Security Challenges and Issues in Cloud Computing. International Journal of Security Challenges and Issues in Cloud Computing. 2013., Dostupno na: http://www.ijeit.com/vol%202/Issue%207/IJEIT1412201301_47.pdf, (pristupljeno 20.ožujka 2021.).
[21] Sathiyapriya K, Malathi D, Vijaya Kumar K, Nagadevi S. A Study on Security Challenges and Issues in Cloud Computing. International Journal of Security Challenges and Issues in Cloud Computing. 2013., Dostupno na: http://www.ijeit.com/vol%202/Issue%207/IJEIT1412201301_47.pdf, (pristupljeno 20.ožujka 2021.).

komponente za pohranu.[22] Umjesto da korisnik troši financijske resurse na kupnju poslužitelja, softvera, licenci, mrežne opreme i uređaja za pohranu, on plaća samo uslugu korištenja virtualne infrastrukture pružatelju usluge. IaaS platforma pogodna je za organizacije koje žele svoje resurse usmjeriti u obavljanje temeljne djelatnosti, a ne žele dodatno trošiti na opremanje i upravljanje lokalnim računalnim resursima. Danas se pojavljuje sve više pružatelja IaaS usluga, a najpoznatiji i najveći pružatelji su Amazon Web Servisi, Windows Azure, Google Compute Engine, IBM SmartCloud Enterprise itd.

Općenito, prijelaz na korištenje oblak usluga zasigurno donosi znatne financijske uštede, no samo ako organizacije prepoznaju svoje stvarne potrebe i u skladu sa njima odaberu određene usluge u oblaku. Prije samog odabira modela oblak usluge, korisnici trebaju pažljivo izabrati model koji najbolje odgovara njihovim potrebama te sukladno tome odabrati i pružatelja usluge.
Ponuda oblak usluga danas je široka, te postoji veliki broj pružatelja usluga čija međusobna konkurentnost dovodi do razvoja novih rješenja i inovacija od kojih krajnji korisnik može profitirati. Također, ovisno o odabranom modelu, korisnik ima ili manje ili više kontrole nad podacima koje stavlja u oblak, a o tome ovisi i njegovo povjerenje u sigurnost same usluge.

2.5. Infrastruktura kao servis (IaaS)

IaaS kao model ukratko je opisan u prethodnom poglavlju, u ovom dijelu istaknute su neke od prednosti IaaS – a.

Glavna prednost IaaS usluge svakako je fleksibilnost u smislu ulaganja i korištenja IT infrastrukture. Na jednom banalnom primjeru može se dočarati kako nekakvo hipotetsko poduzeće može u kratkom periodu fleksibilno utjecati na infrastrukturne resurse. Kada govorimo o banalnom primjeru možemo navesti povećanje broja zaposlenika / korisnika sustava unutar poduzeća kojima je radi povećanog opsega poslovanja potreban dodatan kapacitet resursa u obliku webmail servera, klasičnog

[22] Padhy RP, Patra MR, Sataphy SC. Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2011., Dostupno na: http://ijcsits.org/papers/Vol1no22011/13vol1no2.pdf, (pristupljeno 20.ožujka 2021.).

web servera ili interne platforme za pohranu raznih podataka, a može biti i bilo što drugo.

U klasičnom obliku gdje poduzeće koristi vlastitu infrastrukturu postoji niz stvari koje je potrebno uzeti u obzir, a utječu na brzinu i efikasnost unapređenja sustava. Najuočljivija i najveća stavka svakako su troškovi ulaganja u povećanje kapaciteta sustava jer iziskuje provođenje klasične fizičke nabave komponenti za unapređenje infrastrukture te posljedično zahtjeva određeni vremenski okvir za implementaciju tj. ugradnju komponenti i konfiguriranje sustava. Kao neželjene posljedice odmah su uočljive mogućnosti nastanka poteškoća u radu zaposlenika / korisnika, a protekom vremena pojavljuju se i dodatni troškovi poput redovnog održavanja infrastrukture i zamjene iste uz neophodno kontinuirano ulaganje u ažuriranje. Cijeli proces sa svojim pozitivnim i negativnim učincima još može i biti prihvatljiv ako se radi o unapređenju koje je dugotrajno potrebno, međutim u današnje vrijeme kada je poslovanje poduzeća izrazito dinamično te povećani resursi nisu nužno potrebni na duže vrijeme, postavlja se pitanje opravdanosti i dugotrajne isplativosti ulaganja u takve fizičke kapacitete. U ovom hipotetskom primjeru radilo se o prilično banalnim potrebama, ali danas postoje potrebe raznih znanstveno – istraživački usmjerenih poduzeća i obrazovnih ustanova koje za potrebe istraživanja trebaju resurse na razini super računala ili grupe računala radi izvođenja zahtjevnih matematičkih operacija s ogromnim brojem varijabli. U takvim situacijama, IaaS dolazi do izražaja sa svim svojim prednostima. [23]

Uz već spomenuto reduciranje direktnih i indirektnih troškova konfiguriranja i upravljanja fizičkim resursima postoji i niz drugih prednosti poput sigurnosti aplikacija i podataka, povećanja stabilnosti, pouzdanosti i same podrške u funkcioniranju infrastrukture, u slučaju katastrofe omogućava kontinuitet poslovanja i oporavak od same katastrofe te na kraju krajeva omogućava da gdje god u svijetu želimo, možemo utjecati na performanse infrastrukture da zadovolji trenutne potrebe.

Iako postoji niz prednosti, potrebno je reći kako IaaS ima i svojih određenih manjkavosti te možda nije primjeren za sva poduzeća, osobe ili ustanove. Postoje i stvari koje jednostavno nije moguće povezati s aplikacijama trećih strana te tada jedno od rješenje postaje izgradnja vlastitog IaaS sustava na vlastitoj lokalnoj infrastrukturi. U takvoj situaciji sve troškovne prednosti IaaS-a više ne postoje.

[23] https://azure.microsoft.com/en-us/overview/what-is-iaas/

Fleksibilnost u plaćanju i određivanju resursa koji se žele koristiti predstavlja prednost, ali i određenu manjkavost te nekim korisnicima može biti problem. Naplatni sustav za korištenje IaaS sustava izrazito je detaljan i podijeljen u više segmenata kako bi se postigla što preciznija upotreba usluga i iskorištenost resursa. Zato je potrebno konstantno pratiti što sve uključuje pojedina ugovorena stavka, te istovremeno pratiti i usluge koje se koriste kako bi se izbjeglo naplaćivanje ostalih usluga po većim cijenama jer prvotno u paketu nisu bile specificirane, odnosno korištene su kao dodatne usluge. U takvim situacijama najčešće dolazi do problema i nerazumijevanja stvarnih potreba i ugovorenih resursa što uzrokuje povećane troškove.[24]

Jedan od ne toliko spominjanih problema je i netransparentnost uvida u infrastrukturu. Kako su pružatelji IaaS usluge vlasnici fizičke infrastrukture, rijetko kada daju na uvid detalje konfiguracije same fizičke infrastrukture, a još rjeđe i izvedbu iste. Problem kod takve netransparentnosti predstavlja buduće upravljanje i nadzor nad samim sustavom. Postavlja se pitanje postoji li iza oku ugodnog sučelja i odgovarajuća infrastruktura koja se održava sukladno standardima dobre prakse pogotovo u smislu odgovarajućih prostornih uvjeta, zaštite podataka i slično.

Najspominjaniji problem kod IaaS usluge svakako je otpornost na poteškoće s prometom, spajanjem te utjecaj ostalih korisnika.

Kako je Internet veza tj. propusnost mreže ključna stvar u korištenju IaaS usluge predstavlja pojava "uskog grla" koje otežava pristup zakupljenim resursima i samim time lančano se odražava na sve ostale aplikacije koje se oslanjaju na predmetnu infrastrukturu. Nastavno na propusnost mreže uvijek su moguće poteškoće i u obliku preopterećenosti fizičke infrastrukture jer nije poznato s kime se infrastruktura dijeli, pa je tako moguće da postoji na istoj fizičkoj infrastrukturi još jedan ili više korisnika koji sa svojim većim zahtjevima značajno utječu na ostale korisnike s kojima dijele fizičku infrastrukturu.

U današnje vrijeme poduzeća i institucije sve više se okreću IaaS modelu za svoja radna opterećenja iz razloga što ima visoku stabilnost, pouzdanost te na kraju krajeva podršku koja rješava eventualne probleme. U odnosu na klasične lokalne sustave koji zahtijevaju dodatan prostor za smještaj opreme te značajna financijska sredstva IaaS model ima još jednu dodatnu vrijednost, a to je redundancija koja je u pravilu ugrađena

[24] https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

na svakom sloju, bolju sigurnosnu zaštitu te opseg dodatnih usluga koje se može vrlo brzo aktivirati.

Velika većina ozbiljnih pružatelja oblak usluga tj. usluga u oblaku koristi najnoviju hardversku opremu pa se već samim time eliminira potreba da poduzeće ili ustanova samostalno provodi postupak utvrđivanja kakvu opremu treba kupiti. Isto tako nema potrebe za provođenjem dodatnih edukacija i treninga kako bi se istu moglo nadograditi jer sve to odrađuje pružatelj usluge.[25]

Praktički svi pružatelji usluga u oblaku ističu prednosti njihovog korištenja, ponajprije ističući troškove tj. uštede. Ali treba obratiti pozornost i na manjkavosti koje se mogu pojaviti od pružatelja do pružatelja, zato kod odabira IaaS pružatelja usluge treba obratiti pozornost na reputaciju onoga tko uslugu pruža, ako je moguće provjeriti iskustva korisnika te svakako biti siguran kako su naše potrebe točno specificirane kako bi se izbjegli nepotrebni troškovi korištenjem usluga koje nisu ugovorene u prvotnom paketu. U nastavku rada fokus je stavljen na sustav / platformu Microsoft Azure.

[25] https://www.oracle.com/cloud/what-is-iaas/

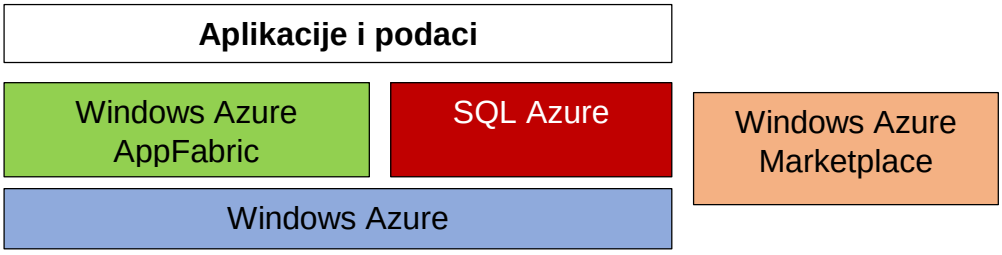
3. Microsoft Azure

Azure je Microsoftova platforma za računalstvo u oblaku, razvijena za stvaranje, postavljanje i upravljanje aplikacijama i uslugama putem globalne mreže, kojom upravlja tvrtka Microsoft ili Microsoftov partner domaćin podatkovnih centara. Azure pruža usluge temeljene na oblaku u sva tri modela sustava: SaaS, PaaS i IaaS. Neovisno o korisničkom odabiru modela sustava, u današnje vrijeme, servisi su nezamislivi bez primjene virtualizacije. U svakom modernom sustavu, virtualizacija osigurava razvojna okruženja i baze podataka u oblaku pa čak i operacijske sustave. IaaS predstavlja značajan sustav u procesu migracije na oblak i u današnje vrijeme je sveprisutan u poslovnom okruženju, bilo da se radi o testnom ili razvojnom okruženju ili proširenju podatkovnog centra.

3.1. Komponente platforme Microsoft Azure

Azure nudi poslužitelj smješten u oblaku i ostale infrastrukturne resurse poput pohrane, mreže i druge integracijske infrastrukture za stvaranje, postavljanje i pokretanje aplikacija bez potrebe za izgradnjom vlastite infrastrukture. Platforma usluge Azure sastoji se od četiri dijela usmjerena na oblak:[26]

- Windows Azure - Windows okruženje za pokretanje aplikacija i pohranu podataka na računalima u Microsoft podatkovnim centrima
- SQL Azure - Relacijske podatkovne usluge u oblaku temeljene na SQL Serveru
- Windows Azure App Fabric - Usluge infrastrukture temeljene na oblaku za programe koji se izvode u oblaku
- Windows Azure Marketplace - Internetska usluga za kupnju podataka i aplikacija temeljenih na oblaku (slika 4.)



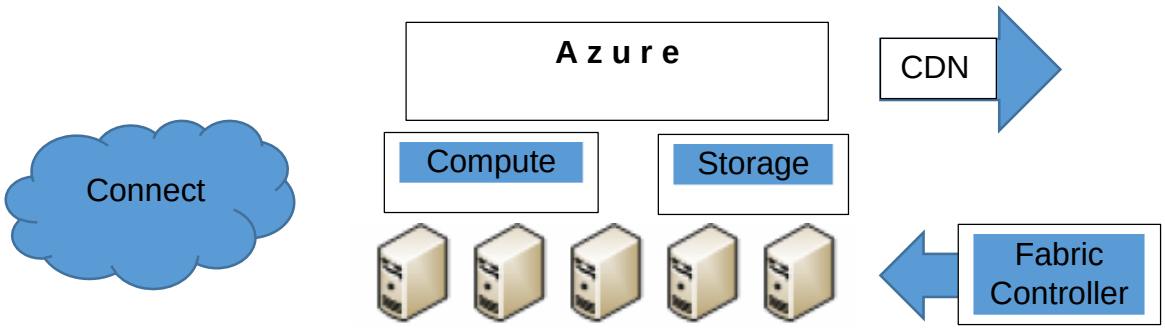
Slika 3. - Entiteti računalstva u oblaku

[26] Chappell D. Introducing the Windows Azure platform. David Chappell & Associates, 2010., str. 3.

Sve ove četiri komponente pokreću se u Microsoftovim podatkovnim centrima smještenim širom svijeta: dvije u Sjevernoj Americi, dvije u Europi i dvije u Aziji. Programeri koji koriste platformu mogu kontrolirati koji podatkovni centar pokreće njihove aplikacije i pohranjuje njihove podatke, pružajući im mogućnost da obje postave bliže svojim korisnicima. Svaki dio ima svoju ulogu što će biti detaljnije opisano u nastavku.

3.2. Windows Azure

Azure u svrhu distribucije aplikacija osigurava potrebitu infrastrukturu i platformu. Aplikacije se razvijaju za određene platforme s operacijskim sustavom, sustavom za pohranu podataka i ostale servise. Razvoj aplikacija za Azure se vrši na isti način kao i za klasične web aplikacije. Azure pokreće Windows programe i pohranjuje podatke u oblak. Slika 4 prikazuje njegove komponente.



Slika 4. - Komponente Azure

3.2.1. Compute

Usluga Azure pokreće aplikacije temeljene na Windows Serveru koje se mogu kreirati pomoću .NET Framework na jezicima kao što su C # i Visual Basic, ili se mogu graditi bez .NET-a na C ++, Javi i drugim jezicima. Programeri mogu koristiti Visual Studio ili druge razvojne alate i mogu slobodno koristiti tehnologije kao što su ASP.NET, Windows Communication Foundation (WCF) i PHP. Izvršavanje aplikacija u Azureu čini kombinacija procesorske snage i fizičke memorije.[27]

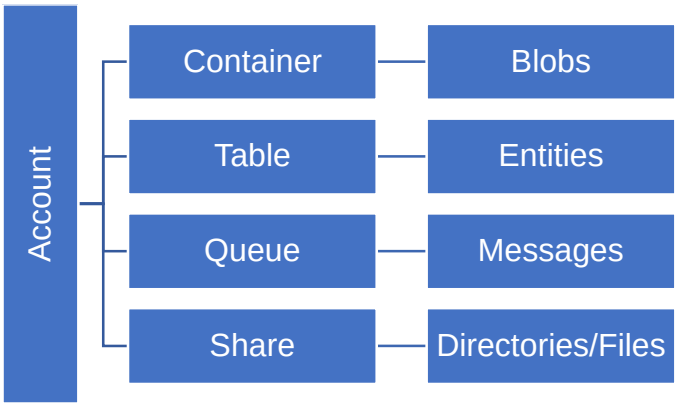
[27] Mazumdar P, Agarwal S, Banerjee A. Pro SQL Server on Microsoft Azure. Apress, 2016., str. 20.

Prema Mazumdar i sur. (2016) kada se započne s raspoređivanjem izvršavanja u Azureu, u osnovi se stvara virtualni stroj s operativnim sustavom potpomognutim lokalnom pohranom u kojoj se nalaze datoteke operativnog sustava i privremeno skladište.[28]

3.2.2. Storage

Usluga Storage omogućuje dohvaćanje i pohranu binarnih velikih objekata (engl. Blobs) koji mogu biti veličine 1 TB. Azure Storage pruža temelj za pohranu svih Azure virtualnih strojeva. To obuhvaća sva načela oblaka, što znači da je Azure pohrana skalabilna, trajna i visoko dostupna. Još jednom. Prednost oblaka je što se plaća ono što se koristi i kada se koristi. Azure Storage koristi sustav automatskog razdvajanja koji automatski uravnotežuje opterećenje podataka na temelju prometa. Kako zahtjevi za pohranom aplikacije rastu, Azure Storage automatski dodjeljuje odgovarajuće resurse za pohranu kako bi ih zadovoljio. Kao i svaka Azure komponenta, Azure Storage je dostupan s bilo kojeg mjesta na svijetu. Jedinstveni aspekt Azure Storage jest da bilo koja vrsta aplikacije, bilo da je pokrenuta iz oblaka, radne površine na računalu, lokalno, s mobilnog uređaja ili tableta, mogu pristupiti usluzi Azure Storage.

Kao što je prikazano na slici 6, Azure Storage je organizirana u različitim formatima - blobs, tablice, redovi i datoteke. Skladištenje je organizirano u obliku spremnika, tablica, redova. Pohrana u Azureu razdvojena je u spremnike određene vrste.



Slika 5. - Koncept Azure Storage (Prema: Mazumdar, 2016:23

[28] Mazumdar P, Agarwal S, Banerjee A. Pro SQL Server on Microsoft Azure. Apress, 2016., str. 20.

3.2.3. Fabric Controler

Fabric Controler se odnosi skupinu usluga koja služi korisnicima za povezivanje i integraciju aplikacija na njihovim serverima ili sa Microsoftovim i drugim aplikacijama i uslugama na Internetu. Usluga služi da programeri iz komponenti raznih aplikacija stvore jednu cjelinu. U svrhu funkcioniranja aplikacije, programeri se moraju osloniti na infrastrukturu aplikacije. Ukratko, usluga ima ulogu osiguranja infrastrukture za izvršavanje aplikacija.

3.2.4. Content delivery network (CDN)

Mreža za isporuku sadržaja služi za ubrzavanje pristupa korisnicima često korištenim podatcima. Windows Azure CDN to omogućuje za velike binarne objekte, osiguravajući kopije koje su pred memorirane na webu diljem svijeta.

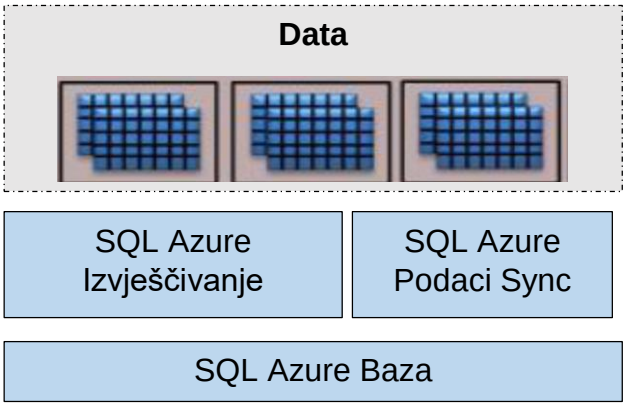
3.2.5. Connect

Organizacijama je često korisno komunicirati s programima u oblaku. Azure Connect to omogućuje, olakšavajući pristup aplikaciji Azure lokalnoj bazi podataka. Pokretanje aplikacija i pohranjivanje podataka u oblaku mogu imati jasne prednosti. Umjesto da organizacija kupuje, instalira ili izrađuje vlastite sustave, organizacija se može osloniti na pružatelja usluga u oblaku koji će to učiniti ih. Također, korisnici plaćaju samo računalne usluge i pohranu koje koriste, umjesto da održavaju set poslužitelja samo za vršna opterećenja. Aplikacije napisane za Windows Azure mogu se bolje skalirati, biti pouzdanije i zahtijevaju manje administracije od onih napisanih pomoću tradicionalnog modela Windows Server programiranja. Da bi stvorili, konfigurirali i nadzirali aplikacije, korisnici Windows Azurea mogu se koristiti portalom. Korisnik se prijavljuje pomoću Windows Live ID-a, a zatim biraju žele li stvoriti račun za hosting pokretanje aplikacija, račun za pohranu podataka ili oboje.

3.3. SQL Azure

Uz pokrenute aplikacije, još jedan atraktivan način korištenja oblaka je pohranjivanje podataka. SQL Azure ima standardna obilježja relacijskih baza podataka i nudi usluge koje se izvode na Azure oblaku te im je moguće pristupati, dodavati ih i mijenjati.

Kao što prikazuje slika 7, SQL Azure uključuje tri komponente: SQL Azure Database, SQL Azure Reporting i SQL Azure Data Sync.



Slika 6. - Komponente SQL Azure

3.3.1. SQL Azure Database

SQL Azure baza podataka je jednostavna za razumijevanje. Pruža temeljnu bazu podataka funkcije SQL Servera kao usluge u oblaku. Slika 7 prikazuje osnove ove tehnologije. Aplikacija koja koristi SQL Azure bazu podataka može se izvoditi na Windows Azureu, u podatkovnom centru poduzeća, na mobilnom uređaju ili negdje drugdje. Gdje god da se izvodi, aplikacija obično pristupa podacima putem protokola Tabular Data Stream (TDS). Ovo je isti protokol koji se koristi za pristup lokalnom SQL poslužitelju baze podataka, pa aplikacija SQL Azure baze podataka može koristiti bilo koji postojeći klijent SQL Servera. Ovo uključuje Entity Framework, ADO.NET, ODBC, PHP i drugi.

Svaki SQL Azure račun može imati jedan ili više logičkih poslužitelja. Svaki poslužitelj tada može imati više baza podataka, od kojih svaki može biti do 50 gigabajta.
Korisnik može slobodno koristiti višestruke baze podataka ako je potrebno, šireći podatke u njima u svrhu boljih performansi ili iz drugih razloga. Budući da

administracijom upravlja Microsoft, usluga ne izlaže fizičko upravne funkcije. Korisnik ne može ugasiti sustav, na primjer, niti izravno komunicirati s hardverom na kojem radi. Upit se može pokretati samo ograničeno vrijeme - niti jedan zahtjev ne može zauzeti više od unaprijed definirane količine resursa.

Kao i kod Windows Azure Storage, svi podaci pohranjeni u SQL Azure. Baza podataka replicira se tri puta, radi visoke dostupnosti. Također, poput usluge Windows Azure Storage pruža snažnu dosljednost: Kada se zapis vrati, podaci su postali trajni. Cilj je pružati pouzdanu pohranu podataka čak i uslijed kvarova u sustavu i na mreži. Bez obzira treba li aplikaciji više baza podataka ili samo jedna, SQL Azure baza podataka može pomoći programerima adresirati niz scenarija. Koji god problem bio riješen, temeljni cilj tehnologije ostaje isti: pružiti poznatu, pouzdanu i jeftinu bazu podataka u oblaku za razne vrste aplikacija.

3.3.2. SQL Azure Reporting

Pohranjivanje podataka u SQL Azure bazu podataka može biti korisno. Međutim, čim ti podaci postoje, vjerojatno će postojati potražnja za izvješćima na temelju tih podataka. Ispunjavanje ovog zahtjeva svrha je SQL Azure Reporting. Na temelju SQL Server Reporting Services (SSRS), ova tehnologija pruža stvaranje izvještaja na temelju računarstva u oblaku. S obzirom na to da SQL Azure baza podataka aplikaciji izgleda kao SQL Server, uvijek je moguće upotrebljavati SSRS s podacima koje sadrži. SQL Azure Reporting ima za cilj da se izvješća kreirana pomoću SQL Azure Reportinga mogu objaviti na portalu SQL Azure Reportinga, dopuštajući da korisnici tamo pristupe ili su im dostupni izravno putem URL-a. SQL Azure Reporting je dizajnirano za rad s podacima pohranjenim u SQL Azure bazi podataka. Izvješća koja se koriste s SQL-om Azure Reporting kreira se lokalno, međutim, pomoću programa Business Intelligence Developer Studio, alat Visual Studio-hosted se također koristi za stvaranje SSRS izvješća. U stvari, SQL Azure izvještavanje oslanja na isti format izvještavanja, izražen u jeziku za definiciju izvješća (RDL), koji se koristi s SSRS-om.

3.3.3. SQL Azure Data Sync

SQL Data Sync je usluga Microsoft Azure koja pruža automatsku sinkronizaciju podataka kroz niz baza podataka.[29]

Pohranjivanje podataka u SQL Azure bazi podataka može ga učiniti dostupnim bilo kojoj aplikaciji s internetskom vezom. Ipak, često postoje situacije u kojima ima smisla zadržati kopiju podataka temeljenih na oblaku na nekim drugim mjestima. Npr. neka organizacija mora imati lokalnu kopiju istih podataka, radi osiguranja pristupa ako mreža zakaže. Za ovakve scenarije, korisna je mogućnost sinkronizacije podataka u SQL Azure bazi podataka s drugim spremištima podataka.

SQL Azure Data Sync koristi model hub-and-spoke. Sve se promjene prvo kopiraju u središte baze podataka SQL Azure, zatim do članova. Članovi bi mogli biti druge baze podataka SQL Azure ili lokalne baze podataka SQL Server. U oba slučaja tehnologija omogućuje sinkronizaciju cjeline baza podataka ili samo određene tablice, s promjenama u bilo kojoj kopiji koja se širi na sve ostale. I dok moguće je pokrenuti sinkronizaciju ručno, SQL Azure Data Sync također uključuje uslugu planiranja. To korisnicima omogućuje satne sinkronizacije između para baza podataka. Kako god se koristi, svrha je ista: pružanje izravnog načina sinkronizacije podataka između SQL Azure baze podataka u Microsoftovom podatkovnom centru i jednoj ili više baza podataka smještenih negdje drugdje.

[29] Lobel G.L, Boyd E.D. Miccrosoft Azure SQL Database Step by Step. Redmond, Washington: Microsoft Press, 2014., str. 202.

3.4 Azure App Fabric

Azure Service Fabric je platforma kao usluga (PaaS) koju nudi Microsoft. Azure SQL baza podataka, Azure DocumentDB, Azure IoT, Cortana, Power BI, Microsoft Intune i Skype za tvrtke, neki su od Microsoftovih proizvoda koji koriste Service Fabric. Azure. Azure App Fabric omogućuje upravljanje životnim ciklusom aplikacija, pruža usluge orkestracije spremnika i procesa, te nadzor monitoringa aplikacija.

Jedna od osnovnih mogućnosti App Fabric-a su:

- Servisna sabirnica: relej za poruke koji mogu koristiti druge .NET tehnologije (i druge). Servisna sabirnica pomaže u povezivanju različitih usluga u oblaku, kao i "hibridnih" usluga. Hibrid je velika stvar, jer servisa sabirnica pomaže da povežemo lokalne usluge s uslugama koje pokrećete u oblaku, bez potrebe za petljanjem s VPN-om, protokolima, postavkama poslužitelja, certifikatima itd.

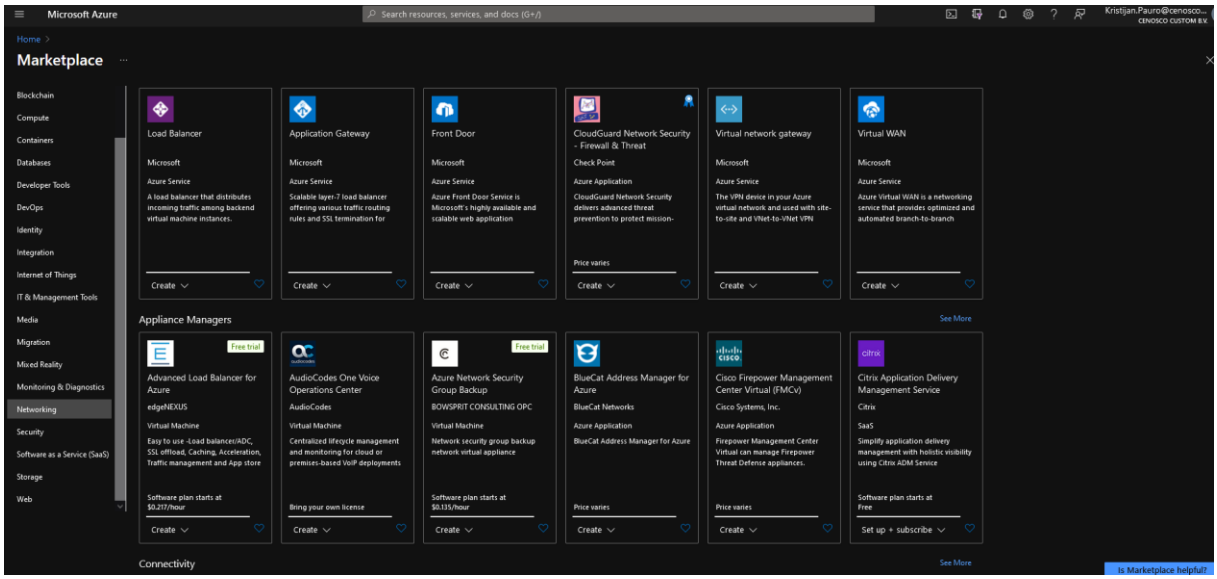
- Kontrola pristupa: Usluga provjere autentičnosti i autorizacije koja pomaže u upravljanju pristupom na razini korisnika bez potrebe za proširivanjem / implementacijom Active Directory, LDAP-a i prilagođenih modula za provjeru identiteta korisnika u cijelom Azureu.

- Integracija: PaaS usluga EDI / transportne tehnologije poput BizTalk poslužitelja.

- Kompozitna aplikacija: U osnovi definiramo svoju aplikaciju pomoću dizajnera kao što bismo to učinili sa EF.Netovim podatkovnim modelom ili Windows Workflowom.

3.5 Windows Azure Marketplace

Internetska trgovina koja nudi programe i usluge, nadograđene ili dizajnirane za integraciju sa Microsoftovim javnim oblakom Azure. Svi proizvodi i usluge od Microsoft Azure dolaze direktno od Microsofta ili njegovih tehnoloških partnera. Sami proizvodi koje nudi Microsoft su certificirani putem Microsoft Azure Certifikata kako bi se osigurala kompatibilnost s javnim oblakom Azure.[30] Jedan od primjera Azure Marketplace prikazan je na slici 7. – Azure Marketplace.



Slika 7. – Azure Marketplace (Prema: Azure portalu Cenosco)

[30] https://docs.microsoft.com/en-us/azure/marketplace/overview

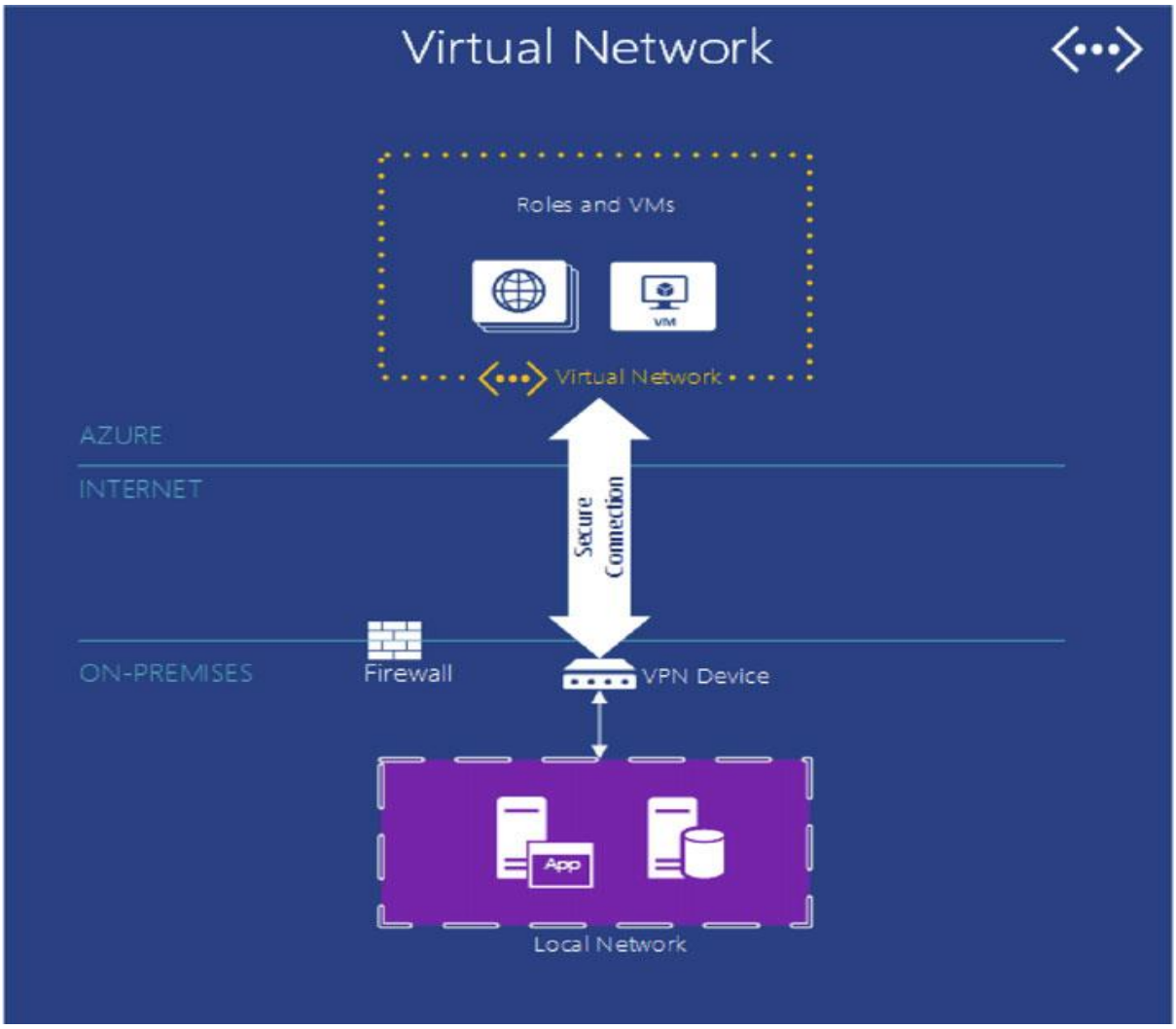
4. Azure virtualna mreža

VPN odnosno virtualna privatna mreža je tehnologija koja se počela značajnije razvijati u bližoj prošlosti. Naime njena popularnost je sve više porasla nakon velikom interesa tvrtki i organizacija koje za cilj imaju proširiti i/ili poboljšati postojeću infrastrukturu, ali naravno uz što manje troškove. VPN se prije svega koristi kad korisnik treba povezati dvije ili više svojih adresa, ali to nije u stanju izvesti zbog loših ili nepostojećih tehničkih uvjeta ili zbog visoke cijene. Zato se umjesto fizičkog spajanja ili virtualnog prividnog voda koristi VPN.
Prije svega, kada se kaže VPN, misli se na korištenje napredne tehnologije kako bi se povezala udaljena računala u privatne virtualne mreže, a pritom se koristi dijeljena ili javna telekomunikacijska infrastruktura (internet).

Sama riječ „virtualna“ odnosi se na način spajanja računala koji ne moraju biti fizički tj. izravno povezana, već posredno preko javnih mreža za prijenos podataka. Pojam „privatna“ se odnosi na „nemogućnost“ prisluškivanja komunikacije ili sudjelovanja u njoj (ili je ne može razumjeti). Naravno ovakva vrsta privatnosti osigurana je algoritmima kriptiranja pomoću kojih samo sudionici komunikacije mogu pročitati izvornu poruku (podatak). Pojam „mreža“ odnosi se na povezanost korisnika koji se nalaze povezani VPN mrežom, znači svi su međusobno povezani i u mogućnosti su komunicirati, slati podatke, informacije te razne druge stvari.

Azure virtualna mreža predstavlja lokalnu mrežu u oblaku. Omogućuje drugim Azure resursima da komuniciraju putem sigurne privatne mreže bez izlaganja krajnje točke putem Interneta.[31] Azure virtualna mreža (engl. Azure Virtual Network-VNet) temeljni je element privatne mreže u Azure-u. VNet omogućuje mnogim vrstama Azure resursa, kao što su Azure virtualni strojevi (engl. Virtual Machines-VM), sigurnu međusobnu komunikaciju, internet i lokalne mreže (slika 8). Virtualna mreža omogućuje komunikaciju Azure resursa s internetom, komunikaciju između Azure resursa, komunikaciju s lokalnim resursima, filtriranje mrežnog prometa, usmjeravanje mrežnog prometa i integraciju s Azure uslugama.[32]

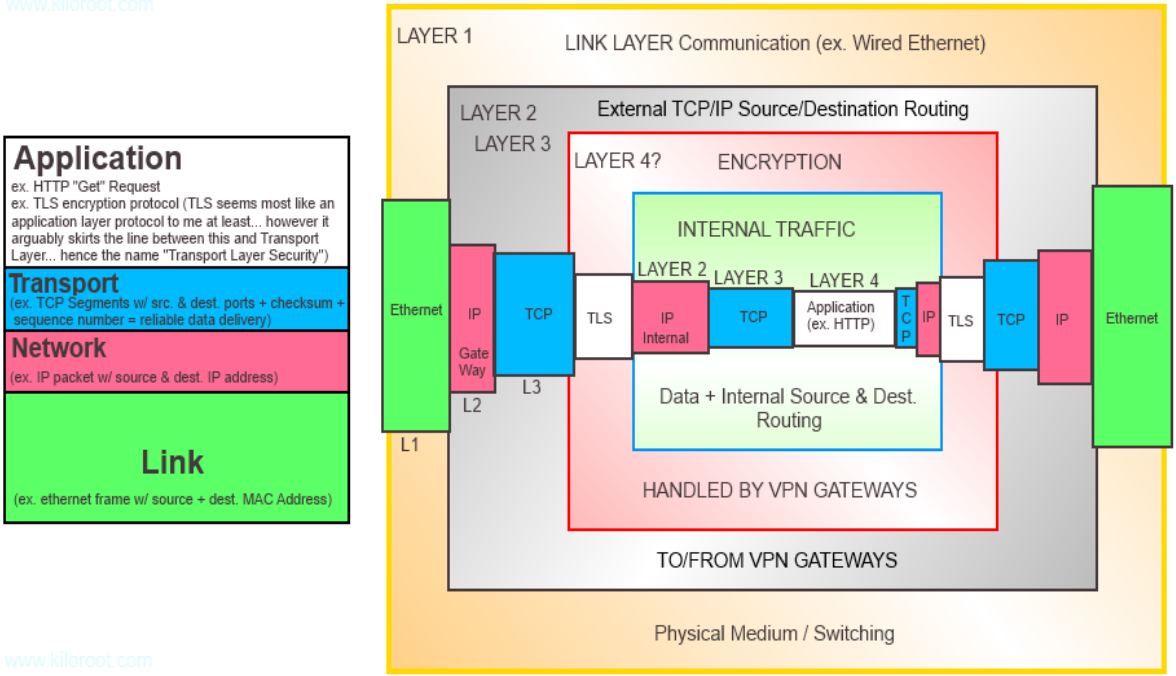
[31] Toroman M. Azure Networking Cookbook. Birmingham, UK: Packt Publishing, 2020., str. 2.
[32] Mazumdar P, Agarwal S, Banerjee A. Pro SQL Server on Microsoft Azure. Apress, 2016., str. 13.



Slika 8. - Azure VPN (Prema: Mazumdar, 2016:13)

Slika 8. Pokazuje mogućnost spajanja putem VPN uređaja u našem slučaju je to Edge Ubiquity usmjerivač koji se koristi za spajanje preko naše lokalne mreže u virtualnu mrežu, koja propušta promet preko vatro zida na naše virtualne mašine koje se nalaze u Azure oblaku. Na Azure strani postavljena su pravila i postavke za spajanje na udaljene mašine prema trećim stranama, odnosno klijentske mašine od Shell-a kojima se pristupa putem RDP konekcije.

4.1. Prikaz VPN enkapsulacije kroz TCP/IP slojeve



Slika 9. – TCP/IP diagram

- Sloj 4: je sloj Aplikacije kojem pripadaju (HTTP, FTP, TLS)
- Sloj 3: je sloj Transporta tu pripadaju (TCP- Protokol za upravljanje prijenosom podataka, (3389 port for RDC- Protokol udaljenje površine), UDP, IPSec
- Sloj 2: je Mrežni sloj (IP- adresa)
- Sloj 1: je sloj veze (fizički mediji + MAC adrese)

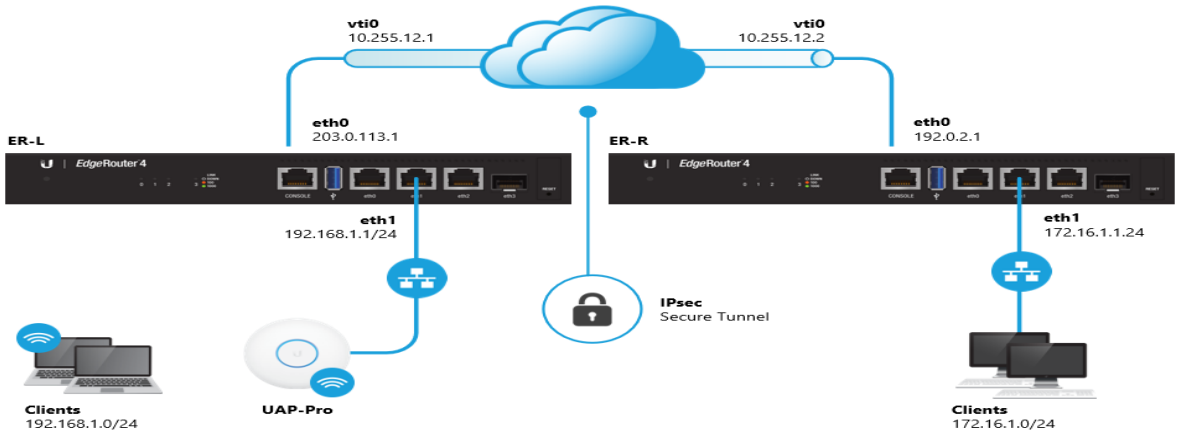
Na primjeru sa desne strane slika.9 koja prikazuje kako VPN enkapsulacija djeluje. Na primjer, HTTP dobiva zahtjev za primanjem (aplikacijski sloj) enkapsuliran unutar TCP segmenta (transportnog sloja) enkapsuliranog unutar IP paketa (Sloj mreže) koji je onda enkapsuliran unutar internet okvira (sloj veze) koji se šalje žicom. Putem našeg VPN mi zapravo „razgovaramo“ sa drugom mrežom, za koju želimo da bude na istoj mreži. Mi zapravo enkapsuliramo naš HTTP GET zahtjev (aplikacijski sloj) unutar transportnog i mrežnog sloja za našu lokalnu mrežu.

Kad se ovakav zahtjev pošalje na naša VPN vrata (VPN klijent koji je instaliran na našem lokalnom računalu) koje koristi TLS 1.2 trenutno, (sa mogućnosti prelaska na 1.3 TLS koji je još uvijek u probnoj fazi), za enkripciju svih informacija te počinje sa enkapsulacijom u sloj transporta i mrežnog sloja sa svrhom preusmjeravanja na odredišnu mrežu VPN vrata. Nakon što stigne na odredišnu točku VPN vrata raspakiraju šifrirane podatke TLS-a koji se zatim dešifriraju, te se nešifrirani mrežni sloj koji sadrži podatke o TCP sloju i aplikacijskom sloju, koji se usmjerava kroz odredišnu mrežu jer su slojevi transporta, mreže i aplikacijski sloj bili pakirani za odredišnu mrežu. Svatko može presresti promet, bio on dijeljen preko naše lokalne mreže ili putem javnog interneta, mogao bi vidjet izvornu i odredišnu adresu VPN pristupnika, ali dalje od toga neće imat bilo kakve informacije o podacima koji se međusobno razmjenjuju, jer je sve šifrirano putem TLS-a.[33]

[33] Radovan M (2010), Računalne mreže (1), Rijeka, od 15str. do 24

4.2. EdgeRuter Site-to-Site VPN spajanje udaljenih lokacija

Jedna od mogućnosti spajanja VPN-a u Cenosco d.o.o je putem Edge usmjerivača bazirana Site-to-Site VPN. IPSec Tradicionalni VPN-a koji je temeljen na IP sigurnosti koji rade na 3 sloju (mrežnom sloju) prema OSI-sloju. 192.168.1.0/24 i 172.16.1.0/24 mreže mogu komunicirat jedna sa drugom putem VPN-a. VPN zasnovan na ruti slika 10. koristi usmjerena tunelska sučelja kao krajnje točke virtualne mreže. Promet koji prolazi kroz sučelje tunela smješta se u VPN. Formiraju se statičke ili dinamičke IP rute za usmjeravanje željenog prometa kroz sučelje VPN tunela. Sama uspostava ovakve VPN mreže kreće tako što se dvije krajnje točke tunela dogovore oko sigurnih pravila, što bi bilo skup nekakvih parametra kao što su algoritmi kriptografije, ključ enkripcije. IPsec koristi uz pomoć IKE ključa, koristeći zajedničku lozinku, ili u našem slučaju djeljiv ključ za autorizaciju. Svaki L2TP paket u komunikaciji između dvije strane se najprije sprema pa tek onda kriptira unutar IPsec paketa. Na takav način se onemogućava pristup bilo kakvih informacija o VPN-u. Nakon što L2TP paket stigne na krajnje odredište gdje je i bio poslan njegov ulaz postaje bitan tek kad krajnji uređaj primi i dekriptira IPsec paket, tj. kad je već prošao kroz vatrozid.[34]



Slika 10.- EdgeRouter - IPsec VPN od web-mjesta do web-mjesta temeljenog na ruti

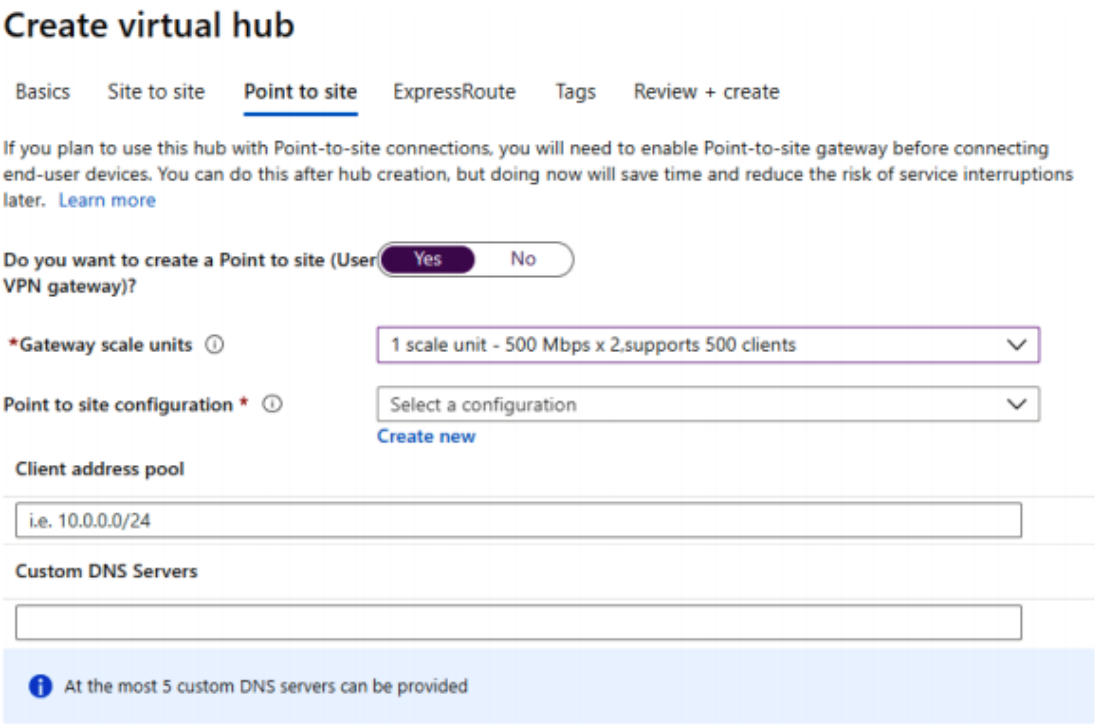
[34] https://security.foi.hr/wiki/index.php/VPN_mre%C5%BEe_-_OpenVPN_i_IPSEC.html

4.3. VPN mogućnosti spajanja na Azure mrežnu infrastrukturu

Opcije povezivanja omogućuju korisnicima da povežu svoje lokalne mreže sa svojim Azure mrežama. Te mogućnosti uključuju: Point-to-site VPN konekcije, Site-to-site VPN konekcije i ExpressRoute konekcije.

4.3.1. Point-to-site VPN

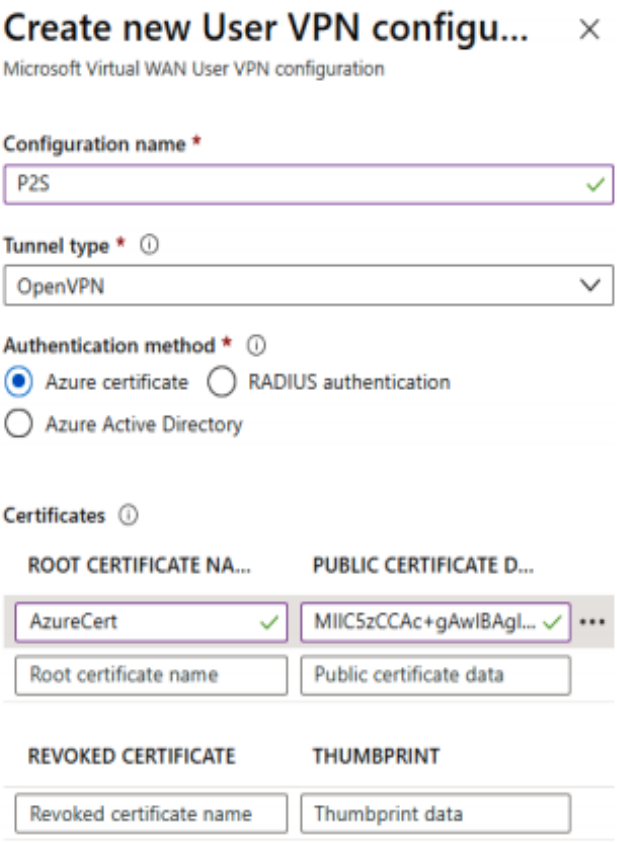
Point-to-site VPN omogućuje korisnicima stvaranje sigurne veze sa svojim Azure virtualnim mrežama s klijentskog računala u lokalnim mrežama. Point-to-site konekcije trebaju biti konfigurirane pojedinačno na svakom klijentskom računalu koje se treba povezati s virtualnom mrežom.[35] Za Point-to-site konekcije nije potreban VPN uređaj, ali je potrebno koristiti VPN klijent koji treba instalirati na svako klijentsko računalo. VPN je uspostavljen ručnim pokretanjem veze s lokalnog računala klijenta. Slika.9 je prikaz kako uz pomoć Azure portala se stvara konekcija Point-to site VPN.



Slika 11. – Konfiguriranje Point-to-site VPN (Prema: Mustafa Toroman, 2020:156)

[35] Mazumdar P, Agarwal S, Banerjee A. Pro SQL Server on Microsoft Azure. Apress, 2016., str. 13.

U novom izborniku, moramo pružiti valjanu informaciju za Konfiguracijsko ime, Tip tunela i metodu autentifikacije. Ako koristimo Azurov certifikat, moramo pružit podatke o potvrdi, koja prikazuje slika 10.- Kreiranje nove VPN konfiguracije.



Slika 12. – Kreiranje nove VPN konfiguracije (Prema: Mustafa Toroman 2020:156)

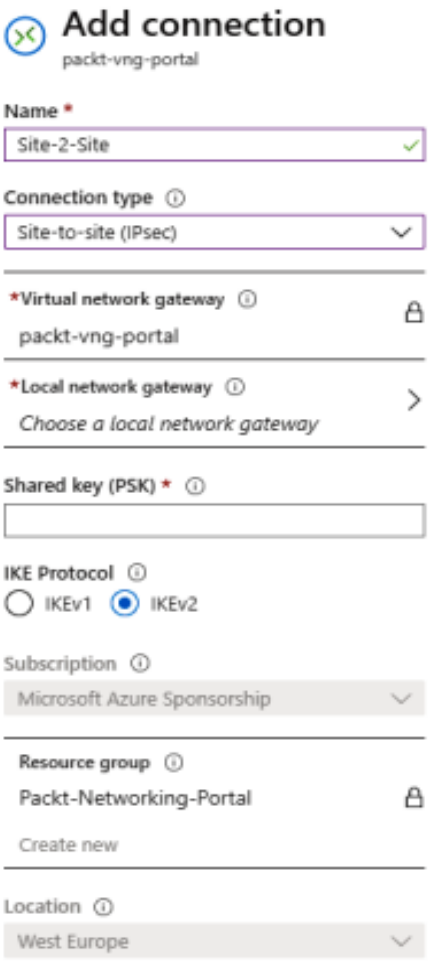
Nakon što smo dodali Site-to-Site konfiguraciju moramo se vratit na prethodnu stranicu kako bismo popunili, tj. dodali ponuđene adrese te opcionalno moguće dodavanje i DNS servera. [36]

4.3.2. Site-to-site VPN

Site-to-site VPN omogućuje korisnicima stvaranje sigurne veze između njihovih lokalnih mreža i njihove Azure virtualne mreže. VPN veze između web lokacija zahtijevaju VPN uređaj koji se nalazi na lokalnoj mreži i mora biti konfiguriran da stvori

[36] M.Toroman (2020). Azure Networking Cookbook Second Edition (2020). Secure network infrastructure, global application delivery, and accessible connectivity in Azure, od str. 130 do str. 136

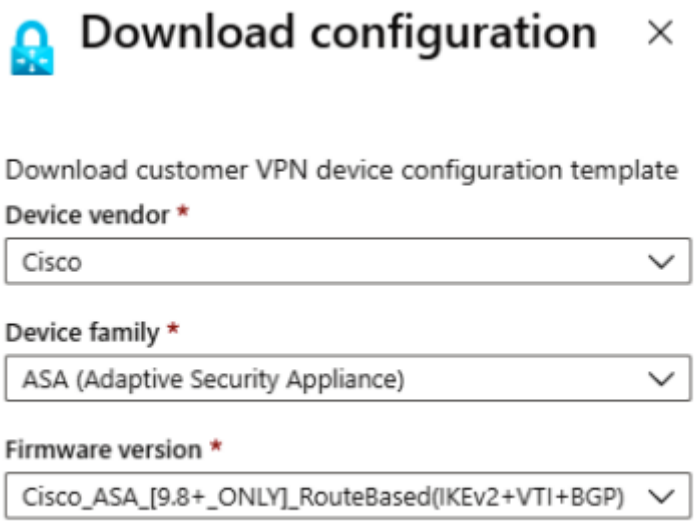
sigurnu vezu s Azure VPN vratima. Jednom kada se veza uspostavi, resursi na lokalnoj mreži i u Azure virtualnoj mreži mogu izravno i sigurno komunicirati. Prema Mazumdar (2016), za razliku od Point-to-site VPN konekcije, Site-to-site konekcije ne zahtijevaju uspostavljanje zasebne veze za svako klijentsko računalo na lokalnoj mreži za pristup resursima u virtualnoj mreži. U Cenosco d.o.o fimi koristimo upravo ovaj Site-to-site VPN kod spajanja lokalnog VPN uređaja koji se nalazi u lokalnoj mreži i spaja se na Azure virtualnu mrežu za pristup web lokacijama.



Slika 13. - Dodavanje nove konekcije site-to-site (Prema: Mustafa Toroman, 2020:126)

Koristeći virtualna mrežna vrata, možemo postaviti Azure stranu sa IPsec tunelom. Lokalna mrežna vrata pruža sve potrebne informacije na lokalnoj mreži, tj. definira lokalnu stranu tunela sa javnom IP adresom i podacima u lokalnoj pod mreži. Sa ovakvim načinom pristupa Azure strana tunela ima sve tražene podatke sa kojima može pristupit i uspješno pokrenut konekciju prema lokalnoj mreži. Međutim ovim putem je samo djelomično obavljen posao, jer suprotna strana konekcije mora također biti konfigurirana. Ovakav dio spajanja ovisi najviše o VPN uređaju koji se koristi lokalno, i svaki uređaj ima drugačiji konfiguracijski korak za obavit. Kad su obje strane konfigurirane, rezultat je sigurna i enkripcijska VPN veza između mreža za obje strane. Jedan od primjera kako postaviti VPN uređaj direktno sa Azure portalom u Cenosco d.o.o za site-to-site.

U Auzre portalu se nalazi konfiguracijski file kojeg je potrebno skinuti i dodat u novi izbornik gdje se nalaze opcije „Device Vendor, Device Family i Firmware Version“. Ponekad je nemoguće odabrat sve opcije jer neki uređaji nisu podržani od samog prodavača. Slika 13.

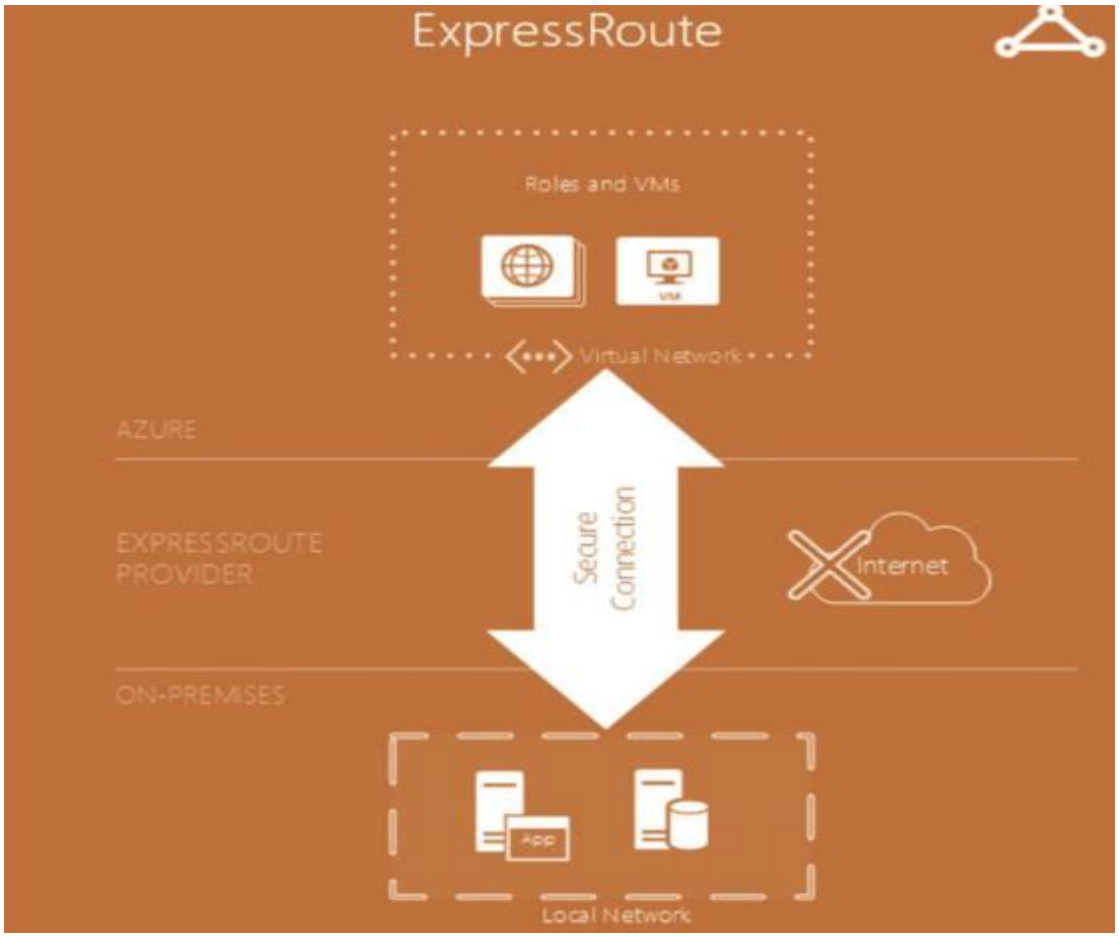


Slika 14. - VPN konfiguracijski predložak (Prema: Mustafa Toroman, 2020:129)

4.3.3. ExpressRoute konekcija

Azure ExpressRoute omogućuje korisnicima stvaranje privatne veze između Azure podatkovnih centara i njihove lokalne mreže. ExpressRoute konekcije ne idu preko

javnog Interneta, ali umjesto toga koriste dodijeljen internetski kanal i tako nude više pouzdanosti, bolju sigurnost i nižu latenciju u odnosu na tipične konekcije putem Interneta. ExpressRoute ne koristi javni Internet za povezivanje lokalnog okruženja s Azure. Povezivanje s Microsoftovim uslugama može biti putem univerzalne točke do točke Ethernet veze, putem pružatelja mrežne povezanosti s podatkovnim centrom.



Slika 15. - Hibridno postavljanje rute (Prema: Mazumdar, 2016)

Express konekcijom postoje dva moguća načina za uspostavljanje privatnih veza sa Microsoft Azure. Prvi način je povezivanje putem usluge eng.Exchange pružateljem usluga kojom je moguće direktno pristupit Azure.

Drugim načinom je moguće povezati direktnu konekciju preko našeg lokalnog internet pružatelja usluga na lokalnoj mreži i Microsoft Azure data centra. Express ruta je vrlo pouzdana te izvrsno funkcionira uz sve vrste topologija, te ima ugrađenu redundanciju. Omogućuje izvrsnu propusnost koja je brža od ostalih konekcija, do 10Gbps. Express

konekcija se može koristiti između prijenosa podatka sa lokalne mreže na Microsoft podatkovne centre sa vrlo malom redundancijom i niskom latencijom kod prebacivanje podataka.

Budući da je brza i pouzdana može se koristi za migraciju podatka i oporavak od gubitka podataka i visokom strategijom dostupnosti. Sa Express konekcijom, možemo iskoristit sami kapacitet Azure-a i dodati ga na postojeće podatkovne centre. Sa Express konekcijom je također moguće izraditi hibridnu aplikaciju.[37]

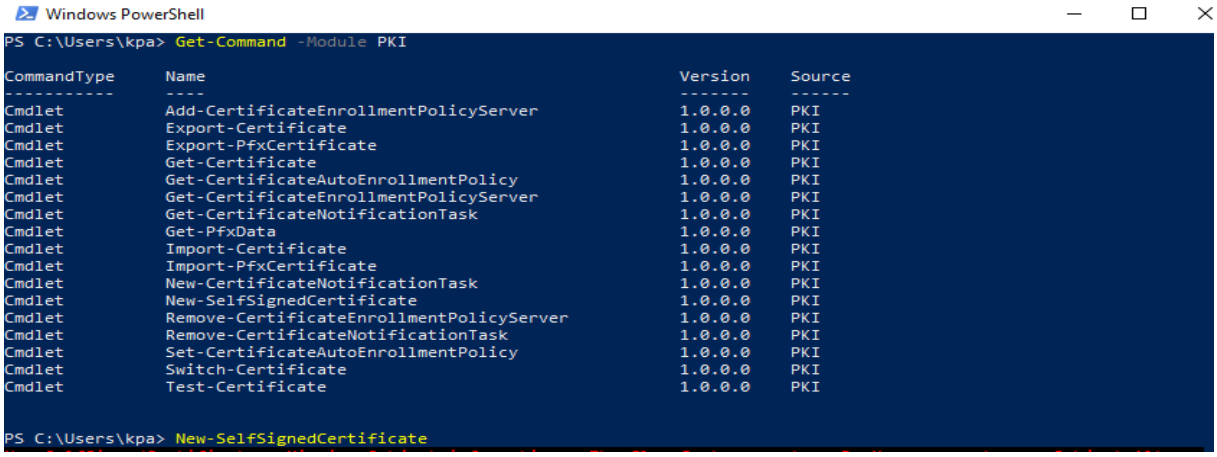
4.4. Stvaranje Site-to-site konekcije

Dobivanje sigurnog pristupa preko sigurne konekcije je važno, i trebalo bi se prevodit sa sigurnošću. Ponekad nije moguće pristupit Site-to-Site konekciji ako nismo u našem uredu gdje je postavljen VPN. Korištenjem Site-to-site VPN možemo podesit na našem osobnom računalu konekciju koja će uspostavljena bilo gdje i bilo kada.

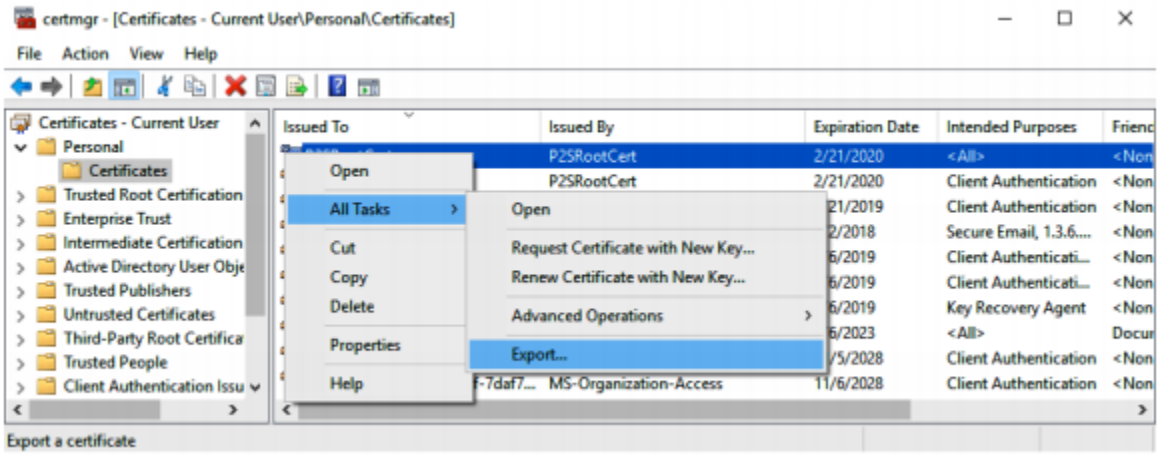
Da bi se sigurna konekcija uspostavila potrebno je kreirati certifikat koji će biti dodan za konekciju. Da bi se certifikat kreirao, koristimo PowerShell naredbu koja kreira proces izrade samog certifikata.

1. Get-Comand -Module PKI
2. Odaberemo New-SelfSignedCertificate
3. Izvezemo certifikat na svoj uređaj
4. Odaberemo Base-64 encoded X-509 (.CER) format
5. U Azure portalu lociramo virtualnu privatnu mrežu i vrata, te VPN konfiguraciju.
6. Kreiranje virtualnog Hub-a.

[37] M.Toroman (2020). Azure Networking Cookbook Second Edition (2020). Secure network infrastructure, global application delivery, and accessible connectivity in Azure, od str. 125 do str.148



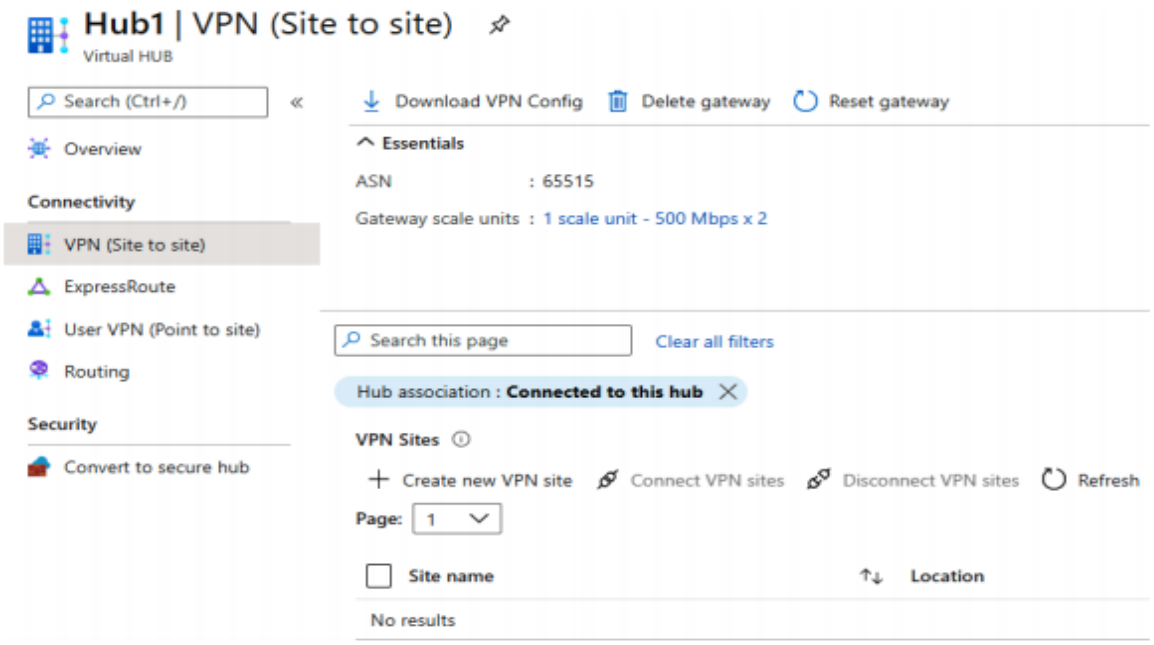
Slika 16. - Powershell Point-to-point certifikat



Slika 17. - Exportiranje certifikata uz pomoć certmgr

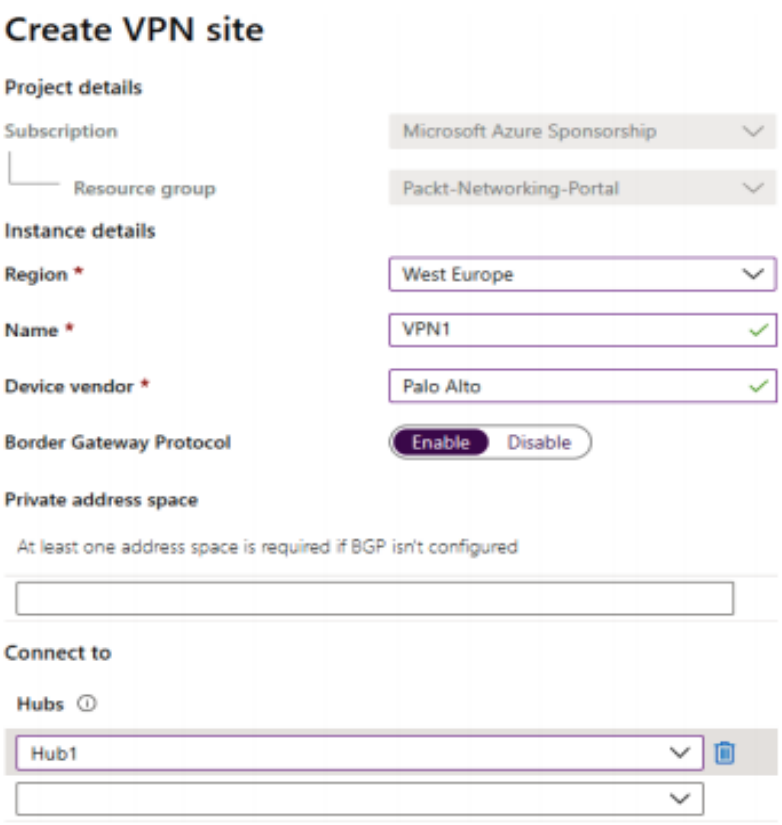
4.5. Stvaranje virtualnog Hub-a za Site-to-Site

U Azure portalu, potrebno je odabrati VPN (site-to-site) postavku za kreiranje VPN site-to-site opcije.

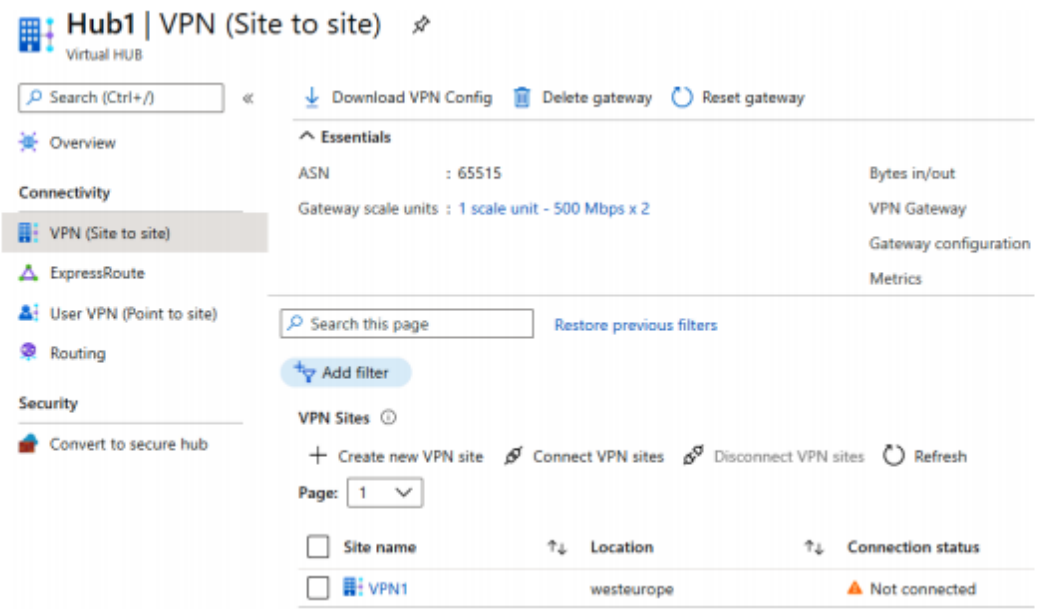


Slika 18. - Kreiranje nove stranice site-to-site preko hub-a (Prema: Mustafa Toroman,2020)

U novom izborniku korisnik dobiva mogućnost odabira pretplate ili grupe resursa koje su onemogućene. Kako je VPN stranica podređeni resurs pod WAN-grupi, mora koristit iste opcije kao i virtualna WAN mreža. Korisnik mora popunit željenu Regiju, Ime od željene VPN stranice i dobavljača. U opcijama također se nalazi opcija za uključivanja protokola graničnog prolaza ili (BGP). BGP je standardizirani protokol vanjskog pristupnika dizajniran za razmjenu podataka o usmjeravanju i dostupnosti između autonomnih sustava. Također protokol može povezani bilo koju mrežu sustava koristeći proizvoljnu topologiju.



Slika 19. - Stvaranje VPN web mjesta (Prema: Mustafa Toroman, 2020)



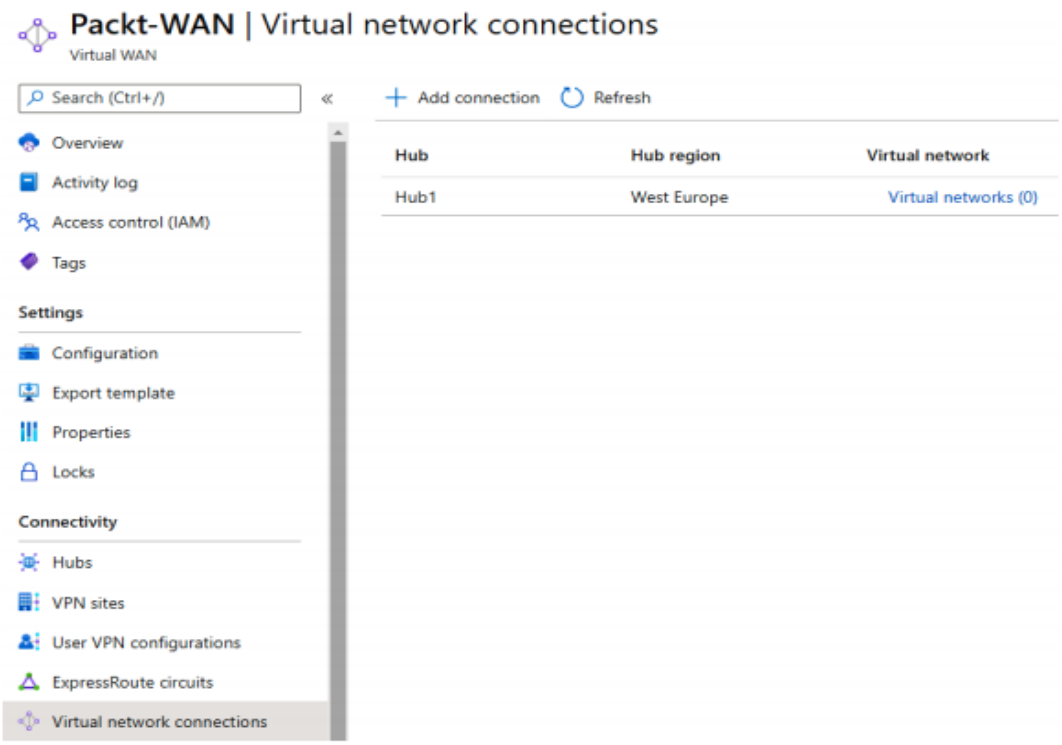
Slika 20. - Odabir konekcije VPN lokacije za pokretanje konekcije (Prema: Mustafa Toroman, 2020)

Nakon što je VPN lokacija napravljena, VPN konfiguracija se može odabrati i konekcija se može uspostaviti za VPN lokacije. Otvara se novi panel u kojem korisnik dodaje Pre-shared key ili unaprijed dodijeljeni ključ (PSK) koji smo napravili u prethodnim koracima te IPsec opciju koja propagira zadanu rutu te odlučujemo dali ćemo omogućit selektor prometa rute. Slika (21.)

Slika 21. - Odabir informacija preko konekcije Virtual Hub-a panela (Prema: Mustafa Toroman, 2020)

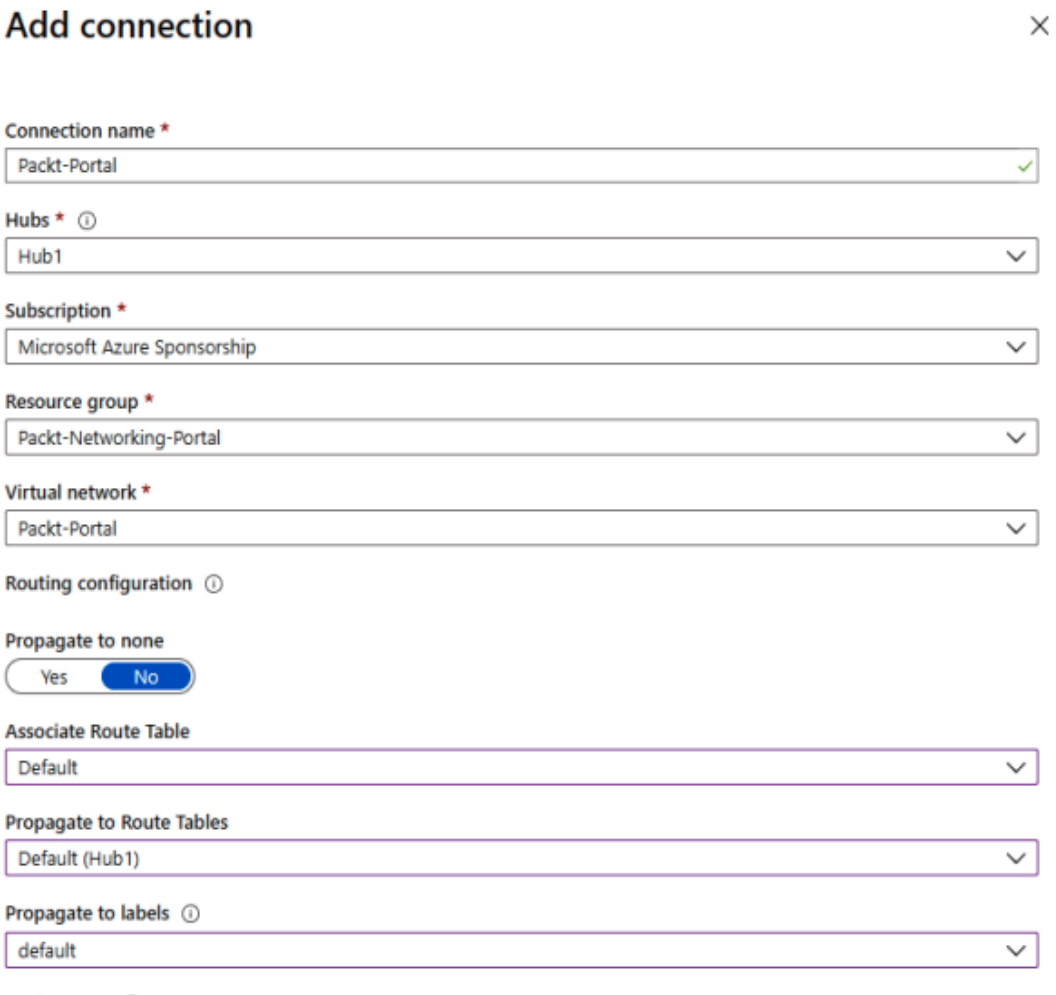
Stvaranjem Site-to-Site konekcije preko virtualnog središta, omogućava se konekcija na virtualno središte u određenoj regiji iz naše lokalne mreže (ili drugim mrežama koristeći virtualni uređaj). Ba bi takva usluga bila valjana, korisnik mora pružiti tj dati informaciju o VPN konekciji u virtualnom središtu (Hub) i konfigurirati VPN uređaj koji će biti korišten za spajanje. Ovim odabirom samo omogućavamo ispravno spajanje na virtualno središte (Hub). Samim time mi kao korisnik moramo dodati virtualne mreže koje su dodijeljene u izborniku, kako bi pristupili Azure resursima.
Virtualno središte (Hub) predstavlja centralno izvorište u pojedinoj Azure regiji.
Da bismo dodali virtualnu mrežu konekciju u virtualno središte (Hub) (unutar virtualne WAN mreže) moramo napraviti sljedeće korake. (Slika 20.)

1. Pronaći virtualnu WAN i odabrati prethodno napravljeni virtualni (Hub) ispod virtualnih mreža pod sekcijom spajanje. Odaberemo dodaj konekciju kao opciju za odabir.



Slika 22. - Dodavanje prethodno kreiranog virtualnog Hub-a (Prema: Mustafa Toroman, 2020)

2. U novom panelu, popunjavamo dodatne informacije kao što su ime konekcije, Hub, pretplate, grupe resursa i virtualne mreže. Nakon što smo to odabrali, sljedeći korak je da odaberemo konfiguraciju usmjerivanja . Možemo odabrati sa da za propagiranje ili ostaviti na ne kao što je u primjeru i odabrano.



Slika 23. - Konfiguriranje virtualnog hub-a (Prema: Mustafa Toroman, 2020)

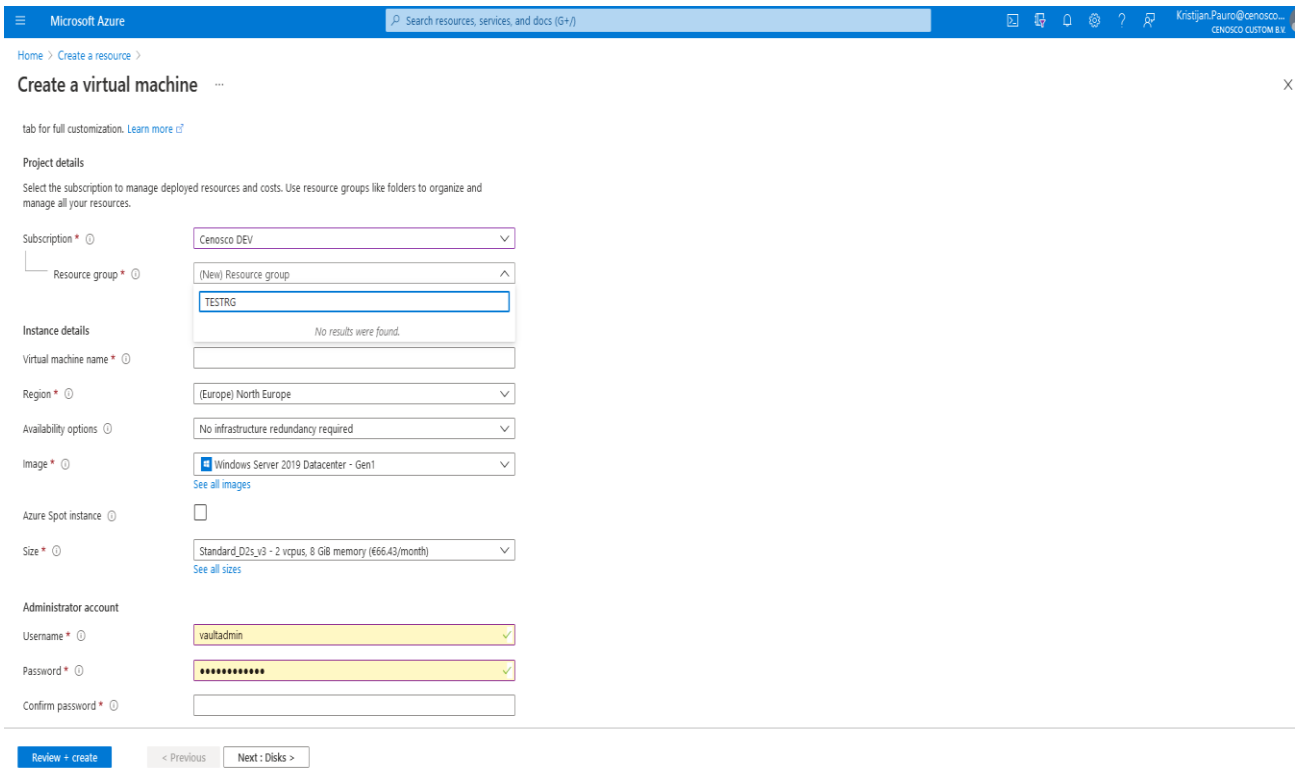
Spajanjem virtualne mreže sa virtualnim središtem (Hub) će nam omogućiti pristup resursa kad se spojimo sa istim virtualnim središtem. Konekcija se može izvršiti nad Site-to-Site konekcijom, Point-to-Site konekcijom, ili sa različitom virtualnom mrežom (spojena samo na isti hub).Također možemo definirat i statičku rutu koja će prisilit sav promet da prolazi kroz istu IP adresu.

4.5. Azure Site-to-Site VPN Cenosco

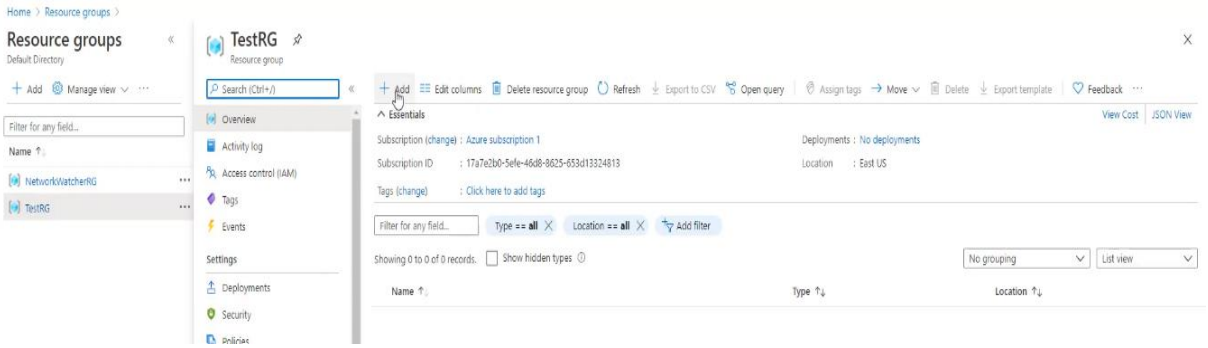
Za kreiranje VPN site to site koji koristimo u Cenosco d.o.o potrebno nam je pet ključnih stvari za pravilnu ili uspješnu konekciju.

1. Virtualno središte
2. Virtualna mreža
3. Mrežni pristupnik/usmjerivač
4. Javna IP adresa
5. Resurs za povezivanje tj. davatelj internetskog prometa

U Azure portalu kreiramo grupu resursa pod opciju pretplata odaberemo neko željeno ime tipa Azure pretplate, a pod grupom resursa, dodajemo Test RG kao na slici 24. Sad nam je željena grupa kreirana i možemo je odabrati pod grupe resursa. Sad na red dolazi kreiranje virtualnog središta ili Hub-a. Kliknemo pod dodaj (add) za otvaranje novog prozora sa izbornikom.

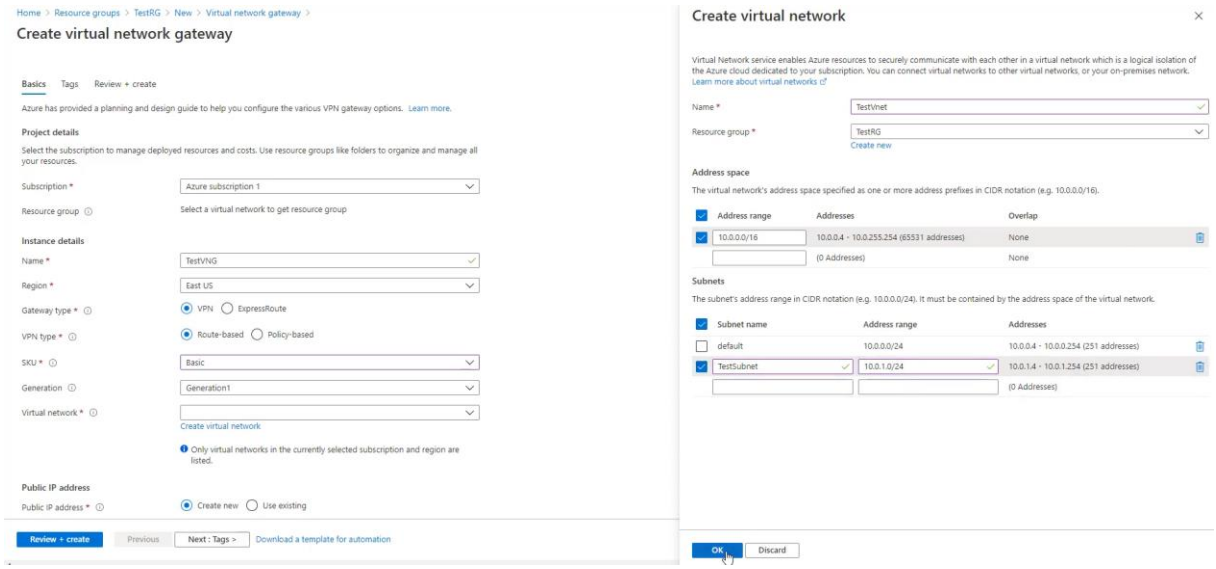


Slika 24. - Kreiranje virtualne grupe resursa (Prema: Azure portal Cenosco)



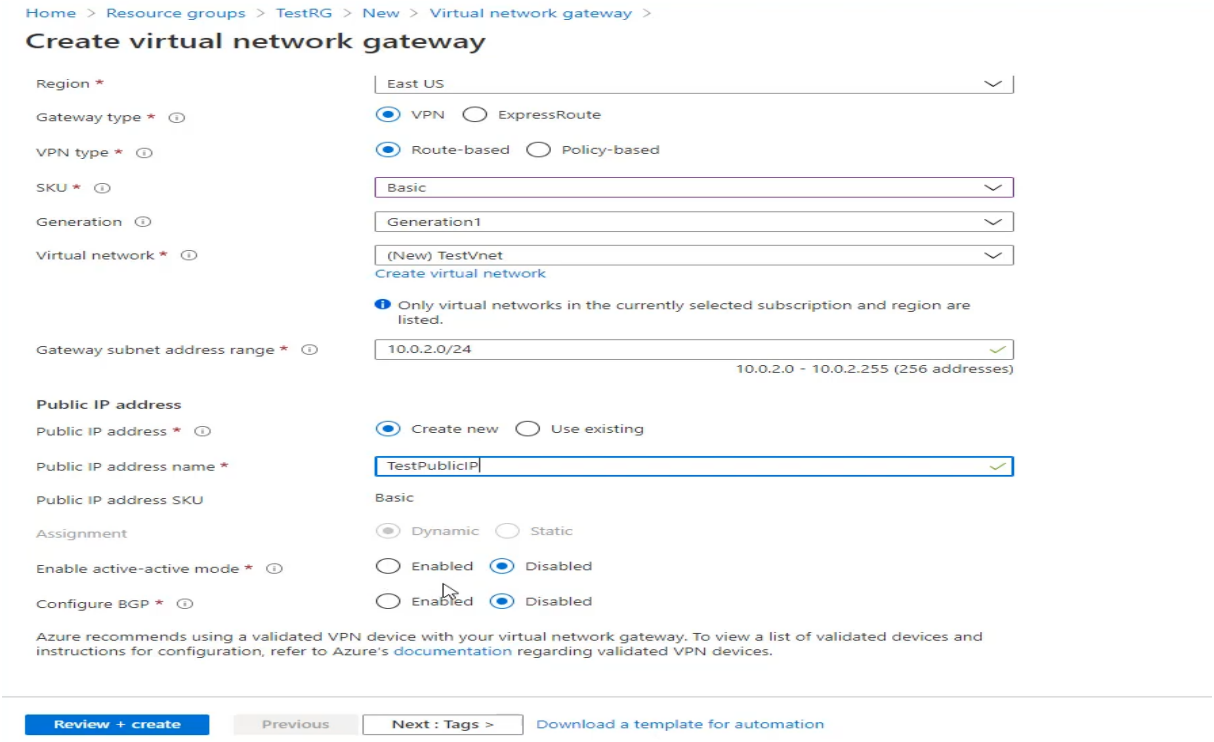
Slika 25. - Test RG (Prema: Azure portalu Cenosco)

U novom izborniku otvara se prozor sa mogućnostima od pretplate, imena, regije, virtualno središte (VPN ili ExpressRoute), te VPN tip (Route-based ili Policy-based).Virtualnu mrežu moramo kreirat TestVnet, pod grupom resursa Test RG koju smo prethodno zadali.

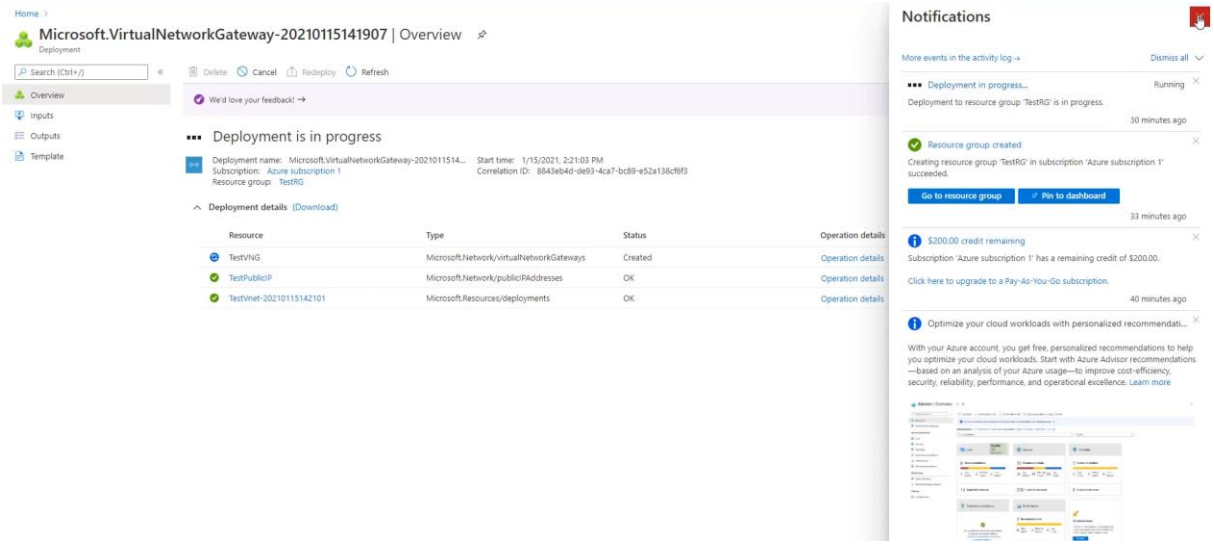


Slika 26. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)

Odaberemo zadanu raspon adresa 10.0.0.0/16 te isto učinimo i za pod naziv mreže. Kao na slici 26. Sljedeći korak je kreiranje javne IP adrese, nazovemo je TestPublicIP. Ako bismo željeli imat dvije aktive VPN konekcije trebalo bi omogućit pod active-active opciju. Pošto je ovo samo primjer stvaranja VPN site-to-site, sad nam to i nije potrebno.



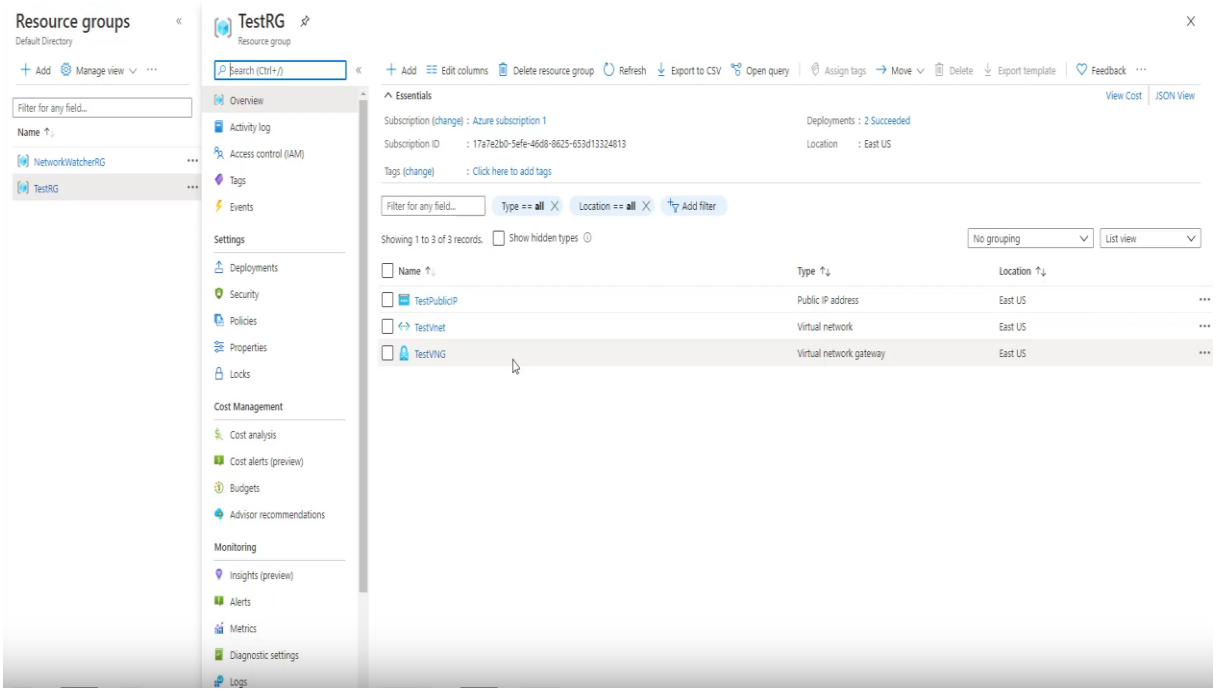
Slika 27. - Stvaranja virtualne mreže (Prema: Azure portalu Cenosco)



Slika 28. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)

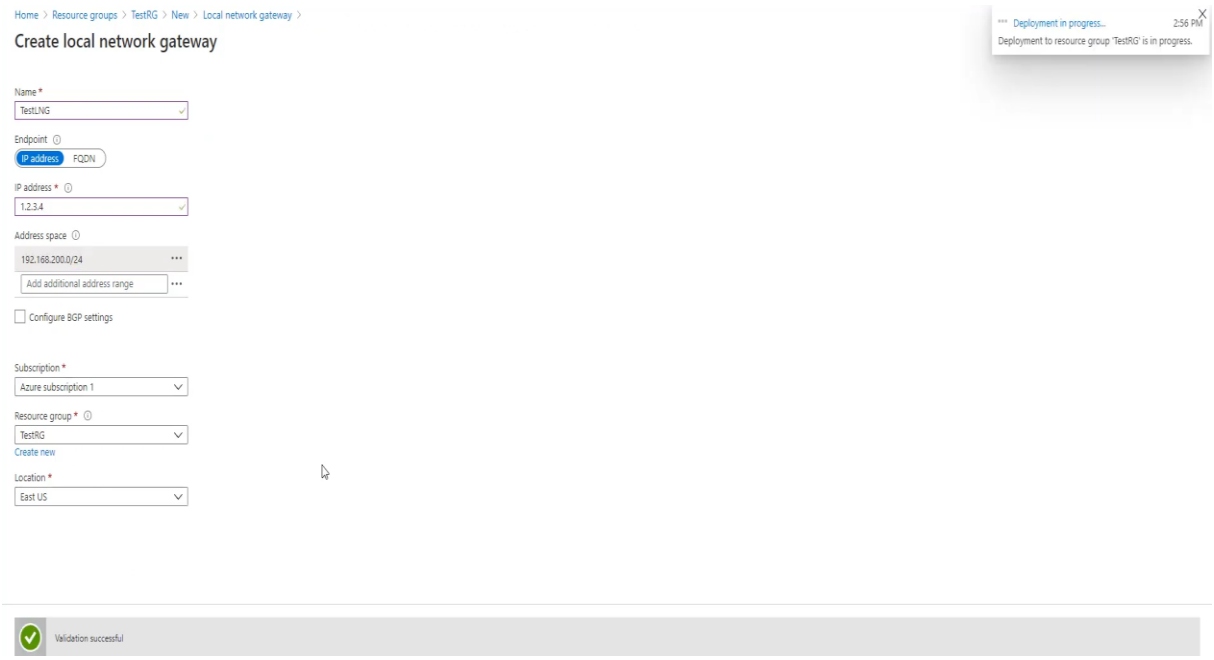
Nakon što je validacijski proces uspješno završen, možemo kreirat virtualno središte koje će potrajat tridesetak minuta do samog završetka. Nakon što je uspješno završen postupak vraćamo se na grupu resursa. Odaberemo Test RG grupu koja ima kreiranu javnu IP adresu, virtualnu mrežu i virtualno odredište. Imamo tri od 5 pet komponenti

potrebnih za Site-to-Site VPN mrežu. Sljedeći korak je kreiranje lokalnog mrežnog pristupnika.



Slika 29. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)

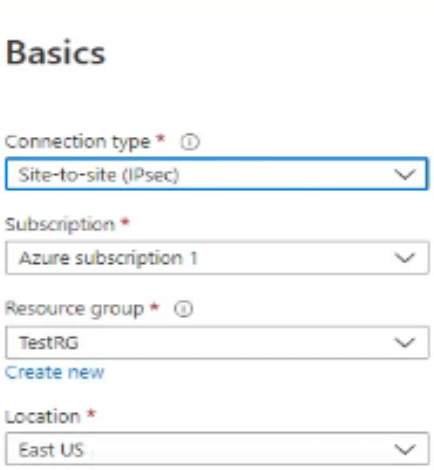
Ime ostaje isto kao i u prethodnom koraku TestLNG. IP adresa će biti lokalna WAN IP adresa 1.2.3.4, adresni prostor je privatna pod mreža u našem lokalnom okruženju. 192.168.200.0/24 (Ovo je nije pravi IP, dodan je za potrebe Testa) slika.29



Slika 30. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)

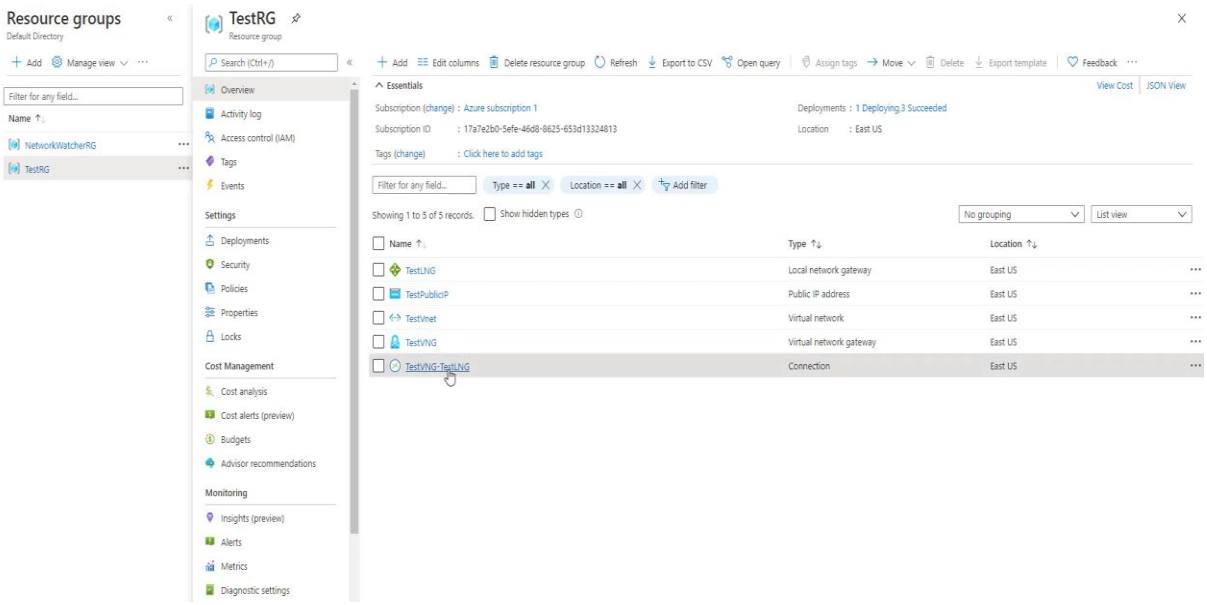
Vratimo se na grupu resursa, gdje imamo 4/5 potrebnih uvjeta. Na samom kraju nam je preostalo kreiranje same konekcije resursa.

U tražilicu upišemo konekcije, te je stvorimo. Ponuđenim odabirom odabiremo Site-to-Site IPsec VPN. Lokaciju odabiremo prema našoj lokaciji ali nije ni zabranjeno odabrati US prema kojem je ovaj primjer i rađen. Naravno, što smo bliže određenim geografskim dana centrima u Europi to je cijena naravno i skuplja radi manje redundancije i latencije. Dok je primjerice US lokacija dosta jeftinija od naše lokacije u EU.



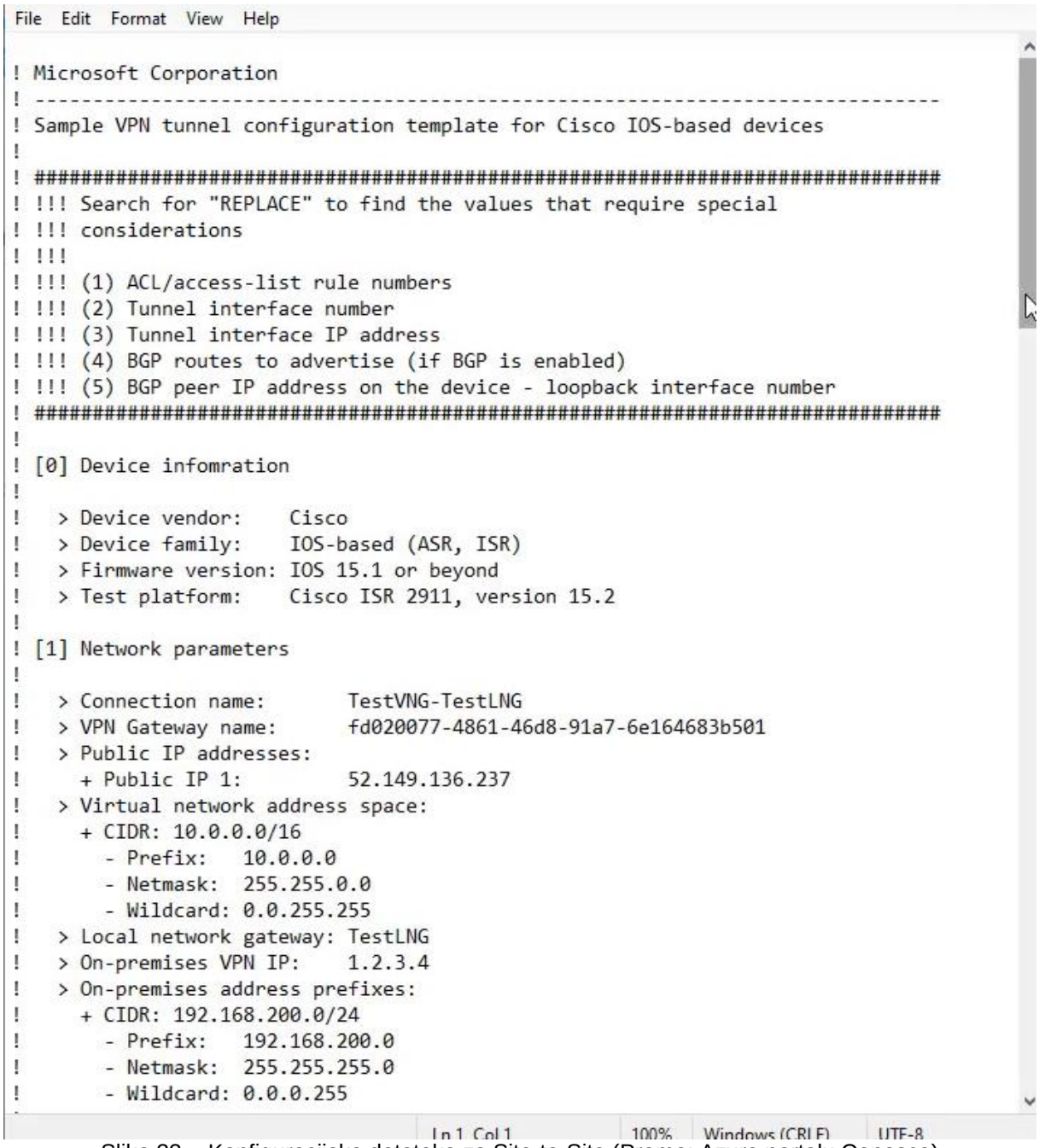
Slika 31. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)

Odaberemo mrežni pristupnik koji smo napravili ranije u koraku, odaberemo naš lokalni mrežni pristupnik koji je također napravljen ranije. Jedan od koraka je stvaranje djeljivog PSK ključa koji može biti bilo koji password odabir. Nakon što je uspješno završen zadnji postupak stvaranja konekcije, sad imamo sve potrebno za kreiranje našeg Site-to-Site VPN-a. Pristupamo konekciji gdje odaberemo korisnički VPN uređaj, u našem slučaju za Cenosco je Edge Ubiquiti usmjerivač.



Slika 32. - Stvaranja virtualne mreže (Prema: Azure portalu Cenocso)

Preuzimamo konfiguracijski file koji smo kreirali u zadnjem koraku koji je potreban za uspostavu VPN Site-to-Site konekciju na lokalnoj mreži.



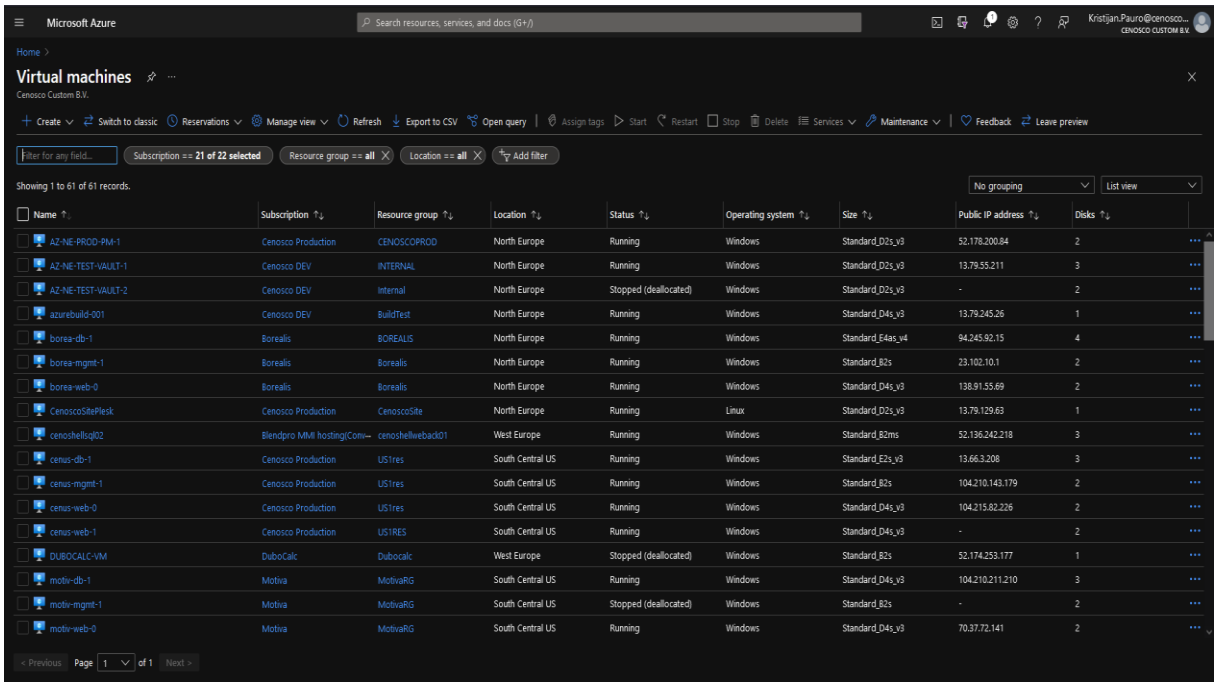
```
File  Edit  Format  View  Help

! Microsoft Corporation
! --------------------------------------------------------------------------------
! Sample VPN tunnel configuration template for Cisco IOS-based devices
!
! ################################################################################
! !!! Search for "REPLACE" to find the values that require special
! !!! considerations
! !!!
! !!! (1) ACL/access-list rule numbers
! !!! (2) Tunnel interface number
! !!! (3) Tunnel interface IP address
! !!! (4) BGP routes to advertise (if BGP is enabled)
! !!! (5) BGP peer IP address on the device - loopback interface number
! ################################################################################
!
! [0] Device infomration
!
!   > Device vendor:    Cisco
!   > Device family:    IOS-based (ASR, ISR)
!   > Firmware version: IOS 15.1 or beyond
!   > Test platform:    Cisco ISR 2911, version 15.2
!
! [1] Network parameters
!
!   > Connection name:       TestVNG-TestLNG
!   > VPN Gateway name:      fd020077-4861-46d8-91a7-6e164683b501
!   > Public IP addresses:
!     + Public IP 1:         52.149.136.237
!   > Virtual network address space:
!     + CIDR: 10.0.0.0/16
!       - Prefix:   10.0.0.0
!       - Netmask:  255.255.0.0
!       - Wildcard: 0.0.255.255
!   > Local network gateway: TestLNG
!   > On-premises VPN IP:    1.2.3.4
!   > On-premises address prefixes:
!     + CIDR: 192.168.200.0/24
!       - Prefix:   192.168.200.0
!       - Netmask:  255.255.255.0
!       - Wildcard: 0.0.0.255

Ln 1, Col 1    100%    Windows (CRLF)    UTF-8
```

Slika 33. - Konfiguracijska datoteka za Site-to-Site (Prema: Azure portalu Cenosco)

Slika 34. - Konfiguracijska datoteka za Site-to-Site (Prema: Azure portalu Cenosco)

5. Primjeri korištenja i upravljanja infrastrukturom Microsoft Azure

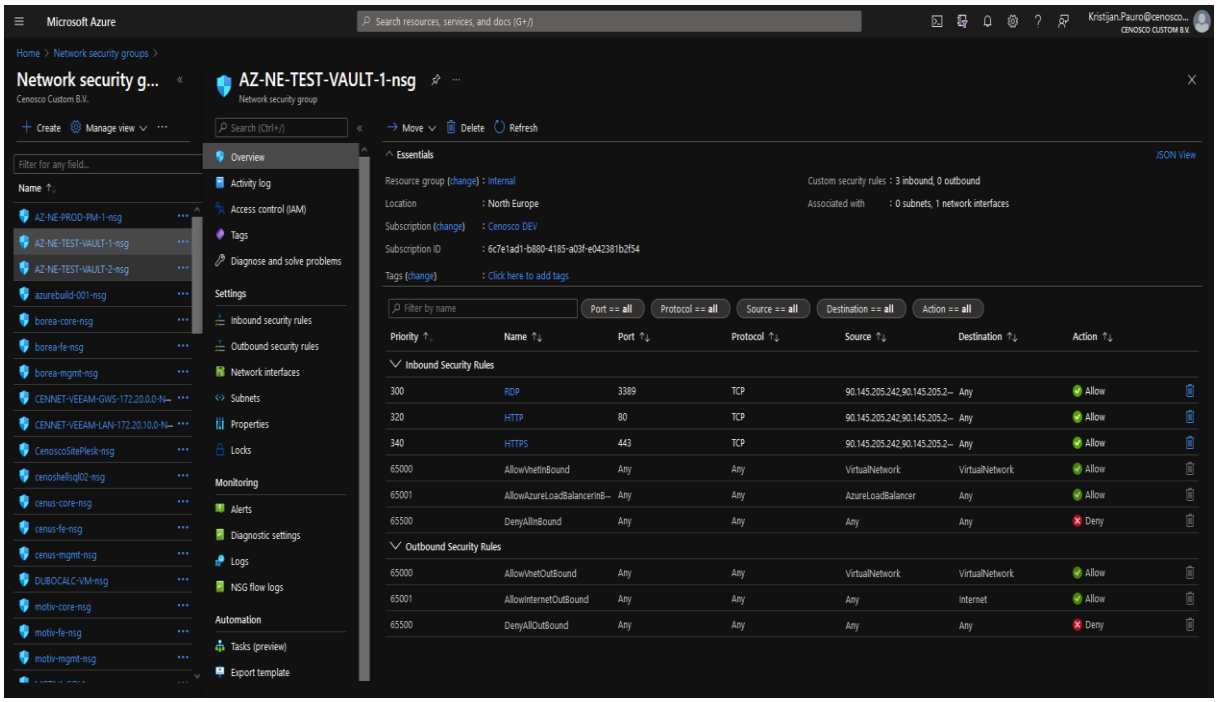
U današnje vrijeme mnoge tvrtke žele svojim klijentima i privatnim korisnicima pružit što bolju uslugu, sa vrlo brzim odazivom za stvaranje novih usluga i aplikacija. Jedna od takvih usluga je koju mi koristimo u našoj tvrtki Cenosco d.o.o je Microsoft Azure. Uz pomoć Microsoft Azure Cenosco d.o.o je prešao u Oblak okruženje gdje sam konfigurira i upravlja svom resursima i načinom odabira za pojedinu vrste usluga. Jedna od takvih usluga je IMS koju je razvio Cenosco d.o.o sa svojim partnerom SHELL, jest kreiranje web stranica za SHELL partnera preko IIS ili Internet Information Service. Prije nego li se stranica izradi, Azure administrator odabire željenu mašinu sa određenim performansama te se ona konfigurira prema potrebama klijenta. Počevši od veličine diska i vrste SSD ili HD, te memorije, procesora i backup podataka. Također odabir virtualne mreže (Internal-vnet), pod mreže, dijagnostike pokretanja OS-a, dijagnostike Azure sigurnog Centra, automatskog gašenja ili (stanje mirovanja do željenog vremena). Na našoj Microsoft Azure strukturi imamo 29 virtualnih mašina. Slika 35.



Slika 35. - Virtualne mašine u Cenosco(Prema: Azure portalu Cenosco)

Sa svoje lokalne LAN mreže Cenosco DevOps administratori pristupaju Azure oblaku na željene mašine radi podešavanja ili kreiranje istih.

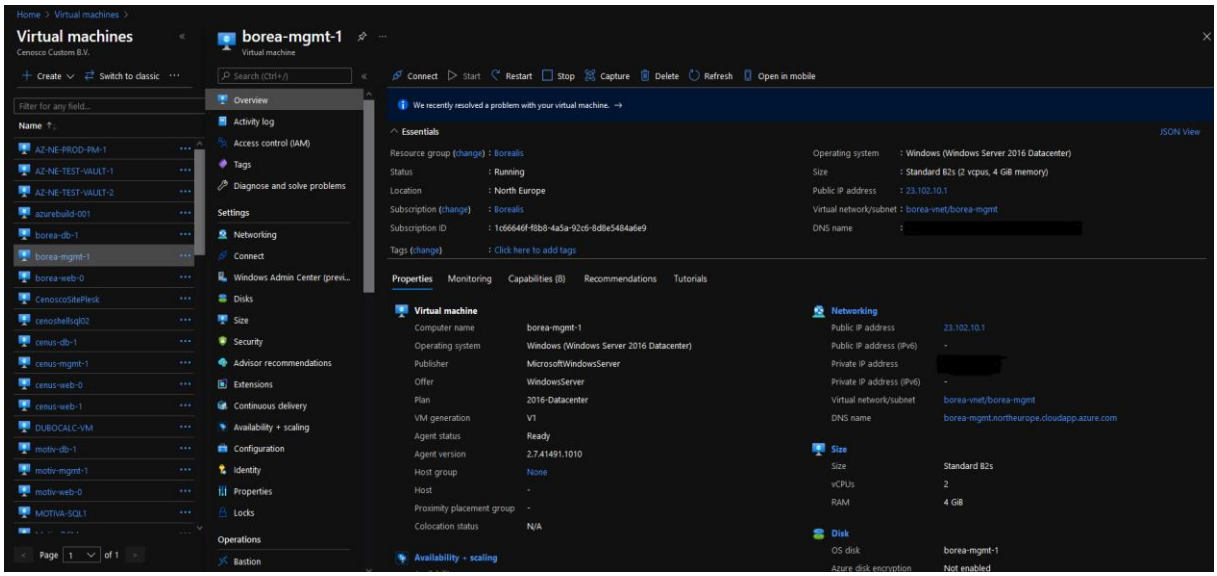
Svaka mašina ima svoju jedinstvenu javnu IP adresu i privatnu IP adresu, svaka od tih 29 virtualnih mašina ima svoju virtualnu mrežu u kojoj je prikazana kojoj grupi resursa pripada određena mreža. Također svakoj mreži pripada druga vrsta lokacije na kojoj se određena mašina nalazi, na primjer: Sjeverna Amerika, Europa ili Azija. Svaka pod mreža ima svoju jedinstvenu IP adresu te jedinstvene postavke u odabiru željene konfiguracije koju želimo postaviti. Za svaku pod mrežu jasno se definira svoj adresni prostor, svoja VPN vrata koja mogu pristupiti toj mreži. Kroz odabirom kojim smo odabrali našu virtualnu mrežu možemo odabrati razne sigurnosne odabire. Na primjer možemo odabrat mrežnu sigurnost u kojoj sami definiramo sigurnosne ulaze po pojedinim virtualnim mašinama koje kreiramo.



Slika 36. - Mrežne sigurnosne skupine u Cenosco(Prema: Azure portalu Cenosco)

Kao što je vidljivo na slici 36. vidimo dolazne sigurnosne postavke koje su postavljene od 300 (RDP) po portu 3389, te protokolu TCP-a na javne ip adrese 90.145.200..itd Također po konekciji HTTP, priključku 80 te protokolu TCP propušteno iste te javne IP adrese tipa 90.148.205.342 itd.

Pojedine virtualne privatne mreže na Azure infrastrukturi imaju konfiguriran pristup preko javnih IP adresa za potrebe klijenata, odnosno našim pristupom preko VPN-a pristupamo Azure portalu za konfiguriranje virtualnih mašina. Mi kao firma Cenosco kupujemo infrastrukturu kao uslugu (Iaas) od Microsofta, a mi je zatim (Cenosco) nudimo kao servis (Paas) kao uslugu za pristup toj infrastrukturi svojim klijentima kao što je SHELL itd. Pojedine virtualne privatne mreže na Azure infrastrukturi imaju konfiguriran pristup preko javnih IP adresa za potrebe klijenta prikazano u slici



Slika 37. - Primjer javne IP adresa za potrebe kljenta (Prema: Azure portalu Cenosco)

5.1 Grupa resursa u Azure okolini

U Azure portalu logički grupiramo resurse kao što su računi za pohranu, virtualne mreže i virtualne mašine. Ovakav pristup olakšava postavljanje aplikacija, a istovremeno zadržava sve povezane resurse na okupu iz perspektive upravljanja ili omogućavanje pristupa drugima toj grupi resursa. Imena grupe resursa mogu imati najviše 90 znakova.
Ključna značajka grupe resursa je sposobnost izgradnje našeg okruženja uz pomoć predložaka eng.Template. Predložak može biti JSON datoteka koja deklarira resurse za pohranu, umrežavanje i računanje. Također možemo definirati sve povezane prilagođene skripte ili konfiguracije koje će se primijeniti.
Ovakav pristup olakšava izgradnju okruženja u razvoju koje imamo u Cenoscu, a zatim koristi isti predložak za stvaranje implementacije proizvodnje.

5.2 Azure Load balancers

Azure load balancer se odnosi na ravnomjernu raspodjelu tereta dolaznog mrežnog prometa kroz grupu pozadinskih resursa ili poslužitelja. Svaki load balancer nalazi se između klijentskih uređaja i pozadinskih poslužitelja, koji prima i zatim distribuira dolazne zahtjeve na bilo koji raspoloživi poslužitelj koji ih može ispuniti.

Load balancer se može konfigurirati tako da cilja skupove dostupnosti ili pojedinačne IP adrese. Svaka HTTPS web stranica treba svoj load balancer, ako se sigurne web stranice objavljuju bez SNI (Server Name Indication).

5.3 Primjer Cenosco skripte za izradu web stranica

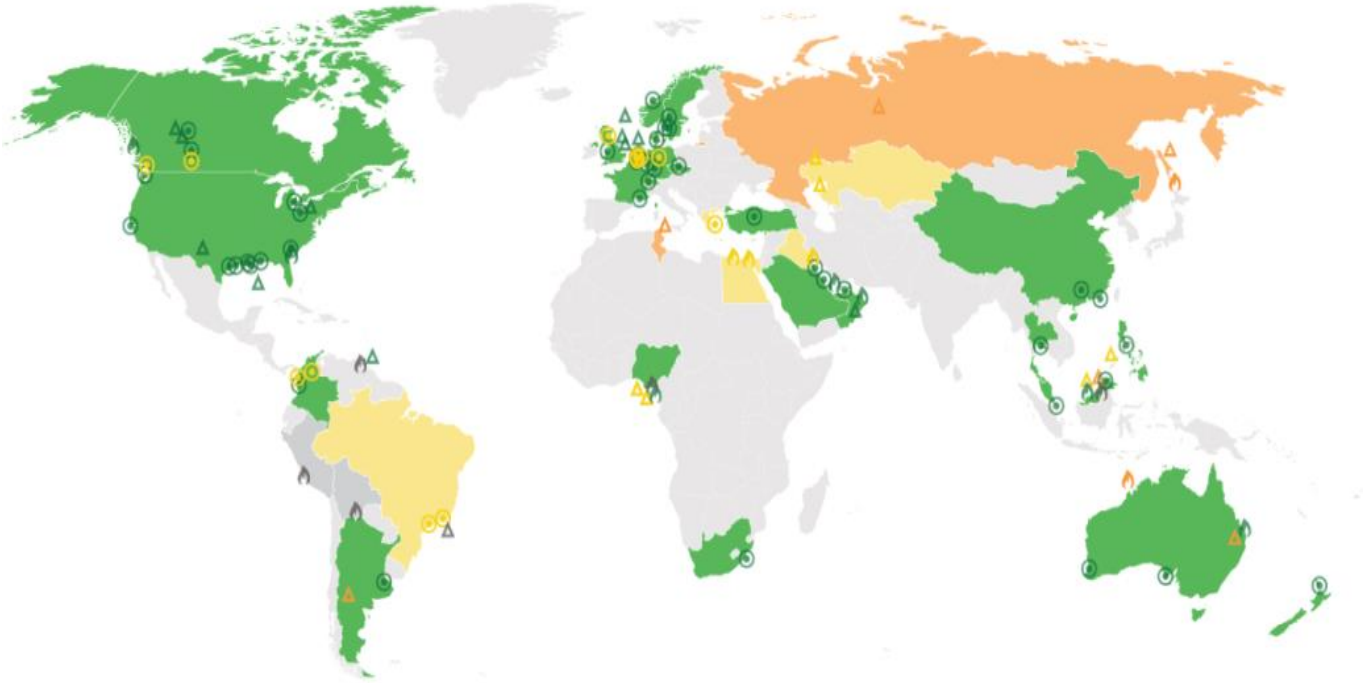
```
. .\Variables.ps1

#--- old way --> all this vars are now in variables.ps1

#$mainDomainURL = "cenosco.software"
#$mainSiteURL = "ims-trinidad"
#app dir
#$mainAppDir = "G:\Apps\IMS\ims-trinidad"

#$AppName = "IMS Trinidad"
#$DataserviceName = $AppName + " Dataservice"
#$TrendingName = $AppName + " Trending"

#data dir
#$dataDir = "G:\Data\IMS-TRINIDAD"

#old way: $UrlApp = "ims-dev01.cenosco.sofware"

#$UrlApp = $mainSiteURL +"." + $mainDomainURL
#$UrlDataservice = $mainSiteURL +"-data Service." + $mainDomainURL
#$UrlTrending = $mainSiteURL +"-trending." + $mainDomainURL

#--end old

# create app

$AppDir = New-Item -ItemType Directory -Path $mainAppDir\Application -Force
$AppPoolName = $AppName


#New-WebSite -Name TestSite -Port 80 -HostHeader TestSite -PhysicalPath
"$env:systemdrive\inetpub\testsite"


New-WebSite -Name $AppName -Port 80 -HostHeader $UrlApp -PhysicalPath $AppDir

# powershell will recognize the certificate that is connected to the domain but the
OLD one needs to be deleted!!!


#New-WebBinding -Name $AppName -Protocol https -Port 443 -HostHeader $UrlApp

#create and define app pool
New-WebAppPool $AppName

Set-ItemProperty IIS:\AppPools\$AppName enable32BitAppOnWin64 true
Set-ItemProperty IIS:\AppPools\$AppName -Name "processModel.loadUserProfile" -Value
"True"
Set-ItemProperty IIS:\AppPools\$AppName -Name "processModel.idleTimeout" -Value (
[TimeSpan]::FromMinutes(120))


# assigne app to app pool
Set-ItemProperty IIS:\Sites\$AppName applicationPool $AppName
```

```
#Dataservice

$DataserviceDir = New-Item -ItemType Directory -Path $mainAppDir\Dataservice -Force
$DataserviceAppPoolName = $DataserviceName


New-WebSite -Name $DataserviceName -Port 80 -HostHeader $UrlDataservice -
PhysicalPath $DataserviceDir

# powershell will recognize the certificate that is connected to the domain but the
OLD one needs to be deleted!!!
#New-WebBinding -Name $DataserviceName -Protocol https -Port 443 -HostHeader
$UrlDataservice

#create and define app pool
New-WebAppPool $DataserviceAppPoolName

Set-ItemProperty IIS:\AppPools\$DataserviceAppPoolName enable32BitAppOnWin64 true
Set-ItemProperty IIS:\AppPools\$DataserviceAppPoolName -Name
"processModel.loadUserProfile" -Value "True"
Set-ItemProperty IIS:\AppPools\$DataserviceAppPoolName -Name
"processModel.idleTimeout" -Value ( [TimeSpan]::FromMinutes(120))

# assigne app to app pool
Set-ItemProperty IIS:\Sites\$DataserviceName applicationPool
$DataserviceAppPoolName



#TrendingService

$TrendingDir = New-Item -ItemType Directory -Path $mainAppDir\MTIAService -Force
$TrendingAppPoolName = $TrendingName

New-WebSite -Name $TrendingName -Port 80 -HostHeader $UrlTrending -PhysicalPath
$TrendingDir

# powershell will recognize the certificate that is connected to the domain but the
OLD one needs to be deleted!!!
#New-WebBinding -Name $TrendingName -Protocol https -Port 443 -HostHeader
$UrlTrending

#create and define app pool
New-WebAppPool $TrendingAppPoolName

Set-ItemProperty IIS:\AppPools\$TrendingAppPoolName enable32BitAppOnWin64 true
Set-ItemProperty IIS:\AppPools\$TrendingAppPoolName -Name
"processModel.loadUserProfile" -Value "false"
Set-ItemProperty IIS:\AppPools\$TrendingAppPoolName -Name
"processModel.idleTimeout" -Value ( [TimeSpan]::FromMinutes(120))
Set-ItemProperty IIS:\AppPools\$TrendingAppPoolName -Name
"failure.rapidFailProtection" -Value false
# assigne app to app pool
Set-ItemProperty IIS:\Sites\$TrendingName applicationPool $TrendingAppPoolName


# SSL Bindings
if ($ssl -like "https") {
 New-WebBinding -Name $AppName -Protocol https -Port 443 -HostHeader $UrlApp
 New-WebBinding -Name $DataserviceName -Protocol https -Port 443 -HostHeader
$UrlDataservice
 New-WebBinding -Name $TrendingName -Protocol https -Port 443 -HostHeader
$UrlTrending
}


#creating the data folder structure
New-Item -ItemType directory -Path $dataDir\ISOS
New-Item -ItemType directory -Path $dataDir\ISOS\ALL_pefs
New-Item -ItemType directory -Path $dataDir\Logs
New-Item -ItemType directory -Path $dataDir\Logs\Client
New-Item -ItemType directory -Path $dataDir\Logs\DataService
New-Item -ItemType directory -Path $dataDir\Pannellum
New-Item -ItemType directory -Path $dataDir\Revisioning
New-Item -ItemType directory -Path $dataDir\Revisioning\Failed
New-Item -ItemType directory -Path $dataDir\Revisioning\Reports
New-Item -ItemType directory -Path $dataDir\TransferLocation
```

```
#
#$confirmation = Read-Host "Did you deployed IMS (y/n):"
#if ($confirmation -eq 'y') {
# Write-Host 'That is awesome!'
#}
#else {
#    $proceed = Read-Host "Do you want to deploy IMS now (y/n):"
#    if ($proceed -eq 'y') {
#      Write-Host 'Ok press any key to continiue'
#      . .\deployIMS.ps1

#        $configMessage = Read-Host "Do you want to adjust web configs (y/n):"
#        if ($configMessage -eq 'y') {
#        . .\update-webconfigs.ps1
#        Write-Host 'Your config files are finished! :)'

#        } else {
#        Write-Host 'You still need to adjust config files'
#        }
#    }else {
#        Write-Host 'You still need to deploy ims'
#    }


#}

 $proceed = Read-Host "Do you want to deploy IMS now (y/n):"
    if ($proceed -eq 'y') {
      . .\deployIMS.ps1
      Write-Host 'Ok press any key to continiue'
      . .\update-webconfigs.ps1
        }else {
        Write-Host 'You still need to deploy ims'
        }


# create update script

. .\create-updatescript.ps1


 Write-Host 'Creating new ims site done!'

 pause
```

6. Opis tvrtke Cenosco

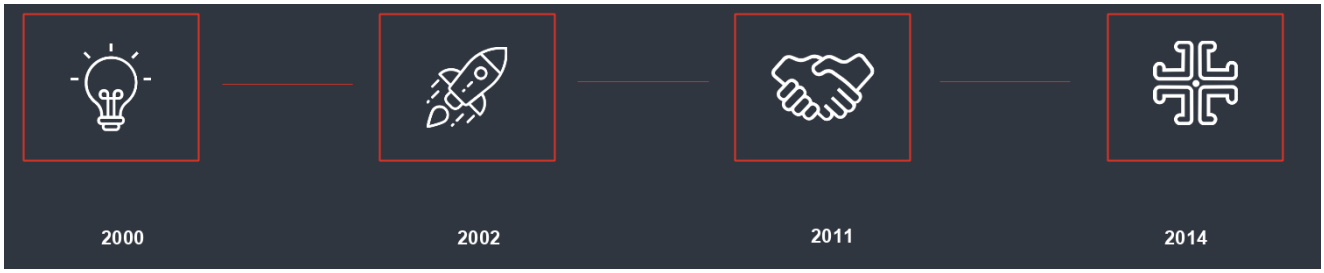
Cenosco je jedna od vodećih tvrtki za izradu programskih rješenja za tvrtke koje se bave zdravljem, zaštitom, okolišem i njegovom kvalitetom, statističkim analizama i menadžmentom rizika integriteta imovine. Na slijedećoj slici je moguće vidjeti zastupljenost IMSa na mapi svijeta.



Slika 38. - Upotreba IMSa u svijetu

Na slici zelenom bojom su označene zemlje gdje je IMS dostavljen. Narančastom bojom su označene zemlje gdje se IMS trenutno implementira, a žutom bojom zemlje koje su trenutno u pregovorima s Cenoscom.

Tvrtka je osnovana 2000 godine. Dvije godine kasnije je napravila Sustav za rizik i pouzdanost za Shell Global Solutions. 2011 godine Cenosco je licencirao ugovor s Shellom o izradi i komercijalizaciji alata o integritetu. Tri godine nakon toga, Cenosco je IMS što znači Integrity Management System. Vremensku crtu najvažnijih događaja u Cenoscu možete vidjeti na slici 10.



Slika 39. - Vremenska crta Cenosca - osnivanje, prvi projekt s Shellom, licenciranje i IMS

IMS je sustav koji je nastao 2015 godine u suradnji s Shellom. On je sposoban predvidjeti održivost različite opreme u naftnim postrojenjima. Sustav je namijenjen svim osobama koje su uključene u održavanje i servis opreme.

IMS se bazira na pretplatama, to jest, IMS je SaaS aplikacija gdje klijent plaća godišnju pretplatu što uključuje:

- Održavanje
- Podrška
- Licenca

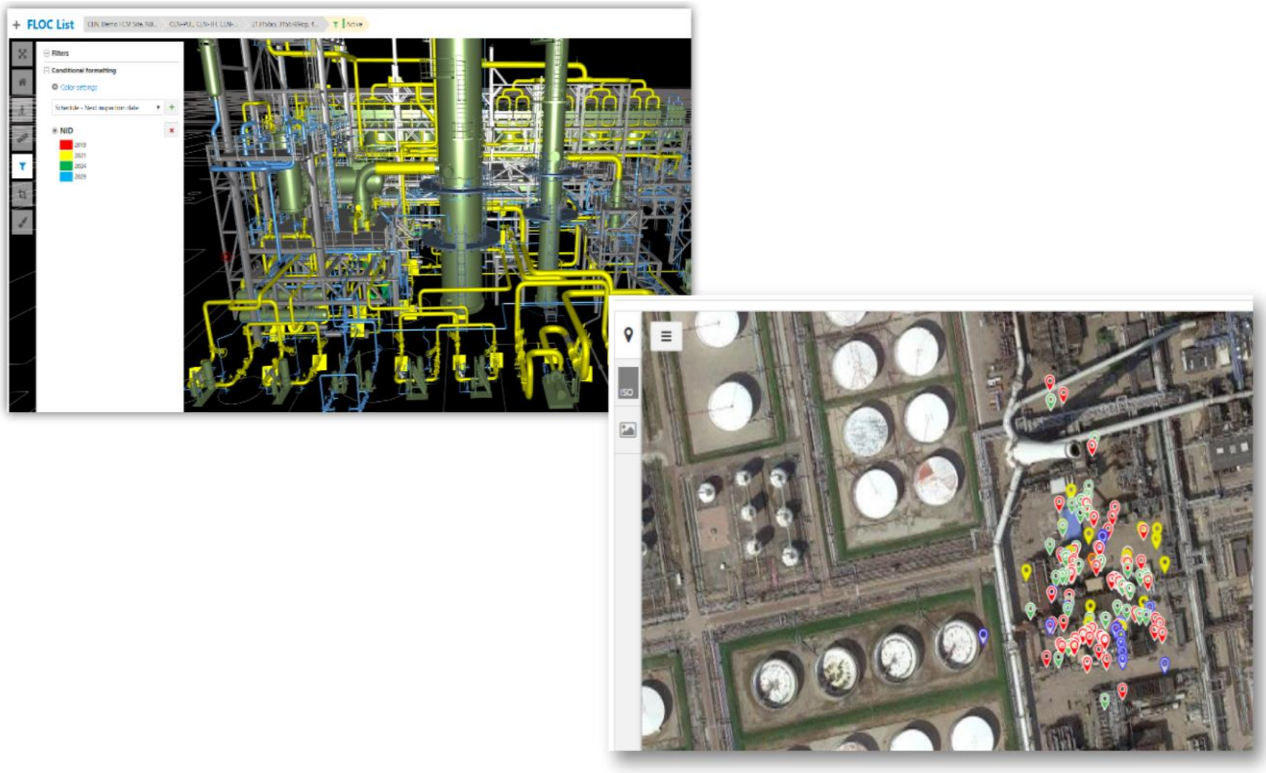
Podrška podrazumijeva obavljanje specifičnih zadataka u slučaju kada klijent traži informacije koje možda nisu dostupne u IMSu. Cenosco ima dva do tri velika unapređenja IMSa godišnje.

IMS ima nekoliko specifičnih mogućnosti u usporedbi s drugim sličnim sustavima:

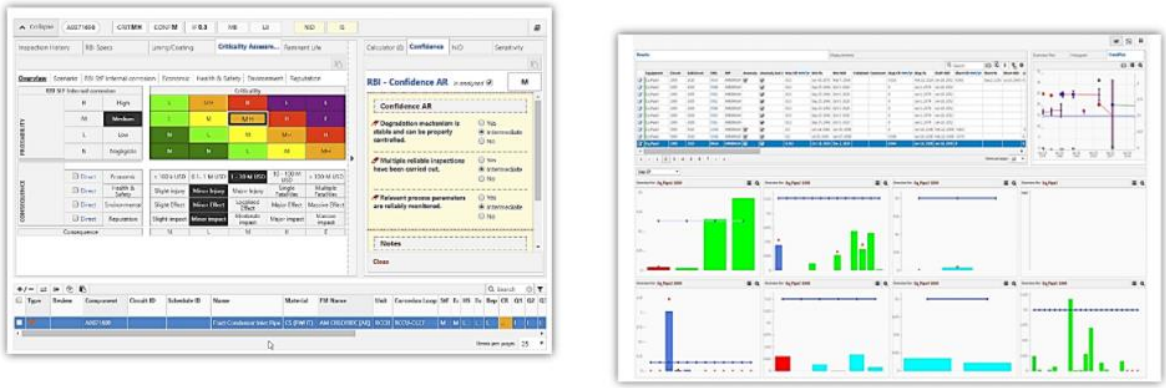
- Mogućnost korištenja aplikacije bez interneta
- AR/3D virtualizacija
- IOW praćenje
- Procesiranje podataka

IMS ima mogućnost rada bez interneta kako bi klijenti mogli koristiti neku od mobilnih platforma u postrojenjima kada im je potreban IMS na lokacijama gdje Internet nije

dostupan. Cenosco je napravio inovaciju kada je odlučio koristiti 3D virtualizaciju za prikaz dijelova postrojenja što se može vidjeti na slici 11.



Slika 40. - IMS virtualizacija



Slika 41. - IMS PEI dashboard

IMS se sastoji od nekoliko modula to jest različitih podsustava koji imaju specifičan način rada. Prvi modul koji je nastao 2015 godine je IMS PEI. On pruža integritetni status za pritisak i civilnu opremu. Kada i što se treba ispitati na uređajima s pritiskom koristeći napredne algoritme za računanje korozije i analitičkih alata. Na kraju IMS PEI to sve sprema kako bi postojao trag svih inspekcija za pojedinačnu uređaja.

IMS PEI ima nekoliko područja primjena:

- Rafinerije
- Terminali
- Terminali za ulje
- Terminali za procesiranje
- Postrojenja za procesiranje
- Cjevovodi
- Elektrane
- Postrojenja za proizvodnju

IMS PEI je prvobitno namijenjen za:

- Opremu za pritisak
- Tenkove
- Prirubnice (eng. flange)
- Ventile za ograničavanje tlaka

IMS PEI koristi Shell RBI metodologiju i API preporučene prakse. RBI je metodologija za optimizaciju inspekcije i praćenje napora. Koristi se za upravljanjem pritiskom. Definira korozijsku petlju i njihovo moguće vrijeme korištenja kako bi se determinirali procesi i korozijski mehanizmi u petlji. IMS također koristi slijedeće certifikate:

- ISO 9001
- Microsoft Gold Partner
- SAP Compatible

IMS PEI je najveći podsustav u IMS i podsustav koji koristi najviše alati u IMSu. Alati koji se koriste u IMS PEI su:

- Shell inspekcija bazirana na riziku (RBI)
- Menadžment sustav za podatke o inspekcijama (IDMS)
- Framework za upravljanje korozijom (CMF)
- Očitanja debljine zidova
- Napredne kalkulacije korozije
- Skupna analiza podataka
- Optimizacija intervala inspekcija
- Domet optimalne operiranja (IOW)
- Dokument kontrole korozije (CCD)
- Predikcijski model za koroziju (CPM)
- Upitnik za katodnu zaštitu
- Analiza osjetljivosti

Drugi najvažniji sustav je IMS RCM koji optimizira planove za preventivno održavanje uređaja. Koristeći profil rizika za svaki uređaj, korisnik određuje najbolji plan održavanja za taj uređaj. Korisnik to može napraviti ručno ili koristeći funkcije u sustavu kako bi dobio plan. Svrha ovog sustava je smanjenje troškova održavanja, ali održati sigurnost uređaja i radnika koji rade na njima.

Treći podsustav u IMSu je IMS PLSS, sustav namijenjen provjeri integriteta cjevovoda. Sustav sprema dizajn cijelog cjevovoda ili samo jedne sekcije. Sustav izvršava različite izračune baziranim na podacima unesenim od korisnika (debljina cijevi, stanje korozije, pritisak, itd..) i izrađuje raspored inspekcija za taj cjevovod. Raspored se radi jednom kada je procjena opreme gotova. Svaka oprema može imati nekoliko planova:

- Inspekcijski plan
- CAIR plan
- Korozijski plan
- Osnovni plan

Osnovni plan je plan u kojem sva oprema bez plana dobiva inspekciju. Korozijski plan je mjerenje debljine (cijevi, zidova itd..). CAIR plan (eng. Corrective Action Inspection Recommendation) je ponovljena inspekcija za opremu prema preporuci. Inspekcijski plan je unutarnja i vanjska inspekcija opreme.

Sustav pomaže pri odlučivanju koja mjerenja se trebaju uzeti i kada. Sva mjerenja se raspoređuju tako da sva mjerenja za istu lokaciju stavljaju u jedan paket te se tako podaci analiziraju prema njihovim lokacijama. Tom analizom se saznaju anomalije, odstupanja, promjene u koroziji. Sustav s tom analizom također upozorava korisnika na krivo unesene mjere. Na temelju ovih mjera, sustav izračunava kada je najbolje napraviti iduća mjerenja.

Četvrti podsustav je IMS SIFpro koji je namijenjen dizajniranju sigurnosnih funkcija (SIF/SIS) poštujući inženjerske prakse kao što je to IEC 61508/61511.

Iako svaki podsustav imaju svoju posebnu logiku ipak postoje neke zajedničke mogućnosti koje su zajedničke svim podsustavima.

- Izrada dashboarda
- KPI (eng. Key Performanse Index) to jest ključni pokazatelji uspješnosti
- Izrada query upita
- Filteri
- Izrada izvještaja
- 3D vizualizacija
- Import/Export podataka

7. Zaključak

Računalstvo u oblaku omogućuje mnoge prednosti u poslovanju IT tvrtke. Tako je jedan od primjera koja ova vrste usluge omogućuje krajnjem korisniku ta da sam odabire svoje željene resurse kod kupnje vlastitog okružena u kojem će resursi biti maksimalno iskorišteni. Dokazano je da su srednja i mala poduzeća kod kupnje oblak okruženja (Microsoft Azure, Amazon ili Google) više uštedjela na resursima i na troškovima od električne energije pa do zamjenskih komponenti, te su takva okruženja mnogo isplativija danas nego u prošlosti. Razlog zbog kojega je računalstvo u oblaku sve više popularno kod malih i srednjih organizacija je činjenica kako se korištenjem tih usluga znatno smanjuju troškovi. Koliko god prednosti korištenja računalstva u oblaku donosi, jednako tako izaziva i sumnje u sigurnost, posebice u današnje vrijeme kada je gotovo bilo koji resurs ili podatak na internetu ranjiv na neki oblik napada. S obzirom kako se sve više usluga i servisa pruža putem računalstva u oblaku, a razvoj tehnologije oblaka konstantno raste za očekivati je kako će se i razina sigurnosti paralelno razvijati, a samim time privući će se još više korisnika koji su sada, u većoj ili manjoj mjeri skeptični prema upotrebi usluga u oblaku. Cenosco već sada polako prelazi sa Iaas na Paas jer glavna prednost same usluge je ta što kompleksnost Iaas usluge više nije potrebna. Developeri pristup resursu dobivaju putem Visual Microsoft Studija ili putem Azure DevOps. Faktori kao što su vrijeme i tržište već sada traže agilniju i bržu prilagodbu pojedinim aplikacijama. Sami Paas omogućava građenje svoje aplikacije, umjesto same konfiguracije i podešavanja samih servera za pristup. Paas nudi fleksibilnije cijene baziranih na plaćanju svojeg modela. Samim tim pristupom korisnik ili firma može prepoloviti svoje troškove održavanja u usporedbi sa tradicionalnim uslugama poslužitelja koje se obično temelje na fiksnom modelu najma. Cenosco d.o.o kao IT firma ima u planu kroz par godina preći sa Iaas okruženja na Paas okruženje. Sama Azure oblak platforma još nije doživjela svoj vrhunac te se još uvijek razvija i napreduje svaki dan po tom pitanju. U današnje vrijeme korisnik može dobit besplatnu probnu verziju od Microsoft Azure ili AWS (Amazona) za pristup svojoj oblak okolini, te tamo graditi svoje buduće odgovarajuće okruženje koje njemu najviše odgovara za svoje uložene novce.

Literatura

Knjige

1. Chappell D. (2010). Introducing the Windows Azure platform. David Chappell & Associates.
2. Krutz R, Vines R. (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, Indiana: Wiley Publishing
3. Lobel G.L, Boyd E.D. (2014). Miccrosoft Azure SQL Database Step by Step. Redmond, Washington: Microsoft Press.
4. Mazumdar P, Agarwal S, Banerjee A. (2016.). Pro SQL Server on Microsoft Azure. Apress.
5. Panian Ž. (2013). Elektroničko poslovanje druge generacije. Zagreb: Ekonomski fakultet Zagreb.
6. Pavlić M. (2011). Oblikovanje baze podataka. Rijeka: Digital Point tiskara d.o.o.
7. Rabuzin K. (2011). Uvod u SQL. Varaždin: Fakultet organizacije i informatike
8. Toroman M. (2020). Azure Networking Cookbook. Birmingham, UK: Packt Publishing.
9. Varga M. (2012). Upravljanje podacima (1. izd.). Zagreb: Element d.o.o.
10. M.Toroman (2020). Azure Networking Cookbook Second Edition (2020). Secure network infrastructure, global application delivery, and accessible connectivity in Azure.
11. Radovan M (2010), Računalne mreže (1), Rijeka, Digital point tiskara

Online članci

1. National Institute of Standards and Technology NIST. 2013., NIST Cloud Computing Standards Roadmap. Dostupno na: http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf, (pristupljeno 20.ožujka 2021.).
2. Tegels K, Model Your Data Hierarchies With SQL Server, 2008., Dostupno na: http://msdn.microsoft.com/en-us/magazine/cc794278.aspx, (pristupljeno 16.ožujka 2021.).
3. Rodrigue J, Network Data Models, 2009., Dostupno na: https://people.hofstra.edu/geotrans/eng/methods/ch2m3en.html (pristupljeno 16.ožujka 2021.)
4. Harrison G, 10 things you should know about NoSQL databases, 2010., Dostupno na: http://www.techrepublic.com/blog/10-things/10-things-you-should-know-about-nosql-databases/, (pristupljeno 17.ožujka 2021.).
5. Bronzin T, „Cloud Computing“ ili programska rješenja u oblacima, 2009., Dostupno na: http://pogledkrozprozor.wordpress.com/2009/08/29/%E2%80%9Ecloud-computing%E2%80%9C-ili-programska-rjesenja-u-oblacima/, (pristupljeno 18.ožujka 2021.).
6. Destefani Neto M, A brief history of cloud computing. 2014., Dostupno na: http://thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/, (pristupljeno 18.ožujka 2021.).
7. Craig D, Cloud computing history. 2014., Dostupno na: http://constructioninformer.com/2010/08/14/cloud-computing-history/, (pristupljeno 18.ožujka 2021.).
8. Childs M, McCarthy J, Computer scientist known as the father of AI. 2011., Dostupno na: http://www.independent.co.uk/news/obituaries/john-mccarthy-computer-scientist-known-as-the-father-of-ai-6255307.html, (pristupljeno 18.ožujka 2021.).
9. Conlon D, Cloud computing & small business-security pros and cons. 2011., Dostupno na: www.trendmicro.com/cloud-content/us_pdfs/security-

intelligence/sb_cloud-computing_small_business-pros-and-cons.pdf, (pristupljeno 18.ožujka 2021.).

10. Shah J, Patel K, Patel H. Security Issues in Cloud Computing. International Journal of Engineering and Innovative Technology (IJEIT). 2013., Dostupno na: http://ijeit.com/vol%202/Issue%2010/IJEIT1412201304_14.pdf, (pristupljeno 20.ožujka 2021.).
11. Padhy RP, Patra MR, Sataphy SC. Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2011., Dostupno na: http://ijcsits.org/papers/Vol1no22011/13vol1no2.pdf, (pristupljeno 20.ožujka 2021.).
12. Sathiyapriya K, Malathi D, Vijaya Kumar K, Nagadevi S. A Study on Security Challenges and Issues in Cloud Computing. International Journal of Security Challenges and Issues in Cloud Computing. 2013., Dostupno na: http://www.ijeit.com/vol%202/Issue%207/IJEIT1412201301_47.pdf, (pristupljeno 20.ožujka 2021.).
13. Cloud Security Alliance CSA (2011) *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.* https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
14. Microsoft Azure Marketplace https://docs.microsoft.com/en-us/azure/marketplace/overview, (pristupljeno 20.lipnja 2021.)

Popis slika

Slika 1. - Model računalstva u oblaku prema NIST-u (Prema: Cloud Security Alliance,2011:13) 9
Slika 2. - Entiteti računalstva u oblaku (Prema: NIST, 2013:23) 9
Slika 3. - Entiteti računalstva u oblaku 16
Slika 4. - Komponente Azure 17
Slika 5. - Koncept Azure Storage (Prema: Mazumdar, 2016:23 18
Slika 6. - Komponente SQL Azure 20
Slika 7. – Azure Marketplace (Prema: Azure portalu Cenosco) 24
Slika 8. - Azure VPN (Prema: Mazumdar, 2016:13) 26
Slika 9. – TCP/IP diagram 27
Slika 10.- EdgeRouter - IPsec VPN od web-mjesta do web-mjesta temeljenog na ruti 29
Slika 11. – Konfiguriranje Point-to-site VPN (Prema: Mustafa Toroman, 2020:156). 30
Slika 12. – Kreiranje nove VPN konfiguracije (Prema: Mustafa Toroman 2020:156)31
Slika 13. - Dodavanje nove konekcije site-to-site (Prema: Mustafa Toroman, 2020:126) 32
Slika 14. - VPN konfiguracijski predožak (Prema: Mustafa Toroman, 2020:129) 33
Slika 15. - Hibridno postavljanje rute (Prema: Mazumdar, 2016) 34
Slika 16. - Powershell Point-to-point certifikat 36
Slika 17. - Exportiranje certifikata uz pomoć certmgr 36
Slika 18. - Kreiranje nove stranice site-to-site preko hub-a (Prema: Mustafa Toroman,2020) 37
Slika 19. - Stvaranje VPN web mjesta (Prema: Mustafa Toroman, 2020) 38
Slika 20. - Odabir konekcije VPN lokacije za pokretanje konekcije (Prema: Mustafa Toroman, 2020) 39
Slika 21. - Odabir informacija preko konekcije Virtual Hub-a panela (Prema: Mustafa Toroman, 2020) 39
Slika 22. - Dodavanje prezhodno kreiranog virtualnog Hub-a (Prema: Mustafa Toroman, 2020) 40
Slika 23. - Konfiguriranje virtualnog hub-a (Prema: Mustafa Toroman, 2020) 41

Slika 24. - Kreiranje virtualne grupe resursa (Prema: Azure portal Cenosco)..... 42
Slika 25. - TestRG (Prema: Azure portalu Cenosco)..... 43
Slika 26. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)..... 43
Slika 27. - Stvaranja virtualne mreže (Prema: Azure portalu Cenosco)..... 44
Slika 28. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)..... 44
Slika 29. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)..... 45
Slika 30. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)..... 46
Slika 31. - Stvaranje virtualne mreže (Prema: Azure portalu Cenosco)..... 47
Slika 32. - Stvaranja virtualne mreže (Prema: Azure portalu Cenocso)..... 48
Slika 33. - Konfiguracijska datoteka za Site-to-Site (Prema: Azure portalu Cenosco) 49
Slika 34. - Konfiguracijska datoteka za Site-to-Site (Prema: Azure portalu Cenosco) 50
Slika 35. - Virtualne mašine u Censoco(Prema: Azure portalu Cenosco)..... 52
Slika 36. - Mrežne sigurnosne skupine u Censoco(Prema: Azure portalu Cenosco) 53
Slika 37. - Primjer javne IP adresa za potrebe kljenta (Prema: Azure portalu Cenosco) 54
Slika 38. - Upotreba IMSa u svijetu 58
Slika 39. - Vremenska crta Cenosca - osnivanje, prvi projekt s Shellom, licenciranje i IMS 58
Slika 40. - IMS virtualizacija..... 60
Slika 41. - IMS PEI dashboard 60

Sažetak

U ovom završnom radu obrađena je tema računalstva u oblaku (Infrastruktura kao usluga unutar tvrtke Cenosco). Na samom početku je opisana je povijest računalstva u oblaku njegove prednosti, modeli, te opis same strukture Iaas na Azure oblak okolini. Također u ovom radu obrađeni su dijelovi Azure virtualne mreže, spajanje i konfiguriranje Site-to-Site VPN-a koji se koriste u tvrtki Cenosco. Na samom kraju, opisana je Azure infrastruktura u Cenosco okolini te mogućnosti konfiguriranje grupe resursa u Azure okolini sa mrežnom sigurnosti, te upotreba powershell skripti za deploy stranica na web. Također opisana je sama povijest tvrtke Cenosco, čime se bavi i koje usluge pruža na svjetskom tržištu i za koga.

Ključne riječi:

IAAS - infrastruktura kao usluga

PAAS - platforma kao usluga

SAAS - softver kao usluga

VPN – virtualna privatna mreža

Microsoft Azure – platforma za računalstvo u oblaku

HTTP – HyperText Transfer Protocol

FTP – protokol za prijenos datoteka

TCP – Transportni sloj podataka

IP – Internet protokol

GATEWAY – vrata

EDGE ROUTER – usmjerivač

BGP – protokol graničnog prolaza

HUB – koncentrator ili čvorište

RDP – protokol za povezivanje udaljene radne površine

LAN – lokalna računalna mreža

WAN – mreža širokog pojasa

LOAD BALANCER – metodična i učinkovita raspodjela mrežnog ili aplikacijskog prometa na više poslužitelja

IMS – softver za upravljanje integritetom

IMS PEI - mrežni alat za upravljanje integritetom imovine više vrsta tlačne i civilne opreme

Summary

In this final thesis, the topic of cloud computing (Infrastructure as a service within Cenosco) is described. At the very beginning, the history of cloud computing its advantages, models and the description of the Iaas structure itself on the Azure cloud environment are described. Also in this paper, parts of the Azure virtual network, connection and configuration of Site-to-Site VPNs used in Cenosco are covered. Finally, the Azure infrastructure in the Cenosco environment is described, as well as the ability to configure a group of resources in the Azure environment with network security, and the use of powershell scripts to deploy pages to the web. It also describes the history of Cenosco, what it deals with and what services it provides on the world market and for whom.

Key words:

IAAS - Infrastructure as a service

PAAS - Platform as a service

SAAS - Software as a service

VPN – Virtual private network

Microsoft Azure – Cloud computing service

HTTP – Hypertext Transfer Protocol

FTP – File Transfer Protocol

TCP – Transmission Control Protocol

IP – Internet protocol

GATEWAY – Hardware device between two networks router, server or firewall

EDGE ROUTER – Networking device

BGP – Border Gateway Protocol

HUB – Physical layer networking device

RDP – Remote Desktop Protocol

LAN – Local area network

WAN – wide area network

LOAD BALANCER – process of distributing a set of tasks over a set of resources

IMS – Integrity Management Solution

IMS PEI - web-based tool for managing the asset integrity of multiple types of pressure