LAMK
Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

PILVIPALVELUIDEN OPTIMAALINEN HALLINTA

LAHDEN AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan insinööri
Tietoliikenne
Syksy 2019
Antti Hutri

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Hutri, Antti	Opinnäytetyö, AMK	Syksy 2019
	Sivumäärä	
	38	

Työn nimi

Pilvipalveluiden optimaalinen hallinta

Tutkinto

Tieto- ja viestintätekniikan insinööri (AMK)

Tiivistelmä

Opinnäytetyön tavoitteena oli selvittää julkisen, yksityisen, yhteisö ja hybridi pilvipalvelun sekä IaaS-, PaaS- ja SaaS-palvelumallien hyötyjä ja eroja. Lisäksi opinnäytetyössä tutkitaan pilvipalveluiden hallintakäytäntöjä ja ratkaisuja eri kokoisille yrityksille.

Opinnäytetyössä selvitetään eri pilvipalveluiden tyyppien ja pilvipalveluiden palvelumallien mahdollisuuksia, riskejä ja mahdollisia ratkaisuja niihin. Pilvipalveluiden hallinnan optimoinnilla tarkoitetaan ympäristön ylläpidon automatisointia ja tehostamista, jotta pilvipalvelun hyödyt tulevat esille unohtamatta kuitenkaan pilvipalveluiden mahdollisia riskejä.

Opinnäytetyössä ohjeistetaan PaaS-ympäristön pystyttäminen infrastruktuuri koodina menetelmällä. Infrastruktuuri koodina tarjoaa mahdollisuuden ympäristöjen tehokkaaseen käyttöönottamiseen, antaen samalla mahdollisuuden versiohallintaan. Infrastruktuuri koodina on devopsin metodi ympäristön nopeaan ja tehokkaaseen käyttöönottoon, muokkaamiseen ja päivittämiseen.

Asiasanat

Pilvipalvelut, Microsoft Azure, Hallinta, Hallittavuus

Abstract

Author(s)	Type of publication	Published
Hutri, Antti	Bachelor's thesis	Autumn 2019
	Number of pages	
	38	

Title of publication

Optimal way of managing cloud services

Name of Degree

Information and Communications Technology Engineer

Abstract

The object of this Bachelor's thesis was to study differences between public, private, community, and hybrid clouds, and in IaaS, PaaS and SaaS service models. The thesis also examines cloud management options and solutions for companies of different sizes.

Opportunities and risks of all the models were studied while trying to offer solutions to manage the risks. Optimizing Cloud management means automation of resource deployment and enhancing the management in order that benefits of cloud computing are magnified while paying attention to possible risks.

The thesis contains instructions for the deployment deployment of the PaaS environment using the Infrastructure as Code method. Infrastructure as Code offers opportunities for enhanced resource deployment while conserving the chance for version control. Infrastructure as Code is used as a tool in devops for fast, reliable and efficient method to deploy, modify or update the environment.

Keywords

cloud management, cloud computing, Microsoft Azure

SISÄLLYS

LYHENNELUETTELO

AAD	Azure Active Directory, Azuressa pyörivä aktiivihakemisto
AAS	Azure Analys Service, Azuren automatisoitu tietokannan käsittely resurssi
AD	Active Directory, Aktiivihakemisto paikallisen ympäristön käyttäjille
ADF	Azure Data Factory, Azuren tietojenkäsittely resurssi
AWS	Amazon Web Services, Amazonin omistama pilvipalvelu
GCP	Google Cloud Platform, Googlen omistama pilvipalvelu
IaaS	Infrastructure as a Service, Infrastruktuuri palveluna
IaC	Infrastructure as Code, Infrastruktuuri koodina
NSG	Network Security Group, Azuren tarjoama palomuuri-ratkaisu
On-prem	Paikallinen palvelin- tai työasemaympäristö
PaaS	Platform as a Service, Alusta palveluna
RG	Resource Group, Resurssiryhmä
RBAC	Role-based access control, Roolipohjainen pääsynhallinta järjestelmä
SaaS	Software as a service, Sovellus palveluna
VNET	Virtual network, Virtuaalinen tietoverkko

1 JOHDANTO

Opinnäytetyön tavoitteena on selvittää optimaalisin tapa hallita pilvipalveluita eri ympäristöissä. Opinnäytetyön tarkoituksena on toteuttaa raportointiympäristö Lahden kaupungille Microsoft Azure-pilvipalveluympäristöön Alusta palveluna -ratkaisulla.

Pilvipalvelut ovat tärkeä osa tulevaisuuden palvelinympäristöjä, minkä takia pilvipalvelut ovat jo tällä hetkellä yrityksille tärkeitä toimintaympäristöjä. Eri palveluntarjoajien pilvipalveluissa on kuitenkin eroja resurssien ja toimintatapojen välillä. Yhteistä niille on kuitenkin se, että ne tarjoavat monipuolisia palveluita kaiken kokoisille yrityksille kilpailukykyiseen hintaan.

Opinnäytetyössä perehdytään pilvipalveluiden hallinnan yleisiin linjoihin, joiden avulla pilviympäristöistä saadaan mahdollisimman paljon hyötyä niin, että palveluita on tehokas käyttöönottaa ja ylläpitää tulevaisuudessa. Työn tavoitteena on luoda tehokas, toimintavarma raportointiympäristö Lahden kaupungille käyttäen PaaS-palveluita. Teoriaosan tavoitteena on selvittää optimaalisia tapoja hallita pilviympäristöjä riippumatta pilvipalveluympäristön koosta ja rakentaa raportointijärjestelmä PaaS-ympäristönä Microsoft Azure-pilvipalveluun.

2 PILVIPALVELUT

2.1 Pilvipalvelut yritysmaailmassa

Pilvipalvelut tuovat uusia mahdollisuuksia perinteisiin yritysten IT-ympäristöihin. Niiden etuna on infrastruktuurin tarjonta yhdeltä palveluntarjoajalta, joka huolehtii pilvialustan riittävästä kapasiteetista ja tarjoaa mahdollisuuden keskitettyyn ylläpitämiseen yhdestä hallintoportaalista. Palveluiden siirtäminen pilveen vähentää yrityksen tarvetta palveluiden ylläpitoon ja laskee mahdollisia infrastruktuurin ylläpidosta johtuvien käyttökatkojen määrää. Pilvipalveluiden olennaisia piirteitä on ”On Demand”-itsepalvelu eli käyttäjä voi pystyttää tarvittavat resurssit heti tarpeen vaatiessa, kyky muokata palveluita ja kapasiteettia etänä yhdestä hallintaliittymästä. Itsepalvelu portaali mahdollistaa pilvipalveluiden tarjoamien ominaisuuksien hyödyntämisen, joihin sisältyy ympäristön tehokas skaalautuvuus sekä pilvipalveluiden käytön monitorointi ja resurssien optimointi verkkoliikenteen, tallennuskapasiteetin ja laskentatehon mukaan. (Sunilkumar & Gopal 2014.)

Palveluntarjoajan vastuulle jää resurssien varaaminen asiakkaan tarpeiden varalle sekä alustan toimivuuden varmistaminen. Palveluiden suurimmat hyödyt ovat palveluiden skaalaus käyttötarpeiden mukaan, joten tarvetta maksaa ylimääräisestä käyttämättömästä palvelimesta ei ole. Kustannukset tulevat puhtaasti käytön mukaan. Palveluiden hallinta paranee, palvelujen kehitys ja julkaisu on tehokkaampaa, koska käyttäjien ei tarvitse huolehtia alustasta. (Sunilkumar & Gopal 2014)

2.2 Suurimmat julkiset pilvipalveluiden tarjoajat

Suurimmat julkisten pilvipalveluiden tarjoajat ovat Amazonin Amazon web services eli Amazon Web Services, Microsoftin Azure, Googlen Cloud Platform ja IBMn tarjoama IBM Cloud. Jokaisella pilvipalvelualustalla on omat etunsa, ja niiden toiminta on painottunut eri alueille. (Wperp 2019)

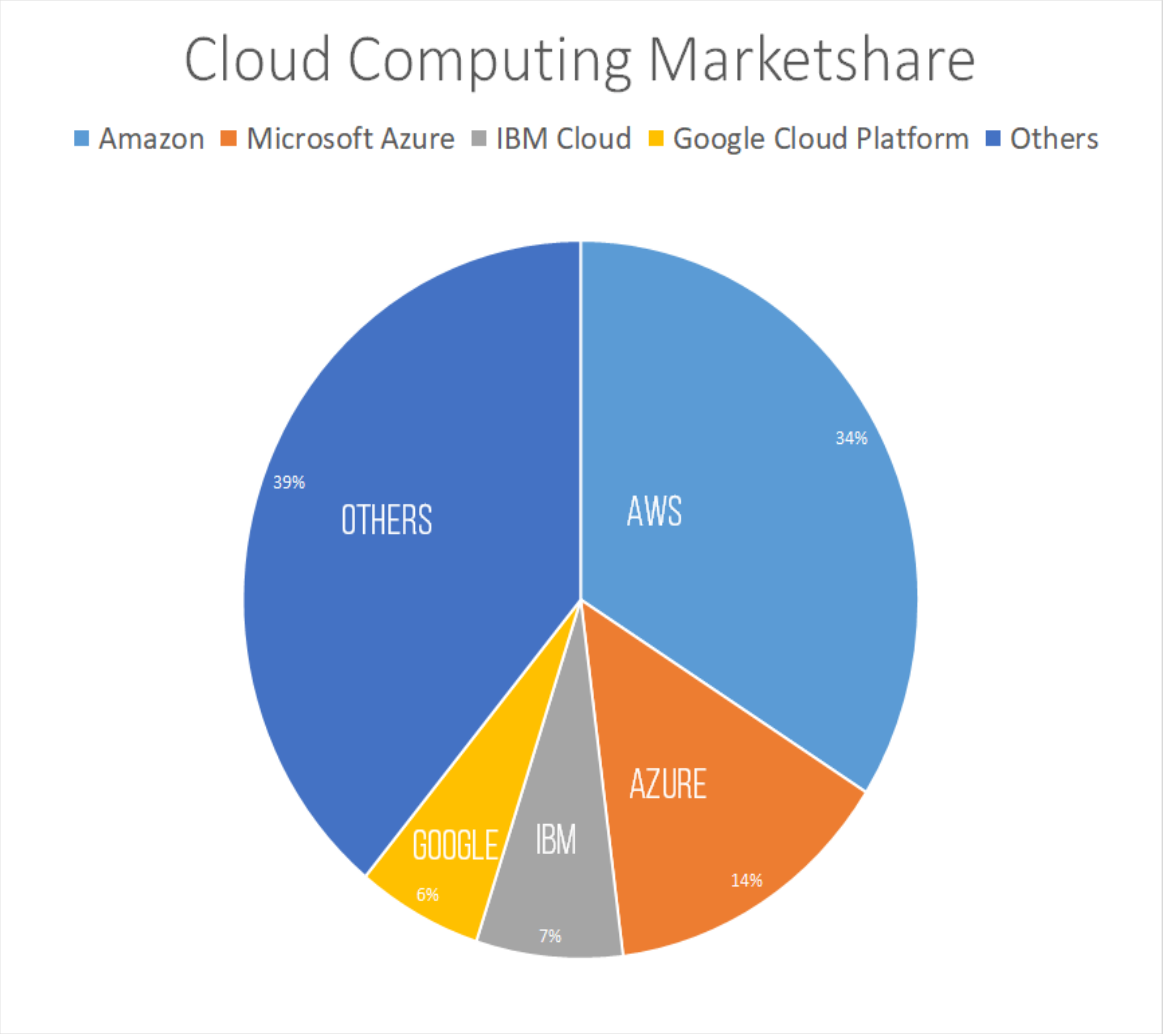
Amazon Web Services eli AWS on pilvipalveluiden pioneeri. AWS tarjoaa suuren määrän erilaisia palveluita sekä kehitys- ja ylläpitotyökaluja. Sen tärkeimmät tuotteet ovat kuitenkin Amazon elastinen pilvilaskentapalvelu (EC2) ja yksinkertainen tallennustilapalvelu S3. AWSn tunnettu logo löytyy kuvio 1. (Wperp 2019)

Microsoft Azure, jonka tunnus löytyy kuviosta 2, on hyvin samankaltainen palvelu AWS:n kanssa ja se on AWS:n lisäksi ainoa palveluntarjoaja, joka voi tarjota suuren määrän kapasiteettia tietojenkäsittelyyn (Kuvio 2). Google Cloud Platfrom eli GCP keskittyy pääasiassa Applikaatio- ja sovelluskehittäjien tarpeisiin. GCP:n palveluiden tarjonta on

rajoittuneempaa kuin AWS:n ja Azuren, mutta se kattaa silti suuren osan pilvipalveluiden käyttäjistä. Pilvipalveluiden käyttäjämäärän jakauma esitetään kuviossa 3. (Wperp, 2019)

Kuvio 1. Amazon Web Services-pilvipalvelu. (AWS, 2019)

Kuvio 2. Microsoft Azure on Microsoftin tarjoama julkinen pilvipalvelu (Microsoft, 2019)

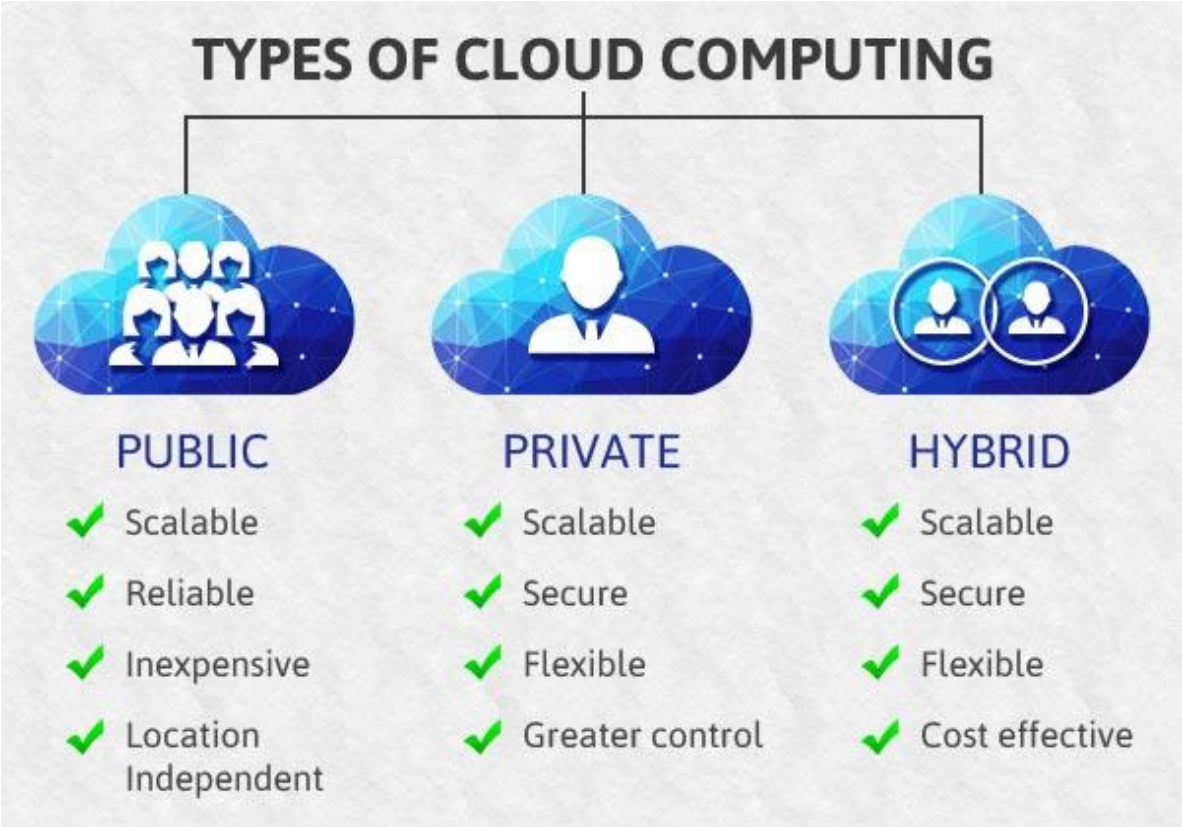


Kuvio 3. Pilvipalveluiden Markkinajakauma (Wperp 2019)

2.3 Pilvipalveluiden tyypit

Pilvipalvelut jakautuvat tyypeittäin neljään eri kategoriaan. Pilviympäristöjen tyyppejä on yksityinen, julkinen, hybridi ja yhteisö pilviympäristö. Jokaisella pilvipalvelutyypillä on omat vahvuutensa ja heikkoutensa, minkä takia pilvipalveluiden käyttöönotossa täytyy ottaa huomioon yrityksen tarpeet. (Mell & Grance 2011)

Vaikka eri teollisuusalojen pilvisiirtymä tapahtuu eri tahtia, suurin osa yrityksistä on jo suunnitellut jonkinlaista pilvisiirtymää. Monet yritykset keskisuuresta suureen etsivät pilviratkaisua yksityiseltä ja hybridi puolelta, kun taas pienemmät yritykset keskittyvät enemmän julkisiin pilviin. Pilvipalveluiden tyyppien erot esitellään kuviossa 4. (Rahman & Jungck 2011)



Kuvio 4. Eri pilvipalveluiden edut (Convergence, 2019)

2.3.1 Julkinen pilvipalvelu

Julkinen pilvi tarkoittaa pilvipalveluja, jossa palvelut ovat tarjolla kaikille. Yleisimmin sen omistaa suurempi yritys tai organisaatio, joka tarjoaa kapasiteettia omista palvelinkeskuksistaan kenelle tahansa. Julkisesta pilvipalvelusta palveluja voi ostaa kuka tahansa yksityishenkilöistä suuriin organisaatioihin. (Mell & Grance 2011)

Suurin osa julkisista pilvistä on multi-tenantteja, joiden avulla voidaan säästää jaetun infrastruktuurin avulla. Julkiset pilvet ovat nopeampia implementoida ja niitä pystytään skaalaaman tarpeiden mukaan. Erityisesti pienille ja keskisuurille yrityksille julkinen pilvipalvelu voi olla ainoa kustannustehokas vaihtoehto. (Rahman & Jungck 2011)

2.3.2 Yksityinen pilvipalvelu

Yksityinen pilvi on yrityksen sisäinen tietoturvallinen pilviympäristö, joka on suojattu palomuurilla. Yksityiseen pilvipalveluun ei yleensä ole pääsyä ulkoisesta verkosta. Yksityinen pilvi on yhden organisaation pilvi, joka voi koostua useasta eri liiketoimintayksiköstä. Yritys voi omistaa ja hallinnoida yksityistä pilveä tai se voi olla ostettu kolmannelta osapuolelta, joka voi omistaa tai hallinnoi pilvipalvelua tai se voi olla sekoitus, jossa omistus, hallinnointi- ja operointi on jaettu molemmille puolille. Pilvipalveluiden infrastruktuuri voi sijaita

paikallisessa palvelinkeskuksessa tai kolmannen osapuolen palvelinkeskuksessa. (Mell & Grance 2011)

Yksityiset pilvet voivat tarjota automaation, resurssien provisioinnin ja resurssien käyttöönoton hallintaa ilman datan hallinnan ja näkyvyyden menettämistä. Yksityiset pilvet vahvuutena on turvallisuus, saatavuus ja palveluvaatimusten täyttyminen tietyssä maantieteellisessä sijainnissa. (Rahman & Jungck 2011)

2.3.3 Yhteisö pilvipalvelu

Yhteisöpilvi on jaettu pilvipalvelu useiden eri organisaatioiden välillä. Ne koostuvat yleensä useista eri tenanteista, joista jokaisesta on pääsy kyseiseen pilveen. Yleisimmin yhteisöpilvipalvelu koostuu kahdesta tai useammasta yksityisestä, julkisesta tai useammasta yhteisöpilvipalveluista, joilla on samat intressit ja vaatimukset, kuten turvallisuus vaatimukset tai yhteistyösuunnitelmat. (Mell & Grance 2011)

Yhteisö pilvipalvelu voi tarjota suuria säästöjä muihin vaihtoehtoihin verrattuna. Luottosuhteet-, vastuu-, lisenssointi-, laki- ja hallintaongelmat ovat kuitenkin suurimpia ongelmia yhteisöpilvessä. (Rahman & Jungck 2011)

2.3.4 Hybridi Pilvipalvelu

Hybridi pilvipalvelussa voi olla jokaista edellä mainittuja pilvipalvelutyyppejä, jotka ovat sidottu toiminnaltaan yhteen niin, että kaikki pilvipalvelut pysyvät omina uniikkeina yksikköinään. Näiden pilvipalvelujen välillä datan ja sovellusten siirtäminen on yleensä mahdollista. (Mell & Grance 2011)

On olemassa useita tilanteita, joissa hybridi pilvipalvelun käyttäminen on hyödyllisempää kuin pelkän yksityisen tai julkisen pilvipalvelun käyttäminen. Hybridi pilvipalveluiden yhteensopivuusvaatimukset voivat vaatia tarkkaa hallintaa tietoturvan takia, mutta se voi mahdollistaa julkisen pilvipalvelun SaaS-sovelluksen käytön yksityisen pilvipalvelun datan käsittelyyn, kuten ”katastrofista palautumis”-vaihtoehto tai varmuuskopioiden tallentamisen virtuaaliseen yksityiseen pilveen. (Rahman & Jungck 2011)

3 PILVIPALVELUKÄSITTEET

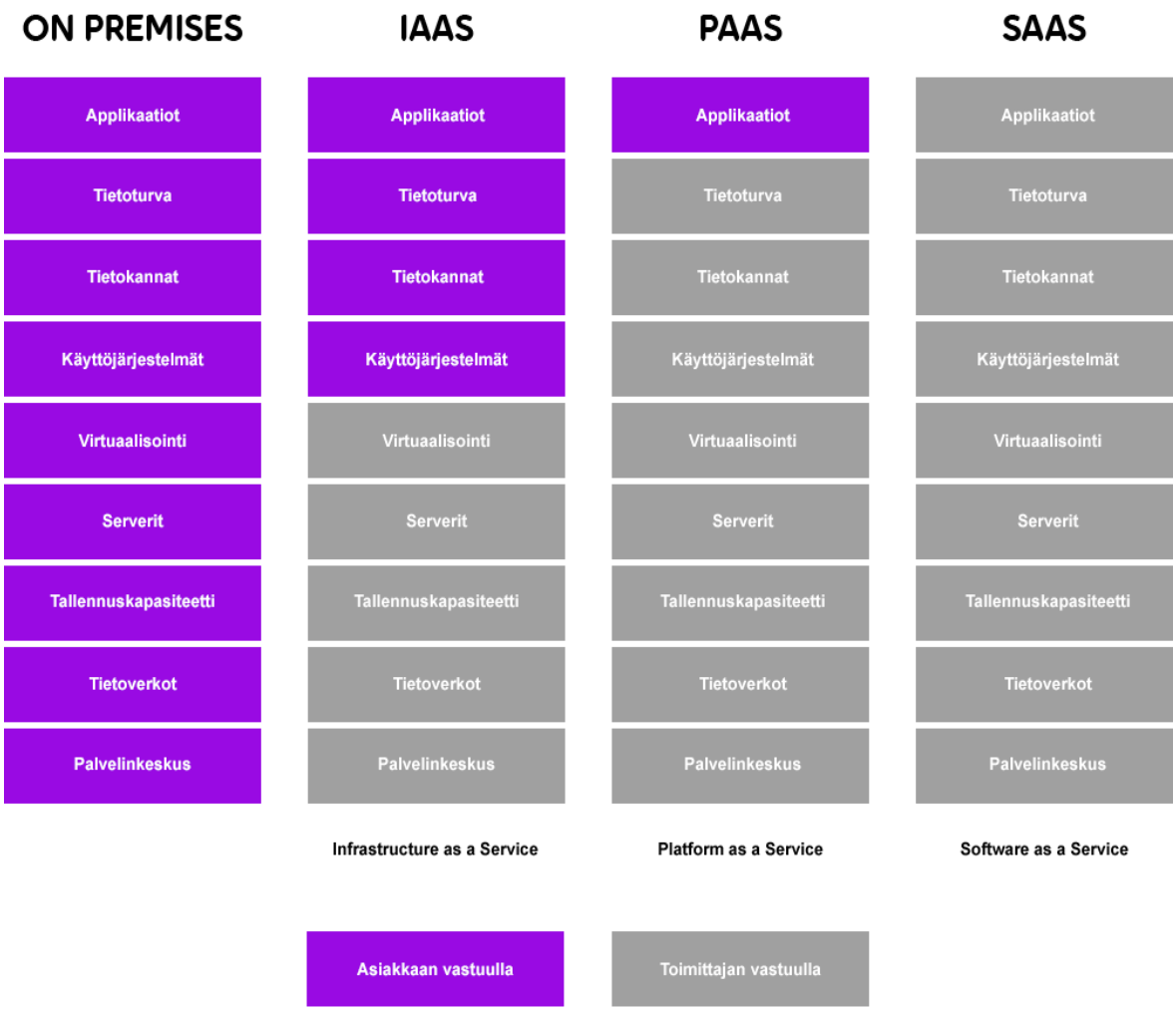
3.1 Pilvipalveluiden palvelumallit

Pilvipalveluiden palvelumallit jakautuvat pääasiassa kolmeen eri kategoriaan, jotka ovat infrastruktuuri palveluna, alusta palveluna ja sovellus palveluna. Näiden kolmen lisäksi on olemassa vielä alusta palveluna -kaltainen malli, joka on käyttäjän näkökulmasta samankaltainen malli kuin alusta palveluna. Jokaisessa palvelumallissa pilvipalvelun tarjoaja on vastuussa vähintäänkin palvelimien virtualisointilaitteistosta, virtualisoinnista ja fyysisistä tietoliikenneyhteyksistä, yhteyksienhallinta ja rajoittaminen palveluiden virtuaaliverkkoihin on käyttäjän vastuulla. Pilvipalvelujen käyttöönotto poistaa tarpeen omalle palvelinsalille ja takaa palveluiden korkean laadun ja toimintavarmuuden. Palveluiden keskittyminen pilviympäristöön laskee palveluiden ylläpitokustannuksia, minkä takia pilvipalveluiden hinta ja palvelutaso voidaan pitää erittäin korkealla. Suurimpien pilvialustojen palvelutasosopimus lupaa 99,9 % toimintavarmuuden riippumatta käytettävistä palveluista. Ylläpitokustannuksien laskemisesta huolimatta pilvisiirtymää ei yleisimmissä tapauksissa tehdä rahallisien säästöjen takia. Pilvipalveluiden lopulliset kustannukset ovat useissa tapauksissa lähes identtiset paikallisen ympäristön ratkaisujen kanssa ilman käyttäjän vastuuta palvelinsalilaitteistosta. (Microsoft 2019)

> *“Riippumatta siitä minkä vaihtoehdon valitset, Pilvisiirtymä on tulevaisuuden teknologiaa kuten me sen tiedämme ja siitä pitää olla tietoinen.” (Watts & Raza, 2019)*

Pilvipalveluiden joustavuus on yksi sen suurimpia vahvuuksia, sen palveluiden skaalautuvuus käyttäjän tarpeisiin ja mahdollisuus hallinnoida kaikkia resursseja yhtenä kokonaisuutena, riippumatta siitä onko kyseessä SaaS-, PaaS- vai IaaS-palvelu. Pienille yrityksille aloituskustannukset laskevat paikalliseen vaihtoehtoon verrattuna ja mahdollistaa erittäin vaativien ominaisuuksien käytön huomattavasti matalammilla kustannuksilla omaan paikalliseen ympäristöön verrattuna. Palvelumallien vastuualueet näkyvät kuviossa 5.

(Avram, 2014)



Kuvio 5. Palvelutasojen erot pilvipalveluissa (Inmics-nebula, 2018)

3.1.1 Infrastuktuuri palveluna (IaaS)

Infrastucture as a Service eli Infrastruktuuri palveluna on yksi pilvipalveluiden suurimmista ja nopeimmin kasvava palvelumalli. Pilvipalvelun tarjoajan tehtävä IaaS-mallissa on järjestää käyttäjille resurssit, kuten virtualisoidut palvelimet, tallennustilat palveluista, palomuurit, verkkoliikenteen kuormituksen tasaajat ja tietoverkkolaitteet. IaaS-ympäristön vahvuuksina käyttäjälle on korkea palvelun taso, resurssien skaalautuvuus omaan käyttöympäristöön sopivaksi ilman tarvetta huolehtia palvelimien fyysisestä laitteistosta ja yksinkertaistettu ylläpito. (Bhardwaj, Jain & Jain 2010)

Resurssien allokointi, provisiointi, mukautuvuus ja kapasiteetin riittävyys ovat pilvipalvelun suurimpia haasteita palveluntarjoajalle, palveluntarjoaja takaa resurssien kapasiteetti riittää korkeimpien käyttöpiikkien aikana, minkä takia käyttöpiikkien ulkopuolella resurssit ovat alikäytettyjä. (Bhardwaj, Jain & Jain 2010)

3.1.2 Alusta palveluna (PaaS)

Platform as a Service eli Alusta palveluna tarjoaa käyttäjille alustan, jolle voidaan lähteä rakentamaan sovellusta ilman huolta käyttöjärjestelmän ja väliohjelmistojen ongelmista ja päivityksistä. Käyttäjä voi keskittyä täysin palvelun tai sovelluksen kehittämiseen mutta vastuu kerätystä datasta ja käytetyistä sovelluksista kuuluu käyttäjälle. PaaS-palvelut tekevät tuotteiden kehityksestä ja julkaisemisesta yksinkertaisempia ja kustannustehokkaampia. (Bhardwaj, Jain & Jain 2010)

PaaS mahdollistaa käyttäjien omien yksittäisten pilvisovelluksien luonnin. Toisin kuin SaaS, jossa sovelluksen muokkaaminen ei ole juurikaan mahdollista, PaaS tarjoaa mahdollisuuden rakentaa yrityksen omaa pilvisovellusta varten sopiva ympäristö. Käyttäjän ei tarvitse huolehtia alustasta, minkä päälle sovellus rakennetaan. (Rahman & Jungck 2011)

3.1.3 Sovellus palveluna (SaaS)

Software as a Service eli Sovellus palveluna on pilvipalvelun tarjoama ratkaisu, jossa palvelut on luotu valmiiksi infrastruktuurista sovellukseen asti. Käyttäjän tarvitsee tuoda data järjestelmään ja lukea se tarjotun sovelluksen web-portaalista tai loppukäyttäjäsovelluksesta. SaaSin etuna on erityisesti se, että käyttäjä maksaa vain sovelluksen käytöstä ilman huolta palvelun kehitys- tai ylläpitotehtävistä. Hallinta tapahtuu yleisesti pilvipalvelun tarjoamasta palvelinkeskuksesta, minkä kautta sovellusta voidaan käyttää useisiin eri tenantteihin ja eri käyttäjille internetin välityksellä. (Inmics-nebula, 2018)

SaaS-palvelun käyttö on suunniteltu pääasiassa epäoleellisten ohjelmien, ominaisuuksien ja palveluiden ulkoistamiseen niin että palvelu täyttää asiakkaan vaatimukset ja laskee kustannuksia asiakkaalle. Yleisimmät SaaS-sovellukset ovatkin HR-, palkanlaskenta ja asiakkuudenhallinta eli CRM-sovellukset erityisesti pienemmillä yrityksillä, joille palveluiden rakentaminen ei olisi kustannustehokasta. Palvelumuotona SaaS ei ole yhtä mukautuva kuin yrityksen oma rakentama sovellus, koska sen tarkoituksena on täyttää mahdollisimman suuri osa asiakkaiden vaatimuksista menemättä kuitenkaan liian yksityiskohtaisiin sovellusmuokkauksiin. (Kavis, 2014)

3.2 Pilvipalvelun hallinnan tavoitteet

Pilvipalveluita tarjoavan yrityksen pitää pystyä saavuttamaan asiakkaiden kannalta kolme tärkeää asiaa; itsepalvelu, työkuorman automatisointi ja palveluiden analysointi. Riippumatta pilvipalvelun tyypistä edellä mainitut ominaisuudet tuovat pilvelle dynaamisen ja skaalautuvan pilvipalvelun jokaisen asiakkaan tarpeiden mukaan, minkä takia pilvipalvelun ylläpitäminen on tehokasta ja se on helposti muokattavissa. (Jyngck & Rahman 2011)

Pilvipalveluiden tavoitteena on saavuttaa korkea automaation, jolloin asiakas voi itse pystyttää tarvitsemansa resurssit suunnittelun jälkeen. Asiakas voi dynaamisesti provisioida laskentaresurssit, jotka sopivat ympäristön vaatimuksiin ilman, että käyttäjä joutuu olemaan yhteydessä toimittajaan. (Jyngck & Rahman, 2011)

3.2.1 Itsepalvelu mahdollisuudet

Pilvipalvelut poistavat tarpeen vanhoille hitaille ja kankeille IT-prosesseille ja mahdollistaa palvelujen sopivuuden jokaiselle käyttäjälle. Itsepalvelunapilvenhallinta portaalista yritys voi ottaa käyttöön resursseja nopeasti ja alkaa rakentamaan tarvittavia palveluita resurssien päälle. Itsepalvelu mahdollistaa myös resurssien lisäämisen ja vähentämisen tarpeiden mukaan. (Jyngck & Rahman, 2011)

Pilvihallinta mahdollistaa työkuorman automaation. Automaation avulla pilvipalveluiden käyttäjät voivat luoda nopeasti resursseja skaalautuvuuden käyttöhuippujen tai vähäisen käytän aikana yrityksen tai organisaation määrittämien sääntöjen puitteissa. Työkuorman automaatiolla voidaan hoitaa skaalautuvuuden lisäksi pilvipalvelu resurssien tietojen keräys, uusien resurssien käyttöönotto ja resurssien ohjeidenmukaisuus sekä raportointi eri palveluista. (Jyngck & Rahman, 2011)

3.2.2 Palveluiden analysointi

Palveluiden analysointi yksityisessä pilvipalvelussa varmistaa infrastruktuurin toiminnan ja tarjoaa tietoa mahdollisiin tarvittaviin muutoksiin esimerkiksi työkuorman jakamiseksi tai kapasiteetin lisäämiseksi. Saatujen tietojen mukaan yritykset ja organisaatiot voivat tehdä päätöksiä esimerkiksi siitä, onko yrityksellä tarvetta vaihtaa pilvipalvelun tarjoajaa tai siirtää palvelut yksityisestä pilvestä julkiseen pilveen. (Jyngck & Rahman 2011)

Monitorointi ja valvonta mahdollistaa resurssien optimaalisen käytön helposti analysoitavilla mittaus tavoilla. Resurssien käyttöä voidaan hallita tehokkaasti ja ympäristön resurssien käytön raportointi tuo selkeyttä palvelujen toimintamalliin. (Jyngck & Rahman 2011)

3.2.3 Pilvipalveluiden riskit

Pilvipalveluiden riskejä ovat siirrettyjen palveluiden poistuminen yrityksen omasta ylläpidosta, minkä takia yrityksen sisäiset palvelut olisivat riippuvaisia ulkoisista toimijoista, mikä puolestaan aiheuttaa datan ja prosessien mahdollisen haavoittuvuuden. Ongelma ei ole niin suuri yksityisien pilvipalveluiden kohdalla kuin muissa pilvipalvelumalleissa. (Jyngck & Rahman, 2011)

Pilvipalveluiden käytön lisääntyminen johtaa myös suuremman internet-kaistanleveyden tarpeeseen ja on toiminnaltaan erittäin riippuvainen verkon yleisestä toiminnasta. Uutena teknologiana ylläpidon osaavien ammattilaisten puute sekä integraatio vanhoihin järjestelmiin voivat aiheuttaa suuria ongelmia. (Jyngck & Rahman, 2011)

4 PILVIPALVELUN HALLINTA

4.1 Käytännöt

Pilvipalvelun resurssien helpompi ja nopeampi provisiointi vaatii myös resurssien valvonnan ja hallinnan tehokkuutta. Infrastruktuurin ylläpitoon vaadittava ammattitaito on ulkoistettu, minkä takia pilvipalveluiden käyttäjät voivat keskittyä resurssien hallintaan. (Jyngck & Rahman, 2011)

Vastuun väheneminen infrastruktuurista ja sen toiminnasta mahdollistaa resurssien julkaisemisen nopeammin kuin aikaisemmin, minkä takia pilvipalvelun käyttäjät voivat julkaista useita eri resursseja useisiin eri tarkoituksiin. Jotta pilvipalveluiden hallinta olisi helpompaa on pilvipalvelun käyttäjän ja ylläpitäjän noudatettava tiettyjä sääntöjä käytännöissä. (Onrego, 2013)

Pilvipalvelun ylläpitäjän täytyy ottaa huomioon mahdollisuus useampaan eri tilaukseen yhdessä pilvipalvelussa. Tästä johtuen on erittäin tärkeää, että resurssien käyttöönoton yhteydessä noudatetaan ylläpitäjän ja asiakkaan sopimia toimintatapoja. (Onrego, 2013)

Erityisesti valvonnan ja resurssien käyttöönoton kannalta nimeämiskäytännöt nousevat suureen rooliin. Microsoft Azuren tapauksessa pilvipalvelua voidaan hallita Windows Powershell -sovelluksella. Resurssien automaatio ja valvonta on mahdollista tehdä paikallisesta ympäristöstä vanhoilla työkaluilla tai käyttämällä vain pilveen tarkoitettuja ratkaisuja, kuten ServiceNow Cloud Management- tai IBM Cloud Orchestrator-sovellusta. (Chang, 2019)

4.1.1 Hallittavuus ja valvonta

Jos hallittavana on useampi pilviympäristö, niin kolmannen osapuolen sovellus niiden hallintaan ja valvontaan normaalien pilvipalvelutyökalujen lisäksi voi olla hallittavuuden kannalta varteenotettava vaihtoehto. Useamman pilvipalvelun hallinta ja valvonta keskitetysti helpottaa ylläpitäjän työkuormaa, koska toistuvia tehtäviä voidaan automatisoida. Molempien tehostumisen ansiosta palveluiden kustannukset vähenevät samalla, kun palveluiden toiminnallisuus ja turvallisuus paranevat. (Chang, 2019)

Resurssien nimeäminen sovittujen käytäntöjen mukaan on tärkeää hallinnan kannalta. Samaan ympäristöön tai projektiin kuuluvat resurssit ovat suositeltavaa nimetä niin, että nimestä selviää mikä resurssi on kyseessä, mihin ympäristöön se kuuluu ja missä tuotantovaiheessa kyseinen resurssi on. (Onrego, 2013)

Availability Zones eli resurssien saatavuusalueet vaihtelevat ja ne mahdollistavat korkean toimintavarmuuden pilvipalveluiden maanosa-alueilla. Resurssien sijoittaminen eri datakeskuksiin samassa maaosa-alueella pienentää riskiä käyttökatkoille johtuen datakeskuksien paikallisista ongelmista. (Modi, 2019)

4.1.2 Resurssien tagit

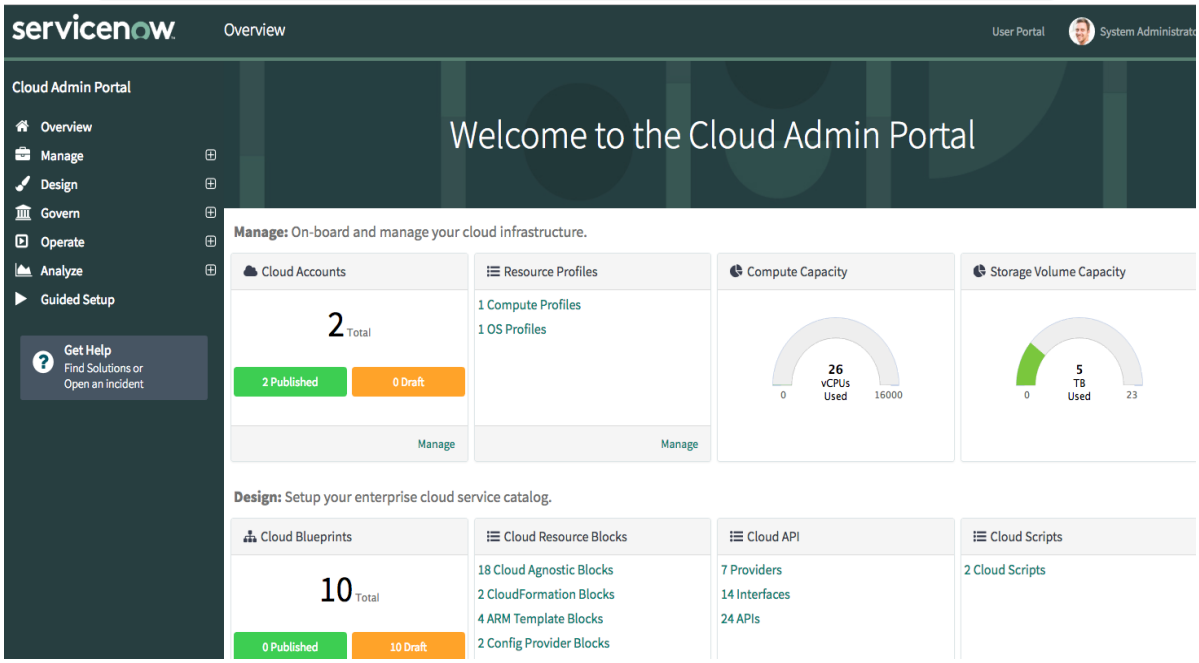
Resurssien tagien perusteella voidaan selventää, missä resurssi on käytössä, mikä on resurssin kustannuspaikka tai mitä automaatiota resursseihin halutaan kohdentaa. Tagien lisääminen on suositeltavaa tehdä suoraan resurssia käyttöön otettaessa, mutta niitä voidaan tarvittaessa muuttaa tai lisätä jälkikäteen.

Azuressa tagien avulla voidaan tarvittaessa ottaa käyttöön resurssi asiakkaan pilvipalveluun kolmannelle osapuolelle ja sen käytön kustannuksia voidaan valvoa tagien perusteella. Tagit voidaan lisätä infrastruktuuri koodina -ratkaisuissa JSON-pohjiin ennen ympäristön käyttöönottoa. (Onrego 2013)

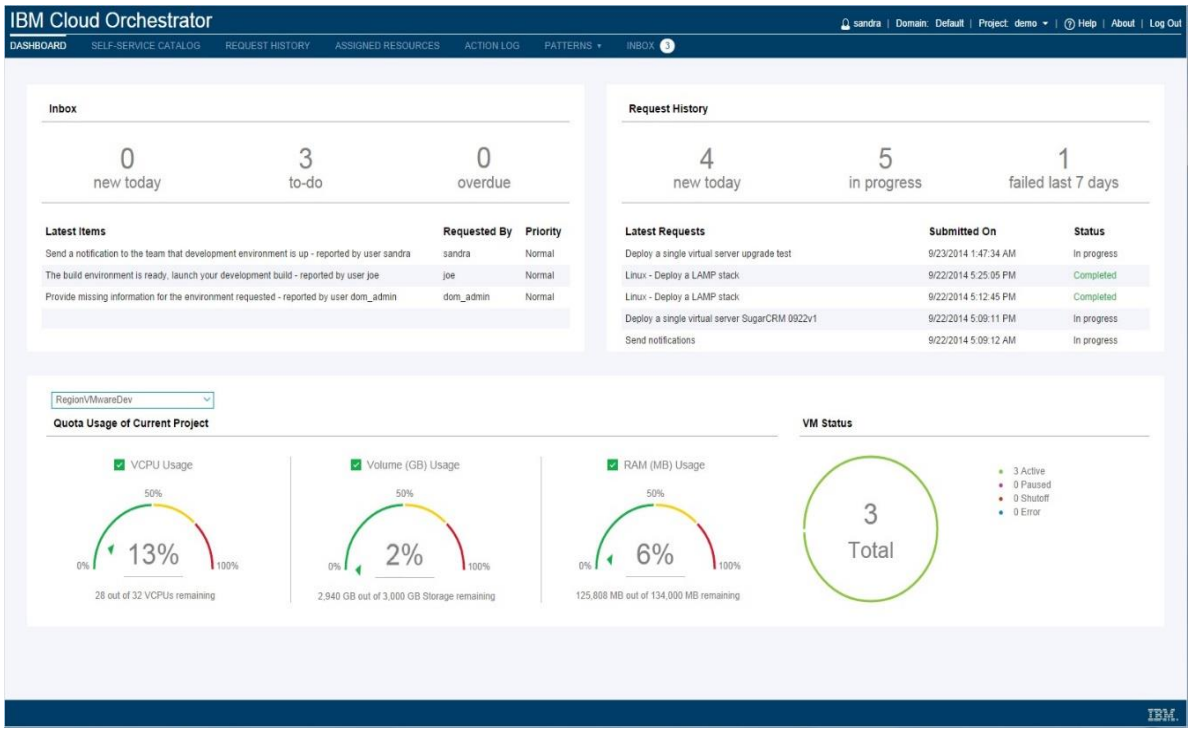
4.2 Pilvihallinnan työkalut

Azuren hallintatyökaluihin kuuluu vakiona RBAC-roolisysteemi, jolla voidaan jakaa oikeuksia käyttäjille eri resursseihin, sekä locks- ja policy-hallintatyökalut, joilla voidaan rajoittaa resurssien käyttöä tai sallia niitä eri tilanteissa. Mainitut työkalut mahdollistavat kunnollisen ja tehokkaan pilvipalveluiden hallitsemisen Azure-natiiveilla työkaluilla. (Modi, 2019)

Pilvipalveluiden hallinta voidaan tehdä paikallisen palvelinympäristön työkaluilla, mutta pilvipalveluita varten on kehitetty useita pilvinatiiveja työkaluja, kuten aikaisemmin mainitut ServiceNow Cloud Management ja IBM Cloud Orchestrator, jotka ovat esitelty kuvioissa 6 ja 7. Molemmat pilvipalveluiden hallintaratkaisut tarjoavat yksinkertaisen ratkaisun tuomalla pilvipalvelut yhteen hallintaportaaliin, joka helpottaa ympäristöjen valvontaa ja ylläpitoa. (Chang, 2019)



Kuvio 6. ServiceNow Cloud -hallintaportaali



Kuvio 7. IBM Cloud Orchestrator -hallintaportaali

4.3 Infrastuktuuri koodina

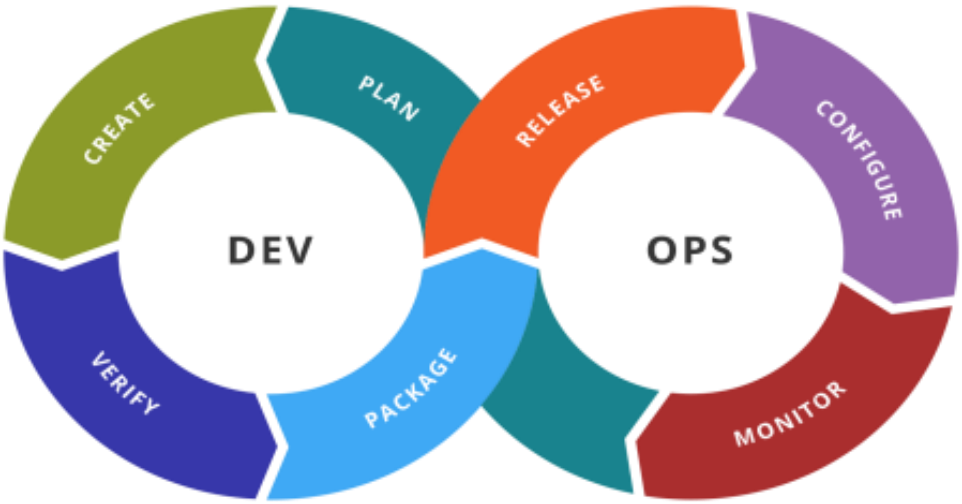
Infrastruktuuri koodina eli IAC (Infrastrukture as Code) ja Devops mahdollistavat resurssien käyttöönottamisen nopeammin, johdonmukaisemmin ja tehokkaasti. IAC mahdollistaa infrastruktuurin ja sen asetuksien määrittämisen koodilla, minkä takia resurssien

käyttöönottamisen voi automatisoida useissa ympäristöissä. Käyttöönotto tapahtuu Azure resurssimanageriin luotavilla pohjilla eli ARM-Templatella. Automatisoinnin takia työkuorma vähenee ja työkuormaa voidaan siirtää palvelujen kehittämiseen ja tehostamiseen. (Modi, 2019)

Infrastruktuuri koodina suurin etu on ympäristön koodin tallentaminen säilöön, joka mahdollistaa versiohallinnan. Versiohallinnan takia vanhoja ympäristöjen asetuksia voidaan ottaa käyttöön uudelleen tarpeen vaatiessa sekä se mahdollistaa kokonaisten ympäristöjen provisioinnin useaan kertaan johdonmukaisemmin ja ennalta-arvattavammin. Versiohallinnan takia vanhoja ympäristöjen asetuksia voidaan ottaa käyttöön uudelleen tarpeen vaatiessa sekä se mahdollistaa kokonaisten ympäristöjen provisioinnin useaan kertaan johdonmukaisemmin ja ennalta-arvattavammin. (Modi, 2019)

4.4 DevOps

DevOps:in ideana on lyhyet käyttöönottovälit, joka pyrkii nopeaan ja riskittömään palveluiden käyttöönottoon, Devopsin toimintalogiikka on selitetty kuviossa 8. Devops vähentää ympäristön toimimattomuusriskiä huomattavasti verrattuna perinteiseen käyttöönottoon ja tarpeen vaatiessa vanhan ympäristön takaisin tuominen on mahdollista. (Modi, 2019)



kuvio 8. Devops-toimintaympyrä (Lane, 2018)

Devopsin käyttäminen tehokkaasti vaatii julkaisuputkiston säätämistä, minkä avulla se pyrkii jatkuvaan käyttöönottoon useissa eri ympäristöissä samaan aikaan. Päivitysten julkaisuun tarvitaan asiakkaan lupa ennen päivityspakettien käyttöönottoa. Hyväksymisprosessi voidaan tehdä manuaalisesti tai se voidaan automatisoida riippuen organisaation devops-kyvyistä. (Modi, 2019)

Devopsin hyödyt eivät kuitenkaan kestä pitkään, jos jatkuvaa loppukäyttäjäpalautetta ei saada ja kehitystä ei voida jatkaa. Devopsin kannalta reaaliaikainen palaute on äärettömän tärkeää, jotta kehittäjät voivat vastata loppukäyttäjän ja operaatiotiimien tarpeisiin. (Modi, 2019)

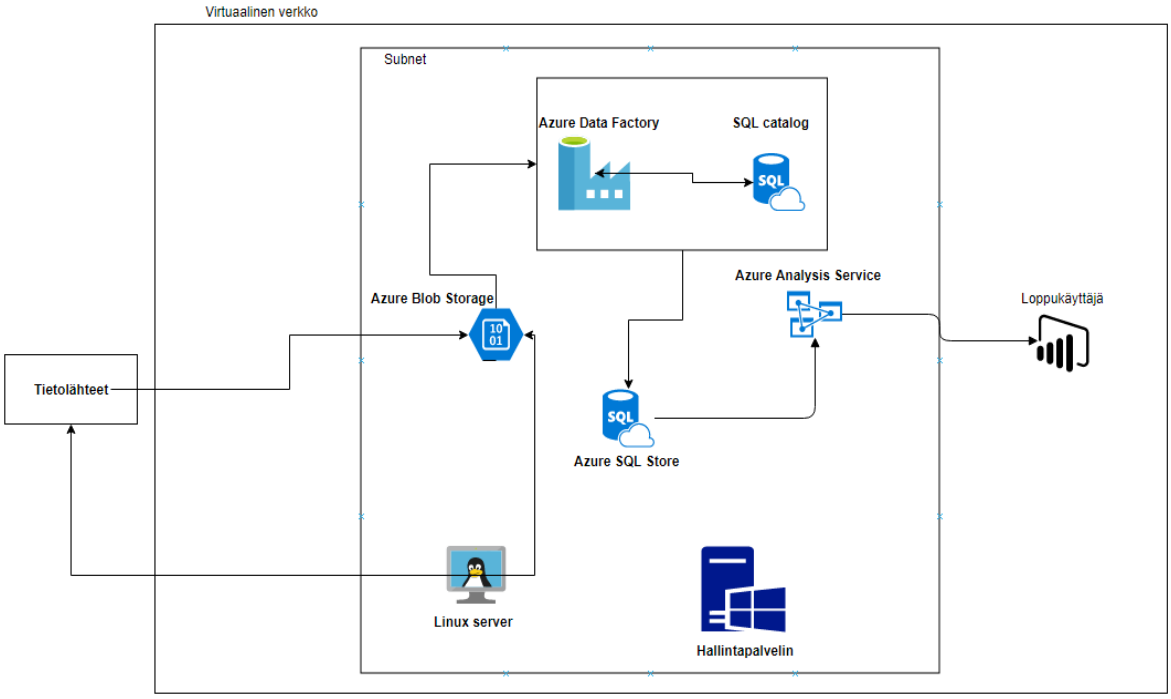
5 CASE RAPORTOINTIJÄRJESTELMÄ

5.1 Arkkitehtuuri ja resurssit

Projektissa lähdettiin rakentamaan raportointijärjestelmää asiakkaan vaatimustarpeisiin. Projektin resurssit haluttiin rakentaa PaaS-palveluna Microsoft Azureen. Ympäristön arkkitehtuuri, joka löytyy kuviosta 9, koostuu Windows 2016 datacenter-hallintapalvelimesta, Linux-palvelimesta, kahdesta eri Azure SQL-kannasta, Azure Blob storage, Azure Analysis Service eli AAS ja Azure Data Factory resursseista.

Ympäristön toiminnan läpikulku yksinkertaistetusti menee niin, että tietolähteistä tuodaan dataa Azure Blob Storageen tai se haetaan Linux-palvelimella palvelimelle esimerkiksi Crontab-sovelluksella tai FTP-siirtona. Tämän jälkeen tiedostot siirretään linux-palvelimelta Azure Blob Storageen.

Blob storagesta Azure Data Factory käsittelee tiedot ensin Azure Blob Storagesta SQL Catalog-tietokannan kautta Azure SQL Store-tietokantaan, josta Azure Analysis Service eli AAS hakee tiedot loppukäyttäjän aloittamasta pyynnöstä. SQL-tietokantojen manuaalinen hallinta tapahtuu tarvittaessa hallintapalvelimelta.



Kuvio 9. Arkkitehtuuri kuva

Resurssit on sijoitettu Azureen Omaan virtuaaliverkkoon, jonne on avattu Azuren tarjoamalla NSG-palomuuriratkaisulla. NSG:n avulla rajoitetaan ympäristöön pääsyä muista

kuin tietolähteiden IP-osoitteista Linux palvelimelle ja Azure Blob Storage-resurssiin. AAS:n yhteys loppukäyttäjille yrityksen työasemaverkkoihin ja ylläpitäjien pääsy hallintapalvelimelle määritetään myös NSG-resurssin avulla.

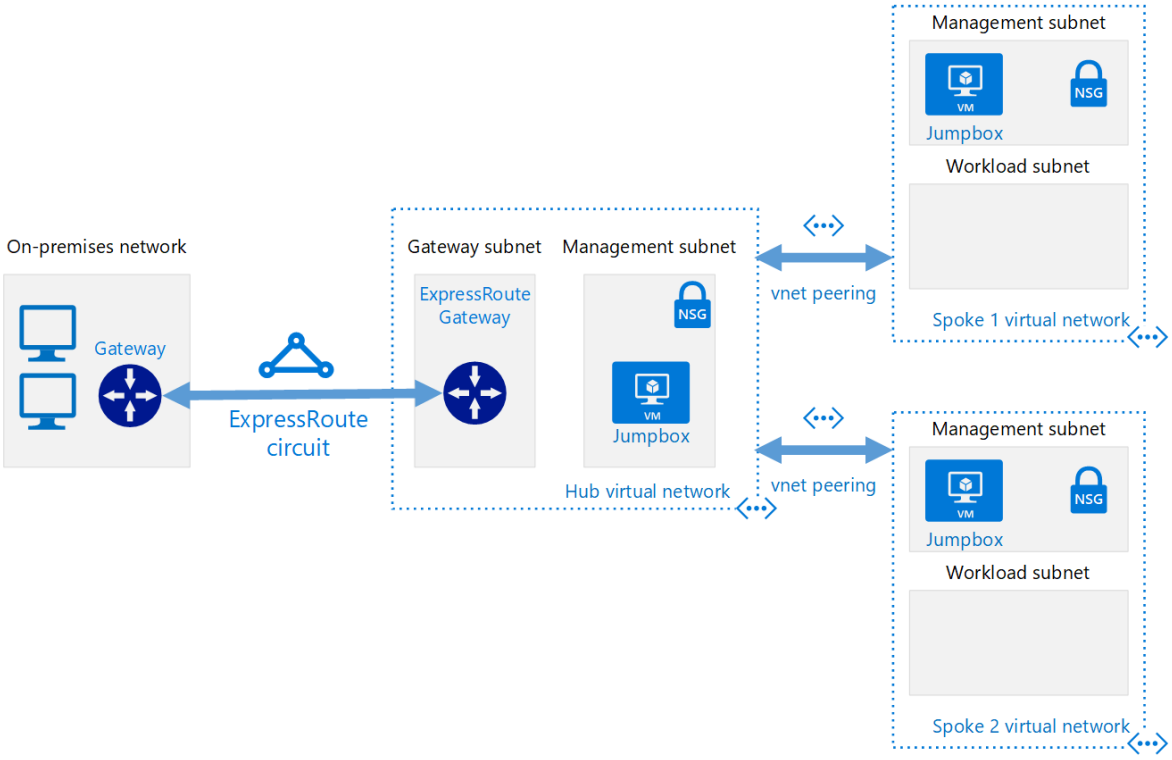
Virtuaalipalvelimeksi määritettiin Windows 2016 Datacenter palvelutasolle D2s V3, joka sisältää kaksi virtuaalista prosessoriydintä ja 8 GB keskusmuistia. Ajastettuna toimintona ympäristön virtuaalipalvelimille on määritetty automaattinen sammutus virka-ajan ulkopuolella. Ylläpitäjän pyynnöstä tuotanto-, kehitys- ja testiympäristöjen hallintaan käytetään samaa hallintapalvelinta.

Infrastuktuuria varten on luotu kaksi erillistä json-tiedostoa, pohja.json ja parametrit.json. pohja.json-tiedostoon on määritetty resurssien tehot, palvelutasot ja tarvittavat määritykset. Erillisiä määrityksiä on esimerkiksi palvelinten automaattinen sammutus virka-ajan ulkopuolella ja virtuaaliverkkojen ja aliverkkojen IP-osoiteavaruudet.

5.1.1 Virtuaaliverkot

Asiakkaan Azure on suunniteltu hub-and-spoke-ratkaisulla, joka löytyy kuviosta 10. Projektia varten luotiin uusi spoke-virtuaaliverkko. Koska resursseja ei ole tarkoitus lisätä jälkikäteen, mitoitettiin ympäristön IP-avaruus /26 maskilla. Yhteys on-premise ympäristöön luotiin Azuren tarjoamalla ExpressRoute-verkkoratkaisulla.

Projektiympäristön spoken verkkoliikenne kulkee aina Hubin palomuurin kautta, minkä tehtävä on valvoa ympäristöä käyttäviä IP-osoitteita ja verkkoliikennettä. Tarvittaessa Hubin palomuurin kautta ympäristöstä voidaan viedä dataa paikalliseen ympäristöön pelkillä palomuuriavauksilla.



Kuvio 10. Hub and spoke-ratkaisu.

5.1.2 Network security group (NSG)

Network Security Group on Azuren oma versio virtuaaliverkkojen palomuurista, jolla voidaan sallia tai estää verkkoliikennettä. Oletuksena luonti hetkellä pohjassa hyväksytään kaikki ulkoa tuleva liikenne. Tarkoituksena on rajoittaa liikennettä siinä vaiheessa, kun on selvillä, mistä ja millä tavalla data tulee Azure blob storageen ja mistä ylläpitohenkilöstön täytyy saada yhteys Azure-resursseihin.

Infrastruktuuriin on tarkoitus ottaa käyttöön kolmannen osapuolen verkkovalvontalaite, joka soveltuu Azuren verkkojenvalvontaan, joka olisi ylläpitäjän on-premise ympäristön kanssa yhteensopiva tai asiakkaan haluama ohjelma. Jos Azure-tilauksessa ei ole käytössä kolmannen osapuolen verkonhallintalaitteita, NGS-resurssi toimii hyvänä korvikkeena tietoliikenteen rajoittamisessa mutta valvontaan se ei sovellu.

5.2 Nimeämiskäytännöt ja infrastruktuuri koodina

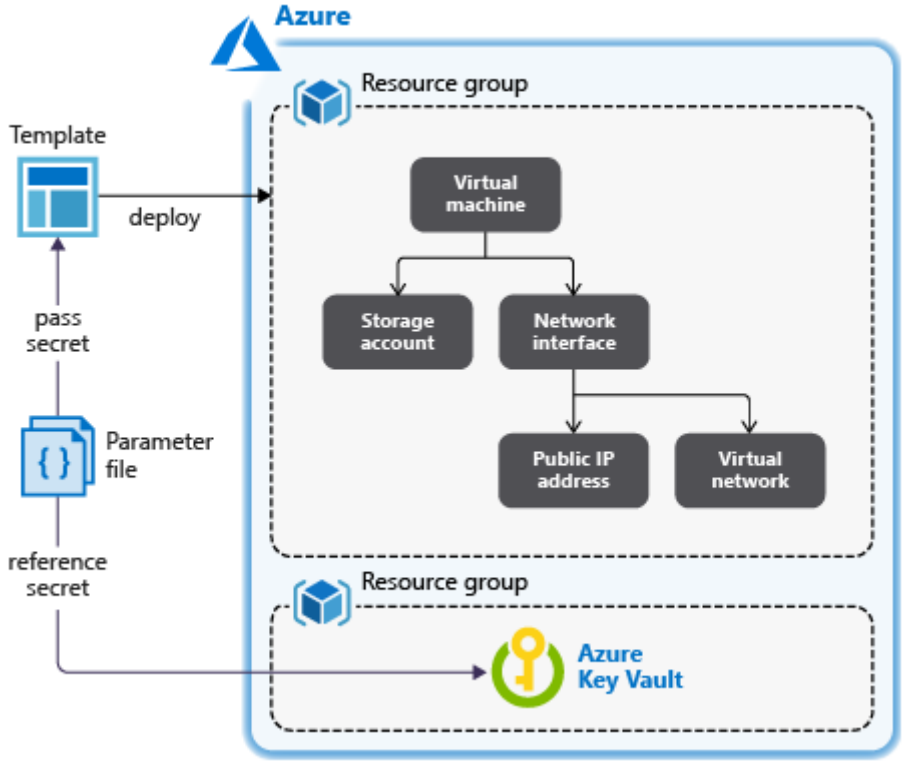
Ympäristön nimeämiskäytännöt tulevat asiakkaan governance-säännöistä, joissa on määritetty, että resurssin nimestä täytyy selvitä projektin nimi, tuotantovaihe, ylläpitäjä ja resurssi. Ympäristön rakentaminen tehdään infrastruktuuri koodina -ratkaisulla, minkä takia ympäristöstä on luotu kaksi erillistä JavaScript Object Notation eli JSON-pohjasta.

Toiseen JSON-pohjassa on määritetty jokainen resurssi mitä projektiin tarvitaan ja toiseen pohjaan on määritetty resurssien nimet. Jos halutaan pystyttää identtinen ympäristö myöhemmin, kun Azuren tarjoamiin sovelluksiin on tullut päivityksiä, vanhat pohjat ovat käyttökelpoisia API-versioiden päivittämisen jälkeen.

5.2.1 Resurssien nimimääritykset JSON-pohjassa

Resurssien nimet on merkitty toiseen JSON-pohjaan, jossa jokaiselle resurssille on oma vastine ja haluttu nimi lisättiin value-kohtaan, jotka on esitetty kuvioissa 12 ja 13. Nimetpohjassa määritetään myös Azure SQL-tietokantojen ja virtuaalipalvelimien pääkäyttäjä salasanat.

Salasanat on säilötty Azure KeyVault-palveluun. Azure KeyVault-resurssin toiminta logiikka esitetty kuviossa 11. Azure KeyVaultin avulla salasanoja ei tarvitse kirjoittaa selkokielisenä JSON-pohjiin vaan salasanojen paikalle lisätään aina ”reference secret” eli KeyVaultin salasana viittaus.



Kuvio 11. Azure Key Vault-resurssin toiminta Infrastruktuuri koodina ratkaisussa. (Microsoft 2019)

```
{
    "$schema":
"https://schema.management.azure.com/schemas/2015-01-01/deployme
ntParameters.json#",
    "contentVersion": "1.0.0.0",
  "parameters": {
    "administratorLogin": {
      "value": "[redacted]"
    },
    "administratorLoginPassword": {
      "value": "SecureString"
    },
    "SQLserver01_name": {
      "value": "[redacted]"
    },
    "SQLserver02_name": {
      "value": "[redacted]"
    },
    "storageAccount01_name": {
      "value": "[redacted]"
    },
    "azureAnalysisService_name": {
      "value": "[redacted]"
    },
    "datafactory_name": {
      "value": "[redacted]"
    },
```

Kuvio 12. Resurssien nimeämiseen käytettävä JSON-pohja

Kuvio 13. Resurssien nimeämiseen käytettävä JSON-pohja

5.2.2 Resurssimääritykset JSON-pohja

Toinen projektissa käytetty JSON-pohja sisältää resurssien määritykset, minkä perusteella Azure allokoi oikeat resurssit halutulla tavalla. Tähän JSON-pohjaan on merkitty jokaisen resurssin versio, resurssikohtaiset määritykset, viittaukset nimimääritystiedostoon ja ympäristöön luotavat virtuaaliverkkoasetukset, jotka löytyvät kuvioista 14, 15, 16 ja 17.

Ylläpitäjän pyynnöstä kehitys- ja testiympäristön molemmat virtuaalipalvelimet poistettiin infrastruktuurista ja niissä käytettäisiin tuotantoympäristössä olevia palvelimia. Ympäristön virtuaaliverkkojen NSG-sääntöihin lisättiin käyttöönoton jälkeen ylläpitäjien IP-avaruuksia, jotta he saisivat yhteyden hallintapalvelimeen ja projektin resursseihin.

```
{
    "$schema":
"https://schema.management.azure.com/schemas/2015-01-01/deployme
ntTemplate.json#",
    "contentVersion": "1.0.0.0",
  "parameters": {
    "administratorLogin": {
      "type": "String"
    },
    "administratorLoginPassword": {
      "type": "SecureString"
    },
    "SQLserver01_name": {
      "type": "String"
    },
    "SQLserver02_name": {
      "type": "String"
    },
    "storageAccount01_name": {
      "type": "String"
    },
    "azureAnalysisService_name": {
      "type": "String"
    },
    "datafactory_name": {
      "type": "String"
    },
    "SQLserver02_database1": {
      "type": "String"
    },
    "databases_master_name": {
      "defaultValue": "master",
      "type": "String"
    },
    "databases_master_name_1": {
      "defaultValue": "master",
      "type": "String"
    },
    "storageaccount_allowed_ip": {
      "type": "String"
    },
    "vnetName": {
      "type": "String"
    },
    "SubnetName": {
      "type": "String"
    },
    "subsciptionID": {
      "type": "String"
    },
    "vnetRG": {
      "type": "String"
    }
  },
  "variables": {
    "virtualNetworkRules_VnetServiceEndpoints_name":
"ServiceEndpointRule",
    "storageAccounts_StorageAccount_id":
"[concat('/subscriptions/',parameters('subsciptionID'),'/resourc
eGroups/',parameters('vnetRG'),'/providers/Microsoft.Network/vir
tualNetworks/',parameters('vnetName'),'/subnets/',parameters('su
bnetName'))]",
    "virtualNetworkRules_newVnetRule1_virtualNetworkSubnetId":
"[concat('/subscriptions/',parameters('subsciptionID'),'/resourc
eGroups/',parameters('vnetRG'),'/providers/Microsoft.Network/vir
tualNetworks/',parameters('vnetName'),'/subnets/',parameters('su
bnetName'))]",

"virtualNetworkRules_ServiceEndpoints_virtualNetworkSubnetId":
"[concat('/subscriptions/',parameters('subsciptionID'),'/resourc
eGroups/',parameters('vnetRG'),'/providers/Microsoft.Network/vir
tualNetworks/',parameters('vnetName'),'/subnets/',parameters('su
bnetName'))]"
  },
```

Kuvio 14. Resurssimääritykset1.6.JSON-pohja osa 1

```
    "resources": [
      {
        "type": "Microsoft.AnalysisServices/servers",
        "sku": {
          "name": "D1",
          "tier": "Development"
        },
        "name": "[parameters('azureAnalysisService_name')]",
        "apiVersion": "2016-05-16",
        "location": "West Europe",
        "tags": {},
        "scale": null,
        "properties": {
          "managedMode": 1
        },
        "dependsOn": []
      },
      {
        "type": "Microsoft.Sql/servers",
        "kind": "v12.0",
        "name": "[parameters('SQLserver02_name')]",
        "apiVersion": "2015-05-01-preview",
        "location": "westeurope",
        "scale": null,
        "properties": {
          "administratorLogin":
'[parameters('administratorLogin')]",
          "administratorLoginPassword":
'[parameters('administratorLoginPassword')]",
          "version": "12.0"
        },
        "dependsOn": []
      },
      {
        "type": "Microsoft.Sql/servers",
        "kind": "v12.0",
        "name": "[parameters('SQLserver01_name')]",
        "apiVersion": "2015-05-01-preview",
        "location": "westeurope",
        "scale": null,
        "properties": {
          "administratorLogin":
'[parameters('administratorLogin')]",
          "administratorLoginPassword":
'[parameters('administratorLoginPassword')]",
          "version": "12.0"
        },
        "dependsOn": []
      },
      {
        "type": "Microsoft.Storage/storageAccounts",
        "sku": {
          "name": "Standard_LRS",
          "tier": "Standard"
        },
        "kind": "StorageV2",
        "name": "[parameters('storageAccount01_name')]",
        "apiVersion": "2018-03-01-preview",
        "location": "westeurope",
        "tags": {},
        "scale": null,
        "properties": {
          "networkAcls": {
            "bypass": "AzureServices",
            "virtualNetworkRules": [
              {
                "id":
'[variables('storageAccounts_StorageAccount_id')]",
                "action": "Allow"
              }
            ],
            "ipRules": [
              {
                "value": "[redacted]",
                "action": "Allow"
              },
              {
                "value":
```

Kuvio 15. Resurssimääritykset1.6.JSON-pohja osa 2

```
"[parameters('storageaccount_allowed_ip')]",
                "action": "Allow"
              }
            ],
            "defaultAction": "Deny"
          },
          "supportsHttpsTrafficOnly": true,
          "encryption": {
            "services": {
              "file": {
                "enabled": true
              },
              "blob": {
                "enabled": true
              }
            },
            "keySource": "Microsoft.Storage"
          },
          "accessTier": "Hot"
        },
        "dependsOn": []
      },
      {
        "type": "Microsoft.Sql/servers/databases",
        "sku": {
          "name": "S0",
          "tier": "Standard"
        },
        "kind": "v12.0,user",
        "name": "[concat(parameters('SQLserver02_name'), '/',
parameters('SQLserver02_database1'))]",
        "apiVersion": "2017-03-01-preview",
        "location": "westeurope",
        "scale": null,
        "properties": {
          "collation": "SQL_Latin1_General_CP1_CI_AS",
          "maxSizeBytes": 268435456000,
          "catalogCollation": "SQL_Latin1_General_CP1_CI_AS",
          "zoneRedundant": false
        },
        "dependsOn": [
          "[resourceId('Microsoft.Sql/servers',
parameters('SQLserver02_name'))]"
        ]
      },
      {
        "type": "Microsoft.Sql/servers/virtualNetworkRules",
        "name": "[concat(parameters('SQLserver02_name'), '/',
variables('virtualNetworkRules_VnetServiceEndpoints_name'))]",
        "apiVersion": "2015-05-01-preview",
        "scale": null,
        "properties": {
          "virtualNetworkSubnetId":
"[variables('virtualNetworkRules_newVnetRule1
_virtualNetworkSubnetId')]",
          "ignoreMissingVnetServiceEndpoint": false
        },
        "dependsOn": [
          "[resourceId('Microsoft.Sql/servers',
parameters('SQLserver02_name'))]"
        ]
      },
      {
        "type": "Microsoft.Sql/servers/virtualNetworkRules",
        "name": "[concat(parameters('SQLserver01_name'), '/',
variables('virtualNetworkRules_VnetServiceEndpoints_name'))]",
        "apiVersion": "2015-05-01-preview",
        "scale": null,
        "properties": {
          "virtualNetworkSubnetId":
"[variables('virtualNetworkRules_ServiceEndpoints_virtualNetwork
SubnetId')]",
          "ignoreMissingVnetServiceEndpoint": false
        },
        "dependsOn": [
          "[resourceId('Microsoft.Sql/servers',
parameters('SQLserver01_name'))]"
        ]
      },
```

Kuvio 16. Resurssimääritykset1.6.JSON-pohja osa 3

```
    {
      "type": "Microsoft.DataFactory/factories",
      "name": "[parameters('datafactory_name')]",
      "apiVersion": "2017-09-01-preview",
      "location": "westeurope",
      "identity": {
        "type": "SystemAssigned"
      }
    }
  ]
}
```

Kuvio 17. Resurssimääritykset1.6.JSON-pohja osa 4

5.3 Käyttöönotto skripta

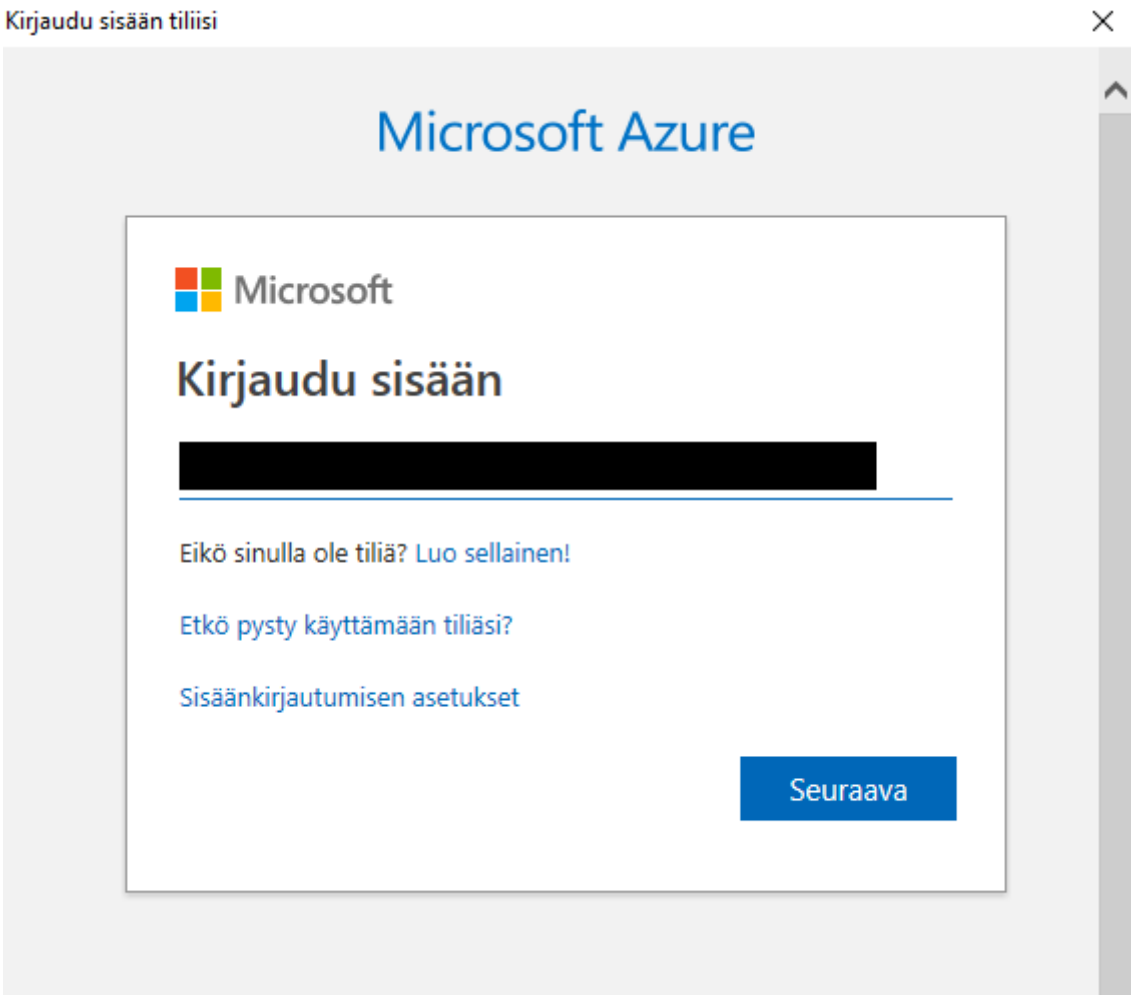
Resurssit ajettiin ylös Windows Powershell-skriptalla, joka ajaa ympäristön pystyyn JSON-pohjiin määritetyillä asetuksilla. Skriptan ensimmäinen osa koostuu tunnistautumisesta Azure-palveluun Windows Powershell-sovelluksella kuviossa 18 näkyvillä komennoilla. Skripta pyytää kirjautumaan Azure Administrator- tai Owner-tason tunnuksella, jolla on oikeudet luoda resursseja Azure tilaukseen, kuten on esitetty kuviossa 19.

Tarvittaessa oikeudet ympäristön pystyttämiseen voidaan antaa yksittäiselle käyttäjälle tai AD-ryhmälle resurssikohtaisesti. Luvittamalla käyttäjä RBAC:in kautta Owner-tasolle Resource Group-resurssiin, käyttäjä saa Owner-oikeudet jokaiseen resurssiin mitä kyseisessä Resource Groupissa on. Nämä henkilöt voivat luoda tai muuttaa resursseja tai resurssien asetuksia tai käynnistää ja sammuttaa tarvittaessa palveluita.

Kun kirjautuminen on tehty hyväksytysti, käyttäjän täytyy valita Azure tilaus, minkä alle ympäristö halutaan pystyttää kuvion 18 viimeisen komennon mukaan. Tilauksen tunnus eli Subscription ID löytyy ”kulunhallinta ja laskutus”-osiosta Azure portaalista, ellei se ole jo etukäteen tiedossa.

```
Login-AzAccount
Get-AzSubscription
Select-AzSubscription -Subscription "[redacted]"
```

Kuvio 18. Windows Powershell kirjautumis- ja tilauksen valinta komento.



Kuvio 19. Microsoft Azure kirjautumisikkuna

```
PS C:\> cd C:\IaC-Azure
```

Kuvio 20. JSON-pohjien tiedostosijainti paikallisella levyllä

Tunnistautumisen jälkeen mennään Windows Powershell-sovelluksen komentorivillä kansioon, jossa molemmat JSON-pohjat sijaitsevat komennolla, joka on esitetty kuviossa 20. JSON-pohjien siirtämien samaan tiedostosijaintiin paikalliselle levylle on suositeltavaa kuten C-levyn juureen. Projektin resurssiryhmä oli luotu etukäteen, mutta tarvittaessa resurssiryhmän voi luoda kuviossa 21 olevalla komennolla lisäämällä -name kohtaan haluttu resurssiryhmän nimi.

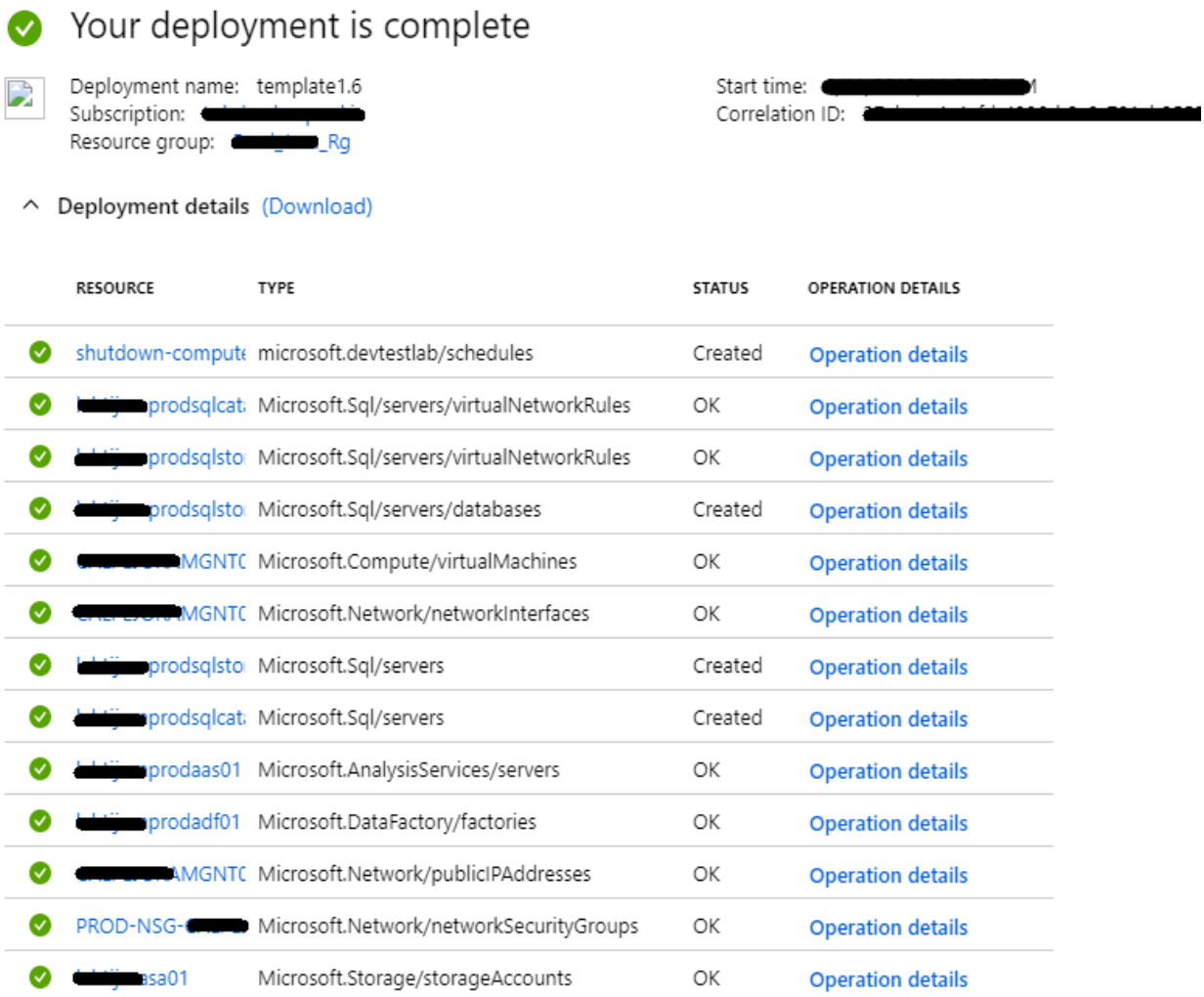
Kun Windows Powershell-sovelluksella on otettu yhteys Azure-palveluun, haluttu subscription on valittu ja JSON-pohjat on siirretty paikalliselle levylle, voidaan Powershellin konsolissa ajaa palveluiden käyttöönotto skripta, joka löytyy kuviosta 22. Komentojen ajamisen jälkeen resurssien allokoitumista voi seurata Azure portaalista, näkymä käyttöönoton onnistumisen jälkeen Azure portaalissa esitetty kuviossa 23.

```
New-AzResourceGroup -Name [redacted] -Location "westeurope"
```

Kuvio 21. Resurssiryhmän luonti Windows Powershell-sovelluksella.

```
New-AzResourceGroupDeployment -ResourceGroupName [redacted] -TemplateFile resurssimaaritykset1.6.json -TemplateParameterFile resurssinimimaaritykset1.6.json
```

Kuvio 22. Palveluiden käyttöönotto skripta

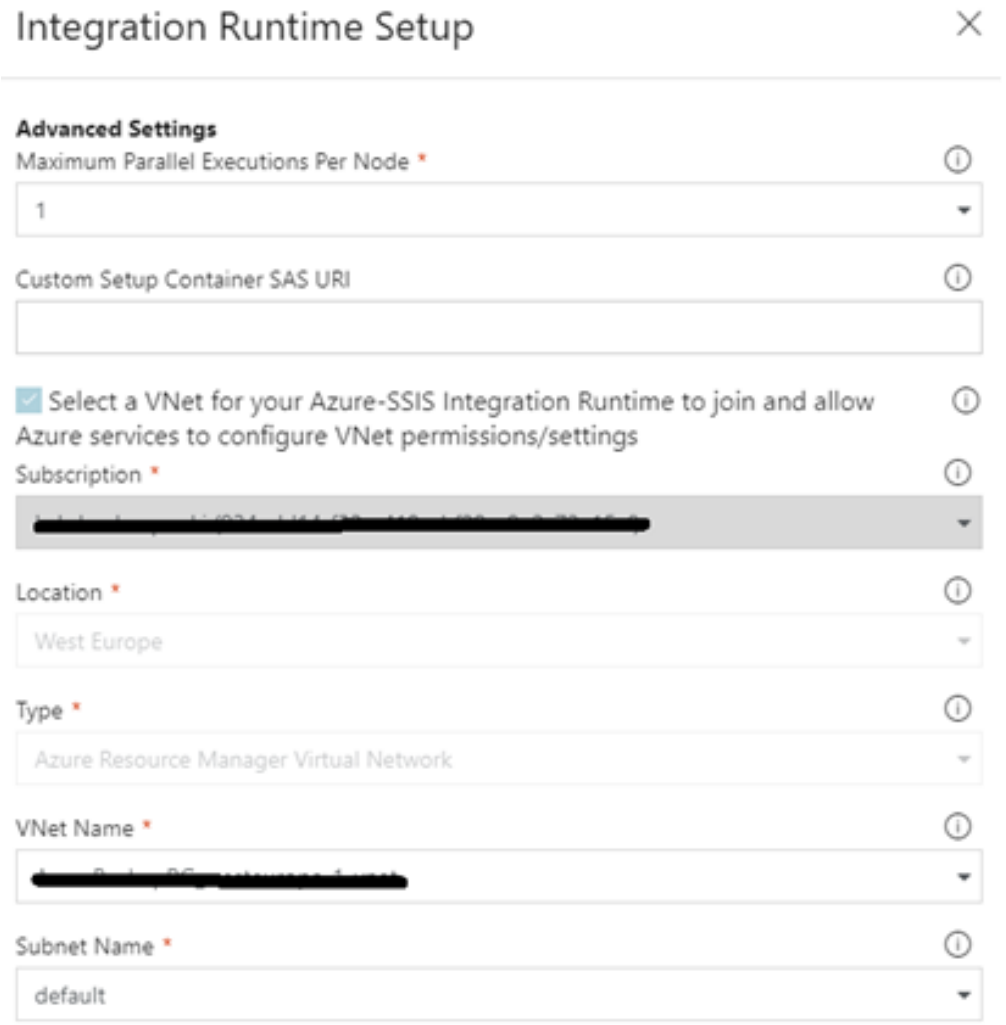


Kuvio 23. Azure Portaalin näkymä resurssien käyttöönoton jälkeen projektin resurssiryhmän alla.

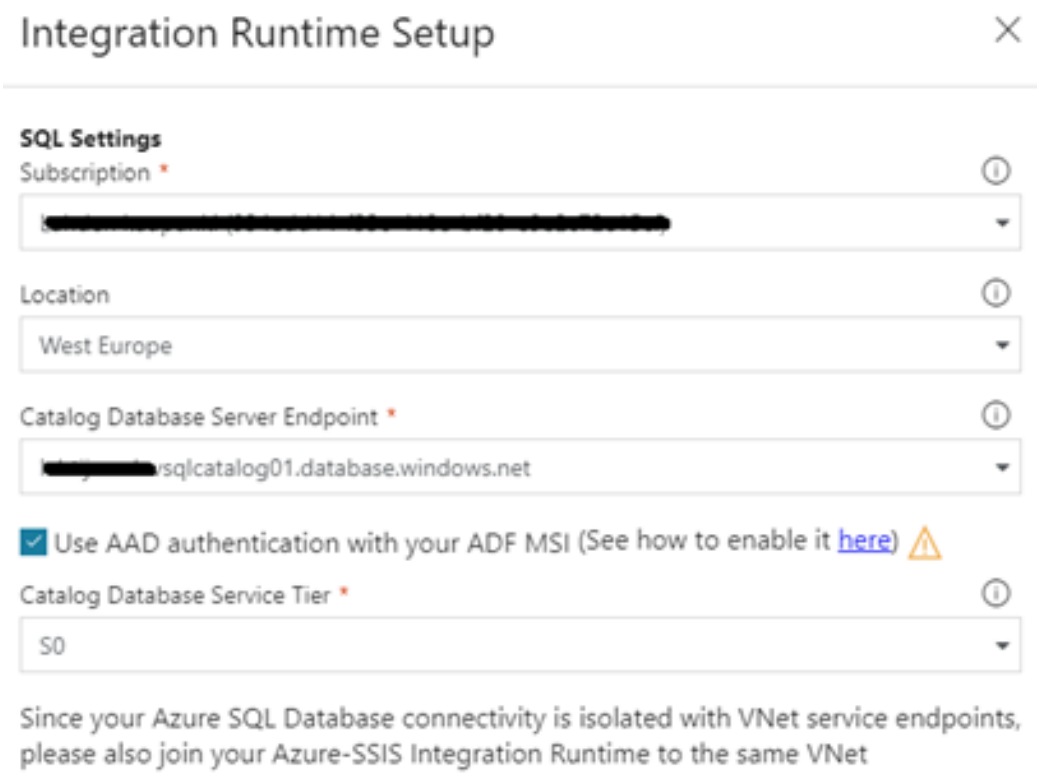
5.3.1 Azure Data Factory autentikaatio (ADF MSI)

ADF:lle ei ole olemassa IP-osoitetta, vaan se käyttää Azuren sisäistä resurssitunnusta. ADF käsittelee dataa Azure Blob Storagesta Azure-SSIS Catalog SQL-tietokannan kautta SQL Store-tietokantaan. Tämän takia ADF Integration runtime komponentti pitää määrittää toimimaan samassa aliverkossa missä SQL-kannat ovat.

Samalla määritetään myös SSIS Integration runtimen määritykset ja palvelutaso. SSIS Integration runtime ei ole Azuren resurssi vaan Data Factoryn sisäinen resurssi, minkä takia toimenpidettä ei voi sisällyttää JSON-pohjiin. Toimenpiteet esitetty kuvioissa 24 ja 25.



kuvio 24. Azure ADF SSIS Intergration runtime alustus ja virtuaaliverkon määritys.



kuvio 25. Azure ADF Azure SQL Catalog-kannan määritys ja MSI autentikoinnin aktivointi.

5.3.2 SQL kantojen oikeusryhmien luonti

ADF autentikoinnin määrittämisen jälkeen jäljellä on enää SQL-tietokantojen oikeuksien määrittäminen sekä ylläpitäjille että ADF-resurssille. Pääasiassa tietokantoja käsittelee ADF-resurssi, mutta jos manuaalisille muutoksille on tarvetta niin tietokantojen muokkaaminen SQL management studiolla hallintapalvelimelta on mahdollista.

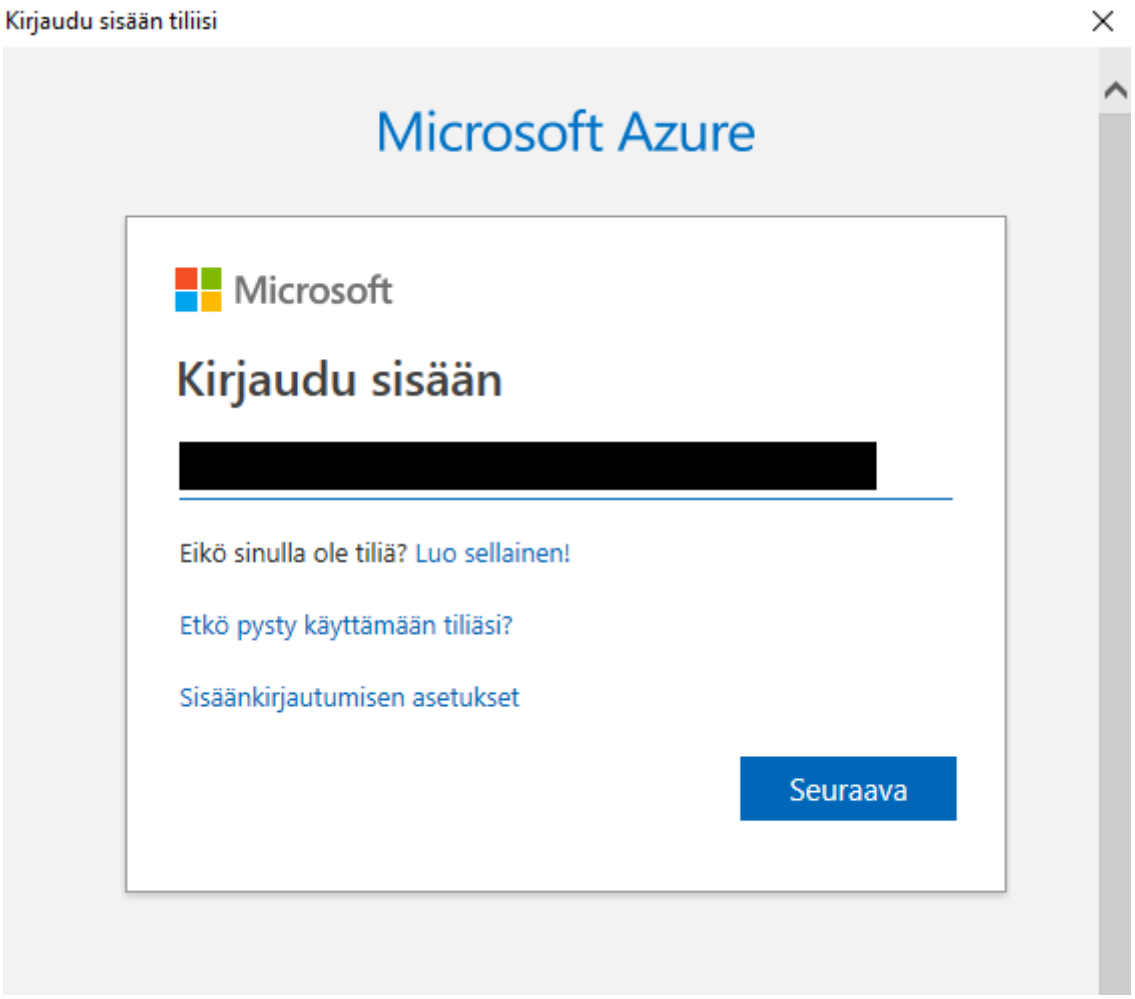
Jotta haluttu SG voidaan luoda, Powershelliin täytyy asentaa AzureAD-moduuli kuvion 26 komennola, minkä jälkeen muodostetaan yhteys AzureAD-resurssiin komennoilla, jotka löytyvät kuvioista 27 ja 28. Ylläpitotunnuksille luodaan Security Group Azuren Aktiivihakemistoon komennolla, joka on esitetty kuviossa 29. Luotuun AAD Securty Group-ryhmään lisätään ADF ServicePrincipal-objekti komennolla, löytyy kuviosta 30.

```
install-module AzureAD -Scope CurrentUser
```

Kuvio 26. Azure AD moduulin asennus Windows Powershell konsoliin

```
Connect-AzureAD
```

Kuvio 27. Yhteydenotto-komento Azure AD-palveluun



Kuvio 28. AzureAD tunnistauminen

```
$Group = New-AzureADGroup -DisplayName "[redacted]" -MailEnabled $false -SecurityEnabled $true -MailNickName "NotSet"
```

Kuvio 29. AAD Security Groupin luominen.

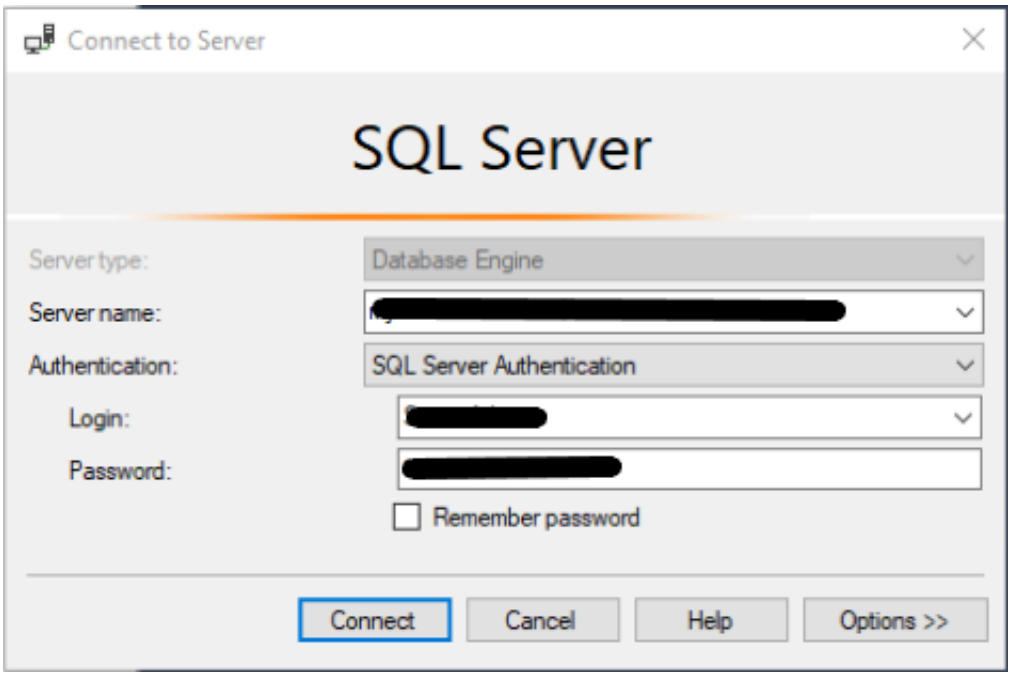
```
#Azure Data Factory Identity ID
Add-AzureADGroupMember -ObjectId $Group.objectId -RefObjectId [redacted]
```

Kuvio 30. ADF-resurssin lisääminen luotuun security group:iin ServicePrincipal-objektina

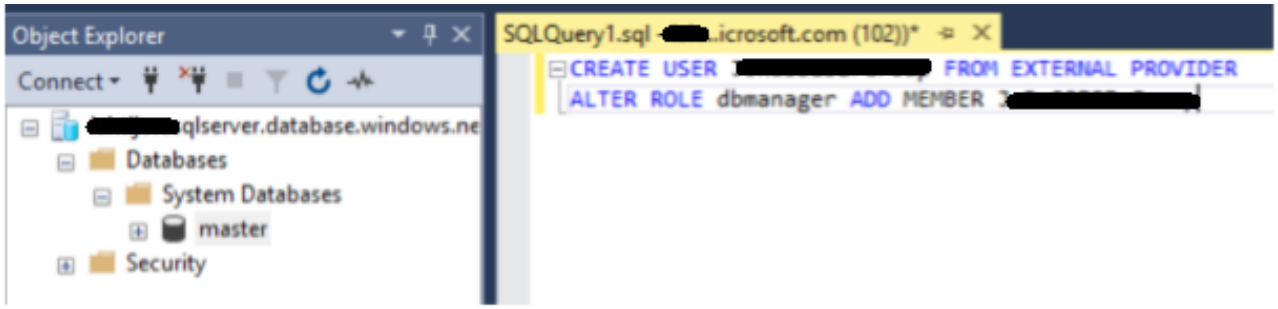
5.3.3 SQL-kannan alustaminen

SQL-Kannan alustaminen tehdään hallintapalvelimelta. Alustaminen antaa oikeudet tietokantojen manuaaliseen ylläpitämiseen, sekä ADF-resurssille. Ryhmän luomisen jälkeen otetaan etätyöpöytäyhteys hallintapalvelimeen ja kirjaudutaan Microsoft SQL management studioon tietokannan master-tunnuksella. Kirjautuminen SQL kantaan on esitetty kuviossa 31.

Yhteyden muodostamisen jälkeen SQL Catalog kantaan suoritetaan kuviossa 32 näkyvät kyselyt Master-tietokantaan. Tämän jälkeen jokainen AAD-tunnus mikä on lisätty kyseiseen ryhmään, saa oikeuden kirjautua ja muokata tietokantaa manuaalisesti tarvittaessa.



Kuvio. 31. Kirjautuminen SQL management studiolla SQL Catalog tietokantaan.



Kuvio 32. SQL kannan alustus komennot SQL management studiossa

5.4 Lopputulos

Infrastruktuuri piti pystyttää valmiiksi neljän viikon sisään projektin alkamisesta. Samanlaisia ympäristöjä luotiin projektin tarpeisiin kolme kappaletta: tuotanto-, kehitys- ja testiympäristö. Ylläpitäjän pyynnöstä ympäristöjä varten määritettiin vain yksi hallintapalvelin, minkä kautta jokaista ympäristöä pystyttäisiin ylläpitämään.

Tuotantoympäristön hallintapalvelimen käytön takia testi- ja kehitysympäristöjen hallintaan Azureen luotujen tuotanto-, kehitys- ja testiympäristön virtuaaliverkkoihin täytyi sallia verkkoliikenne hallintapalvelimelta. Loppukäyttäjät pystyvät lukemaan järjestelmän kerättyjä

tietoja power BI- tai excel-sovelluksella. Järjestelmän avulla käyttäjillä on käytössä mahdollisimman reaaliaikaista tietoa tarvitsemistaan asioita useista eri tietolähteistä.

Ympäristöjen suunnitteleminen ja infrastruktuurin määrittäminen ja pystyttäminen tehtiin ensimmäisen kolmen viikon aikana, minkä jälkeen ympäristöihin tehtiin pieniä muutoksia asiakkaan pyynnöstä ylläpitotyönä. Muutoksina pyydettiin kolmannen osapuolen henkilöiden pääsyn salliminen hallintopalvelimelle.

Kokonaisuudessaan tämä projekti onnistui kiireisestä aikataulusta huolimatta alkuperäisen suunnitelman mukaan, joskin pieniä muutoksia ja ympäristöön liittyvää verkkosuunnittelua ja kustannusvalvontaa täytyy selvittää vielä ympäristön käyttöönoton jälkeen. Järjestelmän avulla loppukäyttäjät saavat mahdollisimman ajanmukaista dataa haluamistaan asioista helposti ja nopeasti. Ympäristöön on tarvittaessa helppo lisätä tietolähteitä, sekä palvelunkapasiteettia on helppo kasvattaa toteutustavan takia.

5.4.1 Projektin tulevaisuus

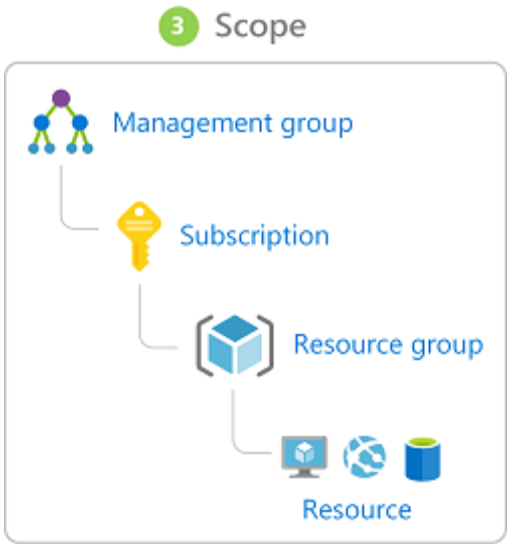
Ympäristöjen pystyttämisen jälkeen Azureen hankittiin Azure ExpressRoute on-premise ympäristöstä Azuren pilviympäristöön, minkä tarkoituksena on luoda ympäristöjen ylläpitäjille ja testaajille VPN-yhteys Azure pilveen paikallisen ympäristön kautta. Tähän ratkaisuun päädyttiin koska Azuren puolelle ei löydy löytynyt projektin aikana ratkaisua, minkä avulla käyttöä ja tietoliikennettä voitaisiin valvoa tehokkaasti.

Tulevaisuudessa tuo VPN-yhteys voitaisiin luoda suoraan hub-virtuaaliverkkoon palvelujen kehittymisen seurauksena. Azure Data Factory sisäisen putkiston, jolla halutut tiedot kerättiin käyttäjille, tehtiin kolmannen osapuolen toimesta. Käytännössä ADF-putkistoon määritettiin mitä tietoja ADF hakee Azure Blob Storagesta ja muuttaa sen luettavaan muotoon SQL Store-tietokantaan.

5.4.2 Azure RBAC-oikeudet

Azuren pilvipalveluiden määrän lisääntyessä ja ylläpitäjä määrän noustessa käyttäjien hallintaan on hyvä soveltaa normaaleja aktiivihakemisto-käytäntöjä. Resurssien luvittaminen voidaan tehdä helposti käyttämällä AAD-ryhmiä, minkä kautta oikeudet eri resursseihin voidaan antaa.

Tämä helpottaa käyttäjien hallintaa ja yksinkertaistaa oikeuksien lisäämistä merkittävästi, Oikeuksien eri tasot on esitetty kuviossa 33. Ulkopuolisille toimijoille paras käytäntö on lisätä oikeudet resurssi- tai resurssiryhmäkohtaisesti. Subscription eli tilaustason oikeus antaa käyttäjälle oikeudet jokaiseen resurssiryhmään kyseisen tilauksen alla.



Kuvio 33. Resurssien oikeuksien ulottuvuus. Ylemmälle tasolle annetut oikeudet periytyvät Azure ympäristössä alemmille tasoille. (Microsoft, 2019)

5.4.3 Infrastruktuuri koodina

Infrastruktuuri koodina käyttöönottotapana oli erittäin tehokas ja ympäristöjen pystyttäminen tapahtui ja ympäristön muokkaaminen tuleviin ympäristöihin on helppoa. Jotta IaC toimisi azure resurssien päivityksien jälkeen, ympäristön uusimpaan IaC-versioon täytyy päivittää Azure resurssien sovellusversio eli apiVersion-parametri, minkä voi nähdä kuviossa 34. PaaS-palveluiden ylläpidon helppouden takia Azure resurssien ylläpito on yksinkertaista.

```
{
  "type": "Microsoft.Sql/servers",
  "kind": "v12.0",
  "name": "[parameters('SQLserver02_name')]",
  "apiVersion": "2015-05-01-preview",
  "location": "westeurope",
  "scale": null,
```

Kuvio 34. apiVersion IaC ratkaisussa.

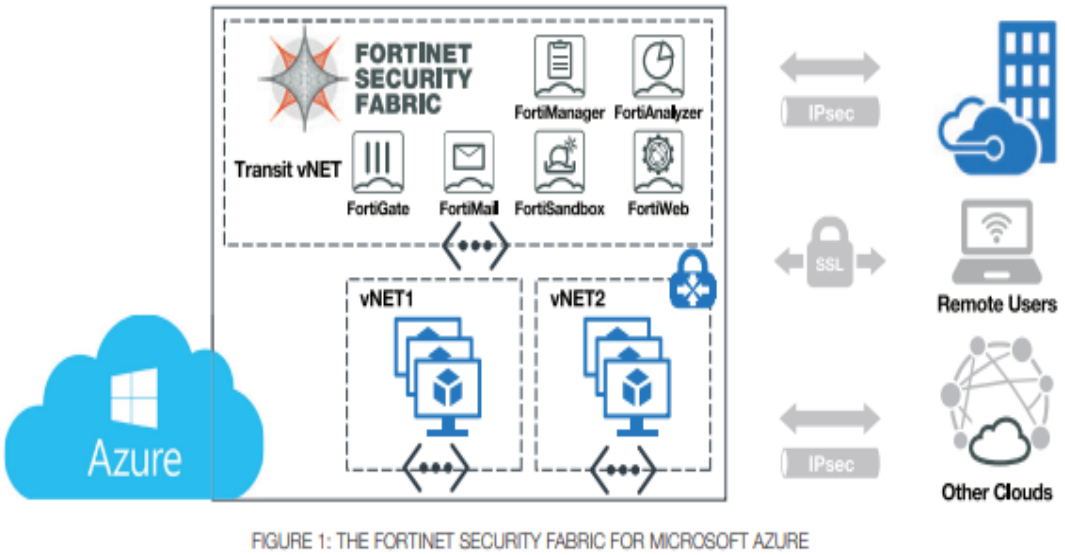
Pilvipalveluiden hallinnan tavat on parasta muokata yrityksen palveluympäristöjen ja resurssien määrän mukaan. Kolmannen osapuolen hallintasovellukset ovat loistava ratkaisu, jos ylläpidettävänä on useampia suuria pilviympäristöjä, mutta pienemmälle yritykselle pilvipalveluiden verkkosivu portaali täyttää lähes kaiken tarpeellisen.

Resurssien käyttöönottoa voidaan automatisoida käyttämällä IaC-käyttöönottoratkaisua, minkä avulla tarvittavia resursseja voidaan vaihtaa nopeasti jo ympäristön suunnittelu vaiheessa. Se myös mahdollistaa ympäristön eri tuotantovaiheiden pystyttämisen ja siirtämisen toiseen pilveen tarpeen vaatiessa ilman suurempaa vaivaa.

5.4.4 Verkkoliikenteen mahdollinen valvontaratkaisu

Verkkoliikenteen valvonta suoritettiin kierrättämällä ensisijaisesti kaikki liikenne Azure ExpressRouten kautta paikalliseen ympäristöön, jossa valvonta hoidetaan toistaiseksi. Tietolähteitä ja ylläpitäjiä varten on suunnitteilla verkkoliikenteen hallintaan ja valvontaan kolmannen osapuolen pilviratkaisu, minkä jälkeen liikennettä voitaisiin valvoa pilvinatiivilla ratkaisulla. Kyseinen Pilvipalomuuri sijoitettaisiin infrastruktuurissa hubin virtuaaliverkkoon, infrastruktuurin voi nähdä kuviosta 10 ja palomuurin infrastruktuurin löytää kuviosta 35.

Hubiin testattiin Fortinetin tarjoamaa palomuuriratkaisua, jonka avulla pilven tietoverkon valvonta voitaisiin suorittaa. Palomuuri toimisi hubissa valvoen verkkoliikennettä paikallisesta verkosta spokeihin ja päinvastoin. Hubissa sijaitseva palomuuri mahdollistaisi myös suorien yhteyksien tuonnin hallitusti pilvipalveluun. Käytännössä palomuuri toimisi niin, että palomuurin molemmille puolille luodaan oma virtuaaliverkko, johon liikenne reititetään. Paikallisesta ympäristöstä reititykset ohjattaisiin vNET1-puolelle ja pilvipalvelun liikenne vNET2-puolelle, mitkä näkyvät kuviossa 35.



Kuvio 35. Microsoft Azure Fortinet-palomuuri ratkaisuvaihtoehto (Fortinet, 2019)

6 YHTEENVETO

Projektin tavoitteena oli luoda raportointi ympäristö Lahden kaupungin käyttöön Microsoft Azure pilvipalveluun käyttäen pääasiassa palvelu alustana-ratkaisua. Palveluiden tuli olla käytettävissä asiakkaan työasemilta sijainnista riippumatta, minkä takia pilvipalvelut sopivat tähän projektiin loistavasti.

Ympäristöön oli tarkoitus tuoda dataa erinäisistä tietolähteistä julkisesta verkosta ja toisilta yrityksiltä. Datan laadusta riippuen, se tuotaisiin ympäristöön julkisen verkon yli ympäristöön asennetulla Linux-palvelimella tai VPN-yhteydellä paikallisen ympäristön kautta.

Projektissa suunniteltu ja pystytetty pilviympäristö onnistui ja on päivittäisessä käytössä loppukäyttäjillä asiakkaan ympäristössä. Palvelu toteutettiin PaaS-palveluina, minkä takia ympäristön ylläpitäminen on helppoa. Ympäristöön tuleva data tuodaan palveluun paikallisen ympäristön kautta VPN-yhteyden yli tai ne haetaan suoraan pilvipalveluympäristöön pilveen asennetulla linux-palvelimella. Pilvipalveluun luodut resurssit käsittelevät ympäristöön tuodun datan kolmannen osapuolen tekemien määrityksien mukaan, minkä jälkeen loppukäyttäjät voivat käyttää tietoja Power BI- tai Excel-sovelluksella.

Ympäristön kasvaessa hallinnan tarve kasvaa, minkä takia ympäristön RBAC-oikeuksien hallintaan tulee kiinnittää huomiota. Luodun ympäristön ja tulevien ympäristöjen hallinta on helpompaa, jos oikeudet tarvittaviin resursseihin voidaan antaa suoraan Azure aktiivihakemistossa olevilla ryhmillä.

Ympäristön verkkoliikenteen valvontaan on suunniteltu kolmannen osapuolen pilvisovellusta. Kolmannen osapuolen pilvipalvelusovellus ratkaisulla pilvipalvelun tietoverkonvalvonta paranee. Pilvipalveluympäristöön asennetulla palomuuriratkaisulla aikaisemmin käytössä ollut paikallisen ympäristön VPN-ratkaisu voitaisiin korvata suoraan pilveen tulevalla VPN-yhteydellä.

Pilvipalveluiden kehittymisen myötä niitä koskevat ongelmat vähenevät ja vahvuudet korostuvat. Yrityksien ei tarvitse enää huolehtia Infrastruktuurin raudan hallinnan siirtymisestä pois yrityksen omasta hallinnasta, koska pilvipalveluiden laatu on noussut todella korkeaksi. Pilvipalveluiden palvelutaso on noussut jo niin korkeaksi, että yrityksien tärkeimmät palvelut voidaan siirtää pyörimään pilvipalveluihin. Palveluiden keskittyminen suuriin datakeskuksiin vähentää käyttökatkojen riskejä ja mahdollistaa palveluiden käytön mistä tahansa maailmassa.

LÄHTEET

Amazon 2018a.A View of Cloud Computing Clearing The C [viitattu 18.8.2019]. Amazon Web Services. Saatavissa: https://s3.amazonaws.com/academia.edu.documents/34578652/a_view_of_cc.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1558633398&Signature=bcWbI5SSkD5gvwMKTRjw%2BXcO%2B8g%3D&response-content-disposition=inline%3B%20filename%3DA_View_of_Cloud_Computing_Clearing_the_c.pdf

Amazon 2018b. Cloud computing A study of infrastructure [viitattu 18.8.2019]. Amazon Web Services. Saatavissa: https://s3.amazonaws.com/academia.edu.documents/7299777/cloud%20computing%20a%20study%20of.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1558630974&Signature=%2FrQeR9B%2Fv23pOegxS8N%2Bw3uKvO4%3D&response-content-disposition=inline%3B%20filename%3DCloud_computing_A_study_of_infrastructur.pdf

Amazon Web Services 2019. AWS Documentation [viitattu 18.8.2019]. Amazon Web Services. Saatavissa: https://docs.aws.amazon.com/

Bulla, C., Hunshal, B & Mehta, S. 2016. Adoptation of Cloud Computing in Education Sstem: A Survey [viitattu 18.8.2019]. ResearchGate. Saatavissa: https://www.researchgate.net/profile/Chetan_Bulla/publication/304131151_Adoption_of_Cloud_Computing_in_Education_System_A_Survey/links/576775de08aedbc345f5fde9.pdf

Chang, J. 2019. 20 Best Cloud Management Software Solutions for 2019 [viitattu 18.8.2019]. Finances Online. Saatavissa: https://financesonline.com/cloud-management/

Computer Science and Applications 2019 Saatavissa: https://thesai.org/Downloads/Volume3No6/Paper%2016-A%20Survey%20on%20Resource%20Allocation%20Strategies%20in%20Cloud%20Computing.pdf

Convergence. 2019. Types of Cloud computing – Advantages and disadvantages! [viitattu 18.8.2019]. Saatavissa: https://convergenceservices.in/blog/corporate-blog/436-public-private-and-hybrid-cloud-computing-advantages-and-disadvantages.html

Editorial Staff. 2019. The comparison of the Best Cloud Computing Service Providers – AWS vs Azure vs Google Cloud [viitattu 18.8.2019]. WP ERP. Saatavissa: https://wperp.com/32339/best-cloud-computer-aws-vs-azure-vs-google-cloud/

EDUCBA. 2019. AWS vs Azure [viitattu 18.8.2019]. EDUCBA. Saatavissa: https://www.educba.com/aws-vs-azure/

Fortinet. 2018 Fortinet Security fabric extends advanced security for Microsoft Azure [Viitattu 18.8.2019]. Fortinet. Saatavissa: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/security-fabric-extends-security-azure.pdf

Hummer, W & Rosenberg, F & Oliveira, F & Eilam, T. 2013. Middleware 2013: Testing Idempotence for Infrastructure as Code [viitattu 18.8.2019].

Inmics-nebula. 2018. Pilven monet kasvot – IAAS, PAAS ja SAAS [viitattu 18.8.2019]. Inmimics nebula. Saatavissa: https://www.inmicsnebula.fi/fi/blogi/pilven-monet-kasvot-iaas-paas-ja-saas?language_content_entity=fi

Jungck, K & Rahman, S. 2011. Cloud Computing Avoids Downfall of Application Service Providers [viitattu 18.8.2019]. International Journal of information Technology Convergence and Services. Saatavissa: https://arxiv.org/ftp/arxiv/papers/1512/1512.00061.pdf

Kavis, J Michael. 2014. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) [viitattu 18.8.2019]. John Wiley & Sons, Inc, Hoboken, New Jersey.

Microsoft. 2019a. Get Started with Azure [viitattu 18.8.2019]. Microsoft. Saatavissa: https://docs.microsoft.com/en-us/azure/

Microsoft. 2019b. SLA summary for Azure services [viitattu 18.8.2019]. Microsoft Azure Documentation. Saatavissa: https://azure.microsoft.com/en-us/support/legal/sla/summary/

Microsoft. 2019c. Tutorial: Integrate Azure Key Vault in your Resource Manager template deployment [Viitattu 18.8.2019]. Saatavissa: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-use-key-vault

Mell,P, Grance, Timothy. 2011. The NIST definition of Cloud Computing [Viitattu 18.8.2019]. National Institute of Standards and Technology. saatavissa: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Mononen, J. 2016. Infrastruktuuri pilvipalveluna [viitattu 18.8.2019]. Lahden ammattikorkeakoulu. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/108314/Mononen_Jami.pdf?sequence=2

Raza, M & Watts, S. 2019. SaaS vs PaaS vs IaaS: What's The Difference and How To Choose [viitattu 18.8.2019]. BMC blogs. Saatavissa: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

Red Hat. 2019. What is middleware? [viitattu 18.8.2019]. Red Hat Enterprise. Saatavissa: https://www.redhat.com/en/topics/middleware/what-is-middleware

Ritesh,M. 2019. Azure for Architects: Implementing cloud design, Devops, IoT, and serverless solutions on your public cloud [viitattu 18.8.2019]. Saatavissa: https://azure.microsoft.com/en-us/resources/azure-for-architects/

Santos, N & Gummadi, P Krishna & Rodrigues, R. 2009. Towards Trusted Cloud Computing [Viitattu 18.8.2019]. Saatavissa: https://www.usenix.org/legacy/event/hotcloud09/tech/full_papers/santos.pdf

Sebastiani, M & Aggarwal, M. 2014. Optimizing your cloud with cloud orchestration [viitattu 18.8.2019]. IBM. Saatavissa: https://www.ibm.com/blogs/cloud-computing/2014/10/07/optimizing-cloud-cloud-orchestration/

Sunilkumar, S Manvi & Gopal, K. 2014. Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey [viitattu 18.8.2019]. Journal of Network and Computer Application. Saatavissa: https://www.sciencedirect.com/science/article/pii/S1084804513002099

Sutter, C. 2017. What the New Multi-Cloud World Means for IT [viitattu 18.8.2019]. BMC blogs. Saatavissa: https://www.bmc.com/blogs/new-multi-cloud-world-means/

Vinothina, V & Sridaran, R & Padmavathi, G. 2012. A Survery on Resource Allocation Strategies in Cloud Computing [viitattu 18.8.2019]. Internation journal of Advanced