

MICROSOFT AZURE - KUORMANTASAUS



Tieto- ja viestintätekniikan opinnäytetyö

Tieto- ja viestintätekniikka, Riihimäki

kevät 2021

Jeremi Andersin

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli tutkia Microsoft Azure -pilvipalvelun käytössä olevien palvelinten kuormantasausta. Työssä keskitytään syventymään virtuaalikoneiden ja pilvipalveluiden teorian tietoon sekä keskeisten työvaiheiden selvittämiseen, joilla perustetaan virtuaalinen verkko ja kuormantasaaminen. Tavoitteena oli, että aluksi luodaan neljä palvelinta, jotka olivat tässä tapauksessa virtuaalikoneita. Virtuaalikoneille luodaan resurssiryhmät, virtuaaliset verkot ja liikenteen johtaja. Kaikkien palvelimien dataa mitataan, jotta voitaisiin analysoida kuormantasauksen toimivuus ja todistaa sen hyöty.

Microsoft Azuren -palvelut ovat helposti skaalattavissa käytön mukaan. Näitä palveluita hyödyntäessä on kuitenkin otettava vahvasti huomioon talous ja kapasiteetti.

Opinnäytetyössä tuodaan esille työprosessi, jolla voidaan yksinkertaisesti tuoda esille palvelinalustan rakentaminen hyödyntäen erilaisia komponentteja, joita Azure tarjoaa. Työn kokonaisuuden hyötyä tutkitaan mittaamalla datankulkua ja sen kuormantasausta kyseisessä ympäristössä. Tulos osoitti onnistuneen kuormantasauksen palvelimien välillä, mikä saatiin testaamalla palvelimien IP-osoitteiden syöttämistä verkkoselaimeen.

Avainsanat Microsoft, kuormantasaus, virtuaalikone, pilvipalvelut

Sivut 40 sivua ja liitteitä 0 sivua

ABSTRACT

The aim of the thesis was to study the load balancing of the servers used by the Microsoft Azure cloud service. The work is focused on theoretical knowledge of virtual machines and cloud services, as well as gaining knowledge of the key work steps for establishing a virtual network and load balancing. The goal was to initially create four servers, which in this case were virtual machines. For virtual machines, there were created resource groups, virtual networks, and a traffic manager. Data from all servers were measured to analyze the functionality of load balancing and to prove its benefit.

Microsoft Azure services are easily scalable according to usage. However, the economy and capacity must be strongly taken into account when using these services. The thesis presents a work process that can be used to simply highlight the construction of a server platform utilizing the various components that Azure provides. The benefits of the whole work are studied by measuring the data flow and its load balancing in the given environment. The result showed a successful load balancing between the servers, which was obtained by testing the IP-addresses of the servers in a web browser.

Keywords Microsoft, load balancing, virtual machine, cloud services

Pages 40 pages and appendices 0 pages

Sisällys

Termit ja lyhenteet	4
1 Johdanto	1
2 Microsoft Azure	2
2.1 Virtuaalikoneet.....	2
2.1.1 Hypervisor	3
2.1.2 Virtualisointi	5
2.1.3 Virtuaalikoneet Microsoft Azuressa.....	8
2.2 Sovellusyhdykäytävät	9
2.3 Resurssiryhmät.....	11
2.4 Virtuaaliset verkot.....	14
2.5 Kustannukset ja laskelmat	16
3 Kuormantasaus.....	17
3.1 Azure kuormantasaaja	17
3.2 Liikenteen valvonta	22
4 Sovellettu projekti	23
4.1 Käytetyt ratkaisut.....	23
4.2 Kustannukset.....	25
4.3 Virtuaalikoneiden konfiguraatio	26
4.4 Sovellusyhdykäytävä ja virtuaalinen verkko.....	32
4.5 Liikenteen valvonta	35
5 Johtopäätökset ja pohdinta.....	39

Kuvat, taulukot ja kaavat

Kuva 1. Hypervisorin toimintatapa (Microsoft, 2021, -b).	4
Kuva 2. Sovellusyhdykäytävän reititys taustajärjestelmään. (Microsoft, 2021, -g).....	11
Kuva 3. Resurssiryhmän rakenne. (Stalcup, 2021)	12
Kuva 4. Resurssinhallinnan kaava. (Microsoft, 2021, -n)	13
Kuva 5. Julkinen ja sisäinen kuormantasaaminen. (Microsoft, 2021, -m)	18
Kuva 6. Opinnäytetyössä tehty palvelin- ja verkkorakenne hahmotettuna.	25
Kuva 7. Resource1-resurssiryhmän sisältö.....	28
Kuva 8. PuTTY -ikkuna kirjautumisen jälkeen.....	29

Kuva 9. Kirjautuminen SSH:n avulla toiselle palvelimelle.	30
Kuva 10. Sisään tulevan liikennesäännön lisääminen.	31
Kuva 11. Uusi palvelimen sivunäkymä.	32
Kuva 12. Aliverkon lisääminen.....	33
Kuva 13. Verkon prioriteettisäännöt.	34
Kuva 14. Pohjois-euroopan ykköspalvelin sovellusyhdykäytävän IP-osoitteella.....	35
Kuva 15. Pohjois-euroopan kakkospalvelin sovellusyhdykäytävän IP-osoitteella.....	35
Kuva 16. Liikenteenvalvoja yhteydessä palvelimeen.	36
Kuva 17. DNS-alueen alla olevat nimipalvelimet.....	37
Kuva 18. Liikenteenvalvonta kohdistuen sovellusyhdykäytävään.....	38

Termit ja lyhenteet

Azure	Microsoft Azure.
Back-end	Taustajärjestelmä. Tietokonejärjestelmän tai sovelluksen osa, johon käyttäjä ei pääse suoraan. Yleensä vastuussa tietojen säilyttämisestä ja käsittelystä.
Front-end	Etujärjestelmä. Tietojärjestelmän tai sovelluksen osa, jonka kanssa käyttäjä on vuorovaikutuksessa suoraan. Käyttäjän käyttöliittymä, jonka kautta tiedot menevät taustajärjestelmään.
Health Probe	Havaitsee taustajärjestelmän tilan. Terveysanturin konfiguraatio määrittää, mitkä taustajärjestelmän esiintymät saavat uusia virtauksia. Jos anturin määritteet epäonnistuvat, virtausten määrä lopetetaan.
Hypervisor	Ohjelmisto, joka käyttää ja luo virtuaalikoneita.
IaaS	Infrastructure as a Service.
PaaS	Platform as a Service.
Pool	Kokoelma resursseja käyttövalmiina sen sijaan, että ne hankittaisiin käytön yhteydessä. Pool-asiakas pyytää

	resursseja ja suorittaa halutut toiminnot sille. Käytön loppuessa, resurssit palautetaan pooliin eikä niitä menetetä.
TCP	Transmission Control Protocol. Tiedonsiirtostandardi, jonka avulla sovellusohjelmat ja tietokonelaitteet voivat viestittää verkon kautta.
TLS	Transport Layer Security. Parannettu versio SSL salauksesta. Salaus, joka suojaa tiedonsiirtoa.
UDP	User Datagram Protocol. Tiedonsiirtoprotokolla, joka ei tunnista sitä, kun lähetettyjä paketteja vastaanotetaan toisessa pisteessä. Se on toinen vaihtoehto TCP-protokollalle.
PuTTY	Ilmainen SSH ja Telnet toteutus tietokoneille, joissa on Windows käyttöjärjestelmä. Hyödyllinen Unix- tai muussa monen käyttäjän järjestelmässä tietokoneelta.

1 Johdanto

Pilvipalvelu on monelle tuttu termi sen vuosien varrella suuren yleistymisen ja kehittymisen myötä. Näihin palveluihin sisältyy palvelin- ja verkkoinfrastruktuurit, verkkopalvelimet ja tietokannat, joita isännöivät palveluntarjoajat kuten Google tai Microsoft. Kyseiset yritykset ovat rakentaneet palvelut oman infrastruktuurinsa päälle, joita hallitaan datakeskuksissa ympäri maailman. Nämä tarjoavat suurta käyttäjäkantaa, joustavuutta sekä skaalautuvuutta.

Pilvipalvelut ovat usein kustannustehokas vaihtoehto perinteiselle paikan päällä sijaitsevalle infrastruktuurille, joka vaatii jatkuvaa ylläpitoa sekä runsaita alkuinvestointeja laitteistoihin ja tiloihin, joissa pitää ottaa huomioon laajentamisen tuomat vaikeudet. (Webber-Cross, 2014)

Kuormantasauksella tarkoitetaan saapuvien datavirtauksien jakamista, jotka saapuvat kuormantasaajan etujärjestelmä (front-end) sekä taustajärjestelmä (back-end) esiintymissä. Virrat on määrätty toimimaan terveystunnistimien ja määritettyjen sääntöjen mukaan, joita on mahdollista muokata kuormantasaukselle. Taustajärjestelmän pool- esiintymät voivat olla virtuaalikoneita tai mittakaavasarjassa olevia esiintymiä. (Microsoft, 2021, -a)

Opinnäytetyön tavoitteena oli tehdä kuormantasaus palvelimien välille käyttäen Microsoft Azure-pilvipalveluita. Työ perustuu Azuren jatkuvaan suosion kasvamiseen ja kehittymiseen, mikä parantaa erilaisia mahdollisuuksia tulevaisuudessa. Korkeimpana tavoitteena oli luoda ympäristö, jossa kuormantasaus on tehty oikein palvelimien välille. Toimivuutta testaamalla ja tekemällä mittauksia saatiin selvitettyä taustajärjestelmä resurssien liikenteen jakautuminen. Toteuttamiseen tarvittavat resurssit, tekijät ja käydyt vaiheet otettiin huomioon työn kokonaisuudessa.

2 Microsoft Azure

2.1 Virtuaalikoneet

Microsoft Azure on Microsoftin pilvipalveluiden yhteisnimi, joka tarjoaa IaaS- ja PaaS-palvelumalleja. IaaS-palvelumalli tuo asiakkaalle mahdollisuuden pilvipohjaisiin palveluihin sekä maksullisiin palveluihin kuten varastointi, verkkoliikenne toiminta ja virtualisointi. Nämä tuodaan virtuaalisten koneiden kautta tilaajien hallintaan. PaaS-palvelumallissa tarjotaan verkossa olevat laitteisto- ja ohjelmistotyökalut tilaajalle. Tämän avulla on mahdollista kehittää, käyttää ja hallita sovelluksia ilman, että rakennetaan ja ylläpidetään tyypillisellä tavalla alusta asti. Omia virtuaalikoneita luodessa Azure selvittää määritystiedoston sijainnin, jonka avulla tulee tietoon, kuinka monta esiintymää on tarve tehdä. Sitä ennen valitaan virtuaalikone, joka tukee sopivaa kokoa. Alusta luo ne käyttäjälle mikä tarkoittaa sitä, että niitä ei nimenomaisesti luoda itse. (Microsoft, 2020, -l)

Virtuaalikonetekniikka on tietokonejärjestelmän virtualisointia. Nämä virtualisoinnit perustuvat tietokone arkkitehtuureihin ja antavat käyttäjälle samanlaisen toiminnallisuuden kuin fyysisessä tietokoneessa. Virtuaalikoneita on kuitenkin kahta erilaista toiminnallisuudeltaan ja ne eivät toimi samalla tavalla. On olemassa järjestelmällisiä virtuaalikoneita ja käsitteleviä virtuaalikoneita. Järjestelmälliset virtuaalikoneet ovat toisin sanoen täydellisen virtualisoinnin koneita. Järjestelmälliset virtuaalikoneet antavat toimintoja kokonaisen käyttöjärjestelmän suorittamiseksi. Käsittelevä virtuaalikone puolestaan antaa yhden prosessin suorittua sovelluksena. Esimerkiksi Java Virtual Machine sallii minkä tahansa järjestelmän suorittaa Java-sovelluksia kuin ne olisivat natiiveja koko järjestelmälle.

Virtuaalikoneet ovat mahdolliseksi tehty virtualisointitekniikan avulla. Virtualisointi käyttää ohjelmistoa simuloimaan virtuaalilaitteistoa, joka tekee monen virtuaalikoneen ajamisen mahdolliseksi. Fyysinen kone on tunnettu isäntänä (host), kun sillä ajettavat virtuaalikoneet ovat vieraita (guest). Tätä prosessia hallinnoi ohjelmisto nimeltään hypervisor. Hypervisor on vastuussa resurssien hallinnasta ja varaamisesta isännältä vieraille. Virtuaalikoneiden

osalta se myös ajoittaa niiden toimintoja, jotta ne eivät ylitä toisiaan niiden käyttäessä resursseja. Virtuaalikoneet toimivat vain, jos on olemassa hypervisor, joka virtualisoi ja jakaa isännän resursseja. (Citrix, 2021, -a)

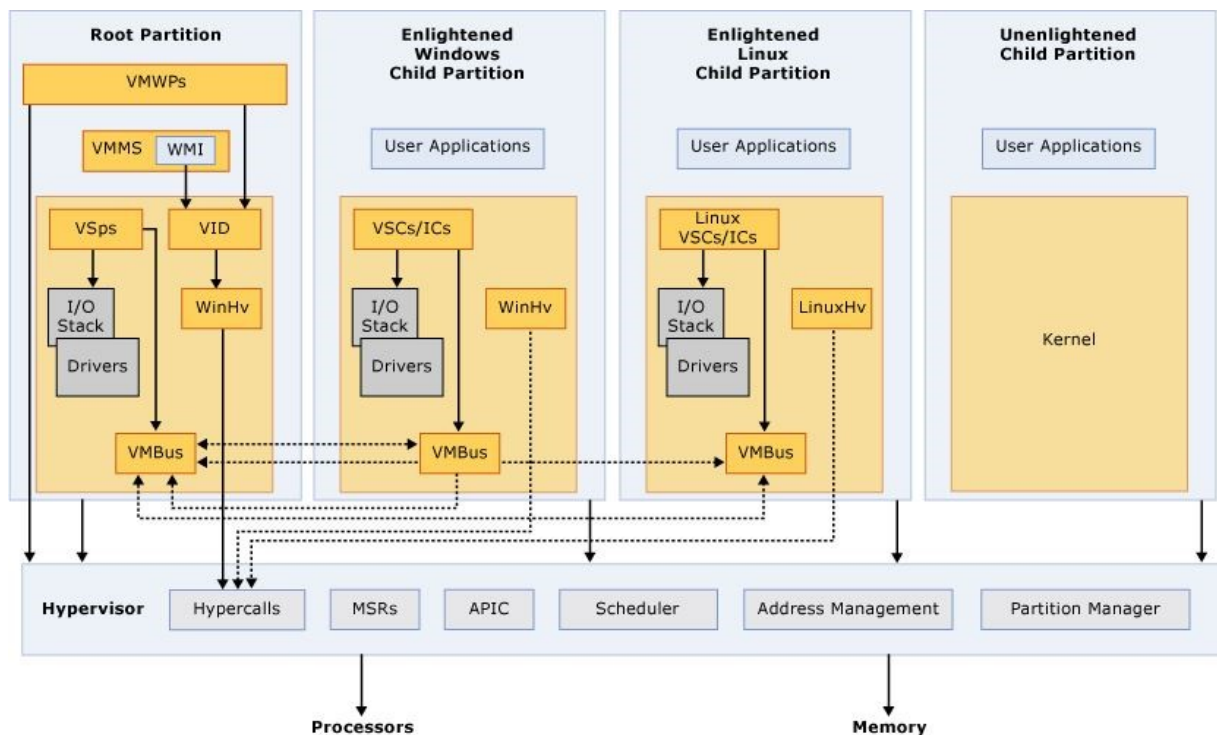
2.1.1 Hypervisor

Virtualisoinnissa käytetään kahta erilaisesti toimivaa hypervisoria. Ensimmäistä kutsutaan nimellä paljasmetallinen hypervisor, joka asennetaan fyysiseen laitteistoon. Virtuaalikoneet ovat vuorovaikutuksessa kaikkien isäntälaitteiden kanssa, jotta ne voivat jakaa laitteistoresursseja ilman ylimääräisiä ohjelmistotasoa niiden välillä. Isäntälaitteet, joissa on tämän tyyppin hypervisor, ovat käytössä vain virtualisointiin tarkoitettuihin tapauksiin. Tämän kaltaisia esiintyy usein palvelinympäristöissä. Microsoft Hyper-V on yksi esimerkki, jossa tällaista rakennetta käytetään. Jos halutaan vierastoimintoja hallita kuten uusien virtuaalikone-esiintymien luominen tai käyttöoikeuksien hallitseminen, tarvitaan erillinen hallintatyökalu. Toisen tyyppin hypervisor puolestaan on kutsuttu isännöidyksi hypervisoriksi, joka toimii isäntälaitteen käyttöjärjestelmässä. Isännöidyt hypervisorit välittävät virtuaalikoneiden pyyntöjä isäntä käyttöjärjestelmälle. Täten se huolehtii fyysisten resurssien jakamisesta jokaiselle vieras laitteelle. Tämän tyyppin hypervisor toimii hitaammin kuin edellä mainittu ensimmäinen hypervisor, koska jokaisen virtuaalikoneen toiminta käy ensin isäntä käyttöjärjestelmän kautta. Toisin kuin paljasmetallisissa hypervisoreissa, vieraskäyttöjärjestelmät eivät olet sidottuina fyysisiin laitteisiin. Käyttäjät voivat käyttää virtuaalikoneita ja tietokoneen järjestelmää normaaliin tapaan. Tämän ansiosta toisen tyyppin hypervisorit ovat hyviä yksityiskäyttäjille tai pienyrityksille, joilla ei ole erillisiä palvelimia virtualisointia varten. (Citrix, 2021, -a)

Hyper-V on hypervisoripohjainen virtualisointialusta, joka käyttää natiivia suoritustehoaan laitteistojen jakamiseen ja hallintaan. Tämä toiminta sallii useiden ympäristöjen eristymisen toisistaan, mutta ovat kuitenkin olemassa samalla fyysisellä koneella. Nykyaikaiset hypervisorit käyttävät laitteistoavusteista virtualisointia ja virtualisointikohtaista laitteistoa.

Hypervisor on ohjelmisto, joka käyttää ja luo virtuaalikoneita. Se tunnetaan myös virtuaalikoneen monitori ja VMM nimillä. Hypervisorin avulla host-kone voi tukea guest-virtuaalikoneita jakamalla resursseja, kuten muistia ja prosessointia (Kuva 1).

Kuva 1. Hypervisorin toimintatapa (Microsoft, 2021, -b).



Hypervisorit mahdollistavat järjestelmän resursseista suurimman osan käytettäväksi ja ne lisäävät IT-liikkuvuutta, koska vierailevat virtuaalikoneet ovat riippumattomia isäntälaitteistosta. Niitä voidaan siis helposti siirtää palvelimien välillä. Koska useat virtuaalikoneet voidaan ajaa yhden fyysisen palvelimen hypervisorilla, se vähentää tilan käyttöä ja ylläpitovaatimuksia.

Laitteistokiihdytystekniikka voi luoda ja hallita virtuaalisia resursseja nopeammin lisäämällä prosessointi nopeutta paljasmetallisille hypervisoreille ja isännöidyille hypervisoreille. Laitteistokiihdytin, joka tunnetaan nimellä virtuaalinen Dedicated Graphics Accelerator, huolehtii 3D-grafiikan lähettämisestä ja päivittämisestä. Tämä vapauttaa pääjärjestelmän

hoitamaan muita tehtäviä ja se lisää kuvien näyttönopeutta huomattavasti. Niillä aloilla tämä tekniikka on hyödyllinen, joissa monimutkaiset tiedot on tarve saada visualisoitua nopeasti.

Molempien tyyppien hypervisorit voivat käyttää useita virtuaalipalvelimia yhdeltä fyysiseltä koneelta. Yksi palvelin saattaa isännöidä useita virtuaalipalvelimia, joissa on eri yritysten työmäärät samanaikaisesti virtaamassa. Tämän tyyppinen resurssien jakaminen voi johtaa muiden käyttäjien ongelmatilanteisiin, koska yhden käyttäjän työtaakka kuormittaa palvelimen suorituskyykyä. Paljasmetalli palvelin tarjoaa aina paremman suorituskyyvyn kuin virtuaalipalvelin, jota hallinnoi yksi yritys. Virtuaalipalvelin jakaa fyysisen palvelimen kaistanleveyden, muistin ja prosessointitehon muiden virtuaalipalvelimien kanssa. Paljasmetallisen palvelimen laitteisto voidaan myös optimoida parantamaan suorituskyykyä, mikä ei päde kuitenkaan julkisiin jaettuihin palvelimiin.

Useita virtuaalikoneita isännöivästä hypervisorista on eri hyötyjä. Hypervisorit mahdollistavat virtuaalikoneiden luomisen välittömästi, toisin kuin paljasmetalliset palvelimet. Se helpottaa resurssien varaamista mitä tarvitaan dynaamisiin työmääriin. Paljasmetalliset hypervisorit antavat käyttöjärjestelmien ja niiden sovellusten toimia erilaisilla laitteistotyypeillä, koska hypervisor erottaa käyttöjärjestelmän taustalla olevasta laitteistosta. Täten ohjelmisto ei ole riippuvainen tietyistä laitteista tai ohjaimista. Kuormituksia voidaan siirtää ja allokoida verkko-, muisti-, tallennus- ja käsittelyresursseja useille palvelimille tarpeen mukaan, sillä hypervisorin käyttämät virtuaalikoneet ovat riippumattomia fyysisestä koneesta. (Vmware, 2020, -a)

2.1.2 Virtualisointi

Organisaatiot käyttävät virtualisointia isännöimään monia virtuaalikoneita yhdelle tietylle palvelimelle. Sen sijaan, että investoisi ylimääräisiin palvelimiin, voidaan käyttää virtuaalikoneita yhdellä palvelimella kutakin sovellusta varten.

Virtualisointi on tietojärjestelmä tekniikka, joka simuloi laitteiston toiminnallisuutta luodakseen ohjelmistopohjaisia IT-palveluita, kuten sovelluksia, palvelimia, tallennustilaa ja verkkoja. Virtualisointi luo siis useita virtuaalikoneita yhdestä fyysisestä koneesta

käyttämällä hypervisoria. Virtualisointi mahdollistaa IT-organisaatioille usean käyttöjärjestelmän ajamisen yhdellä palvelimella. Kyseisten operaatioiden aikana hypervisor kohdentaa resursseja jokaiselle virtuaalikoneelle tarpeen mukaan. Tämä tekee toiminnasta paljon tehokkaampaa sekä kustannustehokkaampaa. Joustava resurssien kohdentaminen on tehnyt virtualisoinnista pilvipalvelujen perustan. Virtualisointimenetelmät voivat vaihdella käyttäjän käyttöjärjestelmän mukaan. Linux-koneet tarjoavat avoimen lähdekoodin hypervisorin, joka tunnetaan nimellä kernel-based virtual machine (KVM). Isäntäkone voi ajaa montaa virtuaalikonetta ilman erillistä hypervisoria. Huomioitavana on se, että kaikki IT-ratkaisujen tarjoajat eivät kuitenkaan tue KVM:ää ja sen toteuttamiseen tarvitaan asiantuntemusta Linux-käyttöjärjestelmistä. Virtualisoinnin avulla voi jakaa palvelimen virtuaalikoneisiin, jonka ansiosta vähennetään ylläpitokustannuksia. Esimerkiksi yksi palvelin voi käsitellä sähköposti- ja verkkoliikennettä, kun toinen isännöi kaikkia liiketoimintasovelluksia. (Citrix, 2021, -b)

Mitä ovat virtualisoinnin hyödyt? Virtualisoinnin avulla yksi kone voi palvella monena virtuaalikoneena. Tämä ei tarkoita vain sitä, että tarvitaan vähemmän palvelimia, vaan jo olemassa olevia palvelimia voidaan käyttää täydellä kapasiteetilla. Nämä hyötysuhteet näkyvät laitteistojen, jäähdytyksen ja ylläpidon kustannussäästöissä. Tämä ratkaisu tuo myös ympäristöhyötyjä esimerkiksi jättämällä pienemmän hiilijalanjäljen. Virtualisoinnin avulla ajetaan useita sovelluksia, työpöytiä ja käyttöjärjestelmiä yhdellä koneella sen sijaan, että tarvitsisi erillisiä palvelimia toimittajilta. Tämä antaa vapauden siitä, että on sidottuna tiettyihin palveluntarjoajiin ja se tekee fyysisten resurssien hallinnasta paljon vähemmän aikaa vievää. Virtualisoinnilla voidaan helposti varmistaa tietojen palauttaminen ja varmuuskopiointi käyttämällä virtuaalikoneen tilannekuvia olemassa olevilta palvelimilta. Varmuuskopioinnin prosessi on myös automatisoitavissa yksinkertaisesti. Jos ongelmatilanteessa jotain on palautettava varmuuskopioidusta virtuaalikoneesta, virtuaalikone on helppo siirtää uuteen sijaintiin muutamassa minuutissa. Tämä lisää luotettavuutta ja liiketoiminnan jatkuvuutta, koska menetyksestä on helpompi toipua. Virtualisoinnin avulla voi luoda pilvistrategian jakamalla virtuaalikoneen resurssit organisaation yhteisesti jaettuun pooliin. Pilvipohjainen infrastruktuuri antaa hallinnan siitä,

kuka voi käyttää resursseja ja millä laitteella. Tämä parantaa tietoturvaa ja joustavuutta. (Citrix, 2021, -b)

Virtualisointeja on erityyppisiä. Ensimmäinen näistä on palvelin virtualisointi. Palvelinten virtualisointi käyttää hypervisoria jakamaan fyysiset palvelimet useisiin virtuaalipalvelimiin, jokaisella niillä on oma käyttöjärjestelmänsä. Tämän avulla voi käyttää fyysisten palvelimien täyttä tehoa, jotta voidaan huomattavasti vähentää tietokoneiden laitteisto- ja käyttökustannuksia. Sovellusten ja työpöydän virtualisoinnissa ei tarvitse simuloida koko palvelinta, koska tämä tekniikka voi virtualisoida yksittäisiä työpöytiä tai sovelluskerroksia. Sovellusten virtualisoinnilla käyttäjät voivat käyttää sovelluksia erillisessä muodossa käytössä olevasta käyttöjärjestelmästä riippumatta. Tätä tapaa käytetään yleensä Windows-sovelluksen suorittamiseen Linux- tai Mac-käyttöjärjestelmässä. Työpöydän virtualisointi antaa käyttäjille mahdollisuuden simuloida työaseman kuormitusta päästääkseen työpöydälle etäyhteydellä liitetystä laitteesta. Tämä tarkoittaa sitä, että työpöydän virtualisointi antaa turvallisemman ja kannettavamman pääsyn datakeskuksen resursseihin. Virtuaalisovellukset ja työpöydät tarjoavat paremman ratkaisun, kun ne ovat keskitetty keskuspalvelimelle. Tallennuksen virtualisoinnilla tarkoitetaan sitä, kun verkon useiden laitteiden fyysinen tallennustila yhdistetään yhtenäiseksi virtuaaliseksi tallennuslaitteeksi, jota hallitaan keskuskonsolista. Varastoinnin ja tallennuksen virtualisoimiseen tarvitaan virtualisointiohjelmisto, joka tunnistaa fyysisistä laitteista käytettävissä olevan vapaan tilan ja yhdistää näiden vapaan kapasiteetin virtuaaliseen ympäristöön. Loppukäyttäjille virtuaalitallennus vaikuttaa fyysiseltä kovalevyiltä. Virtuaalitallennus on tärkeä osa strategiaa, jonka avulla järjestelmänvalvojat voivat virtaviivaistaa tallentamiseen liittyviä toimintoja, kuten varmuuskopiointia, arkistointia ja palautusta. Tietojen virtualisointi puolestaan antaa sovellukselle pääsyn tietoihin ja hyödyntää niitä tarvitsematta tietoa siitä, missä ne fyysisesti sijaitsevat tai mihin formaattiin data on luotu. Tämä tarkoittaa sitä, että tiedot voidaan hakea monesta lähteestä liikuttamatta tai kopioimatta kyseisiä tietoja. Tietojen yhdistäminen perustuu tietojen virtualisointiohjelmistoon, mitä kautta virtuaalinen integrointi ja visuaalinen datan tuonti onnistuu. Tällöin käyttäjät voivat käyttää suuria tiedostomääriä yhdestä tukiasemasta riippumatta siitä mihin nämä tiedot on tallennettu.

Tietojen virtualisointi on tärkeää analytiikan- ja liiketoimintatiedon sovelluksille. (Citrix, 2021, -b)

Virtualisointia on hallittava asianmukaisesti, jotta tiedot pysyvät turvallisesti salassa. Koska virtuaalikoneet ovat kopioita palvelimista ja niiden lukumäärä voi olla suuri, niistä kertyy useampi kohde hyökkääjille, jotka uhkaavat arkaluonteisia tietoja. Tietoturva aukon vuoksi on tärkeää, että olemassa on keskitetty hallintaratkaisu virtuaalikoneiden valvomiseksi ja suojaamiseksi. Virtualisointiturva on olennainen osa virtuaalista työpöytäinfrastruktuuria. Työtilan virtualisointi perustuu sovellusten virtualisointiin niputtamalla useita sovelluksia yhteen yhdistyneeksi digitaaliseksi työtilaksi. Tämä simuloi virtuaalikoneen koko työtilaa, jolloin käyttäjien sovellukset vuorovaikuttavat samalla tavalla kuin fyysisen koneen kanssa. Tavanomaisessa sovelluksen virtualisoinnissa jokainen yksittäinen sovellus virtualisoidaan erikseen, jotta ne eivät olisi vuorovaikutuksessa toistensa kanssa. (Citrix, 2021, -b)

2.1.3 Virtuaalikoneet Microsoft Azuressa

Virtuaalikoneet antavat helposti skaalautuvan palvelininfrastruktuurin järjestelmien rakentamiseen tyhjästä. Azure antaa mahdollisuuden käyttää niitä Windows- tai Linux-käyttöjärjestelminä. Azure Virtual Machine antaa joustavan virtualisoinnin, jonka ansiosta ei ole tarvetta ostaa ja ylläpitää fyysistä laitteistoa. Virtuaalikonetta on kuitenkin ylläpidettävä erilaisilla tehtävillä kuten määrittelemällä, korjaamalla ja asentamalla siihen suoritettavat ohjelmistot. Azuren virtuaalikoneita voidaan käyttää monipuolisesti. Koneita voi luoda nopeasti ja helposti, jotka soveltuvat hyvin koodausta sekä testausta varten. Virtuaalikoneet voi sammuttaa tai käynnistää aina halutessaan. Tämä voi olla taloudellisesti fiksu vaihtoehto, koska niistä maksetaan käytön mukaan. Azuren virtuaaliverkon virtuaalikoneet voidaan helposti yhdistää oman organisaation verkkoon. Laajentamisen mahdollisuudet tarpeen mukaan on tehty niin, että se ei vaadi mahdottomia toimenpiteitä.

Esiasennetuilla SQL-, Oracle- ja SharePoint palvelinohjelmistoilla on useita kuvan monitorointi mahdollisuuksia saatavilla. Tällä hetkellä on erilaista 43 joista kaksi on esikatseltavissa.

Virtuaalikoneisiin voi asentaa omia ohjelmistoja halutessaan, jotka käyttävät Azure Cloud Services -palvelua. Näin voidaan käyttää sekä hallita omia ohjelmistoja etänä. (Microsoft, 2020, -l)

2.2 Sovellusyhdykäytävät

Sovellusyhdykäytävällä eli Application Gatewayllä tarkoitetaan palomuurin välityspalvelinta, joka antaa verkolle suojausta. Se sijaitsee asiakkaan ja palvelimen palomuurissa. Se tarjoaa korkean tason suojattua verkkojärjestelmän viestintää. Kun pyydetään pääsyä palvelinresursseihin, muodostetaan ensin yhteys välityspalvelimeen, joka muodostaa yhteyden pääpalvelimeen. Välityspalvelimen tarkoituksena on piilottaa käyttäjätiedot ja IP-osoitteet asiakkaan puolesta. Sovellusyhdykäytävä ja ulkoinen tietokone toimivat ilman, että kerättäisiin asiakastietoja tai tietoja välityspalvelimen IP-osoitteesta. Tämä tekniikka suodattaa saapuvan liikenteen tiettyjen spesifikaatioiden mukaan mikä tarkoittaa sitä, että vain lähetetyt verkkosovellustiedot suodatetaan. Tämän kaltaisia verkkosovelluksia on esimerkiksi tiedoston siirto protokolla, Telnet ja Real Time Streaming Protokolla. (Techopedia, 2021)

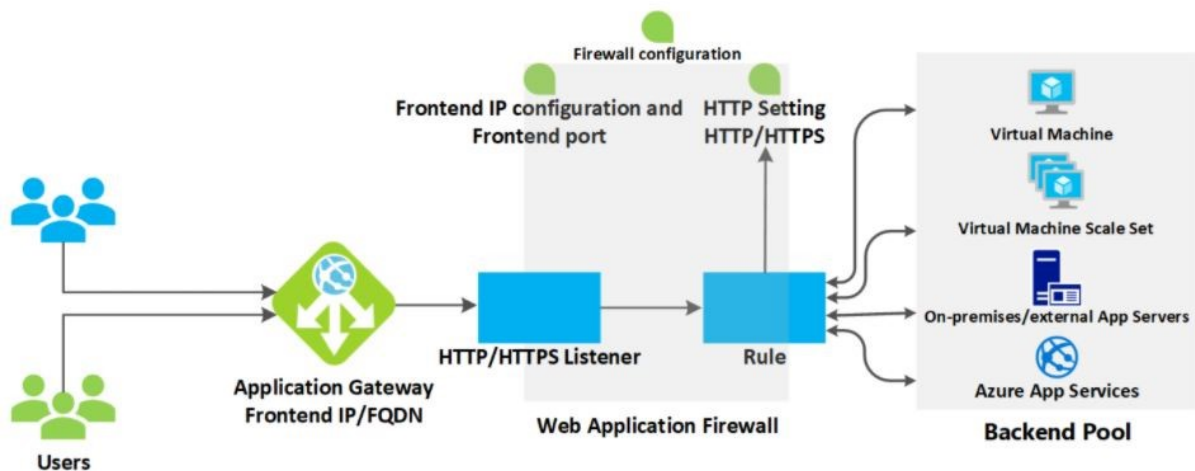
Microsoft Azuren sovellusyhdykäytävä -ohjelmaa voidaan käyttää verkkoliikenteen kuormituksen tasaamiseen, jolla hallitaan liikennettä verkkosovelluksissa. Se voi toimia sisäisenä sovelluksen kuormantasaajana tai Internet-sovelluksen kuormantasaajana. Sovellusyhdykäytävä voi tehdä reitityspäätöksiä HTTP-pyyntöjen lisätribuuttien perusteella. Näitä ovat esimerkiksi URI-polku ja isäntäkentät. Verkkoliikenne määrätään kohdistumaan tietyille palvelimille, joita kutsutaan myös pool-nimellä. Sovellusyhdykäytävän infrastruktuuri sisältää virtuaaliverkon, aliverkkoja, verkon suojausryhmät ja käyttäjän määrittämät reititykset.

Kuinka sovellusyhdykäytävä käytännössä toimii? Ennen kuin käyttäjä lähettää pyynnön sovellusyhdykäytävälle, se ratkaisee ensin toimialueen nimen käyttämällä DNS-palvelinta (Kuvassa 2). Azure DNS palauttaa IP-osoitteen käyttäjälle, joka toimii sovellusyhdykäytävän etujärjestelmän IP-osoitteena. Sovellusyhdykäytävällä on kuuntelija tai kuuntelijoita, jotka hyväksyvät saapuvan liikenteen. Kuuntelija tarkistaa yhteyspyynnöt käyttäjältä. Kuuntelija on

määritetty etujärjestelmän IP-osoitteella, protokollalla ja portin numerolla yhteyksiä varten, jotka saapuvat käyttäjiltä sovellusyhdykäytävälle. Jos verkkosovelluksen palomuuuri eli WAF on käytössä, sovellusyhdykäytävä tarkistaa pyyntöjen otsikot ja rungot laadittujen tietoturva sääntöjen mukaisesti. Tämä toiminto määrittää onko kyseessä tietoturvauhka vai kelvollinen pyyntö. Jos pyyntö on kelvollinen, se osoitetaan taustajärjestelmään. Jos pyyntö on tunnistustilassa, se arvioidaan ja kirjataan, mutta silti osoitetaan taustajärjestelmän palvelimelle.

Pyynnön reitityssäännön perusteella sovellusyhdykäytävä määrittää reititetäänkö kaikki kuuntelijan pyynnot tiettyyn taustajärjestelmään, eri taustajärjestelmään URL-polun perusteella vai ohjataanko pyynnot toiseen porttiin tai ulkoiseen sivustoon. Kun sovellusyhdykäytävä valitsee taustajärjestelmä poolin, se lähettää pyynnön jollekin poolin kunnossa olevista taustajärjestelmä palvelimista. Palvelimien kunto määritetään terveysturilla (Health Probe). Jos taustajärjestelmän pool sisältää useita palvelimia, niin sovellusyhdykäytävä käyttää arviointi algoritmia osoittaakseen pyynnot kunnossa olevien palvelimien välillä. Tämä tasapainottaa pyyntöjen kuormaa palvelimien välillä. HTTP-asetukset määrittävät protokollan, portin ja muut reititykseen liittyvät asetukset, joita tarvitaan uuden istunnon muodostamiseen taustajärjestelmän palvelimen kanssa. Näissä asetuksissa käytetty portti ja protokolla määrittävät, onko sovellusyhdykäytävän ja taustajärjestelmän välinen liikenne salattu vai salaamaton. Sovellusyhdykäytävä lähettää alkuperäisen pyynnön taustajärjestelmä palvelimelle. Tällöin se noudattaa kaikkia mukautettuja kokoonpanoja HTTP-asetuksiin perustuen, jotka liittyvät host-nimen, polun ja protokollan ohittamiseen. Tämä toiminto ylläpitää esimerkiksi evästepohjaisen istunnon affiniteettia, yhteyden tyhjenty mistä ja host-nimen valintaa taustajärjestelmästä. Sovellusyhdykäytävä lisää neljä ylätunnistetta kaikkiin pyyntöihin ennen kuin ne välitetään taustajärjestelmään. Näitä tunnisteita ovat x-forwarded-for, x-forwarded-proto, x-forwarded-port ja x-original-host. (Microsoft, 2021, -g)

Kuva 2. Sovellusyhdykäytävän reititys taustajärjestelmään. (Microsoft, 2021, -g)



Virtuaaliverkossa tarvitaan erillinen aliverkko sovellusyhdykäytävälle. Aliverkossa voi olla useita tietyn sovellusyhdykäytävän esiintymiä. Kyseisessä sovellusyhdykäytävän aliverkossa ei kuitenkaan voi olla käytettävissä muita resursseja. Standard_v2- ja Standard Azure Application Gateway -sovelluksia ei voi sekoittaa samaan aliverkkoon.

Sovellusyhdykäytävä käyttää yksityistä IP-osoitetta yhdelle esiintymälle. Se käyttää myös toista yksityistä IP-osoitetta, jos yksityinen käyttöliittymän IP-osoite on määritetty.

Sovellusyhdykäytävän voi määrittää käyttämään julkista IP-osoitetta, yksityistä IP-osoitetta tai molempia. Julkinen IP-osoite määritetään vain silloin kun isännöidään taustajärjestelmä resursseja, joihin asiakkaiden täytyy päästä internetin avulla virtuaalisen IP-osoitteen kautta. Azure varaa myös viisi IP-osoitetta sisäiseen käyttöön jokaisessa aliverkossa. Esimerkkinä voidaan ottaa 15 sovellusyhdykäytävän esiintymää, joilla ei ole yksityistä etujärjestelmä IP-osoitetta. Tälle aliverkolle tarvitaan vähintään 20 kappaletta IP-osoitteita, joista viisi tulee sisäiseen käyttöön ja loput 15 sovellusyhdykäytävän esiintymiin. (Microsoft, 2021, -c)

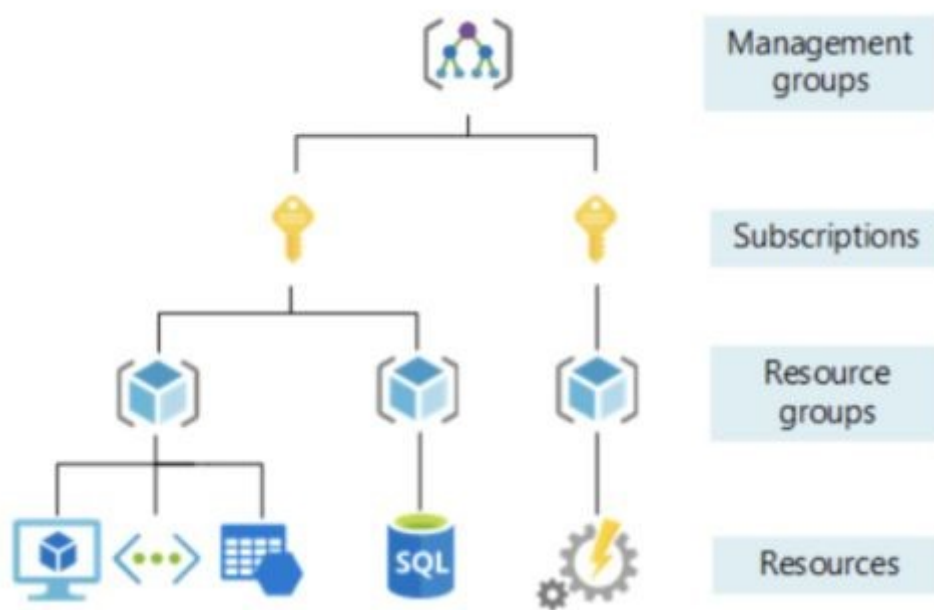
2.3 Resurssiryhmät

Resurssiryhmät tarkoittavat säiliöitä, jotka sisältävät resursseja liittyen tiettyyn Azuren ratkaisuun. Resurssiryhmä voi sisältää kaikki ratkaisun resurssit tai vain ne resurssit, joita halutaan hallita ryhmänä. Yleisesti lisätään samaan resurssiryhmään kaikki ne resurssit, jotka

halutaan käyttöönottaa, päivittää tai on tarkoitus poistaa ryhmänä. Resurssiryhmä säilöö resurssien metadatan. Kun on tarkoitus määrittää resurssiryhmän sijainti, määritetään samalla mihin metatiedot tallennetaan. Kun käyttäjä lähettää pyynnön mistä tahansa Azure-työkalusta, API:sta tai SDK:sta, Resurssienhallitsija vastaanottaa pyynnön. Resurssinhallinta vastaanottaa pyynnön, tulkitsee ja todentaa sille valtuudet läpi päästettäväksi tai ei. Resurssienhallinnan kautta lähetetään pyyntö Azure-palvelulle, joka suorittaa pyydetyn toiminnon. Kaikki pyynnot käsitellään saman sovellusliittymän kautta. Täten nähdään johdonmukaiset tulokset ja ominaisuudet kaikissa eri työkaluissa. (Microsoft, 2021, -j)

Kun virtuaalikone luodaan Microsoft Azuressa, se määritetään tiettyyn resurssiryhmään. Taitavalla käytöllä tätä rakennetta voidaan käyttää parempaan hallintoon ja kustannusten hallintaan infrastruktuurissa. Resurssiryhmät ovat loogisesti tehtyjä kokoelmia virtuaalikoneista, säilöntätileistä, virtuaaliverkoista, verkkosovelluksista ja tietokannoista tai tietokantapalvelimista (Kuva 3). Sovelluksiin liittyvät resurssit ryhmitellään tyypillisesti tuotantoon ja muuhun kuin tuotantoon -tyylisesti.

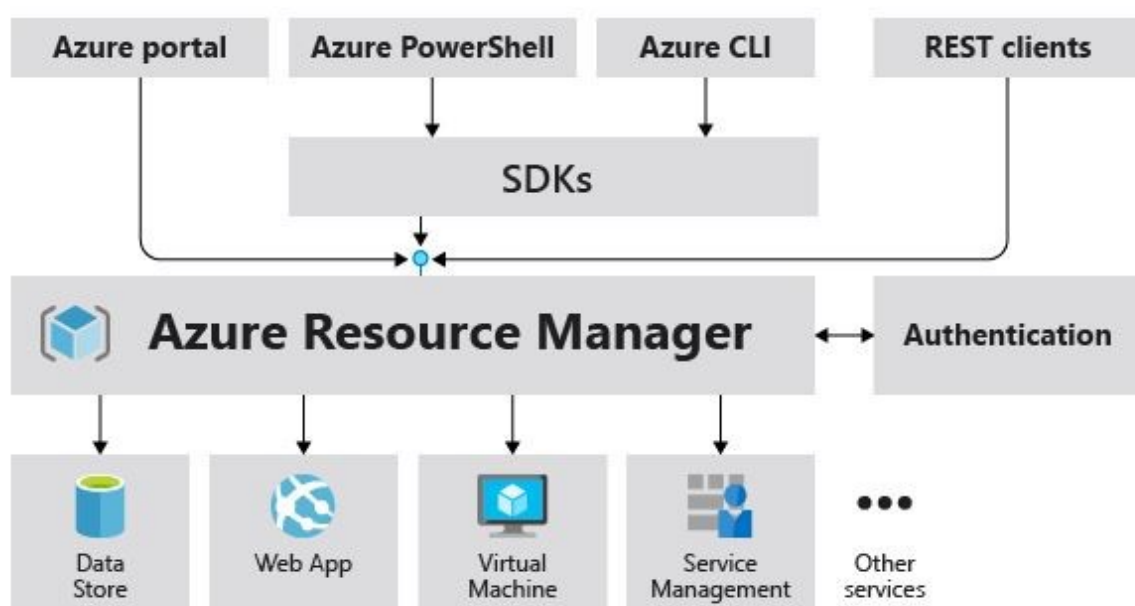
Kuva 3. Resurssiryhmän rakenne. (Stalcup, 2021)



Hallintaryhmät ovat säiliöitä, joiden avulla voi hallita käyttöoikeuksia, käytäntöjä ja laadittuja sääntöjä. Kaikki hallintaryhmän tilaukset perivät automaattisesti kaikki ryhmään sovelletut ehdot. Näitä käytetään usein tilausten ryhmittelyyn sisäisen osaston tai maantieteellisen alueen mukaan. Tilaukset yhdistävät käyttäjätilit ja käyttäjätilien luomat resurssit. Jokaisella tilauksella on rajoituksia tai maksimi kiintiöt resurssien määrälle, jota voi luoda tai käyttää. Organisaatiot voivat käyttää tilauksia kulujen laskemiseen ja hallintaan sekä resurssien hallintaan, joita tiimit, projektit tai käyttäjät ovat luoneet. Hallintaryhmässä ei voi olla Azure-resurssia. Tämä voi sisältää vain toisia hallintaryhmiä tai tilauksia. (Stalcup, 2021)

Resurssiryhmiä hallitaan Azure Resource Manager -palvelun avulla, joka on resurssien hallintataso (Kuva 4). Kyseisen palvelun etuihin kuuluu infrastruktuurien hallitseminen deklaratiivisten mallien avulla komentosarjojen sijaan. Tähän kuuluu myös tunnisteidien hallinta, käyttöönottomallit, riippuvuuden kartoitus, yksinkertaistettu roolipohjainen pääsyn valvonta ja kustannusten hallinta. Resurssiryhmät voidaan järjestää työnkulun suojaukseen, ylläpitoon ja kustannusseurantaan perustuen.

Kuva 4. Resurssinhallinnan kaava. (Microsoft, 2021, -m)



2.4 Virtuaaliset verkot

Virtualisoitujen ympäristöjen suuren lisääntymisen vuoksi monet organisaatiot virtualisoivat myös verkkojaan. Verkon virtualisointi toimii jakamalla käytettävissä oleva kaistanleveys omiksi kanaviksi, joista kukin voidaan määrittää palvelimelle tai laitteelle tarpeen mukaan. Verkon virtualisointi helpottaa verkossa ohjelmointia ja verkon säännöstelyä mukaan lukien kuormantasaamista ja suojausta ilman, että tarvitsee koskettaa taustalla olevaa infrastruktuuria. (Citrix, 2021, -b)

Virtuaalinen verkko mahdollistaa tiedonsiirron useiden tietokoneiden, virtuaalikoneiden, virtuaalipalvelimien tai muiden laitteiden välillä. Se mahdollistaa myös useissa paikoissa olevien laitteiden toiminnan samalla tavalla kuin perinteinen fyysinen verkko. Tämä mahdollistaa datakeskusten määrän skaalaamisen eri fyysisiin paikkoihin sekä kyvyn muokata verkkoa moitteetta ilman, että tarvitsee ostaa tai vaihtaa laitteistoa. Lisäksi sillä on kyky siirtää työkuormituksia infrastruktuuriin vaarantamatta sen turvallisuutta, palveluja tai saatavuutta.

Fyysisiä verkkokortteja ja verkkosovittimia käytetään tietokoneiden ja palvelimien verkkoon liittämiseen. Virtuaalinen verkko siirtää nämä ja muut toiminnot ohjelmistoihin. Virtuaalikytkimeksi kutsuttu sovellus ohjaa ja kohdistaa viestinnän fyysisen verkon ja virtuaalisten osien välillä. Virtuaalisen verkon sovitin päästää tietokoneet ja virtuaalikoneet yhdistämään verkkoon sekä kaikki lähiverkon koneet voivat yhdistää tätä kautta suurempaan verkkoon. Fyysisessä verkossa luodaan lähiverkot yhdistämään laitteet jaettuihin resursseihin, kuten verkkotallennustilaan, kun taas virtuaalinen verkostoituminen luo mahdollisuuden virtuaalisille lähiverkoille, joissa ryhmittely määritetään ohjelmiston avulla. Tämä tarkoittaa, että eri verkkokytkeisiin yhdistetyt tietokoneet voivat käyttäytyä ikään kuin ne olisivat yhdistettynä samaan. Myös tietokoneet, jotka jakavat kaapeloinnin voidaan pitää eri verkoissa sen sijaan, että koneet yhdistettäisiin fyysisesti kaapeloimalla tai muita laitteita käyttäen. Virtuaalinen verkko tarjoaa keskitetyemmän hallinnan ja yksinkertaistetumman verkonhallinnan. Tämä tekniikka on perusta pilviarkkitehtuureille ja sovelluksille, koska se mahdollistaa pääsyn pilviresursseihin, yhdistämisen, suojaamisen ja mahdollisuuden muokata pilviresursseja.

Mitä hyötyä on virtuaalisesta verkosta? Virtuaalinen verkostoituminen antaa erilaisia liiketoiminnallisia etuja investointien ja ylläpitokustannusten alentamisesta verkkojen segmentointiin. Se virtaviivaistaa verkkolaitteiden määrää siirtämällä monia toimintoja ohjelmistoihin, vähentää laitteiden ja ohjelmistojen kustannuksia keskitetyn ohjauksen avulla ja antaa joustavammat vaihtoehdot verkon reititysrakenteelle ja kokoonpanolle. Lisäksi verkkoliikenteen hallintaa voidaan parantaa paremmilla vaihtoehdoilla, kuten palomuurien määrittäminen virtuaalisen verkkokortin tasolla. Virtuaaliset päivitykset, automatisoidut määrittäykset, modulaariset muutokset verkkolaitteissa ja sovelluksissa, etäkäyttö, automatisoidut palvelut sekä suorituskyvyn testaaminen kuuluvat myös näihin ominaisuuksiin. (Vmware, 2020, -b)

Azure Virtual Network eli VNet on yksityisen verkon peruselementti. Vnet mahdollistaa monen tyyppisiä Azure resursseja turvallisesti kommunikoimaan keskenään kuten virtuaalikoneita. Virtuaalikoneiden lisäksi myös internetissä ja paikallisissa verkoissa. VNet on kuin tavallinen verkko, jota käytetään datakeskuksissa. Se tuo Azuren infrastruktuuriin lisäetuja kuten mittakaavan suurennuksen ja pienennyksen, saatavuuden ja eristämisen mahdollisuuden. Tärkeimpiä asioita, joita voidaan toteuttaa virtuaaliverkolla ovat Azure-resurssien viestintä internetin kanssa, viestintä paikallisten resurssien kanssa, verkkoliikenteen suodattaminen, verkkoliikenteen reitittäminen ja integrointi Azure-palveluiden kanssa. Kaikki VNetin lähtevät resurssit voivat oletusarvoisesti kommunikoida internetin kanssa. Saapuvalla resurssille voidaan kommunikoida, kun määritetään julkinen IP-osoite tai julkinen kuormantasaaja. Näitä kahta voidaan käyttää myös lähtevien yhteyksien hallintaan. Azure resurssit kommunikoivat turvallisesti keskenään erilaisilla tavoilla. Virtuaaliverkon kautta voi ottaa esimerkiksi virtuaalikoneita, Azure App Service-ympäristöt, Azure Kubernetes Servicen ja Azure Virtual Machine Scale Setsin. Virtuaaliverkkopalvelun päätepisteen kautta voidaan myös tämä asia hoitaa. Päätepisteiden avulla voi suojata kriittiset Azure-resurssit vain virtuaaliseen verkkoon. Käytännössä laajennetaan verkon yksityistä osoitetilaa ja virtuaaliverkon identiteettiä Azuren resursseja kohti suoralla yhteydellä. Viimeisenä vaihtoehtona on VNet-peering, joka yhdistää virtuaaliverkot toisiinsa, jolloin kummankin verkon resurssit voivat kommunikoida

keskenään. Yhdistetyt virtuaaliverkot voivat olla samoilla tai eri maantieteellisellä alueella. (Microsoft, 2021, -n)

Virtuaaliverkoissa suodatetaan verkkoliikennettä aliverkkojen välillä käyttämällä verkon suojausryhmiä, verkon virtuaalilaitteita tai molempia. Verkon ja sovellusten suojausryhmät voivat sisältää monia saapuvia ja lähteviä suojaussääntöjä. Näiden avulla voidaan suodattaa lähtevää ja tulevaa liikennettä resursseihin. Suodatus toimii lähteen ja kohteen IP-osoitteen, portin ja protokollan mukaan. Verkon virtuaalilaite on puolestaan virtuaalikone, joka suorittaa verkkotoiminnon kuten palomuurin, WAN-optimoinnin tai muun verkkotoiminnon.

2.5 Kustannukset ja laskelmat

Kustannuslaskelmat on tehty perustuen Microsoftin hinnoittelulaskimen antamiin tuloksiin. Ensimmäiset lasketut resurssit ovat virtuaalikoneet Pohjois-Euroopan ja Länsi-Euroopan alueilla. Hinnat vaihtelevat tarjousten, alueen, käyttöjärjestelmän, määrän ja koon mukaan. Virtuaalikoneiden esiintymäsarjat kuuluvat Bs-sarjaan. Koneissa on yksi kappale B1ls virtuaaliprosessoreita, joissa on 1GB keskusmuisti ja 4GB väliaikaista muistia, joka on hinnaltaan 0,006 €/tunti. Käyttöjärjestelmänä on Linux hinnaltaan 8,48 €/kk. Maksutapa on Pay-as-you-go, eli resursseista maksetaan oman käytön mukaan ja niiden poistaminen lopettaa maksettavan summan kertymisen. Hallitut levyt ovat standard SSD luokkaa ja levykoko E1 4GiB hinnaltaan 0,300 €/kk. Yksi levy on yhdessä virtuaalikoneessa ja yhden kappaleen hinta on 0,30 €/kk eli lopuksi 1,20 €/kk. Tallennustapahtumat 0,20 €. Länsi-Euroopan kahden virtuaalikoneen kuukausittainen maksu on 9,73 €/kk ja Pohjois-Euroopan on 9,28 €/kk.

Virtuaalinen verkko Azuressa on ilmainen. Yhdellä tilillä voi tehdä 50 virtuaalista verkkoa kaikkien alueiden välillä. Kuitenkin lähtevä tiedonsiirto ja saapuva tiedonsiirto nopeudella 100GB kerrottuna 0,0350 € on loppuhinnaltaan 3,50 €/kk. Summaksi tulee kahdesta tiedonsiirrosta 7 €/kk. Toinen virtuaalinen verkko on samanhintainen eli loppujen lopuksi 14 €/kk.

Basic-tyypin kuormantasaaja on työssä ollut käytössä ja se on ilmainen toisin kuin Standard-tyypin kuormantasaaja. Sovellusyhdyskäytävän hinta muodostuu tyyppiin, alueen, esiintymien ja tuntimäärien perusteella. Lisäksi siihen vaikuttaa tiedonsiirto ja ulkoinen tiedonsiirto. Yksittäinen Standard V2 sovellusyhdyskäytävä sekä esiintymä ja tuntimäärä asetettuna 730 muodostaa hinnan 177,83 €/kk. Tiedonsiirto sisäisenä ja ulkoisena tiedonsiirtona 5GB on yhteensä 0,0 €/kk. Loppusummaksi tulee 177,83 €/kk kummallekin Euroopan alueelle.

Liikenteenvalvojat ovat samanhintaisia kummallakin Euroopan alueella. DNS-kyselyitä miljoona kappaletta kuukaudessa on 0,54 €. Tilan kunnon tarkastus on hinnaltaan 0,36 € ja yksi kappaletta jokaiselle palvelimelle tekee yhteensä 1,44 €/kk. Lisäksi maksuja tuovat todellisen käyttäjän mittaukset, joita on kaksi kappaletta. Kappalehinnaltaan ne ovat 2 € ja yhteensä 4 €/kk. Liikenteen näkymiä on myös kaksi, jotka maksavat saman verran kuin edellä olevat mittaukset eli 4 €/kk. Nämä muodostavat yhteensä 9,98 €/kk. Resurssiryhmät ovat ilmaisia ilman lisäosia ja työssä on käytetty ilman lisäosia. Lopuksi kaikki yhteen laskettuna kokonaissummaksi saatiin 220,82 €/kk.

3 Kuormantasaus

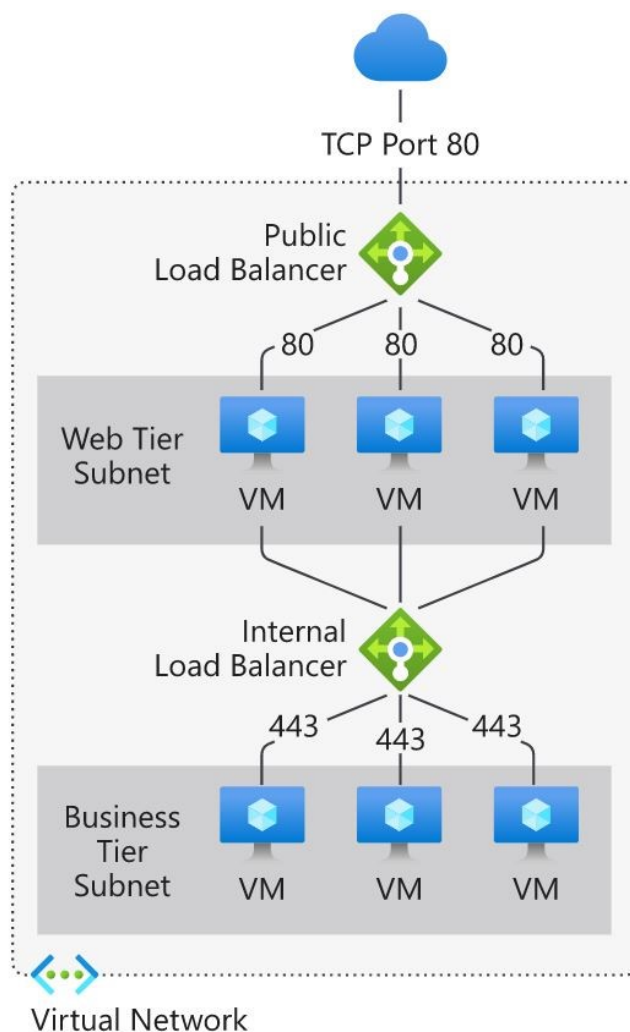
3.1 Azure kuormantasaaja

Kuormantasauksella tarkoitetaan saapuvan verkkoliikenteen jakamista tasaisesti palvelinryhmille tai taustajärjestelmän resurssien kesken. Azuren kuormantasaaja toimii Open Systems Interconnection (OSI) mallin kerroksessa 4. Tämä on käyttäjien yksittäinen yhteyspiste. Kuormantasaaja jakaa saapuvan liikenteen virtaukset, jotka saapuvat kuormantasaajan etujärjestelmän esiintymiin ja taustajärjestelmän esiintymiin (Kuva 5). Nämä virtaukset toimivat sen mukaisesti, mitä on asetettu kuormantasaajan säännöissä ja terveystantureiden tilojen mukaan. Taustajärjestelmän pooli esiintymät voivat olla virtuaalikoneita tai virtuaalikoneen mittakaavassa asetettuja esiintymiä.

Julkinen kuormantasaaja voi tarjota lähteviä yhteyksiä virtuaalikoneille, jotka ovat virtuaaliverkossa. Nämä yhteydet saadaan kääntämällä yksityiset IP-osoitteet julkisiksi IP-osoitteiksi. Julkisia kuormantasaajia käytetään tasaamaan internetistä tulevaa liikennettä virtuaalikoneisiin.

Yksityinen kuormantasaaja on käytössä silloin, kun yksityisiä IP-osoitteita tarvitaan vain etujärjestelmässä. Näitä käytetään tasaamaan liikennettä virtuaalisen verkon sisällä. Kuormantasaajan etujärjestelmään voidaan päästä paikallisverkosta hybridiskenaariossa. (Microsoft, 2021, -a)

Kuva 5. Julkinen ja sisäinen kuormantasaaminen. (Microsoft, 2021, -a)



IP-osoitteen luonne määrittää luodun kuormantasaajan tyypin. Yksityisen IP-osoitteen valinta luo sisäisen kuormantasaajan ja julkisen IP-osoitteen valitseminen luo julkisen kuormantasaajan. Julkinen kuormantasaaja kartoittaa reitin saapuvan julkisen IP-osoitteen ja portin virtuaalikoneen yksityiseen IP-osoitteeseen ja porttiin. Kuormantasaaja kartoittaa reitin päinvastaisella tavalla, kun virtuaalikoneesta lähtee liikennettä. Tietyn tyyppistä liikennettä voidaan jakaa useille virtuaalikoneille ja palveluille säätämällä kuormantasaajan sääntöjä. On mahdollista esimerkiksi jakaa verkkopyyntöliikenne monelle verkkopalvelimelle. Sisäinen kuormantasaaja jakaa liikenteen virtuaalisen verkon sisällä oleville resursseille. Azure rajoittaa pääsyä etujärjestelmän IP-osoitteisiin, jotka on jo jaettu kohteisiin kuormantasauksen avulla. Etujärjestelmän IP-osoitteet ja virtuaaliset verkot eivät ole koskaan suoraan avoimia päätepisteelle, joka on internet yhteydessä. Sisäiset yrityksen sovellukset toimivat Azuren kautta ja niihin päästään käsiksi vain Azuresta tai paikallisista resursseista.

Kuormantasaaja uudelleen konfiguroi itsensä uudelleen heti kun skaalataan esiintymien määrää isommaksi tai pienemmäksi. Virtuaalikoneiden lisääminen tai poistaminen taustajärjestelmän poolista uudelleen konfiguroi kuormantasaajan ilman lisätoimenpiteitä. Taustajärjestelmän poolin suunnittelussa on syytä suunnitella pienimmälle määrälle sen yksittäisiä resursseja hallintatoimintojen määrän optimoimiseksi. Kuormantasaajaa tehdessä kannattaa tehdä sille terveysanturi, sillä se huomioi kuormantasaajan tilan ja täten huomaa onko se valmis vastaanottamaan liikennettä. Tila ja kynnys, jossa kuormantasaaja ei vastaanota liikennettä, on mahdollista itse räätälöidä. Yhteydet jatkuvat siihen asti, kunnes ohjelma päättää liikennevirtauksen, valmiustilan aikakatkaisu tapahtuu tai virtuaalikone sammuu. Kuormantasaajan sääntöjä käytetään määrittämään, kuinka saapuva liikenne jaetaan kaikille taustajärjestelmän poolissa oleville esiintymille tasaisesti. Käytännössä säännöt kartoittavat etujärjestelmän IP-konfiguraatiot ja portin useisiin taustajärjestelmän IP-osoitteisiin ja portteihin. (Microsoft, 2021, -e)

Azure kuormantasaaja tukee käytettävyyssalueiden skenaarioita. Standard Load Balancer -ohjelmaa voidaan käyttää käytettävyyden parantamiseen koko skenaariossa kohdentamalla resurssit ja jakelulla vyöhykkeiden välillä. Kuormantasaaja voi toimia joko vyöhykkeen redundanssina eli se karsii ylimääräisiä tai päällekkäisiä tietoja, vain vyöhykkeellisenä tai ei-

vyöhykkeellisenä kuormantasaajana. Voidaksesi määrittää vyöhykkeeseen liittyvät ominaisuudet kuormantasaajalle, tulee valita sille sopiva käyttöliittymän tyyppi.

Saatavuusvyöhyke-alueella tavallinen kuormantasaaja voi olla vyöhyke redundanssissa. Tätä liikennettä palvelee yksi IP-osoite. Yksi etujärjestelmän IP-osoite selviää vyöhykevirheestä. Etujärjestelmän IP-osoitetta voidaan käyttää saavuttamaan taustajärjestelmän poolin jäseniä vyöhykkeestä riippumatta. Yksi tai useampi saatavuusvyöhyke voi epäonnistua ja dataliikenteen reitti säilyy niin kauan, kun yhden vyöhykkeen tila alueella pysyy terveenä. Etujärjestelmän IP-osoitetta palvelee samanaikaisesti useilla itsenäisillä infrastruktuurin käyttöönotoilla useilla saatavuusalueilla. Uudelleenasetukset tai uudelleenyritykset toimivat muilla alueilla, joihin vyöhykevika ei vaikuta.

On mahdollista valita etujärjestelmä, joka taataan yhdelle vyöhykkeelle. Se tunnetaan nimellä ”Zonal”, eli vyöhykkeellinen. Tämä skenaario tarkoittaa, että mitä tahansa saapuvaa tai lähtevää virtausta palvelee yksi vyöhyke alueella. Etujärjestelmä jakaa kohtalonsa vyöhykkeen terveydentilan kanssa. Datapolkuun ei vaikuta viat muilla vyöhykkeillä kuin missä se on taattu. Vyöhykkeellisiä etujärjestelmiä voidaan käyttää paljastamaan IP-osoite yhtä käytettävyyssaluetta kohti. Lisäksi tuetaan alueellisten etujärjestelmien suoraa käyttöä kunkin vyöhykkeen päätepisteille, joiden kuormitus on tasattu. Tätä määritelmää voi käyttää paljastaakseen vyöhykekohtaisesti tasapainotetut päätepisteet. Sen ansiosta valvonta kutakin vyöhykettä kohtaan erikseen onnistuu. Julkisia päätepisteitä voi integroida DNS kuormantasaajan kanssa, esimerkiksi Traffic Managerin kanssa ja siten käyttää yhtä ainutta DNS-nimeä.

Julkisen kuormantasaajan etujärjestelmässä lisätään vyöhykkeen parametri julkiseen IP-osoitteeseen. Tähän julkiseen IP-osoitteeseen tässä tapauksessa viitataan etujärjestelmän IP-määritelmällä, jota käyttää sitä vastaava sääntö. Sisäisessä kuormantasaajan etujärjestelmässä sen sijaan vyöhykkeen parametri lisätään suoraan sen IP-määrittelyyn. Täten vyöhykkeen etujärjestelmä takaa IP-osoitteen tietyn vyöhykkeen aliverkkoon. (Microsoft, 2021, -i)

Kuormituksen tasaussääntöjä voidaan luoda niin, että se jakaa liikennettä etujärjestelmästä taustajärjestelmään oikealla halutulla tavalla. Azure kuormantasaaja käyttää hajautusalgoritmia saapuvien liikennevirtausten jakamiseen. Palvelimet ovat valmiita vastaanottamaan liikennettä, kun terveysanturi osoittaa, että päätepisteen tila on kunnossa.

Kuormantasaajan algoritmi käyttää oletusarvoisesti viiden monikko -hajautusta. Hajautus sisältää lähteen IP-osoitteen, lähdeportin, kohteen IP-osoitteen, kohdeportin ja IP-protokollanumeron kartoittamaan käytettävissä olevien palvelinten virtauksia. Taipumus lähde IP-osoitteeseen luodaan käyttämällä kahden tai kolmen monikon hajautusta. Saman virtauksen paketit saapuvat samalle esiintymälle tasatun etujärjestelmän taustalle. Lähdeportti muuttuu, kun käyttäjä aloittaa uuden liikennevirtauksen samasta lähde IP-osoitteesta. Tämän seurauksena viiden monikon hajautus saattaa aiheuttaa liikenteen siirtymisen eri taustajärjestelmän päätepisteeseen.

Kuormantasaaja ei ole suoraan vuorovaikutuksessa TCP:n, UDP:n tai sovelluserroksen kanssa. Kuormantasaaja ei sulje tai aloita virtauksia eikä ole vuorovaikutuksessa hyötykuorman virtauksen kanssa. Protokollan käsittely tapahtuu aina suoraan käyttäjän ja taustajärjestelmän pool-esiintymän välillä. Vastaus saapuvaan virtaukseen on aina vastaus virtuaalikoneelta. Kun liikennevirta saapuu virtuaalikoneelle, alkuperäisen lähteen IP-osoite säilyy. Jokaiseen päätetapahtumaan vastaa virtuaalikone, esimerkiksi TCP-käsittely tapahtuu käyttäjän ja valitun taustajärjestelmä virtuaalikoneen välillä. Vastaus etujärjestelmän pyyntöön on vastaus, jonka taustajärjestelmän virtuaalikone on luonut. Kun vahvistetaan yhteyden liitos etujärjestelmään onnistuneesti, vahvistuu samalla yhteys taustajärjestelmän yhteen virtuaalikoneeseen. Koska kuormantasaaja ei ole vuorovaikutuksessa TCP-hyötykuorman kanssa eikä tarjoa TLS-purkua, voidaan rakentaa salattuja skenaarioita. Kuormantasaajan käyttö antaa suuren laajennuksen TLS-sovelluksille lopettamalla TLS-yhteyden itse virtuaalikoneelta. Esimerkiksi TLS-istunnon avainkapasiteettia rajoittaa vain taustajärjestelmän poolin virtuaalikoneiden tyyppi ja määrä. (Microsoft, 2021, -d)

3.2 Liikenteen valvonta

Azuressa liikenteen valvontaa ja kontrollointia hallitaan Traffic Managerilla. Traffic Manager on DNS-pohjainen liikenteen kuormituksen tasaaja, jonka avulla voidaan jakaa liikennettä julkisiin sovelluksiin globaaleilla Azure-alueilla. Se on joustava vikojen sattuessa, mukaan lukien, jos koko Azure-alueessa sattuu vika. Käytössä on DNS sitä varten, että sillä ohjataan käyttäjäpyynnöt asianmukaiselle pääte pisteelle liikenteen reititysmenetelmän perusteella. Liikenteen valvoja tarkkailee myös jokaisen pääte pisteen tilaa. Pääte pisteenä voi olla mikä tahansa internetiin päin oleva palvelu, jota isännöidään Azuren sisällä tai sen ulkopuolella. Traffic Manager sisältää useita erilaisia liikennereititysmenetelmiä, joiden avulla voidaan hallita, kuinka Traffic Manager valitsee minkä pääte pisteen tulisi vastaanottaa liikennettä kultakin loppukäyttäjältä. (Microsoft, 2021, -o)

Kun käyttäjä haluaa muodostaa yhteyden palveluun, sen on ensin selvitettävä DNS-nimi IP-osoitteeksi. Tällä tavoin käyttäjä yhdistää kyseiseen IP-osoitteeseen päästäkseen palveluihin käsiksi. Yksi tärkeimmistä huomioista on se, että liikenteen valvonta toimii DNS-tasolla, joka on Azuressa sovelluskerroksessa 7 (Layer-7). Käyttäjät muodostavat yhteyden valittuun pääte pisteeseen suoraan. Traffic Manager ei siis ole välityspalvelin tai yhdyskäytävä, eikä se näe liikennettä kulkemassa käyttäjän ja palvelun välillä.

Kuinka käyttäjät todellisuudessa yhdistävät Traffic Managerin avulla? Käyttäjä lähettää DNS-kyselyn konfiguroidulle rekursiiviselle DNS-palvelulle selvittääkseen sen verkkotunnuksen nimen. Rekursiivinen DNS-palvelu ei isännöi DNS-verkkotunnuksia suoraan. Käyttäjä purkaa työn ottamalla yhteyttä eri arvovaltaisiin DNS-palveluihin internetissä, joita tarvitaan DNS-nimen ratkaisemiseen.

DNS-nimen selvittämiseksi rekursiivinen DNS-palvelu löytää palvelimet oikealle verkkotunnukselle. Tämän jälkeen se ottaa yhteyden palvelimiin kysyäkseen DNS-tietueen. Seuraavaksi rekursiivinen DNS-palvelu etsii palvelinten nimet, jotka Traffic Manager tarjoaa. Sitten se lähettää pyynnön DNS-tietueelta DNS-palvelimille. Traffic Managerin palvelimet vastaanottavat pyynnot ja ne valitsevat pääte pisteet tietyin perustein. Perusteita valinnalle on kunkin pääte pisteen määritetty tila, pääte pisteen tila, joka on määritetty Traffic

Managerin tilatarkastuksien avulla ja liikenteen reititysmenetelmän perusteella valitseminen. Valittu pääte piste palautetaan DNS CNAME -tietueena. CNAME osoittaa tiettyyn domainiin, johon on tarkoitus muodostaa yhteys. Rekursiivinen DNS-palvelu löytää palvelimet cloudapp.net-toimialueella. Palautuksena tulee DNS "A" -tietue, joka sisältää EU-pohjaisen palvelun pääte pisteen IP-osoitteen. Rekursiivinen DNS yhdistää tulokset ja palauttaa yhden DNS-vastauksen käyttäjälle. Käyttäjä vastaanottaa DNS-tulokset ja muodostaa yhteyden IP-osoitteeseen. Yhteys muodostuu suoraan eikä Traffic Managerin kautta. Kyseessä on HTTPS-pääte piste, käyttäjä suorittaa tarvittavan SSL/TLS-käsittelyn ja tekee sitten HTTP GET-pyyynnön /login.aspx -sivulle.

Rekursiivinen DNS-palvelu tallentaa välimuistiin vastaanotetut vastaukset, mitkä ovat tulleet DNS-palvelimilta. DNS-resolver käyttäjän laitteessa tallentaa myös välimuistiin tulokset. Välimuistin avulla voidaan vastata nopeammin myöhempiin DNS-kyselyihin, joka helpottaa myös kuormitusta, koska se poimitaan välimuistista eikä suoraan nimipalvelimilta. Välimuistin kesto määräytyy kunkin DNS-tietueen "time-to-live" -ominaisuuden mukaan (TTL). Lyhyemmän haun arvot aiheuttavat nopeamman välimuistin vanhenemisen, mikä johtaa useampiin edestakaisin meneviin pyyntöihin Traffic Managerin nimipalvelimille. Pidemmän arvon hauissa liikenteen ohjaus epäonnistuneesta pääte pisteestä voi kestää kauemmin. (Microsoft, 2021, -h)

4 Sovellettu projekti

4.1 Käytetyt ratkaisut

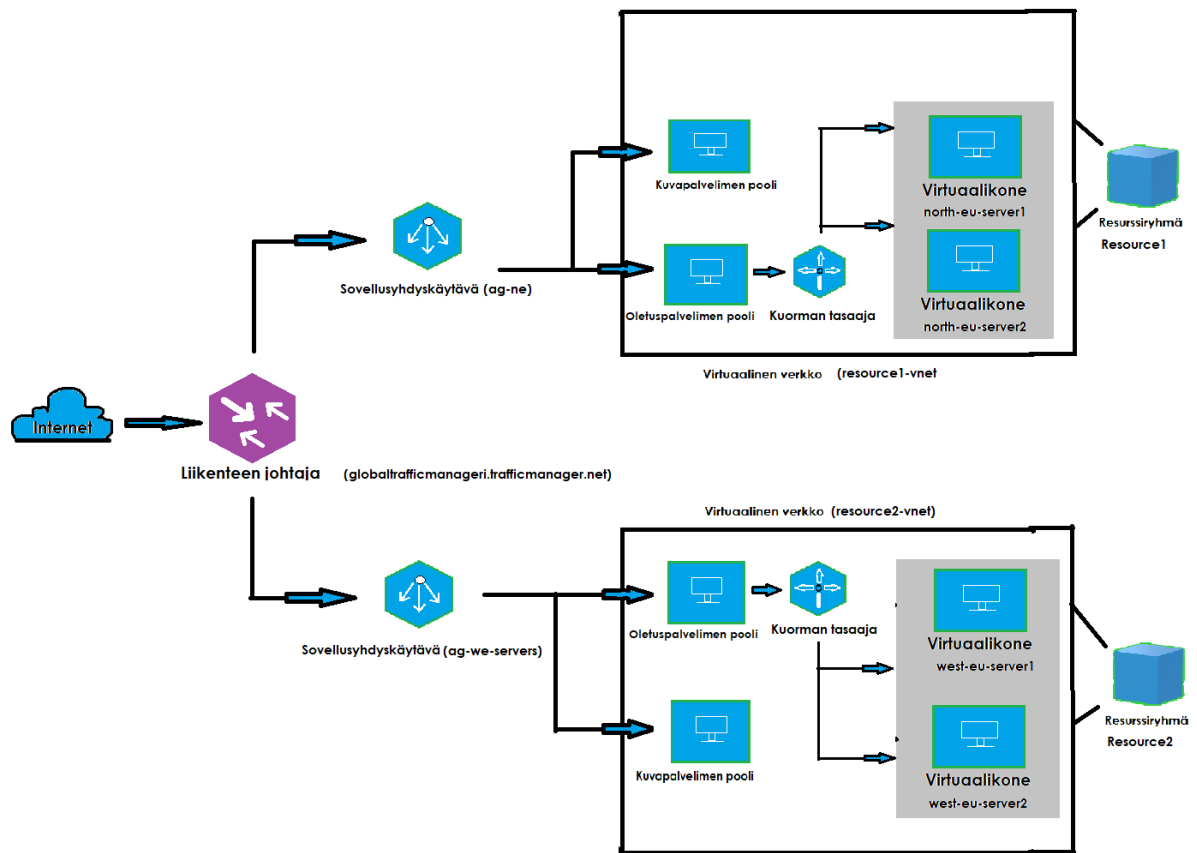
Sovelletun projektin osuus koostuu käytännön osuuden suunnittelusta, dokumentoinnin suunnittelusta ja kuormantasaamisen toteuttamisesta Microsoft Azure pilvipalveluita hyödyntäen. Kaikki työ on tehty omaan käyttöön ilman asiakaskohtaista tapausta tai työnantajan antamaa tehtävää. Tavoitteena oli saada toimintavalmiiksi kuormantasaus neljän palvelimen välille Azure-pilvipalveluiden teknologiaa käyttäen. Tässä osuudessa on

otettu huomioon kustannusten määrä, mikä on ollut tarkoituksena pitää mahdollisimman pienenä. Työstä saatua lopputulosta on mahdollista muokata ja soveltaa skaalaamalla sitä suuremmaksi tai pienemmäksi.

Microsoft Azure pitää sisällään kattavan määrän tuotteita. Suunnittelu helpottaa omalle kohdalle sopivien tuotteiden valitsemista, joita riittää erilaisten tarpeiden mukaan. Suunnittelulla voidaan myös helpottaa konfiguraatioiden tekemistä eri työvaiheissa tuotteiden kanssa sekä ongelmatilanteiden tullessa on helpompi löytää korvaavia vaihtoehtoja. Suunnittelutyö helpotti oman työn rakenteen perustamista halutulla tavalla (Kuva 6).

Virtuaalikoneet on valittu kustannustehokkuuden ja käytettävyyden perusteella. Työhön sopivin vaihtoehto oli Standard_B1ls -sarjaan kuuluva kone. Kyseessä on virtuaalikone, jolla on tasapainotettu suorittimen ja muistin suhde. Se sopii hyvin pieniin tietokantoihin sekä pienen verkkoliikenteen verkkopalvelimiin.

Kuva 6. Opinnäytetyössä tehty palvelin- ja verkkorakenne hahmotettuna.



4.2 Kustannukset

Työ koostuu erilaisista resursseista ja hinnat ovat tuotekohtaisia. Kustannuksia muodostui resurssien datankäytön mukaan kuukausihinnan lisäksi. Maksettavan summan kertyminen alkoi siitä hetkestä, kun resurssi oli liitetty tiliin. Työn kustannusten kertymisen osalta on syytä huomioida se, että Azuressa tehty työ on nopealla tahdilla hoidettu, jotta maksettava summa ei nousisi liian korkeaksi.

Kahdella virtuaalikoneella oli alueenaan Pohjois-Eurooppa ja toisella kaksikolla Länsi-Eurooppa. Näiden käyttöönoton jälkeen alkoi muodostumaan maksettavaa summaa alueen mukaan kaikista resursseista mitä niihin oli liitettyinä. Virtuaalikoneen luonnin yhteydessä se sai itselleen oman IP-osoitteen, joka oli ilmainen. Virtuaalikoneesta maksu kertyi sen sarjan

resurssista. Virtuaalikoneet kuuluivat Bs-sarjaan, sillä niillä oli käytössä B1ls. Kyseisistä sarjoista Pohjois-Euroopan ja Länsi-Euroopan alueilla tuli yhteensä 0,15 € maksettavaa.

Virtuaaliverkko sai luonnin yhteydessä vakion staattisen julkisen IP-osoitteen hinnaltaan 0,1 € ja dynaamisen julkisen IP-osoitteen, jonka käytöstä muodostui 0,15 €. Virtuaaliverkot tulivat sillä hetkellä omiin resursseihin, kun palvelimet ja resurssiryhmät luotiin.

Virtuaaliverkkojen ominaisuuksia voi räätälöidä. Näitä ei tarvitse pitää oletusasetuksilla ja niiden asetuksia on hyvä määrittää jo aikaisessa vaiheessa.

Tallennustilan käyttämisestä muodostui Standard SSD tyyppin ja E4-sarjan levyjä käyttäen 0,1 € maksettavaa. Premium SSD P4-levyjen käyttö Länsi-Euroopassa oli hinnaltaan 0,4 € ja Pohjois-Euroopassa 0,2 €.

Standard V2 tason sovellusyhdykäytävä Pohjois-Euroopan alueella kiinteältä hinnaltaan oli 2,52 € ja kapasiteetin käytöstä koitui 1,45 € maksettavaa. Länsi-Euroopan kiinteä kustannus 2,83 € ja kapasiteetin käyttö 1,91 €. Nämä resurssit kasasivat eniten kustannuksia, sillä ne ovat avainasemassa tämäntyyppisissä rakenteissa. Loppusumma veroineen kaikkien käytettyjen resurssien kanssa oli 9,81 € noin neljän tunnin käytöstä.

4.3 Virtuaalikoneiden konfiguraatio

Jotta on mahdollista luoda virtuaalikoneita Microsoft Azuressa, on kirjauduttava ensin sisään Azure Portalissa. Palvelimia voidaan luoda erilaisia, esimerkiksi Windows-palvelin tai Linux-palvelin. Tässä työssä valitsin Linux-palvelimen, sillä sen käyttö oli jo ennestään tuttu.

Virtuaalikoneelle tulee valita tietyt ominaisuudet sen konfiguraatiota tehdessä.







Ensimmäisenä valitaan maksutapa, mikä tässä työssä oli Pay-as-go. Pay-as-go tarkoittaa sitä, että kuukausittaisen maksun summa kertyy vain oman käytön ja omistamiensa palveluiden mukaan. Sijoitetaan virtuaalikone tiettyyn resurssiryhmään tai luodaan uusi resurssiryhmä virtuaalikonetta varten. Tämä voidaan nimetä oman mielen mukaan. Resurssiryhmä pitää sisällään Azure ratkaisuun liittyviä resursseja. Nimetään virtuaalikone. Työssäni olen virtuaalikoneet nimennyt niiden sijainnin mukaan. Ensimmäiset kaksi ovat nimeltään: north-eu-server1 ja north-eu-server2, toiset kaksi ovat west-eu-server1 ja west-eu-server2. Koneita

luodessa valitaan myös laitteelle alue, kahdelle koneelle on määritetty alueeksi Pohjois-Eurooppa ja toiselle kahdelle Länsi-Eurooppa. Käyttöjärjestelmän valitsemisessa on monta eri vaihtoehtoa. Tässä tapauksessa Ubuntu-server 18.04 LTS on Linux-palvelin, jonka valitsin omalle työlle. Virtuaalikoneen koko on syytä olla mietittynä jo etukäteen, sillä niiden ominaisuudet ja kustannusmäärät ovat huomattavasti erilaiset. Kuten aikaisemmin on mainittu, virtuaalikoneiksi on valittu Standard_B1ls -sarjan kone. Tämä virtuaalikone kuuluu siis B-sarjaan ja sarjoja on yhteensä kahdeksan erilaista.

Ominaisuuksiltaan Standard_B1ls on 0.5GiB muistiltaan, välimuisti 4GiB, yksi virtuaalinen prosessori, virtuaalikoneen prosessorin perussuorituskyky 5 %, virtuaalikoneen korkein suorituskyky 100 %, datalevyjä maksimissaan kaksi, välimuistin ja väliaikaisen tallennustilan enimmäiskapasiteetti IOPS/MBps: 200/10, välimuistissa olevan levyn enimmäiskapasiteetti IOPS/MBps: 160/10 ja maksimi verkkokorttien määrä on kaksi. (Microsoft, 2020, -f)

Virtuaalikoneen valitsemisen jälkeen täytyy valita tunnistautumistapa. Valitaan joko SSH julkinen avain tai salasana. Tässä työssä valitsin käyttäjänimen ja salasanan. Tämän lisäksi avataan portti palomuurista. Kun halutaan yhdistää Linux-koneeseen, siihen käytetään SSH protokollaa. SSH protokolla toimii periaatteessa aina portista 22, joten se avataan palomuurista. Valitaan virtuaalikoneelle levyn tyyppi Standard SSD, joka vaikuttaa sen suorituskykyyn. Verkon käyttöliittymä luodaan automaattisesti virtuaalikonetta tehdessä. Se luo automaattisesti oletusarvoisen virtuaaliverkon, aliverkon ja julkisen IP-osoitteen palvelimelle. Valvonnan ja diagnostiikan konfiguroinnissa kytkin valvonnat pois päältä, mukaan lukien käynnistysdiagnostiikan, joka on oletuksena päällä. Näihin sisältyy siis käynnistysdiagnostiikka ja käyttöjärjestelmän vierasdiagnostiikka. Järjestelmälle määritetty hallittu identiteetti sekä Azure aktiivihakemistosta kirjautuminen AAD-tunnuksilla on kytketty pois. Lopuksi luodaan palvelin, jonka latautumisessa saattaa kestää useita minuutteja. Resurssiryhmä latautuu mukaan kokoonpanoon palvelinta ladattaessa, koska se määritettiin virtuaalikonetta tehdessä ja sen oikea nimi sekä paikka on hyvä varmistaa heti (Kuva 7). Resurssiryhmiin ja virtuaalikoneisiin generoitui automaattisesti omat virtuaaliverkot.

Kuva 7. Resource1-resurssiryhmän sisältö.

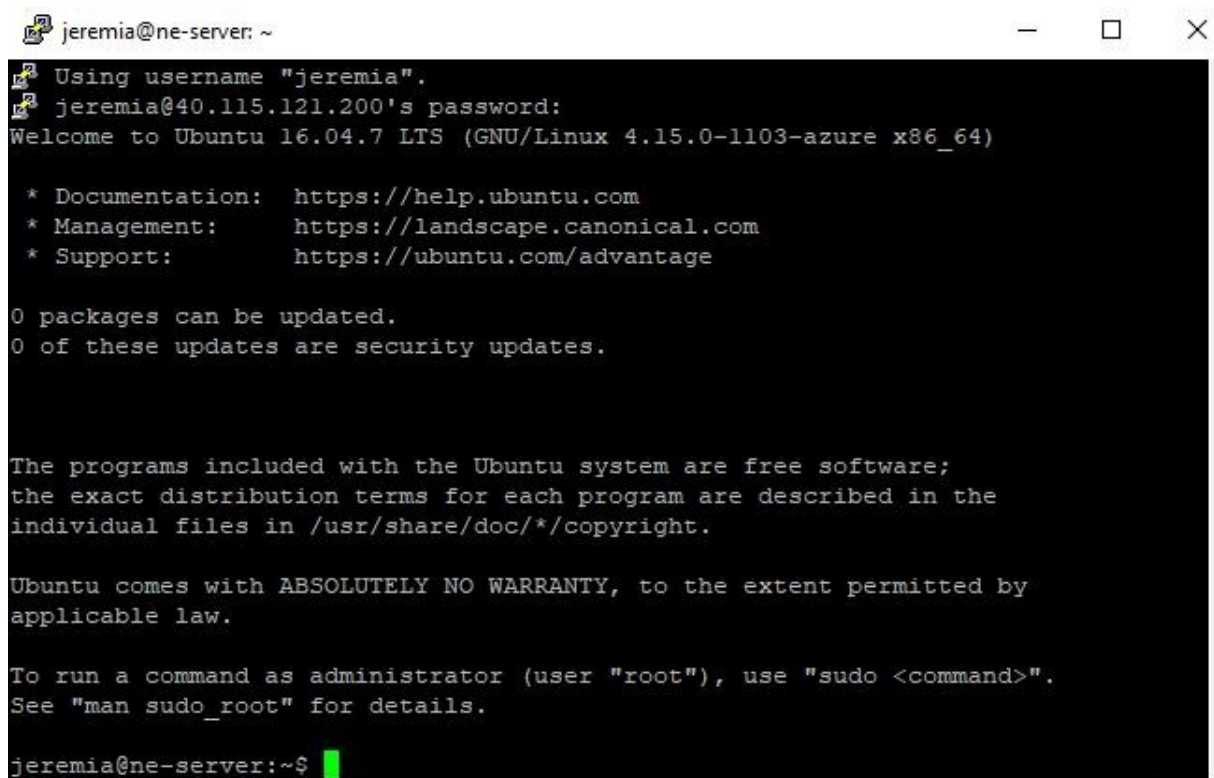
<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/>  north-eu-server1	Virtual machine	North Europe
<input type="checkbox"/>  north-eu-server1-ip	Public IP address	North Europe
<input type="checkbox"/>  north-eu-server1-nsg	Network security group	North Europe
<input type="checkbox"/>  north-eu-server1817	Network interface	North Europe
<input type="checkbox"/>  north-eu-server1_OsDisk_1_28aef66d5d204350b4f8596f2caacc6d	Disk	North Europe
<input type="checkbox"/>  Resource1-vnet	Virtual network	North Europe

Kyseisen ensimmäisen palvelimen nimeksi tuli north-eu-server1 ja tämän jälkeen luotiin samoilla asetuksilla north-eu-server2. Nämä ovat samassa resurssiryhmässä.

Uudet virtuaalikoneet nimeltään west-eu-server1 ja west-eu-server2 tehtiin Resource2 resurssiryhmän alle. Näiden alueeksi on asetettu Länsi-Eurooppa, mutta muuten ne ovat samoilla asetuksilla kuin aikaisemmat palvelimet.

Palvelinten määrittäminen oli sopiva työ aloittaa seuraavaksi. Ensimmäiseksi Pohjois-Euroopan resurssiryhmässä oli tarkoitus tarkastella ja määrittää palvelimet selvittämällä niiden IP-osoitteet, jotka löytyvät kyseisten virtuaalikoneiden käyttönäkymästä. IP-osoitteiden selvittämisen jälkeen oli aika käynnistää PuTTY-ohjelma. PuTTY pyytää syöttämään isäntänimen tai IP-osoitteen ja tässä tapauksessa annettiin virtuaalikoneen IP-osoite. PuTTY avautuessaan antaa näkymän, josta näkee käyttäjänimen sekä IP-osoitteen, jota käytetään sillä hetkellä (Kuva 8).

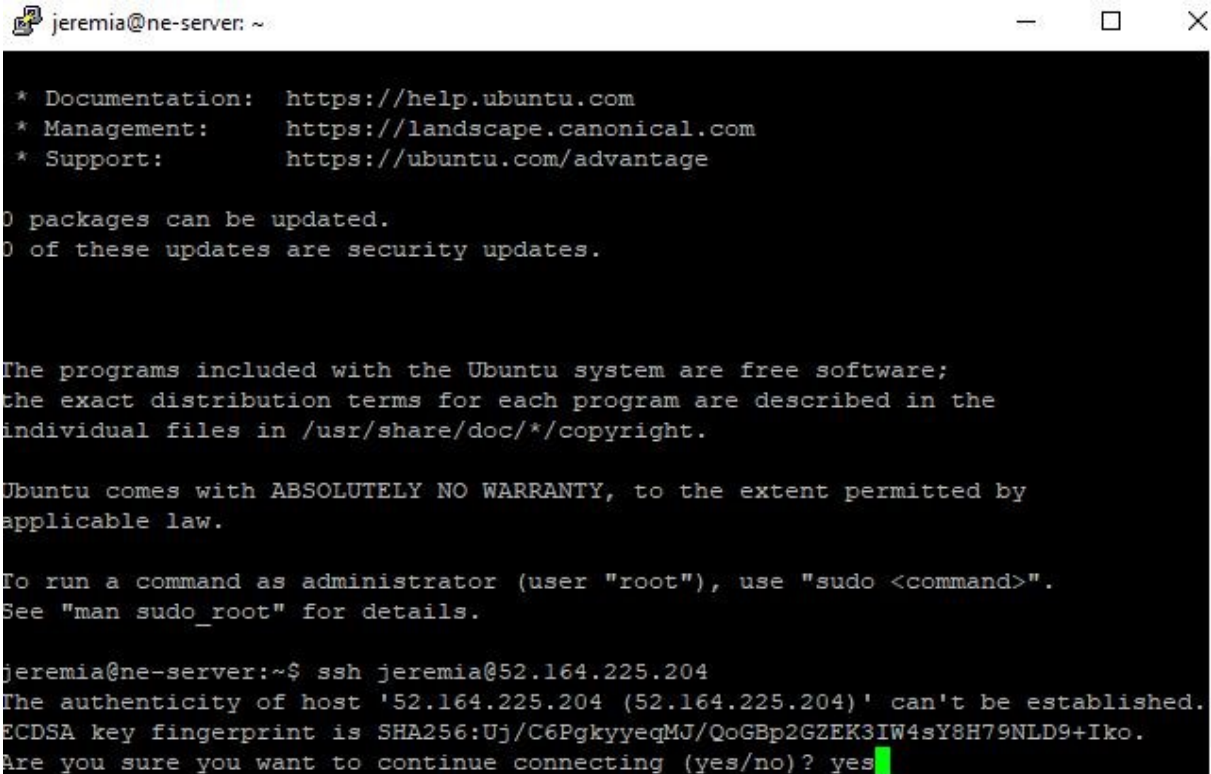
Kuva 8. PuTTY -ikkuna kirjautumisen jälkeen.



```
jeremia@ne-server: ~  
Using username "jeremia".  
jeremia@40.115.121.200's password:  
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-1103-azure x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
0 packages can be updated.  
0 of these updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
jeremia@ne-server:~$
```

Yllä olevan kuvan palvelin on Pohjois-Euroopan ykköspalvelin. Sen north-eu-server1 palvelinta vastaa 40.115.121.200 IP-osoite. PuTTY -ikkuna jätettiin auki, sillä avataan samanaikaisesti yhteys myös kolmeen muuhun palvelimeen. Toinen yhdistettävä palvelin on north-eu-server2, jota vastaa 52.164.225.204 IP-osoite. Yhdistämiseen ja porttiin pääsyyn käytetään SSH-protokollaa (Kuva 9). Komennon jälkeen se kysyy salasanaa, joka määritettiin jo palvelinta tehdessä Microsoft Azuressa.

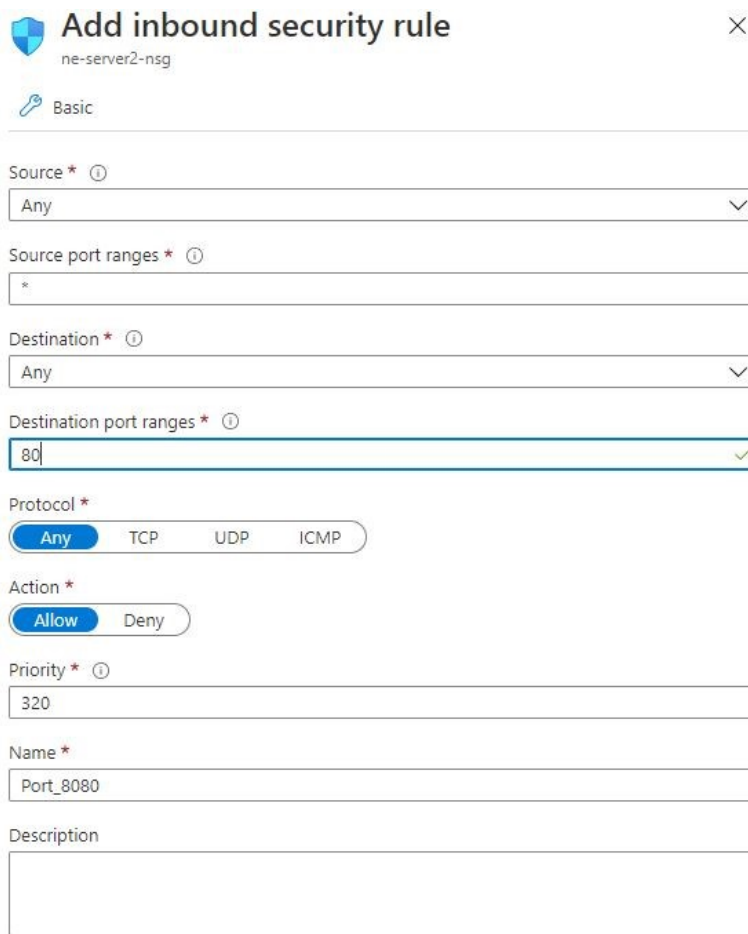
Kuva 9. Kirjautuminen SSH:n avulla toiselle palvelimelle.



```
jeremia@ne-server: ~  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
0 packages can be updated.  
0 of these updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
jeremia@ne-server:~$ ssh jeremia@52.164.225.204  
The authenticity of host '52.164.225.204 (52.164.225.204)' can't be established.  
ECDSA key fingerprint is SHA256:Uj/C6PgkyyeqMJ/QoGBp2GZEK3IW4sY8H79NLD9+Iko.  
Are you sure you want to continue connecting (yes/no)? yes
```


Kyseisille palvelimille ladattiin web-palvelinohjelmisto Apache2. Ennen lataamista varmistettiin, että ohjelmiston uusin versio on saatavilla ja ladattavissa. Apache2 tulee olemaan jokaisella palvelimella toimiakseen oikein. Kun annetaan palvelimen IP-osoite selaimeen, sen kuuluisi tällöin yhdistää ja avata sille kohdistettu sivu. Yhdistäminen ei kuitenkaan onnistu, sillä palomuuria ei ole avattu http-protokollaan. Azuren määrittelyssä oli asetettu portiksi 22, mutta oletuksena selain etsii aina porttia 80. Ongelman korjaamiseksi palvelimen verkottuminen-välilehdellä navigoidaan kohtaan, jossa voidaan lisätä saapuvan liikenteen sääntö (Kuva 10).

Kuva 10. Sisään tulevan liikennesäännön lisääminen.



Add inbound security rule ✕

ne-server2-nsg

 Basic

Source * ⓘ
Any

Source port ranges * ⓘ
*

Destination * ⓘ
Any

Destination port ranges * ⓘ
80

Protocol *
Any TCP UDP ICMP

Action *
Allow Deny

Priority * ⓘ
320

Name *
Port_8080

Description

Porttien kohdealueena oli oletuksena 8080, joka muutettiin vastaamaan portteja 80. Tämä lisätään sääntöihin ja se antaa palomuurilta luvan 80 portille, kun sitä pyydetään tältä palvelimelta. Sääntö tehtiin jokaiselle palvelimelle. Selaimen päivittyessä saadaan näkyviin Apache2 -sivu auki, mikä tarkoittaa yhdistämisen onnistumista porttiin. Jotta sai paremmin selkoa mille palvelimelle on yhdistetty, tuli Apache2 -sivu poistaa ja tehdä omia muutoksia sen tilalle. PuTTY:ssä navigoitiin Apache2 -sivun sisältävään kansioon, jossa sivua sisältävä tiedosto ensin poistettiin ja luotiin uusi tilalle. Yhdistetty sivu sai uuden näkymän omien muokkauksien ja sivun päivityksen jälkeen (Kuva 11).

Kuva 11. Uusi palvelimen sivunäkymä.



Jokainen palvelinkohtainen sivu avautui niin, että oli helposti huomattavissa mitä palvelinta ollaan tarkkailemassa.

4.4 Sovellusyhdykäytävä ja virtuaalinen verkko

Sovellusyhdykäytävä oli tarkoitus lisätä seuraavaksi työhön sen tarvittavien ominaisuuksien takia. Sovellusyhdykäytävä toimii palomuurin välityspalvelimena ja sitä voidaan käyttää verkkoliikenteen kuorman tasaamisessa. Konfiguroinnissa asetetaan nimi, alue ja oikea resurssiryhmä, johon kyseinen ratkaisu kohdistuu. Kun valitaan virtuaaliverkko, siihen tulee asettaa oikea aliverkko. Aliverkko päästään määrittämään navigoimalla omiin virtuaaliverkkoihin. Resource1-vnet on ensimmäisen puoliskon virtuaaliverkko. Virtuaaliverkon "aliverkot" välilehdeltä saa mahdollisuuden luoda uuden. Aliverkon asetuksia tarkastellessa oli ilmoitus siitä, että oma aliverkkoni ei sisältynyt virtuaaliverkon osoitetilaan. Tätä piti käydä muuttamassa osoitetilan hallinnasta. Osoitetilan muutoksen jälkeen palattiin takaisin aliverkko välilehdelle. Aliverkolle annettiin nimeksi ag-subnet ja osoitteeksi 10.0.5.0/24 (Kuva 12). Lisäämisen jälkeen menee hetki ennen kuin se latautuu palvelimelle ja voidaan palata takaisin sovellusyhdykäytävän pariin.

Kuva 12. Aliverkon lisääminen.

Add subnet ✕

Name *

ag-subnet ✓

Subnet address range * ⓘ

10.0.5.0/24 ✓

10.0.5.0 - 10.0.5.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space ⓘ

Sovellusyhdykäytävän konfiguroinnissa on Resource1-vnet virtuaaliverkko valittuna ja tämän aliverkoksi asetetaan äskettäin tehty aliverkko ag-subnet (10.0.5.0/24). Liikenne reitittyy sovellusyhdykäytävän etujärjestelmän IP-osoitteiden kautta taustajärjestelmän palvelimille. Sovellusyhdykäytävässä voidaan käyttää julkista, yksityistä tai kumpaakin, mutta tässä tapauksessa käytetään julkista. Tehtiin uusi julkinen IP-osoite ip-ag-eu-north, jonka jälkeen lisätään taustajärjestelmän pooli. Poolin nimeksi tuli eu-north-pool. Taustajärjestelmän pooliin pitää lisätä kohteen tyyppi ja kohde. Tyypiksi valitaan virtuaalikone ja kohteeksi tulee haluttu virtuaalikone. Tämä tehtiin Pohjois-Euroopan sekä Länsi-Euroopan sovellusyhdykäytäviin. Vain ne palvelimet, jotka ovat kyseisen sovellusyhdykäytävän virtuaaliverkossa voidaan valita. Yksittäisen virtuaaliverkon näkymästä voidaan tarkastella sääntöjen prioriteettinumeroita (Kuva 13). Prioriteettinúmero tarkoittaa etusijalle laittamista luvun mukaan, mitä pienempi numero on, sitä vahvemman vallan se ottaa. Jos yksi sääntö päästää liikenteen sisään, mutta toinen sääntö ei päästä ja tällä toisella on pienempi numero, liikenne ei pääse sisään.

Kuva 13. Verkon prioriteettisäännöt.

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group north-eu-server2-nsg (attached to network interface: north-eu-server2060)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action	
300	SSH	22	TCP	Any	Any	Allow	***
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	***
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	***
65500	DenyAllInBound	Any	Any	Any	Any	Deny	***

Sovellusyhdykäytävässä voidaan asettaa sääntöjä, jotka uudelleenohjaavat reitityksen ohjaamisen mukaan. Voidaan esimerkiksi ohjata liikenne tulemaan pelkästään north-eu-server1 palvelimelle. Verkon kuormantasaajassa ei reititetä polkupohjaisilla säännöillä. Sen sijaan verkon kuormantasaaja voi erottaa verkon yhteydet tai käyttäjäyhteydet perustuen verkkoon mistä yritetään yhdistää. Verkon kuormantasaaja uudelleenohjaa perustuen verkkoihin ja sovellusyhdykäytävän uudelleenohjaus perustuu käyttäjien polkuihin.

Taustajärjestelmän pooliin asetetaan vähintään yksi reitityssääntö. Reitityssääntö päästää lähettämään tietyn etujärjestelmän IP-osoitteen liikenteen suoraan taustajärjestelmän kohteeseen. Kohteita voi olla useita. Sääntö tarvitsee kuuntelijan ja vähintään yhden taustajärjestelmän kohteen. Asetetaan kuuntelijalle nimi, etujärjestelmän muoto, mikä on tässä tapauksessa julkinen, protokolla portti ja kuuntelijan tyyppi. Taustajärjestelmän kohteeksi annetaan eunorthbackend, jonka jälkeen lisätään vielä HTTP-asetus. Kyseiseen kuormantasaajaan ei asetettu polkusääntöä. Lopuksi luodaan sovellusyhdykäytävä. Sama tehdään Länsi-Euroopalle.

Sovellusyhdykäytävän yhteys pitää testata kopioimalla sen IP-osoite ja liittämällä selaimeen. Yhdistäminen ei aluksi onnistu, koska sovellusyhdykäytävän asetuksissa ei ole asetettu taustajärjestelmän poolin kohdetta erikseen. Kohteet määritettiin jo aikaisemmassa vaiheessa, mutta ne tuli vielä uudelleen varmistaa asetusten kautta. Virtuaalikoneet north-eu-server1 ja north-eu-server2 ovat kohteita sovellusyhdykäytävällä ag-ne. Kun kaikki asetukset saatiin valmiiksi, oli kokeiltava yhteyden toimivuutta uudelleen. Huomataan, että

samalla sovellusyhdykäytävän IP-osoitteella saadaan kaksi eri sivua. Kun sivun lataa tasaisin välein uudelleen, se ohjaa eri palvelimelle (Kuva 14 ja kuva 15).

Kuva 14. Pohjois-euroopan ykköspalvelin sovellusyhdykäytävän IP-osoitteella.



Kuva 15. Pohjois-euroopan kakkospalvelin sovellusyhdykäytävän IP-osoitteella.



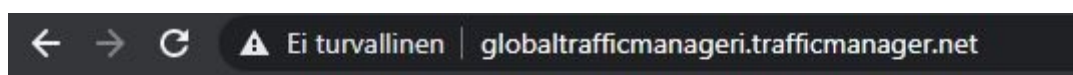
Sivuilla on sama sovellusyhdykäytävän IP-osoite. Reititys toimii kumpaankin palvelimeen satunnaisesti vastaamalla käyttäjän antamiin pyyntöihin.

4.5 Liikenteen valvonta

Työssä on tarkoitus mitata ja selvittää miten liikenne tasaantuu kuormantasauksen avulla. Liikenteen valvoja on hyvä työkalu antamaan erilaisia tuloksia halutuista mittauksista. Tehdään uusi liikenteen valvoja Azuressa antamalla sille nimi, reititystapa, maksutapa ja resurssiryhmä. Reititystapa on erittäin tärkeä asetus mikä vaikuttaa liikenteen valvojan toimivuuteen halutulla tavalla. Reititystavaksi annetaan maantieteellinen. Mistä ikinä pyyntö

tulee, pyyntö reitittyy palvelimille, jotka ovat maantieteellisesti lähellä sitä. Luodaan sovellusyhdykäytävä lopuksi. Liikenteen valvojalla ei ole aluksi määritettynä minkäänlaisia päätepisteitä, joten tarkoituksena on luoda kaksi päätepistettä. Päätepistettä tehdessä asetetaan julkiseksi IP-osoitteeksi sovellusyhdykäytävän IP. Tässä konfiguraatiossa tarvitaan DNS nimi. DNS nimi voidaan käydä tekemässä julkisten IP-osoitteiden hallinnasta. Navigoitiin halutulle sovellusyhdykäytävälle ja konfiguraatio välilehdeltä löytyi kenttä, johon pystyi asettamaan halutun DNS nimen. Päätepisteelle tehdään myös asetuksissa maantieteellinen kartoitus, joka jakaa liikenteen tietyn maantieteellisen sijainnin perusteella. Samaa sijaintia ei voi käyttää muissa päätepisteissä. Alueelliseksi ryhmittymäksi tuli asettaa Eurooppa ja maaksi Suomi. Käyttöönoton jälkeen selaimeen kopioitiin liikenteenvalvojan DNS nimi. Näin saadaan tarkistettua liikenteenvalvojan yhteyden toimivuus omien palvelimien kanssa (Kuva 16).

Kuva 16. Liikenteenvalvoja yhteydessä palvelimeen.



Welcome to north eu server2

Päivittäessä sivua hypittiin ensimmäisen ja toisen palvelimen välillä, mikä oli tarkoitus. DNS-alueet välilehdellä voidaan asettaa sääntö tai mukautettu oma URL-osoite, jolla voidaan yhdistää liikenteenvalvojaan.

Kun haluttiin tehdä oma verkkotunnus mukautettua URL varten, siihen löytyi hyvä ratkaisu freenom.com verkkosivulta. Freenom antaa mahdollisuuden ilmaiselle verkkotunnukselle. Freenomin ilmainen verkkotunnus edellyttää sivulle kirjautumista omilla tunnuksilla. Sivulle syötettiin haluttu verkkotunnuksen nimi ja sivu antoi vaihtoehtoiset nimet mistä valita. Ensimmäiseksi oli kuitenkin tehtävä uusi DNS-alue, johon asetetaan nimi ja oikea resurssiryhmä. Tähän tulee laittaa oman verkkotunnuksen nimi ja työssä se sai nimeksi

azure-projekti.tk. Luomisen jälkeen neljä nimipalvelinta ilmestyy uuden DNS-alueen alle, joita määritetään oman verkkosivun tai verkkotunnuksen kanssa (Kuva 17). Verkkotunnus yhdistetään DNS-alueeseen ja tätä kautta DNS-alue yhdistää omaan liikenteenvalvojaan.

Kuva 17. DNS-alueen alla olevat nimipalvelimet.

@.azure-projekti.tk

Save Discard Delete Users Metadata

Copy to clipboard

@.azure-projekti.tk

Type

NS

TTL * 2 TTL unit Days

Name server 1 ns1-06.azure-dns.com.

Name server 2 ns2-06.azure-dns.net.

Name server 3 ns3-06.azure-dns.org.

Name server 4 ns4-06.azure-dns.info.

Additional name servers

ns.contoso.com

Freenom -verkkosivulla määritetään omaan verkkotunnukseen nimipalvelimet hallintatyökaluista. Kaikki neljä nimipalvelinta tulee määrittää näissä asetuksissa, jotta oma verkkosivu voi saada yhteyden DNS-alueeseen. DNS-alue tulee osoittaa liikenteenvalvojaan määrittämisen jälkeen mikä voidaan tehdä lisäämällä tietuejoukko. Tietueen tyyppiä tuli CNAME. Tämä tarkoittaa sitä, että se yhdistää tietyn verkkotunnuksen ensisijaiseen verkkotunnukseen. Tällöin ensisijainen verkkotunnus on Azure-isännöity azure-projekti.tk verkkotunnus. CNAME-tyyppi ratkaisee palvelun IP-osoitteen automaattisesti, joten jos IP-

osoite muuttuu, niin ei tarvitse itse tehdä mitään. Azure resurssiksi valitaan globaltrafficmanageri mikä on liikenteenvalvojan nimi. Nyt voitiin tarkastella sovellusyhdykäytävän hallinnasta taustajärjestelmien tiloja. Palvelimien tila näytti hyvältä ja määritykset olivat oikein. Liikenteenvalvoja reitittyi selaimessa Pohjois-Euroopan palvelimien välillä. Yhdistäminen azure-projekti.tk sivuun yhdisti myös Pohjois-Euroopan palvelimille. Tämä johtuu siitä, koska oman laitteen sijainti on Pohjois-Euroopan alueella. Laitteen ollessa esimerkiksi Belgiassa, se olisi yhdistänyt Länsi-Euroopan palvelimiin.

Liikenteenvalvojan ansiosta erilaisia mittaustuloksia saatiin graafisina esityksinä (Kuva 18). Valvontaa voitiin pitää haluamastaan resurssista. Tässä tapauksessa sovellusyhdykäytävän valvonta antoi tarpeeksi erilaisia mittauksia, joita halusi tarkastella. Yhteyksien toimivuuden pystyi päättämään erittäin toimivaksi kyseisten mittausten avulla. Menetetetyt datapaketit jäivät vähälle onnistuneiden määritysten ansiosta.

Kuva 18. Liikenteenvalvonta kohdistuen sovellusyhdykäytävään.



5 Johtopäätökset ja pohdinta

Ensikokemuksena Microsoft Azure vaikutti mielenkiintoiselta ja selkeältä, vaikka ominaisuuksia löytyi jokaisesta osa-alueesta kattavasti. Microsoftin monien vuosien työ näkyy laadussa ja se, että pieniin tärkeisiin asioihin on myös kiinnitetty huomiota. Tämä näkyy myös laajassa dokumentaatiossa mitä on tarjolla. Oma halukkuus oppia Microsoft -alueesta enemmän sai tekemään työn hyvin omiin tavoitteisiin perustuen.

Ensimmäinen kysymys, johon työllä pyrittiin vastaamaan koski työnkulkua kuormantasaamiseen pääsemiseksi ja siihen huomioitavia asioita. Työnkulku vaikuttaa koko rakenteeseen, kustannuksiin ja kokonaisuuden toimintaan, joten on välttämätöntä ymmärtää teoreettinen tausta parhaan tuloksen saamiseksi. Työnkulkuun sisältyi kustannuslaskelmat, virtuaalikoneet, sovellusyhdykät, virtuaaliset verkot, resurssiryhmät, liikenteen valvonta ja niiden luominen sekä konfigurointi. Rakennetta luodessa oli syytä edetä systemaattisesti, koska resursseja oli monia. Suuremmissa rakenteissa se on välttämätöntä niiden suurien resurssimäärien ja laskelmien takia.

Projektia pystyisi jatkokehittämään skaalaamalla sitä suuremmaksi. Voisi esimerkiksi lisätä enemmän palvelimia ja sen mukaan lisätä myös suojauksen tehokkuutta. Azuressa suojaus on räätälöitävissä omien halukkuuksien mukaan. Tietokantojen lisääminen edistäisi tietojenhakua ja säilömistä. Mahdollisuuksien mukaan voisi kokeilla, kuinka Windows SQL palvelimelta yhdistetään Linux SQL palvelimeen etäisesti.

Aluksi itselle oli ongelma löytää sopiva aihe, mistä työn tekisi. Aloitus oli omalla kohdalla ongelmallisin, mutta siitä päästessä alkoi työ etenemään hyvällä tahdilla. Tuloksiin olin tyytyväinen pienistä työn tekemisen tauoista huolimatta.

6 Lähdeluettelo

Citrix. (2021, -a). *What is a Virtual Machine and How Does it Work?*

<https://www.citrix.com/en-in/glossary/what-is-a-virtual-machine.html>

Citrix. (2021, -b). *What is virtualization?* <https://www.citrix.com/en-in/glossary/what-is-virtualization.html>

Microsoft. (25. 1 2021, -a). *What is Azure Load Balancer?* <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

Microsoft. (2021, -b). *Appendix B: Hyper-V Architecture and Feature Overview.*

<https://docs.microsoft.com/en-us/biztalk/technical-guides/appendix-b-hyper-v-architecture-and-feature-overview>

Microsoft. (2021, -c). *Application Gateway infrastructure configuration.*

<https://docs.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure>

Microsoft. (2021, -d). *Azure Load Balancer Algorithm.* <https://docs.microsoft.com/en-us/azure/load-balancer/concepts>

Microsoft. (2021, -e). *Azure Load Balancer Components.* <https://docs.microsoft.com/en-us/azure/load-balancer/components>

Microsoft. (2020, -f). *B-series burstable virtual machine sizes.*

<https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-b-series-burstable>

Microsoft. (2021, -g). *How an application gateway works.* <https://docs.microsoft.com/en-us/azure/application-gateway/how-application-gateway-works>

Microsoft. (2021, -h). *How Traffic Manager Works.* <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-how-it-works>

Microsoft. (2021, -i). *Load Balancer and Availability Zones.* <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-availability-zones>

Microsoft. (2021, -j). *Manage Azure Resource Manager resource groups by using the Azure portal.* <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal>

- Microsoft. (2021, -k). *Microsoft Azure Application Gateway front-end IP address configuration*. <https://docs.microsoft.com/en-us/azure/application-gateway/configuration-front-end-ip>
- Microsoft. (14. 10 2020, -l). *Overview of Azure Cloud Services (classic)* <https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-choose-me>
- Microsoft. (2021, -m). *What is Azure Resource Manager?* <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>
- Microsoft. (2021, -n). *What is Azure Virtual Network?* <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>
- Microsoft. (2021, -o). *What is Traffic Manager?* <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>
- Stalcup, K. (2. 4 2021). *How to Use Azure Resource Groups for Better VM Management*. <https://www.parkmycloud.com/blog/azure-resource-groups/>
- Techopedia. (2021). *Application Gateway* <https://www.techopedia.com/definition/4189/application-gateway>
- Vmware. (2020, -a). *Hypervisor*. <https://www.vmware.com/topics/glossary/content/hypervisor>
- Vmware. (2020, -b). *Virtual Networking*. <https://www.vmware.com/topics/glossary/content/virtual-networking>
- Webber-Cross, G. (16. 10 2014). *Learning Microsoft Azure*. Pack Publishing, Limited. N <https://ebookcentral-proquest-com.ezproxy.hamk.fi/lib/hamk-ebooks/reader.action?docID=1818072&query=>