

Mike Kuusela

PK-yritysten IT-järjestelmien tukeminen pilvipalveluilla

Opinnäytetyö
Tieto- ja viestintätekniikan koulutus

2019



**Kaakkois-Suomen
ammattikorkeakoulu**

Tekijä/Tekijät	Tutkinto	Aika
Mike Kuusela	Insinööri (AMK)	Marraskuu 2019
Opinnäytetyön nimi PK-yritysten IT-järjestelmien tukeminen pilvipalveluilla <div> <div>48 sivua</div> <div>3 liitesivua</div> </div>		
Toimeksiantaja Bit Group Finland Oy		
Ohjaaja Yliopettaja Martti Kettunen		
Tiivistelmä <p>Opinnäytetyön tavoitteiksi asetettiin potentiaalisten puutteiden ja parannuskohteiden havaitseminen tyypillisten pien- ja keskisuurten yritysten IT-järjestelmistä, sekä näiden järjestelmien toiminnallisuuden täydentäminen Amazon Web Services- ja Microsoft Azure pilvipalveluilla. Työn pohjimmaisena tarkoituksena oli tuottaa työn aihealueista koostettu tietopohja sekä jatkoa varten testausympäristö.</p> <p>Työssä suoritettiin teoreettinen vertailu näiden kahden pilvipalveluntarjoajan välillä, jotta optimaalisimman CSP:n valinta käyttökohteittain löytyisi helpommin. Kohteeksi valittiin PK-yritykset, jotta laajahko aihealue saataisiin rajattua spesifisimmillä käyttötarkoituksilla ja ympäristöillä. AWS ja Azure valittiin palveluntarjoajien joukosta markkinadominanssinsa ansiosta.</p> <p>Työn alkuvaiheiden initiaalinen painotus oli alan dokumentaation tutkimisella ja pian kiintopisteeksi muodostui PK-yritykset. Teoriaosiossa myös käytiin aiherajatusti läpi Amazon Web Services sekä Azure ja näiden kahden CSP:n välinen vertailu. Tämän lisäksi teoriaosuudessa korostui yritystoiminnalle ominaiset infrastruktuurilliset elementit kuten toimialueet, virtuaalikoneet ja -verkot, sekä järjestelmien redundanssi. Käytännön osiossa toteutettiin Windows-järjestelmiin vahvasti nojaavan paikallisen testiympäristön laajennus Azuren pilveen IPsec site-to-site VPN:n kautta, sekä luotiin Windows-järjestelmiin pohjautuva hybriditoimialue.</p> <p>Tavoitteet saavutettiin pääasiallisesti ja lopputuloksena syntyi opinnäytetyön toimeksiantaneelle yritykselle aihepiiriä avaava dokumentaatio sekä toimialueen hybridiympäristö tämän tueksi. Työ antaa hyvän pohjan pilviympäristön kanssa työskentelyyn ja jatkoimplementaation suunnitteluun.</p>		
Asiasanat Amazon Web Services, Microsoft Azure, pilvipalvelu, PK-yritys		

Author (authors)	Degree	Time
Mike Kuusela	Bachelor of Information Technology	November 2019
Thesis title		
Enhancing SME IT infrastructure with cloud services		48 pages 3 pages of appendices
Commissioned by		
Bit Group Finland Ltd.		
Supervisor		
Martti Kettunen, Principal Lecturer		
Abstract		
<p>The objectives of this thesis were to identify potential shortcomings and areas for improvement in typical small and medium enterprise IT systems and to supplement the functionality of these systems with Amazon Web Services and Microsoft Azure cloud services. The main purpose of the thesis was to provide a knowledge base constructed of the discussed topics and a testing environment for further studies.</p> <p>A theoretical comparison was made between the two cloud providers to help find the optimal CSP for each scenario. Small and medium-sized enterprises (SMEs) were selected in order to delimit the broader theme to specific uses and environments. AWS and Azure were chosen among service providers due to their respective market dominance.</p> <p>Initial emphasis in the early stages of the work was on studying relevant documentation, and soon SMEs became the focus. The theory section also dealt with the subject matter of Amazon Web Services and the comparison between Azure and the two CSPs. In addition, the theoretical part emphasized business-specific infrastructure elements such as domains, virtual machines and networks, as well as system redundancy. The practical section included extending the local test environment, which relied heavily on Windows systems, over to the Azure cloud via IPsec site-to-site VPN, as well as created a Windows-based hybrid domain.</p> <p>The goals were mainly achieved, and the end result was a valuable documentation for the company commissioning the thesis, including a hybrid-domain testbed for further development. The work provides a good basis for working with the cloud environment and planning for further implementation.</p>		
Keywords		
Amazon Web Services, Microsoft Azure, cloud services, SME		

SISÄLLYS

TERMISTÖ.....	6
1 JOHDANTO	7
1.1 Tausta	8
1.2 Opinnäytetyön tavoitteet.....	8
1.3 Tutkimusmenetelmä	9
1.4 Tietoperusta	9
2 PILVILASKENTA.....	10
2.1 Palveluntarjoajat ja markkinaosuudet.....	11
2.2 Kustannukset	12
2.3 Sumu pilven jatkeena	13
3 PK-YRITYKSET JA IT-JÄRJESTELMÄT	14
3.1 IT-arkkitehtuuri	16
3.2 Toimialue ja Active Directory.....	17
3.3 VPN.....	18
3.4 Järjestelmän saatavuus.....	18
3.5 Järjestelmien käyttöönottomalli	19
4 AMAZON WEB SERVICES.....	21
4.1 Elastic Computer Cloud (EC2)	22
4.2 Simple Storage Service (S3) ja Elastic Book Store (EBS).....	22
4.3 AWS BCDR.....	23
4.4 AWS IAM.....	24
5 MICROSOFT AZURE.....	24
5.1 Azure VM	26
5.2 Azure Storage ja BCDR	28
5.3 Tietoturva	28
5.4 Azure Active Directory.....	30
5.5 Azure Active Directory Domain Services.....	31

6	VERTAILU.....	32
7	INFRASTRUKTUURIN LAAJENTAMINEN AZUREN PILVEEN	35
7.1	Testiympäristö	36
8	JOHTOPÄÄTÖS	42
	LÄHTEET	45
	LIITTEET	

Liite 1. Kuvaluettelo

TERMISTÖ

ACL	<i>Access-control List</i>
AD	<i>Active Directory</i>
AD DS	<i>Active Directory Domain Service</i>
AWS	<i>Amazon Web Services</i>
BCDR	<i>Business Continuity and Disaster Recovery</i>
CSP	<i>Cloud Service Provider</i>
DR	<i>Disaster Recovery</i>
DC	<i>Domain Controller</i>
EBS	<i>Elastic Book Store</i>
EC2	<i>Elastic Compute Cloud</i>
LDAP	<i>Lightweight Directory Access Protocol</i>
IaaS	<i>Infrastructure as a Service</i>
O365	<i>Microsoft Office 365</i>
OU	<i>Organizational Unit</i>
UPN	<i>User Principal Name</i>
PaaS	<i>Platform as a Service</i>
SaaS	<i>Software as a Service</i>
SLA	<i>Service Level Agreement</i>
SSO	<i>Single Sign-on</i>
TCOS	<i>Total Cost of Ownership</i>
VHD	<i>Virtual Hard Disk</i>
VM	<i>Virtual Machine</i>
VPN	<i>Virtual Private Network</i>

1 JOHDANTO

Vankka IT-infrastruktuuri on yritykselle ehdottoman tärkeä, sillä se takaa yrityksen toiminnan saumattoman jatkuvuuden. Teknologisen kehityksen sekä tarjonnan alati muuttuvan luonteen myötä herää kuitenkin kysymys, onko täysin paikallinen eli ns. perinteinen on-premise-ratkaisu aina paras mahdollinen vaihtoehto? Pilvipalvelumalli minimoi fyysisen raudan tarpeen ja sen tuomat vaatimukset: tilan palvelinkaapeille, jäähdytyksen, redundanttisen virransyötön, sekä ammattitaitoisen henkilöstön pyörittämään tätä järjestelmää.

Pilvipalvelut valtaavat jatkuvasti suurempaa markkinasiivua informaatiotekniikan saralla, pääosin IaaS-, PaaS- ja SaaS-palvelumallien johtamina. Yhtenä avaintekijänä murroksen takana on tietoverkkojen kehitys, jonka myötä ollaan päästy tiedonsiirtonopeuksiin, joilla saadaan täytettyä hyväksyttävästi suurin osa vaatimuksista palvelujen pilvestä pyörittämiseen. Tarkastelen työssäni kirjoituksen ajanhetkellä kahta suurinta olevaa CSP:tä (Cloud Service Provider) eli pilvipalveluntarjoajaa, Amazonia sekä Microsoftia. Työssäni tarkastelemista palveluntarjoajista keskeisin tulee kuitenkin olemaan Microsoft, ja vielä tarkemmin heidän tuotteensa Azure. Kohteeksi valittiin PK-yritykset, jotta laajahko aihealue saataisiin rajattua spesifisimmillä käyttötarkoituksilla ja ympäristöillä, mutta myös yleisyytensä ansiosta. Suomessa PK-yritysten käsittävien yritysten osuus kaikista yrityksistä on noin 99,8 % (Tilastokeskus 2013.)

Työn toimeksiantaja on kotkalainen Bit Group Finland Oy, eli vuonna 2005 perustettu ICT-alan asiantuntijayritys, jonka toimialaan kuuluu pääsääntöisesti ylläpito, konsultointi ja laitemyynti. Palveltavina pitkäaikaisina asiakkaina on sekä suuria että pieniä yrityksiä. (Vahteri 2019.)

Bit Group Finland Oy oli myös osallisena työn suuntauksen määrittämisessä työn edetessä sekä tarjosi työhön tarvittavat resurssit: palvelinraudan, verkkolaitteet, staattisen julkisen IP-osoitteen ynnä muuta.

1.1 Tausta

Idea työlle syntyi, kun sain työnantajaltani projektiluontoisen tehtävän tutkia pilvipalveluita ja niiden soveltuvuutta eri käyttötarkoituksiin. Tutkimus kohdentui nopeasti Microsoftin Azure-pilvipalveluun, jonka tarjoamista asiakkaille IT-ratkaisuna pohdittiin. Microsoft valittiin pilvipalveluntarjoajaksi olemassaolevien järjestelmien integraatiomahdollisuuksien vuoksi.

Opinnäytetyöni nojaa siis hyvin vahvasti yritysympäristöön ja erityisesti PK-yrityksiin, sillä kokonsa ja resurssiansa puolesta niiden IT-ympäristö ei välttämättä ole optimaalinen.

Tarve tälle tutkimukselle syntyi osittain asiakkaan toiveesta sekä tilannekartoituksesta, miten eri IT-kysymyksiä tulisi lähestyä lähitulevaisuudessa.

1.2 Opinnäytetyön tavoitteet

Tämän opinnäytetyön tavoitteena oli kartoittaa Amazonin (AWS) ja Microsoftin (Azure) tarjoamat erityisesti PK-yrityksille soveltuvat pilvipalvelut sekä suunnitella ja toteuttaa testiympäristö, jossa paikallinen infrastruktuuri laajennettiin Azuren pilveen, tässä tapauksessa site-to-site IPsec VPN -tunnelin kautta. IaaS-palvelut valittiin lähemmin tarkasteltavaksi, sillä infrastruktuurin skaalautuminen, kustannustehokas redundanssi sekä Disaster Recovery (DR) ovat tärkeitä kysymyksiä kohdekategorialle.

Opinnäytetyön tutkimusongelmaksi muodostui ryhmä toisiinsa punoutuneita kysymyksiä, joten tutkimuskysymykset voidaan kompaktisti esittää seuraavanlaisesti:

1. Kannattaako PK-yrityksen hyödyntää pilvipalveluita?
2. Valitaanko palveluntarjoajaksi Amazon Web Services vai Microsoft Azure?
3. Voiko Windows-toimialuetta tai muita tärkeitä funktioita toteuttaa pilvipalveluilla järkevästi?

Valintojen ja tapauskohtaisten skenaarioiden runsauden johdosta työssä edetään iteratiivisesti rakentaen aina edellisen tiedon päälle.

Palveluntarjoajien välisellä vertailulla pyritään osoittamaan geneerinen soveltuvuus kohderyhmälle ottaen huomioon järjestelmien yhteensopivuus,

käyttöönoton sujuvuus, hinta sekä tarjottujen palveluiden kattavuus. Testiympäristön rakentamisella ja palveluiden käyttöönnotolla pyritään konkreettisesti saamaan ensikäden tietoa konfigurointiprosessista sekä osoittamaan toimivuus yleisellä käyttöympäristöllä.

1.3 Tutkimusmenetelmä

Työssä käytetty tutkimusmenetelmä on yhdistelmä, joka ottaa vaikutteita kvantitatiivisen (määrällisen) että kvalitatiivisen (laadullisen) tutkimustyön malleista. Toimintatutkimuksen ominaisiin piirteisiin lukeutuu tapauskohtaisuus, käytännönläheisyys sekä pyrkimys toiminnan muutokseen. Toimintatutkimuksen oppi-isänä pidetään Kurt Lewiniä. ”Ei toimenpiteitä ilman tutkimusta, eikä tutkimusta ilman toimenpiteitä”. (Lewin 1946, 38.)

Toimintatutkimuksen malli on syklinen siinä mielessä, että tutkimuksen edetessä havainnoidaan, analysoidaan sekä muokataan toimintaa iteraatiokierroksissa. Toimintatutkimus myös pyrkii aina muuttamaan tutkijaa itsessään tutkimukseen osallistujana. Etuna tässä on se, että tutkija saa näin ollen kattavamman kuvan ongelmasta. Havainnointi toimiikin yhtenä ydinmetodina tiedonkeruussa. (Kananen 2015, 33.)

Tutkimuskysymys tulee pysymään vakiona, mutta mallin mukaisesti lähestymistavat sekä menetelmät saavat lopulliset muotonsa työn lähestyessä valmistumista. Tietoa kerätään ja sovelletaan tutkimusmenetelmän mukaisesti mahdollisimman monipuolisista lähteistä: kirjat, verkkodokumentit, vastaavat insinööriyöt, julkaisut.

1.4 Tietoperusta

Teoria- ja tietopohja koostuu pääasiallisesti yritysten ja palveluntarjoajien dokumentoinnista, kirjoista, työn edetessä omista havainnoista sekä erilaisista internet-lähteistä. Microsoftin ja Amazonin verkkosivuillansa tarjoama dokumentaatio ja palveluiden esittely tarjosi runsaasti ajankohtaista lähdemateriaalia. Pilvisektorin vauhdikkaan kehittymisen myötä relevantin, ajankohtaisen kirjallisuuden löytäminen osoittautui melko haastavaksi.

Työtä sivuavia pilvipalveluihin liittyviä kirjoja löytyi kohtalaisesti, mutta suurta osaa näistä ei käytetty lähteinä vanhentuneen tiedon takia, vaan pääasiallisesti suuntaa-antavina referenssitöinä.

2 PILVILASKENTA

Pilvilaskennalla (engl. Cloud Computing) tarkoitetaan mallia, jossa tarvittavia prosessointi- ja tiedonhallintaresursseja käytetään tietoverkon yli oman paikallisen laitteen sijasta. Palvelun tarjoamiseen käytettävä laitteisto sijaitsee fyysisesti datakeskuksissa. NIST (National Institute of Standards and Technology) määrittää sen koostuvan viidestä ominaisesta piirteestä, kolmesta palvelumallista ja neljästä käyttöönottomallista. (Mell ja Grance 2011, 2–3.)

NIST listaakin ominaispiirteet seuraavasti:

- Itsepalvelu. Käyttäjä voi itse provisoida esim. verkkolevykapasiteettia ilman yhteydenottamista palveluntarjoajaan.
- Saatavuus. Ominaisuudet ovat saatavilla verkon ylitse, sekä pääsy palveluihin onnistuu eri päätelaitteilla.
- Resurssivaranto. Palveluntarjoajan laitteiston resurssit pystytään tarjoamaan usealle asiakkaalle samanaikaisesti multi-tenant-mallin mukaisesti dynaamisesti kysynnän mukaisesti. Esimerkkejä resursseista ovat prosessointiteho ja tallennustila.
- Nopea joustavuus. Provisiointi sekä resurssien vapautus tapahtuu nopeasti ja joissakin tapauksissa automaattisesti.
- Käytön seuraaminen. Palveluntarjoaja optimoi resursseja käytön mukaisesti. Monitorointi tarjoaa avoimuuden molemmille osapuolille.

NIST:n mukaiset palvelumallit:

- SaaS (Software as a Service). Asiakas käyttää applikaatioita suoraan pilvestä esim. verkkoselaimella, eikä hänellä ole back-end-hallintaa. Esimerkkejä: Microsoft Office 365, Google Apps.
- PaaS (Platform as a Service). Palveluna alustan tarjoaminen asiakkaan applikaatiotarpeisiin. Ei back-end-hallintaa. Esimerkkejä: Microsoft Azure, AWS.
- IaaS (Infrastructure as a Service). Laskentaresurssien tarjoaminen asiakkaan tarpeisiin. Ei pilvi-infrastruktuurin back-end-hallintaa, mutta palveluun kuuluvan esim. palomuurin hallinta on. Esimerkkejä: Microsoft Azure, Amazon Elastic Compute Cloud (EC2).

Käyttöönottomalleihin kuuluu yksityinen pilvi, jaettu pilvi, julkinen pilvi ja hybridiratkaisu. Azure kuuluu Microsoftin mukaan (2019a) julkisen pilven luokitukseen, joka on kaikista yleisin markkinoilla. Tässä mallissa asiakkaan käyttämän raudan, ohjelmistojen ja yleisen infrastruktuurin omistus on kolmannella osapuolella eli palveluaan tarjoavalla yrityksellä. Näin ollen asiakas voi helposti skaalata investointiaan järjestelmätarpeittensa mukaan ylös- tai alaspäin. Nämä mallit ovat yleisesti pilvipalveluntarjoajien luomia ja hallitsemia. (Tutunea 2014.) NIST:n määrityksien ulkopuolelta löytyy kuitenkin useita variaatioita, joista esimerkkeinä ovat Firewall-as-a-Service (FWaaS) sekä Blockchain-as-a-Service (BaaS).

2.1 Palveluntarjoajat ja markkinaosuudet

Kokonsa ja kasvunopeutensa ansiosta pilvipalvelut ovat yksi tärkeimmistä sektoreista IT-alalla. Vuonna 2018 pilvi-infrastruktuuriin sijoitettiin 80 miljardia dollaria, kun vuonna 2017 vastaava luku oli vain 55 miljardia. (Canalys 2019.) Vuoteen 2024 mennessä markkinoitten odotetaan kasvavan vielä n. 500 %. Kuvassa alla esitettynä palveluntarjoajien vuotuinen kasvu prosentteina.

Worldwide cloud infrastructure spending and annual growth
Canalys estimates: Q4 2018

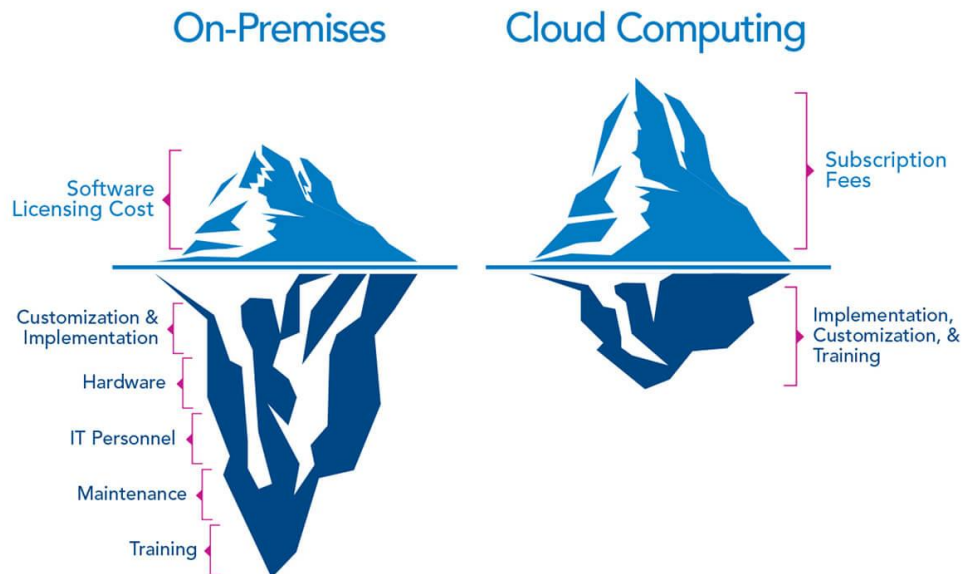
Vendor	Q4 2018 (US\$ billion)	Q4 2018 Market share	Q4 2017 (US\$ billion)	Q4 2017 Market share	Annual growth
AWS	7.3	32.3%	5.0	32.2%	+46.3%
Microsoft Azure	3.7	16.5%	2.1	13.7%	+75.9%
Google Cloud	2.2	9.5%	1.2	7.6%	+81.7%
Alibaba Cloud	1.0	4.2%	0.6	3.5%	+73.8%
IBM Cloud	0.8	3.6%	0.6	4.2%	+27.6%
Others	7.7	33.8%	6.1	38.9%	+26.7%
Total	22.7	100.0%	15.6	100.0%	+45.6%

Kuva 1. Pilvipalveluiden markkinaosuudet ja kasvu (Canalys 2019.)

Listalla mainitsemattomiin merkittäviin palveluntarjoajiin kuuluu mm. Oracle, Rackspace, VMware, SAP sekä Salesforce.

2.2 Kustannukset

Paikallisen järjestelmän totaalihintaa eli total cost of ownership (TCOS) muodostuu useasta ilmeisestä sekä vähemmän ilmeisestä lähteestä, kun taas pilvipalvelun hintalappu on yksiselitteisempi. Usein nykyään kuitenkin käytetään yhdistelmää, jossa hyödynnetään pilveä paikallisen järjestelmän tueksi. Alla oleva kuva 2 havainnollistaa kustannuslähteet karkeasti.



Kuva 2. Paikallisen infrastruktuurin ja pilven kustannuksien graafinen esitys (Kodak 2017.)

Edellä mainittujen kohtien lisäksi reilussa vertailussa pitää myös ottaa huomioon derivatiiviset ilmiöt:

- Menoerät ovat ennalta-arvattavia, ei esimerkiksi laiterikosta aiheutuvia kuluja. On huomioitavaa, että laiterikoista aiheutuu joskus mittavia katkoksia ennenkuin korvaava järjestelmä saadaan pystyyn.
- 24/7-tuen ja skaalautuvuuden/joustavuuden arvo
- Tietoturva on ulkoistettu (myös fyysinen). Esimerkiksi ransomwarea vastaan hyvin turvallinen systeemi, sillä virtuaalikoneilla on melko helppo luoda uusia instansseja.
- Tarvittava tila laitteistolle sekä toimitilojen muuttaminen, eli fyysisen sijainnin vaihdos onnistuu sujuvammin.
- Kertainvestointiin verrattuna säästetty pääoma voidaan uudelleen allokoida eli sijoittaa muuhun toimintaan.

2.3 Sumu pilven jatkeena

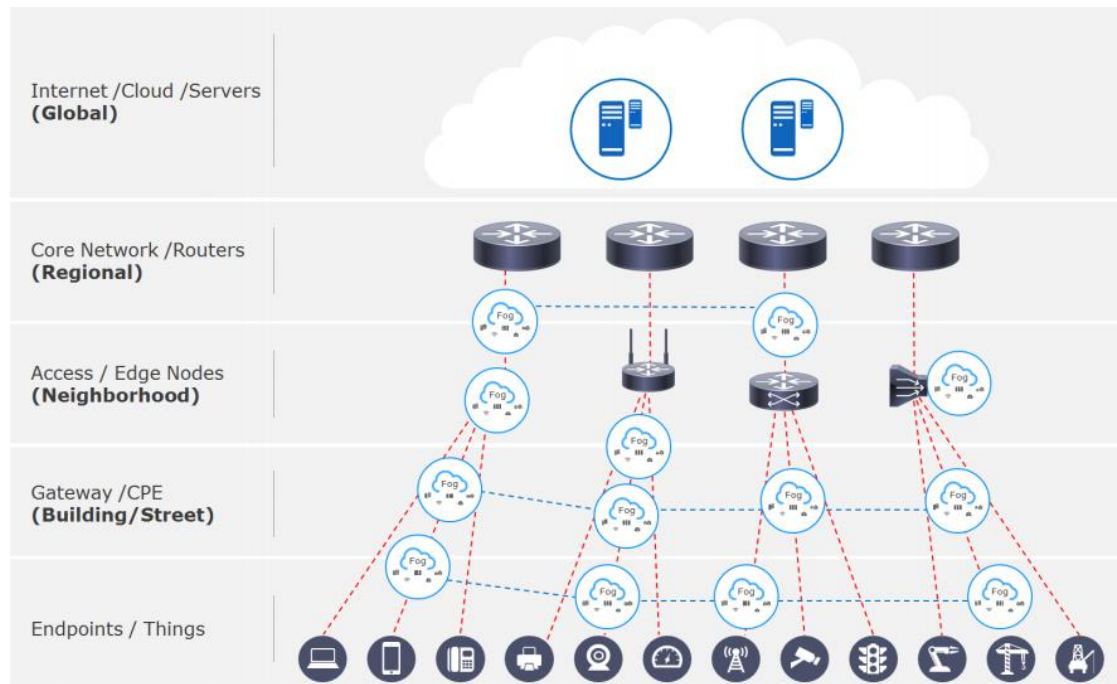
Reunalaskenta (edge computing) on konsepti, jossa tuotettu data säilötään ja prosessoidaan lähellä alkuperää. Tämä on looginen jatkumo pilvipalvelumallille. Software Defined Networking- ja Network Function Virtualization -teknologiat ovat keskeisessä asemassa mahdollistamassa lokaattiotietoisien, tehokkaan tiedonsiirron heterogeenisestä laitekannasta koostuvasta verkon reunasta. (ETSI 2015.)

Ciscon (2014) määrittelemä sumulaskenta (fog computing) on reunalaskentaan perustuva standardi, jonka mukaisesti uusi verkkoarkkitehtuuri määritetään. Internet of Things -laitteiden määrän räjähdysmäinen kasvu ja mobiilipäätelaitteiden kehitys on johtanut tämän uuden verkkoarkkitehtuurin tarpeeseen.

Mainittavina ongelmakohtina nykyisessä keskitetyn pilven palvelumallissa ovat runkoliityntäyhteyden rasitus, latenssi, heikohko spektraalinen tehokkuus eli bit/s/Hz. Täytyy ottaa myös huomioon, että IoT-laitteet eivät välttämättä keskustele Internetprotokollan eli IP:n välityksellä. Sumua voidaankin pitää pilven jatkeena, sillä loppukädessä valikoitu data kulkee aggregoituna pilvipalveluntarjoajalle ja sieltä takaisin isossa osassa tapauksista. (Ai ym. 2018.)

IDC (2017) arvioi, että vuoteen 2025 mennessä n. 45 % maailman datasta on siirretty lähemmäksi verkon reunaa, ja että sumu on ainoa arkkitehtuuri, joka mahdollistaa IoT-, 5G- ja AI-teknologioiden valjastamisen täyteen potentiaaliinsa. Sumun rakennuspalikkana on hyvin pitkälti ”fog node”, eli mikä tahansa laite, joka prosessoi dataa, omaa tallennustilaa sekä pystyy liittymään verkkoon. (Cisco 2015.)

Kuvassa 3 esitettynä OpenFog-järjestön referenssiarkkitehtuuri, jossa hajautettu laitteisto hoitaa laskenta- ja tiedonsiirtofunktiot lateraalisesti lähellä reunaa, pääasiallisesti langattomasti. Ylempänä hierarkiassa verkossa sijaitsee jykevämpiä aggregaattinodeja, jotka hoitavat tarvittaessa liittynnän runkoyhteyteen. (OpenFog 2017.)



Kuva 3. Fog-verkon hierarkinen referenssiarkkitehtuuri (OpenFog 2017.)

OpenFog Consortium on nykyään Industrial Internet Consortiumiin (IIC) liittynyt teknologiajättien (Cisco, Intel, IBM ym.) muodostama yhteisö, joka kehittää yhteistyössä ETSI:n ja IEEE:n kanssa Ciscon määrittelemää horisontaalista sumuverkkoarkkitehtuuria.

3 PK-YRITYKSET JA IT-JÄRJESTELMÄT

Ennen järjestelmän käyttöönottoa tulisi kartoittaa yrityksen tarpeet, jotta niihin voitaisiin tarjota ratkaisut parhaalla mahdollisella tavalla. Keskitymme oletusarvoisesti IT-järjestelmiä käyttävän PK-yrityksen yleisiin tarpeisiin ensiksi. PK-yritys on Tilastokeskuksen määritelmän mukaan yritys, joka on henkilöstökooltaan alle 250 ja on vuosiliikevaihdoiltaan alle 43 miljoonaa euroa. PK-yritys käsitteenä sisältää mikroyritykset, pienyritykset ja keskikokoiset yritykset. (Tilastokeskus 2019.)

Vuonna 2012 Suomessa 99,8 % yrityksistä oli kooltaan alle 250 henkilöä käsittäviä (Tilastokeskus 2013.)

Kuvasta 4 huomataan, että vain noin puolet Suomessa vuonna 2011 aloittaneista yrityksistä jatkoivat toimintaansa ensimmäisen viiden vuoden jälkeen. Tämä statistinen trendi ei ole poikkeuksellinen verrattaessa vastaaviin tilastoihin. (Tilastokeskus 2017.)

Aloituvuosi	Aloitaneita yrityksiä	2011	2012	2013	2014	2015	2016	3 ensimmäisen vuoden lopetukset	Toiminta jatkuu 2016 jälkeen
2011	32 390	5,8	12,3	10,2	8,9	6,0	4,9	28,3	51,9
2012	31 169	..	6,0	12,2	11,4	7,4	5,9	29,6	57,1
2013	30 235	5,7	13,1	9,2	7,1	28,0	64,9
2014	28 770	5,6	10,9	9,1	25,5	74,5
2015	28 310	5,3	10,6	..	84,1
2016	28 532	4,8	..	95,2

Kuva 4. Lopettaneiden yritysten osuudet tarkasteluvuosina (Tilastokeskus 2017.)

Harvalla PK-yrityksellä on omaa laajaa dedikoitua IT-osastoa, jolloin välillä tarvittavat hankkeet ja toimenpiteet suorittaa palkattu kolmas osapuoli. Usein tämä kuitenkin johtaa hitaampaan vasteaikaan ongelman ilmetessä. Nykypäivänä palvelun saatavuus ja taso on entistä kriittisempää, sillä elämme sosiaalisen median aikakaudella. Pienikin palvelukatkos saattaa poikia isot tappiot, kun tyytymättömät asiakkaat levittävät huonoja kokemuksiaan eteenpäin. Bring Your Own Device -ilmiö on yleistymisensä myötä avannut verrattain laajan hyökkäysvektorin mahdollisille ”mustahattuisille” pahantekijöille. WannaCry, Cryptolocker sekä niiden derivatiiviset ym. yrityksiin suuntautuvat ransomware/haittaojelmot ovat aiheuttaneet maailmanlaajuisesti mittavia tappioita niille, jotka eivät ole etukäteen valmistelleet suojaustoimenpiteitä ongelmatilanteita varten. Tietoturva on siis yksi ydinkysymys.

Yleisimmät vaatimukset toiminnalle ovat:

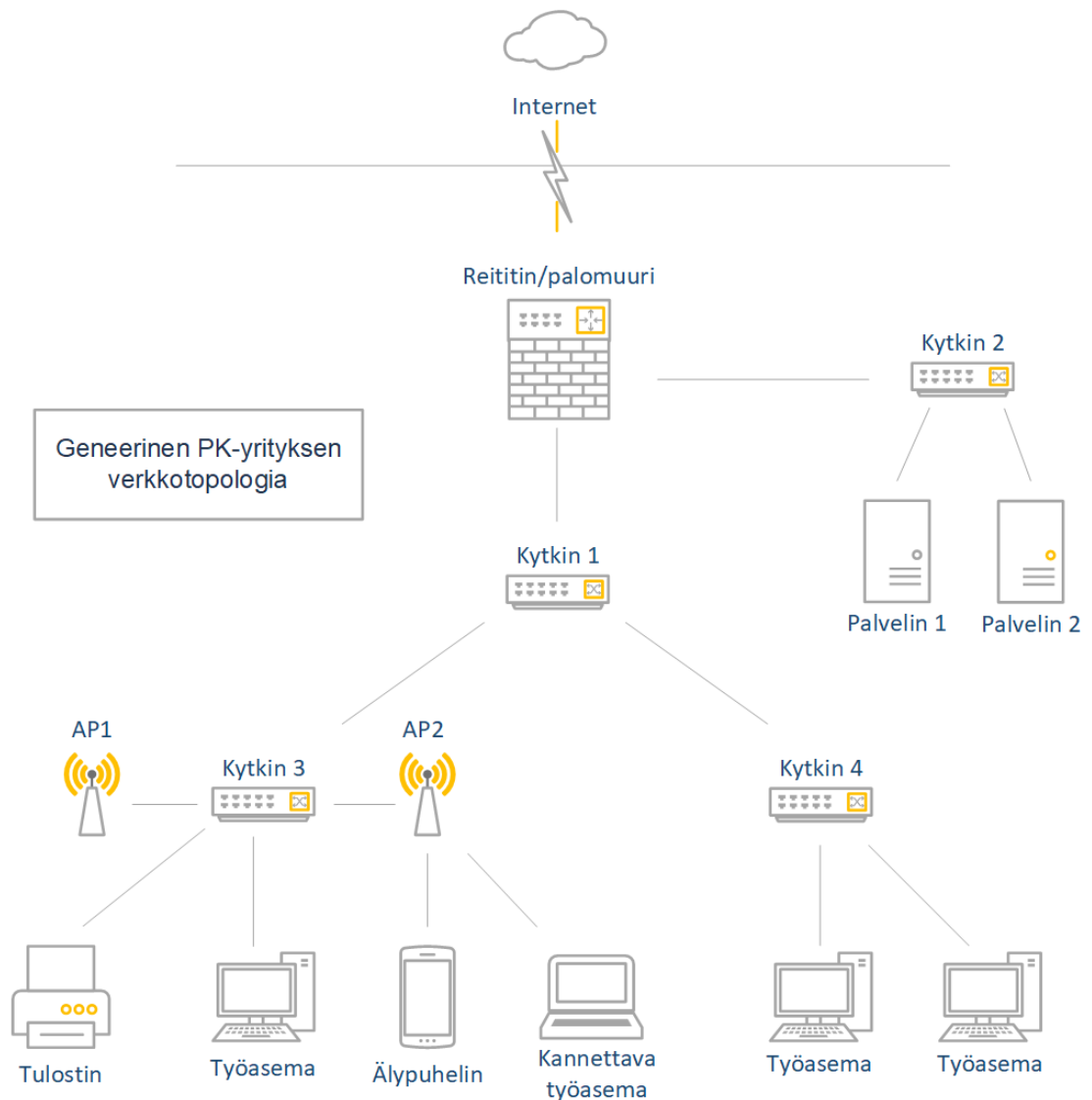
- käyttäjänhallinta
- etätyömahdollisuus
- redundanssi
- käytön sujuvuus
- kustannustehokkuus
- tietoturvallisuus
- skaalautuvuus
- ylläpidettävyys.

Kaikkialla nämä kohdat eivät aina toteudu optimaalisesti. Tutkimme myöhemmässä osiossa Microsoft Azurea ja Amazon Web Serviceä näitä kriteereitä silmällä pitäen. Aiheen laajuuden vuoksi rajausta keskittyy niihin palveluihin sekä ominaisuuksiin, jotka täyttäisivät edellä mainitut kriteerit mahdollisimman kattavasti ja kustannustehokkaasti.

3.1 IT-arkkitehtuuri

American National Standards Institute/Institute of Electrical and Electronics Engineers (ANSI/IEEE) määrittelee 1471-2000 standardissaan arkkitehtuurin kuvailevan järjestelmän fundamentaalista rakennetta, sen komponenttien keskenäisiä sekä ympäristöllisiä riippuvuussuhteita ja periaatteita, jotka määrittävät sen suunnittelun ja kehityksen. Yrityksen IT-arkkitehtuurisuunnittelulla tähdätään järjestelmään, jossa voidaan tehokkaasti allokoida tarvittavat resurssit työprosesseihin. (Dixit ja Dube 2011.)

PK-yritysten olosuhteet usein muovaavatkin IT-arkkitehtuurin nojaamaan pelkistettyihin ja yksinkertaisempiin ratkaisuihin. Alla kuvassa geneerinen epäredundantti PK-yritysverkko.



Kuva 5. Hahmotelma yleisestä verkkotopologiasta pienyrityksessä

Etuina tälle on yksinkertaisuus ja kulujen pienuus, mutta samalla karsitaan toiminnan varmuudesta. Esimerkiksi reititin on tässä tapauksessa yksittäisenä pisteenä, jonka toimintahäiriö rikkoisi koko verkon tarkoituksenmukaisen toiminnan. Tämä on huomionarvoinen riskitekijä palveluiden siirtyessä yhä enenevän määrin verkkoon. Tehtäväkriittisen järjestelmän suunnitteluun, toteuttamiseen sekä ylläpitoon tarvitaan ammattitaitoista henkilöstä. Tämä voidaan toteuttaa omilla ”in-house”-insinööreillä, tai vaihtoehtoisesti ostaa ulkoisena palveluna. Kaikilla yrityksillä ei kuitenkaan ole omaa IT-osastoa, jolloin on turvauduttava ulkoiseen palveluun. Pilvipalvelut tarjoavatkin mahdollisuuden siirtää osan tästä vastuusta kolmannelle osapuolelle.

3.2 Toimialue ja Active Directory

Hakemisto on hierarkkinen rakenne, joka tallettaa ja ylläpitää tietoa verkossa olevista objekteista, asioista ja toimijoista. Esimerkiksi talletettuihin käyttäjätietoihin voi kuulua nimi, puhelinnumerot, salasanat, osoite. Windows-käyttöjärjestelmien maailmanlaajuinen markkinaosuus vuonna 2016 oli n. 85 % (Ganguli 2017), mistä johtuen yritykset oletusarvoisesti käyttävät Microsoftin kehittämää Active Directoryä hakemistopalvelunaan. Käyttöoikeuksien hallinta on yksi ydinfunktio tässä järjestelmässä ja se perustuu Windows NT:n ja Windows 2000:n hallintamalleille, jonka avaintekijöinä ovat esimerkiksi turvallisuuskuvaukset, security identifier (SID), access control list (ACL) sekä access control entity (ACE). (Price ym. 2008, 59.)

Hakemistopalvelu, kuten aiemmin mainittu Windowsin Active Directory (AD), mahdollistaa jäsennetyn datan tarjoamisen verkon käyttäjille ja administraattoreille. Toimialueessa Active Directory Domain Services -palvelua (AD DS) pyörittävää palvelinta kutsutaan toimialueen ohjauskoneeksi eli domain controlleriksi. AD:n ”best practices” eli parhaisiin käytäntöihin kuuluu redundanttinen suunnittelu, jolloin puhutaan primääristä (PDC) ja sekundäärisestä (BDC) ohjauskoneesta, joiden välillä tapahtuu säännöllisesti datan kahdennus eli datan replikaatio. (Price ym. 2008, 4.)

Active Directoryn autentikaatio perustuu Kerberos-protokollaan sekä LDAP:iin. Tämän seikan sekä SMB:n Linux-yhteensopivuuden ansiosta Windows toimialueeseen voidaan myös liittää Linux-koneita, kuten RHEL-palvelimia.

3.3 VPN

Etätyöskentelyn ja geografisesti pirstaloituneen palveluympäristön yleistymisen myötä virtuaaliset erillisverkot ansaitsevat erityismaininnan. Virtuaalisella erillisverkolla (VPN) tarkoitetaan keinoa liittää verkkoja toisiinsa julkisen verkon yli käyttämällä kryptografisesti suojattua yksityistä reittiä. Data salataan tunnelin eli reitin alkupäädyssä ja puretaan kohteessa salatun/julkisen avainparin avulla. TCP/IP-pinoon kuuluvassa IPsec-protokollassa avaintenvaihto suoritetaan Diffie-Hellman-algoritmia apuna käyttäen. IPsec-suojatut IKEv2, L2TP ja MPLS IP VPN (VPLS) sekä SSL VPN ovat virtuaalisen erillisverkon implementointitapoja. (Frankel ja Krishnan 2011.)

VPN voidaan toteuttaa esimerkiksi käyttöjärjestelmässä ohjelmallisesti tai erillisellä fyysisellä raudalla, kuten palomuurilla. IPsec-protokollassa IP:n hallinta ei ole määritelty, joten staattinen IP-osoite on tarpeellinen yhteyden toimimisen kannalta. Vaihtoehtoisesti voidaan soveltaa käyttämällä DDNS:ää (Dynamic DNS), joka päivittää tiedon vaihtuvasta IP-osoitteesta (Oracle 2019.)

3.4 Järjestelmän saatavuus

Järjestelmän saatavuus on ydinkysymys yritysmaailmassa. Järjestelmän redundanttisuudella, eli vikasietoisuudella pyritään takaamaan järjestelmän saatavuus (Availability). Organisaation järjestelmä voidaan jakaa komponentteihin; Fyysinen ympäristö, laitteisto, ohjelmisto, data ja verkkoyhteydet. Jokaisen näistä osa-alueista tulisi olla redundanttinen, jonka lisäksi tarvitaan kesketymätön virransyöttö (UPS) järjestelmän selkärangaksi.

High-availability (HA) ja Fault Tolerance (FT) tarkoittavat termeinä järjestelmän korkeatasoista toimintakykyisyyttä ominaisuutena. Yksi HA:n ydinperiaatteista onkin single point of failuren eliminoiminen eli suunnittelu niin, ettei yksittäisen tekijän toimintavirhe riko koko järjestelmän toimintaa.

Saatavuutta usein mitataan prosentteina. 99 %:n saatavuus tarkoittaa vuodessa 3,65:n päivän toimintakatkoa. (DigitalOcean 2016.)

Unplanned downtime (mission-critical)	Typical uptime	Hours down per year	Productivity cost*	Downtime risk
Worse than average	98%	174.72	\$42,000	\$7,338,240
Average	99%	87.36	\$42,000	\$3,669,120
Better than average	99.5%	43.68	\$42,000	\$1,834,560
Good	99.9%	8.736	\$42,000	\$366,912
Best in class	99.999 %	.09	\$42,000	\$3,780

Kuva 6. Esimerkki saatavuuden ja tappion suhteesta (Pisello ja Quirk 2004.)

Yllä kuvassa esitetty saatavuuden vaikutus rahallisiin menetyksiin.

Vähenevien tuottojen periaatteen mukaan mitä korkeampi saatavuus, sitä kalliimpi implementaatio. Yritykselle hintaoptimoitu tarvittavan redundanssin taso voidaan karkeasti laskea antamalla arvo ajalle, jolloin järjestelmä ei ole saatavilla sekä ottamalla huomioon mean time between failures (MTBF) eli keskimääräinen aika vikatilanteiden ilmenemisen välillä ja mean time to repair (MTTR) eli korjaukseen käytettävä aika. Kuvassa 6 esitettynä kyselytulokset, kyselyn kohteena oli Fortune 1000 -yrityksien IT-työntekijät (IDC 2014.)

Average Time to Repair an Infrastructure Failure

Q. What is the average time to repair an infrastructure failure?

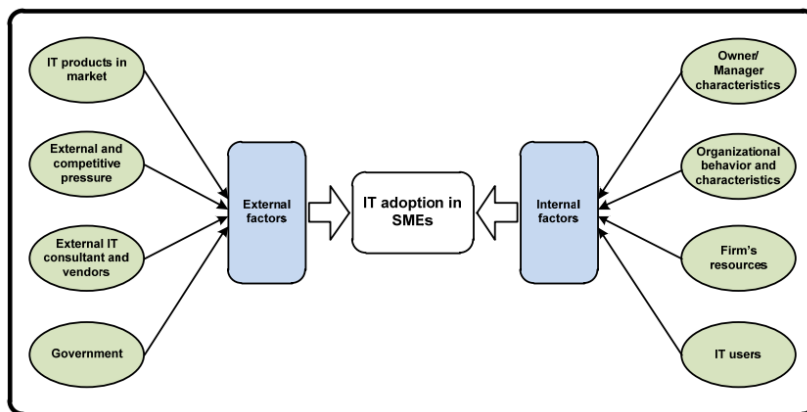
	% of Respondents
1–5 minutes	9
11–59 minutes	17
1–12 hours	35
2–7 days	17
Don't know	22

Kuva 7. Keskimääräinen korjausaika infrastruktuurin vikatilanteissa (IDC 2014.)

Saatavuuden ehdoilla järjestelmää suunnitellessa tulee myös ottaa huomioon kylpyammekäyrä, sekä sen esittämä laitteen alku- ja loppupään korostunut vikataajuus.

3.5 Järjestelmien käyttöönottomalli

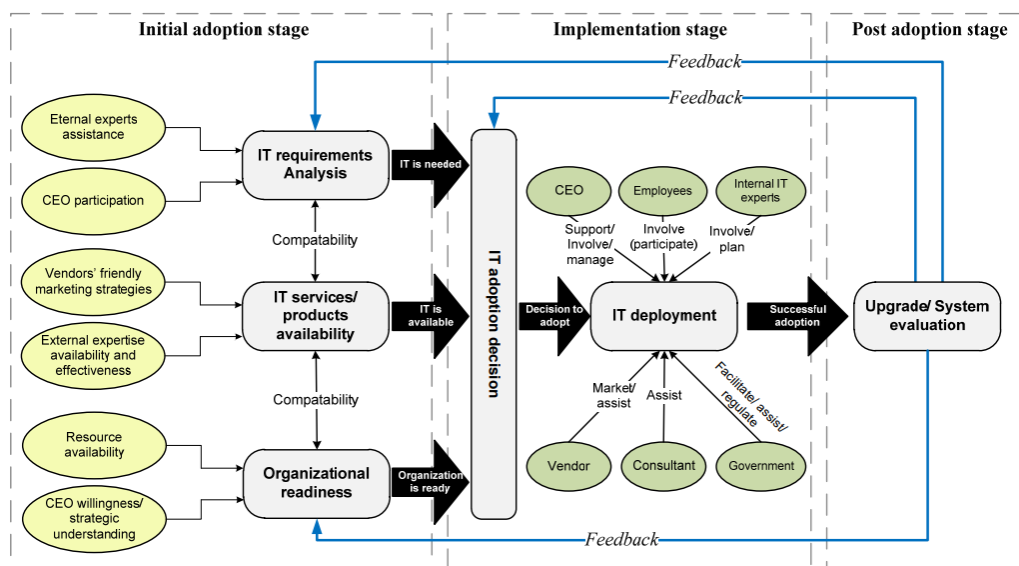
Alla kuvassa 8 havainnollistetaan, miten hankintapäätös koostuu sekä ulkoisista että sisäisistä tekijöistä. Kaava on johdettu meta-analyysisestä tutkimuksesta (Ghobakloo ym. 2012.)



Kuva 8. Päätökseen vaikuttavat tekijät (Ghobakloo ym. 2012.)

Ideaalisessa tilanteessa yritys pystyy sisäisesti tunnistamaan tarpeen ja punnitsemaan potentiaaliset implikaatiot, jolloin järjestelmän räätälöinti onnistuu parhaiten. IT-konsultit kuitenkin pystyvät tarjoamaan näkemyksiään tilanteiden mukaisesti. Systemaattisen lähestymistavan mukaan käyttöönotto koostuu kolmesta vaiheesta: alustavasta, toimeenpanevasta ja käyttöönoton jälkeisestä ajasta. (Ghobakloo ym. 2012.)

Seuraavassa kuvassa hahmoteltuna kolmivaiheinen pseudosyklinen malli, joka perustuu Ghobakloon ym. (2012) suorittamaan tutkimustyöhön sekä alan kirjallisuuteen. Tärkeää on huomata, että kehitysprosessi on jatkuva. Pilvipalvelua harkitessa tulee ottaa huomioon myös yrityksen organisatonaalinen näkökulma muutosta kohtaan. Uusi järjestelmä todennäköisesti otetaan käyttöön askeleittain.



Kuva 9. Konseptuaalinen malli tehokkaaseen IT-järjestelmän käyttöönottoon (Ghobakloo ym. 2012.)

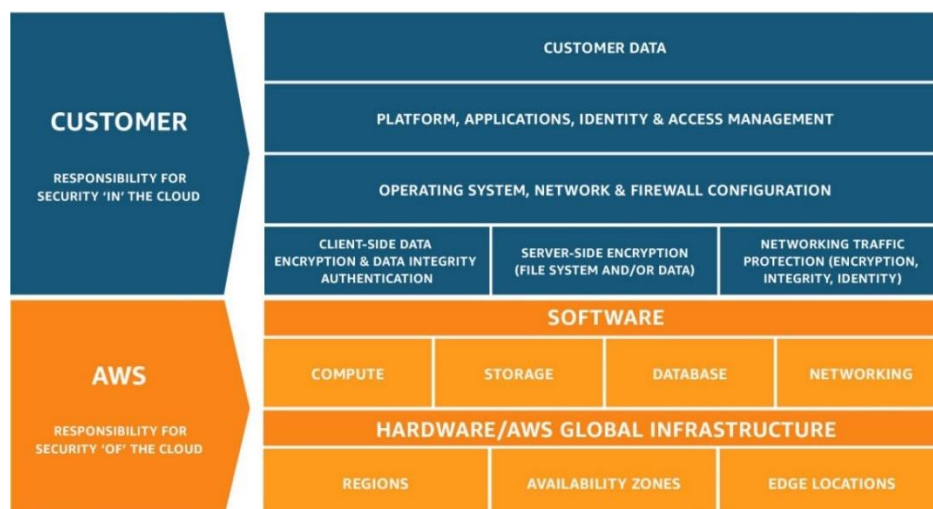
4 AMAZON WEB SERVICES

Amazon Web Services on käytetyin sekä 165:llä palvelullaan maailman laajin pilvialusta. AWS:n palveluverkko koostuu 22:sta seudusta sekä 69:stä saatavuusalueesta. Seudun käsitteellä tarkoitetaan niitä fyysisiä alueita, jotka ovat alueellisiin verkkoihin kuuluvien datakeskusten latenssitoleranssien sisällä. Lailliset seikat, kuten esim. GDPR ja datan sijaintiin liittyvät määräykset ovat seutukohtaisia. Saatavuusalueella tarkoitetaan erillisiä redundanttisia jaotelmia seudun sisällä. (Amazon 2019a.)

AWS:n keskeisimpiin palveluihin lukeutuu Elastic Computer Cloud -virtuaalikonepalvelu, redundanttinen tiedostomuisti Simple Storage Service (S3) sekä heidän skaalautuva tietokantapalvelunsa Relational Database Service (RDS). Amazonin palveluja hallitaan yleisimmin ohjelmointirajapinnan (API), AWS-konsolin graafisen käyttöliittymän (GUI) tai ohjelmistokehityspaketin (SDK) avulla. Huomioitavaa on, että Amazon tarjoaa hands-on-laboratorioita, joissa pääsee harjoittelemaan opastetussa AWS:n ympäristössä ilmaiseksi.

Tietoturva

Järjestelmän ylläpitoon ja toimintaan liittyvät vastuualueet ovat tyypillisesti jaettuna asiakkaan ja palveluntarjoajan välillä. Alla kuvassa 10 graafinen esitys vastuualuejaosta. (Amazon 2019b.)



Kuva 10. Vastuualuejako asiakkaan ja Amazonin välillä (Amazon 2019b.)

4.1 Elastic Computer Cloud (EC2)

Virtual Machine -termillä tarkoitetaan ohjelmallisesti emuloitua tietokonejärjestelmää, joka on kuitenkin funktionaalisesti verrattavissa fyysiseen tietokoneeseen.

EC2 on Amazonin skaalautuva VM- ja resurssienprovisiopalvelu, jonka muokattavat Amazon Machine Image -konfiguraatiopohjat nopeuttavat instanssien luomista. Tuettuihin käyttöjärjestelmiin kuuluu Red Hat Package Manager -yhteensopiva Amazon Linux, Windows Server, CentOS ja Debian. EC2 tarjoaa mahdollisuuden käyttää Dedicated Hosts -palvelussaan ”bare metal” -instansseja, jolloin sovellukset ja ohjelmat pääsevät käyttämään palvelimensa rautaa suoraan, eli ilman pilvessä yleisesti käytettyä abstraktiokerrosta jota virtualisaatioksi kutsutaan. Dedicated Hosts mahdollistaa omien lisenssien tuomisen (BYOL) AWS:n pilveen. (Amazon 2019c.)

EC2:n oletuksena käyttöperäinen laskutus jaetaan neljään kategoriaan: on-demand, reserved instances, spot instances ja dedicated hosts. Microsoftin tavoin Amazon tarjoaa jopa 75 %:n alennusta varattuja instansseja käytettäessä, mutta myös mahdollisuuden käyttää ylijäämäresursseja vapaan markkinan määrittelemän hinnan mukaisesti. (Amazon 2019c.)

VPC

Virtual Private Cloud (VPC) on Amazonin tarjoama yksityinen, virtuaalinen verkkoympäristö joka vastaa Azuren VNet-palvelua. Reitityksen hallinta, NAT, IP-osoitealueiden määrittäminen, aliverkotus ym. ovat käyttäjän hallussa.

4.2 Simple Storage Service (S3) ja Elastic Block Store (EBS)

S3

Amazonin tallennustilan kulmakivenä toimii Simple Storage Service (S3), joka ylittää yhdentoista yhdeksikön (99,999999999 %) saatavuusluokitelman hyödyntämällä vähintään kolmea saatavuusaluetta kerralla. Tämän lisäksi Amazonin best practice -käytäntöihin kuuluu pääsynhallinta, seutujenvälinen datareplikaatio, versionhallinta, varmuuskopioiden toimivuuden säännöllinen testaus sekä datan eheyden todentaminen tarkistussummalla. SLA:n

mukaisesti alle 95 %:n saatavuuksilla asiakas saa täyden hyvityksen siltä kuukaudelta. (Amazon 2019d.)

S3 tarjoaa valikoiman tallennusluokkia, jotka on suunniteltu erilaisiin käyttötarkoituksiin. Niihin sisältyy S3 Standard usein käytetyn datan yleiskäyttöä varten. Tallennusluokat ovat seuraavanlaiset:

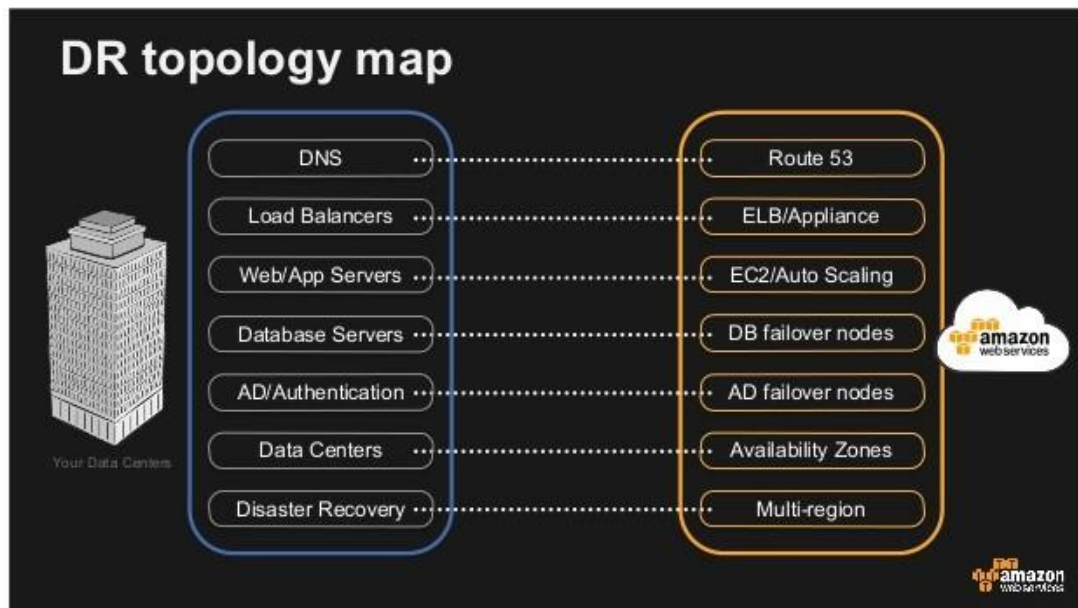
- S3 Intelligent Tiering datalle, jolla on määrittelemätön tai vaihteleva käyttömalli.
- S3 Standard-IA nopeasti saatavissa olevalle datalle, sekä tästä edullisempi versio S3 One Zone-IA pitkäikäiselle, mutta harvemmin käytetylle datalle.
- S3 Glacier toimii pitkän aikavälin tallennusratkaisuna. Verrattavissa Azure Blob -palveluun.
- S3 Glacier Deep Archive pitkäaikaista arkistointia ja digitaalista säilyttämistä varten. Verrattavissa Azure Archive -palveluun.

EBS

Elastic Book Store on skaalautuva kovalevyn kaltainen itsenäinen tallennusvolyyymi EC2 instansseille. Tarjolla on SSD- ja HDD-vaihtoehdot, jotka voidaan alustaa esimerkiksi ext3-formaattiin. Instanssien data voidaan varmentaa EBS:n snapshotteilla, joista ensimmäinen on täysi replikaatio, mutta tätä seuraavat ovat inkrementaalisesti täydentäviä versioita.

4.3 AWS BCDR

Business continuity and disaster recovery (BCDR) tarkoittaa lyhyesti toimintasuunnitelmaa ja toteutusta, jonka päämääränä on taata palveluiden jatkuva saatavuus sekä katastrofaalisesta häiriöstä palautuminen. Kuvassa 11 esitettynä millä pilven vastaavilla palveluilla yrityksen järjestelmän ydinpalveluiden jatkuvuus saavutetaan. Esimerkkinä Route 53, joka on AWS:n pilvessä toimiva DNS-palvelu. (Uhl 2015.)



Kuva 11. Paikallisen infrastruktuurin heitto komponenteittain pilveen vikatilanteessa (Uhl 2015.)

4.4 AWS IAM

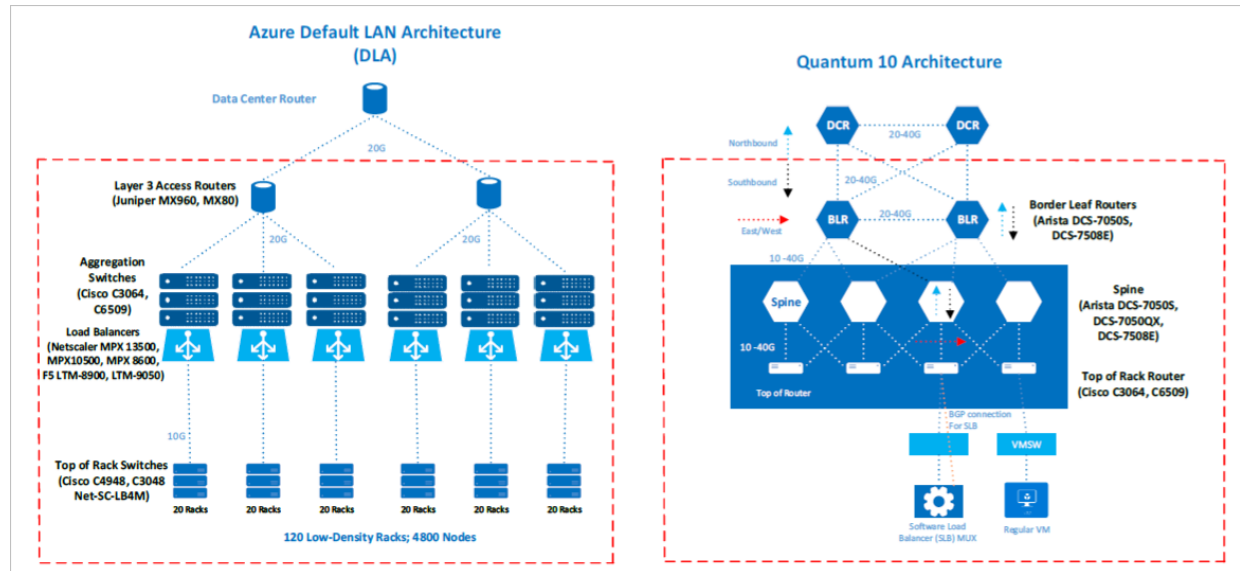
IAM on lyhenne sanoista Identity and Access Management, jolla karkeasti käsitetään käyttäjän- ja pääsynhallinta pilven resursseihin. AD Connector -komponentilla AWS:n ympäristö saadaan liitettyä paikalliseen hakemistopalveluun, jolloin muunmuassa SSO:n käyttö sekä EC2-virtuaalikoneiden liittäminen paikalliseen toimialueeseen mahdollistetaan. (Amazon 2019e.)

5 MICROSOFT AZURE

Azure on General Data Protection Regulation eli GDPR:n mukainen pilvialusta, joka tarjoaa yli sataa erilaista palvelua 54:llä alueella ympäri maailmaa hajautetuissa datakeskuksissaan. Pohjois-Euroopan lähimmät keskuksat sijaitsevat Alankomaissa (West Europe) ja Irlannissa (North Europe). Keskimääräinen latenssi Etelä-Suomesta Irlantiin sekä Alankomaihin on n. 50 millisekuntia. Microsoft rakennuttaa Norjaan kaksi uutta datakeskusta Azurea varten, jotka suunnitelmien mukaan valmistuvat loppuvuodesta 2019. (Microsoft 2019a.)

SLA:n mukaisesti Microsoft takaa yleisesti vähintään 99,9 %:n saatavuuden maksullisille palveluilleen. Jos Microsoft ei tähän kykene, niin asiakas saa hyvitystä ilmaisen palvelun muodossa. (Microsoft 2019a.)

Microsoft käyttää Azure-datakeskuksissaan kahta erilaista verkkoarkkitehtuuria, joista uudempi Clos/mesh-tyylinen Quantum 10 tukee suurempaa kapasiteettia ja skaalautuvuutta. Alla kuvassa 12 havainnollistettuna DLA- ja Quantum 10 -arkkitehtuurit. (Microsoft 2019b.)



Kuva 12. Azure-datakeskusten DLA- ja Q10 Clos verkkotopologiat (Microsoft 2019b.)

Microsoft tarjoaa Azuressa site-to-site VPN:ää, sekä OpenVPN-, SSTP- ja IKEv2-tekniologioita tukevaa point-to-site VPN -palveluaan nimellä VPN Gateway. Perustason VPN:n nopeus on 100 Mb/s ja SLA takaa 99,9 % saatavuuden, mutta nämä voidaan lisäkustannuksella skaalata yli gigabitin nopeuksiin sekä 99,95 % saatavuuteen. Suurempia asiakkaitaan varten Microsoft tarjoaa Layer 3 –liitäntää, yli 10 Gb/s nopeuteen yltävää yksityistä ExpressRoute WAN-yhteyttä. (Microsoft 2019c.)

Seuraavaksi tutkimme Azuren tarjoamia yrityksille relevantteja ydinpalveluita, joihin kuuluu esimerkiksi toimialueen käyttäjien/resurssienhallinta (AD), virtuaaliset erillisverkot (VPN), datan käsittely ja säilöntä, verkkopohjaiset ohjelmat, redundanssi ja tietoturva. Huomioitavaa on, että Azuresta löytyy myös hands-on-laboratorioita, joissa pääsee harjoittelemaan ohjeistetussa verkkoympäristössä skenaarioita ilmaiseksi.

5.1 Azure VM

Azuren virtuaalikoneet ovat jaoteltuna yhteentoista kategoriaan, jotka ovat rautakonfiguraatioiltaan optimoitu käyttötarkoituksittain. Jokaiseen VM:ään kuuluu kuormantasausta sekä automaattinen skaalaus. OS-vaihtoehtoihin kuuluu sekä Windows-järjestelmät että Linux-distribuutiot. Microsoft tarjoaa kolmea maksuvaihtoehtoa:

- laskutus käytön mukaan
- vuoden varaus
- kolmen vuoden varaus.

Varatut virtuaalikoneet maksetaan etukäteen, mutta instanssit voidaan vaihtaa lennosta toisiin. Microsoft mainostaa jopa 72 % alennusta kolmen vuoden varaukselle, kun vertailukohteena on käytön mukainen laskutus. On myös mahdollista käyttää olemassa olevaa lisensointia virtuaalikoneisiin, jolloin säästöt ovat vielä suuremmat. Edellämainittujen seikkojen ansiosta Windows- ja SQL palvelimien kustannukset ovat Azuressa huomattavasti halvemmat kuin AWS:llä. Amazonin tavoin Microsoft tarjoaa myös bare metal -instansseja Azure Dedicated Host -palvelullaan. Kuvassa alla esimerkki instanssien luokkaperäisestä hinnoittelusta. (Microsoft 2019d.)

D2-64 v3 latest generation

D2-64 v3 instances are the latest, hyper-threaded general purpose generation running on both the 2.4 GHz Intel Xeon® E5-2673 v3 (Haswell) and the 2.3 GHz Intel Xeon® E5-2673 v4 (Broadwell) processor. With the Intel Turbo Boost Technology 2.0, the Dv3 can achieve up to 3.5 gigahertz (GHz). The Dv3-series sizes offer a combination of vCPU, memory and local disk best suited for most production workloads.

ADD TO ESTIMATE	INSTANCE	VCPU	RAM	TEMPORARY STORAGE	PAY AS YOU GO	ONE YEAR RESERVED (% SAVINGS)	THREE YEAR RESERVED (% SAVINGS)	3 YEAR RESERVED WITH AZURE HYBRID BENEFIT (% SAVINGS)
	D2 v3	2	8 GiB	50 GiB	~€122.5062/month	~€99.7841/month (~19%)	~€85.0957/month (~31%)	~€28.4597/month (~77%)
	D4 v3	4	16 GiB	100 GiB	~€245.0124/month	~€199.6420/month (~19%)	~€170.2159/month (~31%)	~€56.9439/month (~77%)
	D8 v3	8	32 GiB	200 GiB	~€490.0248/month	~€399.2102/month (~19%)	~€340.4380/month (~31%)	~€113.8939/month (~77%)

Kuva 13. D-luokan virtuaalikoneiden hintalistaus (Microsoft 2019d.)

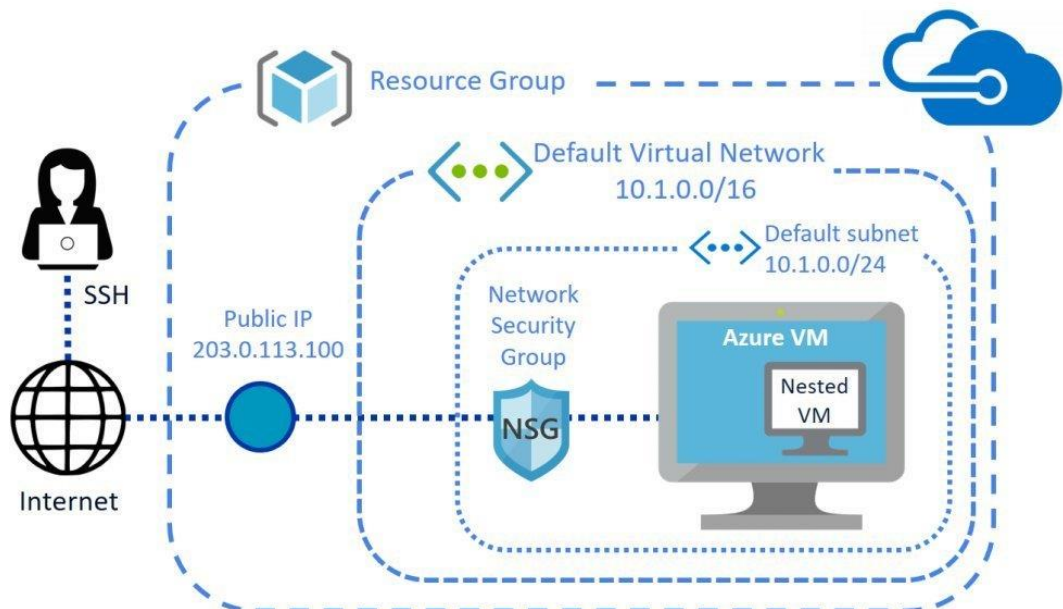
Virtuaalikonekategoriat ovat jaettu sekä käyttötarkoituksittain että hintaluokittain, jotka ovat jaettuna seuraavanlaisesti: yleiskäyttö, muistioptimoitu (RAM), laskentaoptimoitu (CPU), graafinen suorituskyky (GPU), HPC ja tallennustilaoptimoitu (SSD, NVMe).

Täysi Active Directory Domain Services -palvelu Azuren pilvessä saavutetaan käyttämällä virtuaalikonetta, joka on loogisesti liitetty yrityksen sisäverkkoon Site-to-Site VPN -tunnelin avulla. Tähän palataan vielä työn viimeisessä

osiossa. Jos pilvessä oleva VM DC halutaan synkronoida paikallisen (on-premise) DC:n kanssa, on käytettävä paikallista DNS-palvelinta johon Azuressa sijaitseva VM DC osoittaa. (Microsoft 2019e.)

Azuren julkista IP:tä kutsutaan VIP:ksi (Virtual IP) ja se on liitetty Azuressa kuormantasaajaan itse virtuaalikoneen sijasta, jonka ansiosta yhdellä IP-osoitteella voidaan hallita useampaa virtuaalikonetta. Hallintaan tarjotaan työkaluiksi Azure CLI, Azure portal (GUI) sekä Azure PowerShell. (Microsoft 2017.)

Alla kuvassa 14 esitettynä verkkotopologia Azuren pilvessä sijaitsevalle virtuaalikoneelle SSH-hallintayhteyden kera.



Kuva 14. Virtuaalikoneen ympäristö Azuren pilvessä (Linkletter 2018.)

Azuren virtuaalikoneiden käyttöjärjestelmälle, datalle ja tilapäistiedostoille on kaikille varattu omat levynsä. OS:lle varatun levyn kapasiteetti on maksimissaan noin 2 TB. Näille järjestelmälevyille voidaan helposti siirtää virtuaalikone VHD- tai VHDX-muodossa. Datakäytössä on SCSI-levyjä, joiden kapasiteetti on maksimissaan noin 35 TB. Tämä on sinänsä tärkeää ottaa huomioon varsinkin AD:ta konfiguroidessa, sillä Azure implementoi "write caching" -tekniikan vakiona käyttöjärjestelmän levyille, jolloin esimerkiksi riskeerataan AD:n tietokantojen välinen virheellinen replikointi USN rollback -tapahtumilla. Suosituksena on siirtää AD DS:n tietokanta, lokitiedot sekä SYSVOL erilliselle levyille. (Finn 2016.)

VNET

Pilven yksityinen tietoliikenne pohjautuu virtuaalisten tietoverkkojen (VNet) käyttöön, joka tukee OSI-mallin L3-tason hallintaa ja esimerkiksi BGP-reitityksen konfigurointia. Pääsilystojen (ACL) muokkaus sekä tietoliikenteen monitorointi onnistuu myös. (Karthikeyan 2018.)

5.2 Azure Storage ja BCDR

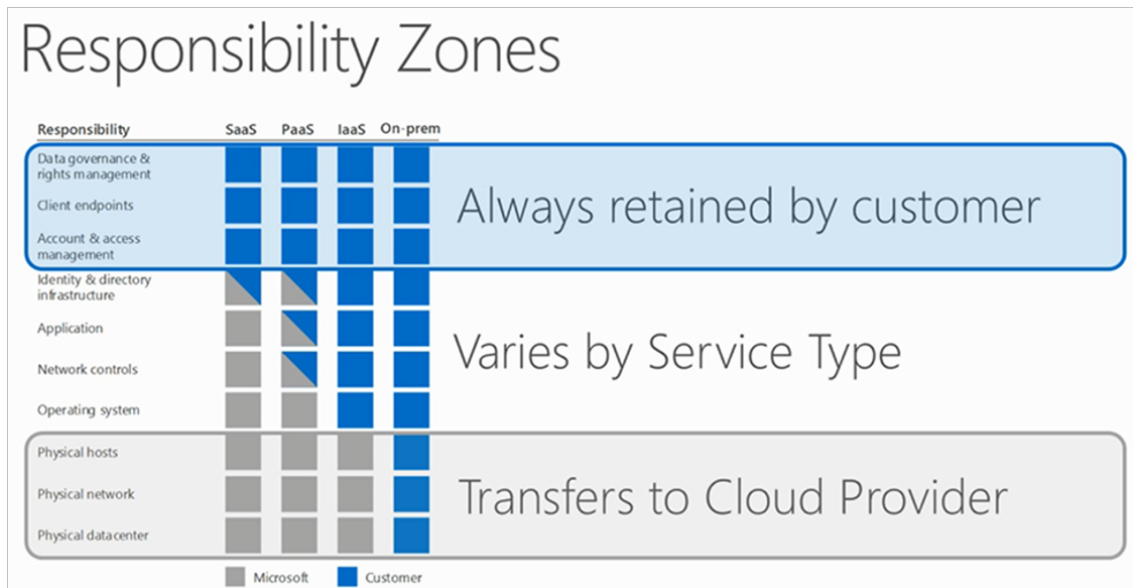
Kaikki data Azuressa on vakiona varmennettua ja replikoitua sekä verifioitu syklisellä redundanssitarkistuksella eli CRC:llä. Tallennuspalvelut ovat virtuaalikoneiden lailla jaoteltu käyttökohtaisesti, alla lyhyt esittely:

- File – Yksinkertainen ja edullinen, hajautettu tiedostojärjestelmä
- Disk – Matala latenssi ja korkea suorituskyky, korkea luotettavuus
- Blob – Edullinen runsaiden datamäärien säilömiseen
- Data Lake Storage – Analyytisen datan käsittelyyn
- Archive – Datan pitkäaikaiseen säilömiseen tarkoitettu
- Azure vFXT for Azure – HPC käyttöön tarkoitettu

Backup ja Site Recovery ovat Azuren natiivit varmuuskopiointi- ja Disaster Recovery -ratkaisut. Disaster Recoveryyn (DR) tarkoituksena on toimia turvaverkkona sekä ylläpitää järjestelmien ja ohjelmien saumatonta toimintakykyä siirtymällä rinnalla pidettyyn replikoituun varajärjestelmään kunnes primäärin järjestelmän toimintakyky on palautettu. Site Recoveryllä voidaan replikoida virtuaalikoneita lähestulkoon mistä alustalta tahansa, mm. fyysiseltä palvelimelta, Vmwaren ESXi:ltä tai Hyper-V:stä. Alkuperäisestä käyttötarkoituksestaan huolimatta tätä voidaan käyttää virtuaalikoneiden helppoon pilvimigraatioon. Huomioitavaa on myös, että pilvipohjaisten varmennusjärjestelmien myötä saavutetaan geografinen hajautus. Tämä antaa suojan sijaintisidonnaisia uhkia, kuten tulipaloja vastaan. (De Tender 2016.)

5.3 Tietoturva

Pilvimalleissa tyypillisesti vastuualueet jaetaan asiakkaan ja CSP:n välillä. Yleisimmin CSP huolehtii fyysisestä infrastruktuurista ja verkkopuolesta, kun taas asiakas vastaa esimerkiksi omista päätelaitteistaan ja pääsynhallinnasta. Alla kuvassa 15 graafinen esitys vastuualueista.

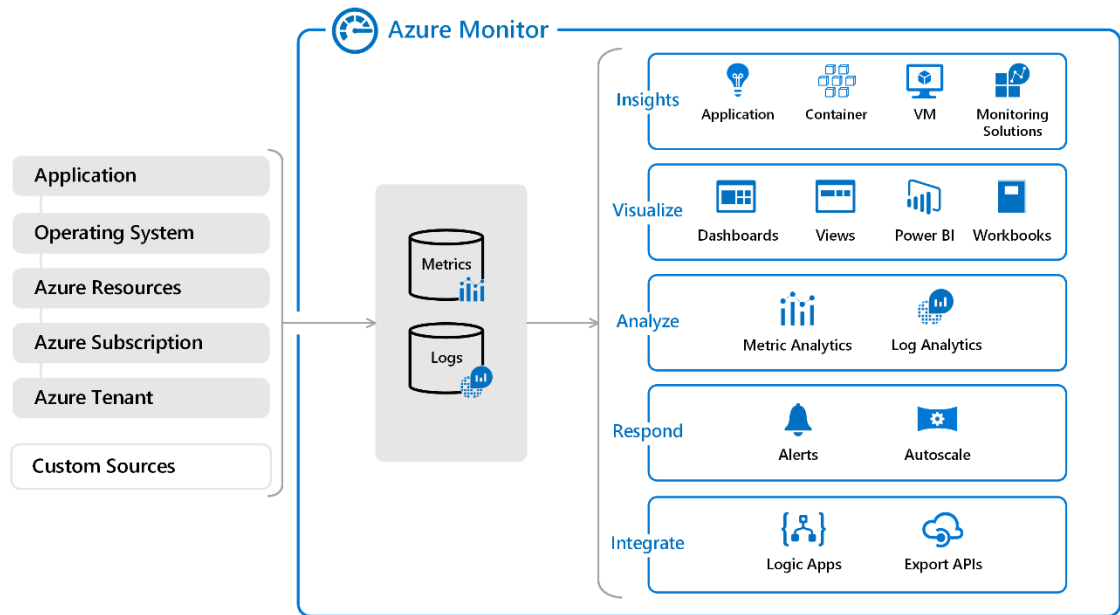


Kuva 15. Vastuualueet palvelumalleittain

Yhtenä Azuren tietoturvan peruseriaatteena toimii CIA-kolmiomalli, jonka tavoitteina ovat luottamuksellisuus (confidentiality), saatavuus (availability) ja eheys (integrity). (Freato 2015.)

Azure tarjoaa tietoturvan tueksi ratkaisuja, joista esimerkkinä monitorointityökalu Azure Monitor, joka on suunniteltu myös käytettäväksi osana olemassaolevia turvatietojen ja -tapahtumien hallinnan (SIEM) järjestelmiä. Azurelle pilvinatiivina skaalautuvana SIEM-ratkaisuna toimii koneoppimista hyödyntävä Azure Sentinel. (De Tender 2019.)

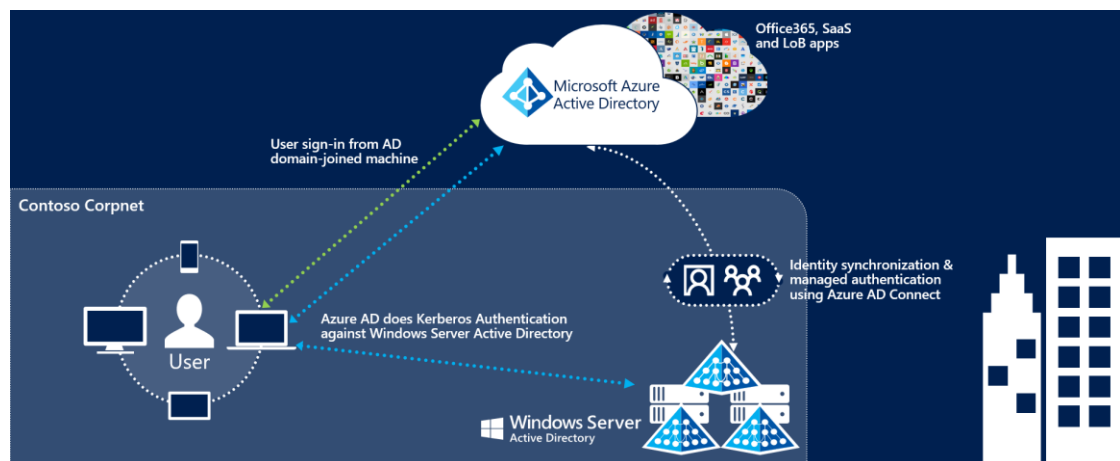
3500:n tietoturva-ammattilaisen ja jatkuvan sisäisen kehityksen sekä "red team" -penetraatiotestauksen ansiosta Microsoft pysyy uhkatekijöiden tasalla. Saatavilla oleviin palveluihin lukeutuu mainittujen lisäksi Security Center, Key Vault, Azure Information Protection, Azure Dedicated HSM, Azure DDoS protection sekä Application Gateway. Huomattakoon, että mittava osuus näistä tietoturvapalveluista ja analytiikkaratkaisuista vaativat ammattitaitoista henkilökuntaa. Alla kuvassa 16 Azure Monitorin läpileikkaus. (Microsoft 2019f.)



Kuva 16. Azure Monitorin läpileikkaus (Microsoft 2019f.)

5.4 Azure Active Directory

Azure Active Directory on pilvessä toimiva palvelu, joka keskittyy identiteetinhallintaan (IDaaS) sekä SaaS-aplikaatioiden hallinnan selkärangaksi. Synkronointi pilveen onnistuu Azure AD Connect -ohjelman avulla. Microsoftin Office 365 käyttää Azure AD:tä identiteetinhallinnan backendinä ja O365:n tilaukseen sisältyykin Azure AD:n ilmainen käyttö. Tämä tarjoaa mahdollisuuden esimerkiksi salasanojen synkronointiin ja seamless single sign-on (SSSO) ominaisuuden implementaatioon. Alla kuvassa 17 esitettynä seamless single sign-on ja AAD/AD-välinen käyttäjän autentikaatio. (Microsoft 2019g.)



Kuva 17. Paikallisen toimialueen ja Azuren välinen Kerberos autentikaatio (Microsoft 2019g.)

Laitteet voidaan lisätä Azure Active Directoryyn kolmella eri tavalla:

- Azure AD Join
- Azure AD Registration
- Hybrid Azure AD Join (paikallinen + pilvi)

Tällä hetkellä vain Windows 10 tukee natiivisti Azure AD:hen liittymistä, sekä ohjauskoneiden tulee olla versioltaan Windows Server 2008 R2 tai uudempi. Toisena rajoittavan tekijänä on kahdesta osasta (prefix/suffix) muodostuva User Principal Name (UPN), jonka pitää olla sama sekä pilvessä että paikallisessa AD:ssa. Tästä syystä yleisimmin käytetty .local-päätteinen paikallinen ei-reititettävä toimialuenimi ei yksinään kelpaa. Tarvitaan siis verifioitu reitityskelpoinen toimialuenimi UPN-suffiksiksi eli päätteeksi. Vakiona O365 tarjoaa onmicrosoft.com muotoista suffiksia. (Microsoft 2019h.)

Vaikka AAD onkin melko pätevä käyttäjänhallintaan, tulee AAD:tä harkittaessa ottaa huomioon, ettei se natiivisti tue group policyjä eli ryhmäkäytäntöjä. Azure AD:hen liitetty kone ei ole loogisesti paikallisessa toimialueessa, mutta Hybrid Azure AD Join mahdollistaa molemmissa ympäristöissä toimimisen, jolloin identiteetti sijaitsee sekä pilvessä että paikallisessa aktiivihakemistossa. Azure AD:n hallintajärjestelmä perustuu MDM-alustoihin, esimerkiksi Microsoftin Intuneen sekä lisäksi rinnakkaisesti System Center Configuration Manageriin (SCCM). AAD tarjoaa käyttäjille itsepalveluportaaleita, joista voi esimerkiksi resetoida oman salasanansa.

5.5 Azure Active Directory Domain Services

Azure ADDS on nimensä mukaisesti Directory-as-a-Service (DaaS), joka toimii muuten perinteisen ohjauskoneen tavoin, mutta on osittain puutteellinen ominaisuuksiensa puolesta. Palvelu perustuu Microsoftin ylläpitämään ja valmiiksi konfiguroimaan virtuaalikoneeseen, jonka asiakas saa haltuunsa ilman ylimpiä käyttöäioikeuksia. Tätä Azuren virtuaalista ohjauskonetta ei pystytä replikoimaan paikallisen DC:n kanssa, mutta se pystyy toimimaan rinnalla mm. LDAP- ja Kerberos-protokollien ja Azure AD:n yhteensopivuuden ansiosta. Yhtenä etuna tälle palvelulle on se, että infrastruktuurin liittäminen ei tarvita VPN-yhteyttä. Alla kuvassa 18 Azure AD:n ja Azure AD DS:n ominaisuuksien välinen vertailu. (Microsoft 2019i.)

Aspect	Azure AD-joined	Azure AD DS-joined
Device controlled by	Azure AD	Azure AD DS managed domain
Representation in the directory	Device objects in the Azure AD directory	Computer objects in the Azure AD DS managed domain
Authentication	OAuth / OpenID Connect based protocols	Kerberos and NTLM protocols
Management	Mobile Device Management (MDM) software like Intune	Group Policy
Networking	Works over the internet	Requires machines to be on the same virtual network as the managed domain
Great for...	End-user mobile or desktop devices	Server VMs deployed in Azure

Kuva 18. AAD ja AAD DS palveluiden vertailu (Microsoft 2019i.)

6 VERTAILU

Tärkeää on aluksi mainita, että Microsoft sekä Amazon pitävät hintoja kilpailukykyisenä, jolloin palveluiden hinnat ovat pääsääntöisesti verrattavissa toisiinsa. Vertailu suoritettiin palveluntarjoajien Total Cost of Ownership -laskureita apuna käyttäen. Hintavertailuun valittiin pilvivastine kuvitteellisen sadan hengen insinööritoimiston palvelinympäristöön, johon kuuluu kaksi fyysistä keskitason palvelinta varustettuina 8-ydin prosessorilla, 16 GB RAM-muistilla sekä 4 TB SAS-kiintolevytilalla RAID10-konfiguraatiossa. Tämän lisäksi yrityksellä on nauhavarmistus käytössä, jolloin pilvivertailukohteeseen sisällytetään myös datan varmistus. Oletuksena ainakin toisen palvelimen käyttöjärjestelmänä on Windows Server 2016 ja ulospäin suuntautuva tiedonsiirtoliikenne palvelimilla on n. 300 GB kuukaudessa. Tarkkailuväli on 36 kk (reserved VM), Administraattorin palkkiona 70 €/h ja lisenssi löytyy omasta takaa. Todellisuudessa käytössä olisi myös muita palveluita, mutta tasaisen vertailun vuoksi parametrit ovat rajoitettuna näihin.

Vertailua paikalliseen järjestelmään ei laskureilla suoritettu, sillä molempien palveluntarjoajien laskurit olivat best practice -käytännön mukaisen hintavahkon suunnittelun järjestelmille.

Paikallinen järjestelmä 36 kk

Tämä paikallisen järjestelmän karkea hinta-arvio toimii referenssinä, mutta ei sisällä tai ota tarkoituksella kaikkea huomioon. Esimerkiksi jäähdytyksen hinnoittelu ei sisälly tähän. Hinnat perustuvat kirjoituksen hetkellä oleviin

vallitseviin yleisiin listauksiin. Lähteinä valmistajien tai verkkokauppojen hinnat.

Palvelimet: 2 x HPE ProLiant DL360 Gen10 SMB Performance = 2 000 €/kpl

Lisenssit: 2 x Windows server 2016 Standard = 800 €/kpl

Kiintolevyt: 4 + 4 TB SFF Hot-Plug SAS-kiintolevytilaa = 1 600 €

Nauha-asema: 1 000 €

Räkkikaappi: 650 €

Sähkö: oletuksena 5 snt/kWh, palvelimien virrankulutus 500 W = 1 000 €

Asennus/ylläpito: 2 000 €

Fyysinen tila: 30 €/m² x 2 m² x 36 kk = 2 160 €

Kokonaishinta (TCO): 14 010 €

Azure 36 kk

Laskuri (Microsoft 2019j) olettaa kahden fyysisen palvelimen roolin yhdelle Azuren pilven palvelimelle, jossa on kaksi virtuaalikonetta. Jos halutaan kaksi teholtaan vastaavaa bare metal -instanssia, niin tulee käyttää Azure Dedicated Host -palvelua. Tämä on kuitenkin keskeneräinen tuote, joten lopullista dataa ei ole saatavilla. Laskuriin valitut spesifikaatiot:

- VM: 2 x F8sv2 Standard (8 core, 16 GB RAM) Windows (Azure Hybrid Benefit)
- Hyper-V
- 4 TB File storage
- 4 TB Backup.

€16,928

Cost over 3 year(s)

Azure cost breakdown summary

Category	Cost
Compute	€6,140.98
Data Center	€0.00
Networking	€779.01
Storage	€8,381.16
IT Labor	€1,627.5542
Total	€16,928.40

Kuva 19. Azuren TCOS-laskurin suuntaa antava tulos (Microsoft 2019j.)

Yllä kuvassa laskurin antama tulos hintakomponentteihin eriteltynä. Yhteensä 4 TB käytettävissä olevan tallennustilan kuukausihinnaksi muodostuu 0,038 €/GB ja datan varmennus Azuren Backup Storagella 0,0189 €/GB.

Virtuaalisten levyjen redundanssi on Microsoftin puolelta hoidettu, joten RAID-konfiguraatiolle ei ole tarvetta.

Microsoftin etuna on Windows-käyttöjärjestelmän markkinadominanssi sekä olemassaolevan lisenssionnin sekä päivitystuen helppo hyötykäyttö, jolloin tämä on kustannuksiensa puolesta houkutteleva vaihtoehto Windows-järjestelmiä runsaasti käytävissä yrityksissä.

AWS 36 kk ja Spot-hinnoittelu

Amazon sisällyttää mukaan yritystason tuen, josta saa esimerkiksi opastusta järjestelmien konfiguraatioon tapauskohtaisesti. Tallennustilan kuukausihinnaksi EBS st1 -tason HDD:lla muodostuu noin 0,05 €/GB. AWS:n TCOS-laskurin mukaan ulospäin suuntautuvan tiedonsiirron kuukausittainen hinta on 0,08 €/GB, jolloin 300 GB määrällä saadaan 36 kk hinnaksi 864 €. Virtuaalikoneinstanssien hinnaksi saadaan 5 095 €, tallennustilan kokonaishinnaksi 7 405 € initiaalisella täydellä snapshotilla ja tuen sekä IT-työn kokonaishinnaksi 1 270 €. Kolmen vuoden kokonaishinnaksi saadaan näin ollen 14 634 euroa. Huomioitavaa on, että snapshot-varmuuskopiointi maksaa 0,05 €/GB, mutta siitä laskutetaan vain käytetyn tilan mukaisesti. Tässä tapauksessa ei sisällytetty snapshoteja, mutta kyseisellä kokoonpanolla AWS:n kokonaishinnan vaihteluväliksi saadaan näin ollen 14 634 € – 21 834 €. Kuvassa alla esitettynä sopivin saatavilla oleva EC2-instanssi. (Amazon 2019f.)

Your AWS environment : EU (Ireland)

Closest AWS Instances					
# Instances	Instance	vCPU	RAM (GiB)	Optimize by	Instance type
2	m4.xlarge	4	16	RAM	3 Yr. Partial Upfront RI

Kuva 20. Parhaiten parametreihin sopiva EC2-instanssi (Amazon 2019f.)

Amazonin ekosysteemi on verrattavissa Microsoftin vastaavan tarjonnan hintoihin, joten lähinnä vain yksittäisissä palveluissa ja erikoistapauksissa syntyy merkittävä hintaero. Laskelmissa huomattiin, että EBS:ään verrattuna Azure Storage tarjoaa halvempaa tallennustilaa, varsinkin kun varmuuskopiointi otetaan huomioon.

Amazonin erikoisuutena on markkinataloudestakin tuttu Spot pricing eli spot-hinta. Ylimääräinen kapasiteetti kaupataan kysynnän ja tarjonnan lain mukaisesti ennalta määräämättömään, senhetkiseen hintaan aina maksimissaan kuusi tuntia eteenpäin kerrallaan. Referenssinä eli pohjahintana toimii on-demand-tuotehinnoittelu ja alennuskattona toimii 90 %:n alennus. Järjestelmä toimii jättämällä AWS:lle resurssipyyntö halutulla konfiguraatiolla ja lisämääreillä kuten maksimihinnalla. Jos kapasiteettia löytyy, niin ehtojen täytyttyä asiakas saa haltuunsa tilaamansa palvelut tai instanssit. Tämä soveltuu erityisen hyvin eräajoihin ja muihin intensiivisiin, mutta lyhytaikaisiin työtaakkoihin. Esimerkiksi suunnitteluohjelmistojätti Autodesk käyttää spot-hinnoiteltua kapasiteettia Rendering-as-a-Service -palvelunsa tukena, jonka ansiosta he puolittivat renderointikulunsa sekä kaksinkertaistivat renderointitöiden määrän. (Amazon 2019g.)

Yhteenveto	Hinta suhteessa paikalliseen
Paikallinen: 14 010 €	Referenssi
Azure: 16 928 €	+21 %
AWS: 14 634 € – 21 834 €	+5–56 %

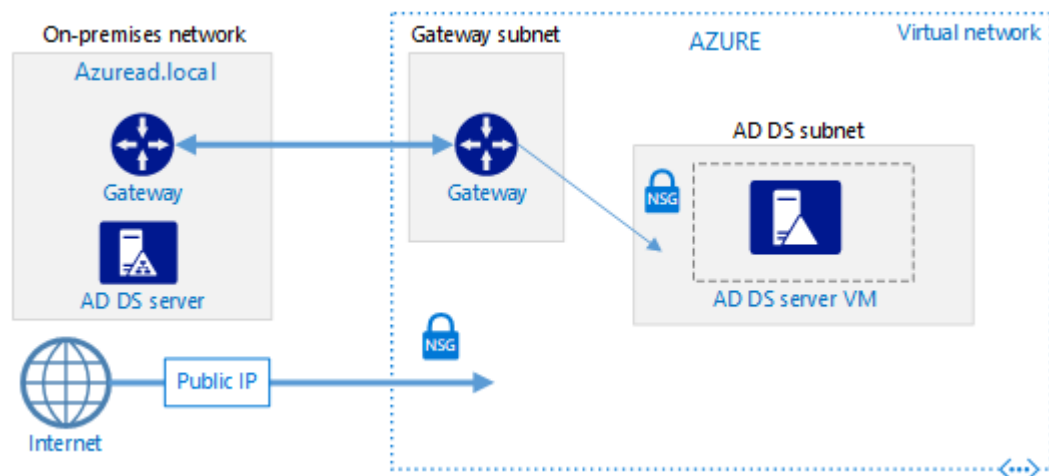
Pilvipalvelut edustavat noin neljäsosan kalliimpia hintoja näillä parametreilla, mutta tämä ei kata abstraktimpien asioiden kuten tietoturvan ulkoistamisen sekä georedundanssin arvoa.

7 INFRASTRUKTUURIN LAAJENTAMINEN AZUREN PILVEEN

Insinööriyön suorittavana osuutena toimi teoreettisen pienyrityksen palvelininfrastruktuurin laajentaminen Azuren pilveen. Ideana oli testata, miten paikalliset toiminnallisuudet kuten toimialue voitaisiin laajentaa pilveen, ja mitä uusia mahdollisuuksia tämä avaa esimerkiksi ympäristön rakentamisen,

konfiguroinnin, palveluiden saatavuuteen ja DR:n saralla. Azuren tarjoamat "Active Directory" -palvelut jätettiin teoreettiseksi osuudeksi samankaltaisuutensa takia, ja työssä päädyttiinkin pilvessä sijaitsevaan virtuaalikonepohjaiseen ratkaisuun. Paikallisen toimialueen ohjauskoneen toimintaa tukemaan liitettiin Azuren pilvestä toinen ohjauskone samaan forestiin, sekä tämän lisäksi liuta pilvipohjaisia palveluita kuten varmuuskopiointi. Replikaatio ohjauskoneiden välillä toimii kaksisuuntaisesti Remote Procedure Call -protokollalla, ja ohjauskoneet pystyvätkin toimimaan toisistaan riippumatta tarvittaessa. Operations master -roolit jätettiin paikallisen ohjauskoneen hartioille. Toimialueen ohjauskoneen sijoittaminen pilveen tarjoaa muutamia etuja, kuten georedundanssin, tietoturvan ulkoistamisen sekä latenssin vähentämisen, jos applikaatiot tai muut järjestelmät sijaitsevat myös pilvessä. (Microsoft 2018.)

Kuvassa 21 alla esitettynä käytetty testiympäristön verkkotopologia.

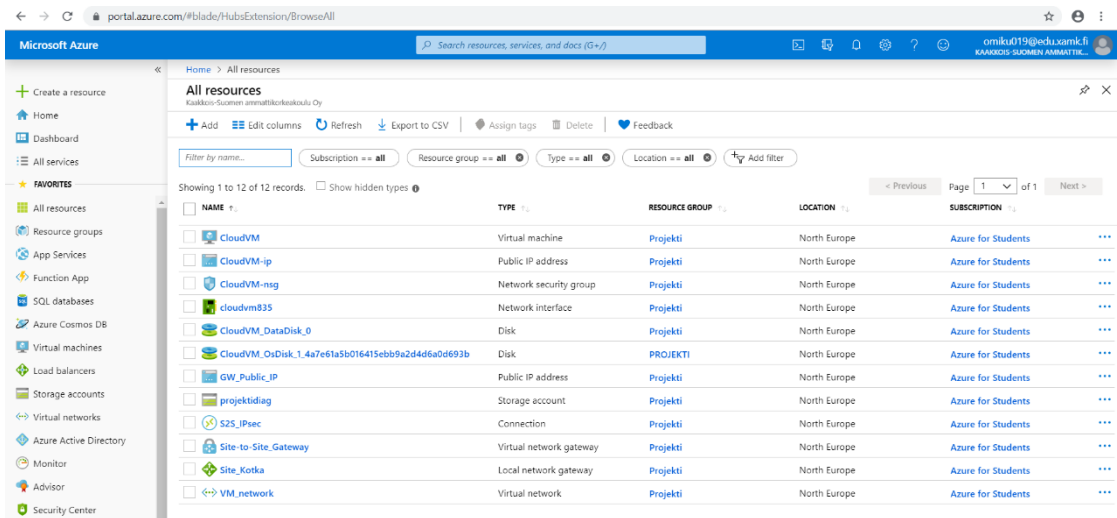


Kuva 21. Testiympäristön verkkotopologia

7.1 Testiympäristö

Valtaosa testauksista suoritettiin työpaikalla sijaitsevassa testiympäristössä, jonka ytimenä toimi HP:n ProLiant D380 -palvelinraudalle asennettu Windows Server 2016, Azuren pilveen perustettu Standard B2s -virtuaalikone Windows Server 2016 Datacenter -käyttöjärjestelmällä sekä hallintaan käytetty kannettava tietokone. Työlle relevanttina verkkolaitteena toimi ZyXELL ZyWALL USG50 -palomuuuri. Työ suoritettiin kahta Azure-tiliä käyttäen, joista toista käytettiin Azure AD Connect -ohjelmaa sekä hakemistoa varten.

Järjestely oli tämä puhtaasti logistisista syistä ja työ voitaisiin suorittaa myös yhtä tiliä käyttäen. Alla kuvassa 22 näkymä Azuren hallintaportaalista.



NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
CloudVM	Virtual machine	Projekti	North Europe	Azure for Students
CloudVM-ip	Public IP address	Projekti	North Europe	Azure for Students
CloudVM-nsg	Network security group	Projekti	North Europe	Azure for Students
cloudvm835	Network interface	Projekti	North Europe	Azure for Students
CloudVM_DataDisk_0	Disk	Projekti	North Europe	Azure for Students
CloudVM_OsDisk_1_4a7e61a5b016415ebb9a2d4d6a0d693b	Disk	PROJEKTI	North Europe	Azure for Students
GW_Public_IP	Public IP address	Projekti	North Europe	Azure for Students
projektidiag	Storage account	Projekti	North Europe	Azure for Students
S2S_IPsec	Connection	Projekti	North Europe	Azure for Students
Site-to-Site_Gateway	Virtual network gateway	Projekti	North Europe	Azure for Students
Site_Kotka	Local network gateway	Projekti	North Europe	Azure for Students
VM_network	Virtual network	Projekti	North Europe	Azure for Students

Kuva 22. Azuren hallintaportaali ja provisoidut resurssit

Virtuaaliverkon luominen

Työ aloitettiin luomalla Azureen Resource Group eli resurssiryhmä, mihin käytetyt palvelukomponentit voidaan kerätä helppoa hallintaa varten. Ensimmäisenä varsinaisena kokonaisuuden osana konfiguroitiin Azuren pilveen yksityisellä IP-osoitealueella sijaitseva VM_network-virtuaaliverkko sekä vastaavasti VM_subnet-aliverkko. Huomionarvoista on se, että luodun verkon piti olla eri alueella kuin paikallisen (on-site) verkon. Tämä virtuaaliverkko toimi pohjana site-to-site VPN:lle sekä pilven virtuaalipalvelimelle. Esimerkki käytetystä konfiguraatiosta CIDR-notaatiolla: VM_network - 172.20.0.0 /16 [172.20.0.0 – 172.20.255.255] 65 536 osoitetta VM_subnet - 172.20.1.0 /24 [172.20.1.0 – 172.20.1.255] 251 + 5 osoitetta varattu Azurelle.

Site-to-site IPsec VPN

Virtuaalisen verkon lisäksi Azuren hallintaportaalista luotiin staattisella julkisella IP-osoitteella varustettu yhdyskäytävä, jonka tyyppiä määriteltiin Policy-based VPN. Virtuaaliselle yhdyskäytävälle myös määritettiin "VM_network" -virtuaaliverkko sekä 172.20.0.0 /26 aliverkko. Alla kuva virtuaalisen yhdyskäytävän konfiguraatiosta.

Home > Virtual network gateways > Create virtual network gateway

Create virtual network gateway

* Subscription ▼ Azure for Students

Resource group ? Projekti (derived from virtual network's resource group)

Instance details

* Name ✓ Site-to-Site_Gateway

* Region ▼ (Europe) North Europe

* Gateway type ? ☒ VPN ☐ ExpressRoute

* VPN type ? ☐ Route-based ☒ Policy-based

* SKU ? Basic ▼

? Only virtual networks in the currently selected subscription and region are listed.

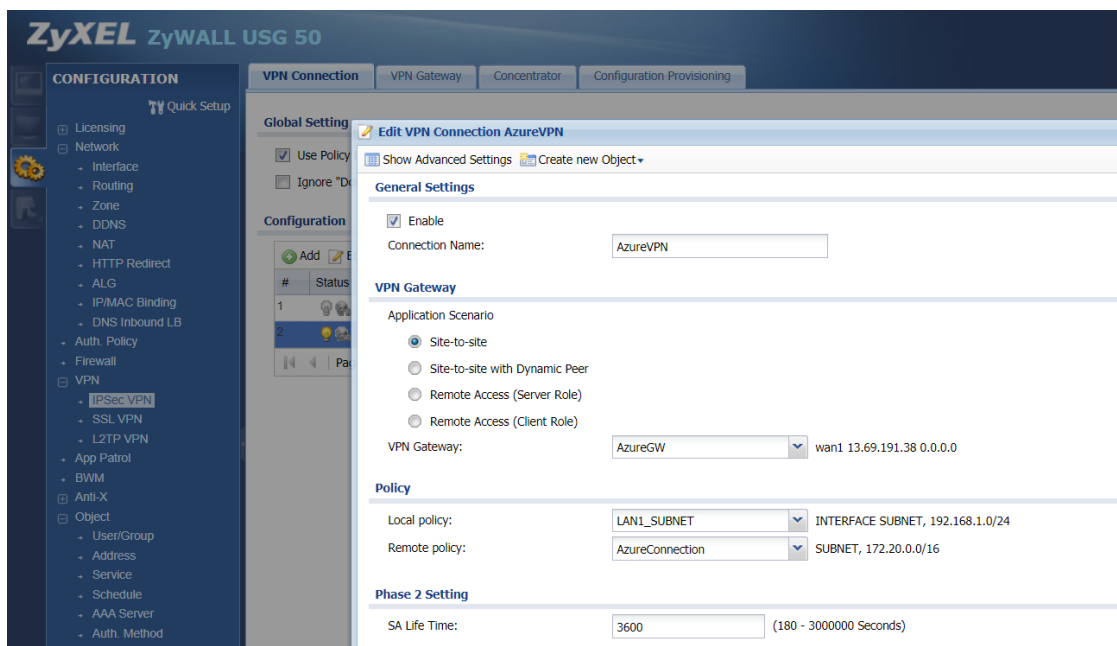
VIRTUAL NETWORK

* Virtual network ? VM_network ▼

Gateway subnet address range 172.20.0.0/26

Kuva 23. Virtuaalisen oletusyhdyskäytävän luonti Azuren portaalissa

Tämän vastapariksi hallintaportaaliin luotiin myös paikallinen yhdyskäytävä ”Site_Kotka” konfiguroituna palomuurin staattisella julkisella IP-osoitteella sekä sisäverkon yksityisellä osoitealueella. Seuraavaksi konfiguroitiin ZyWALL USG50 -palomuurin päähän VPN-yhdyskäytävä ja VPN-yhteys AES256- ja SHA2-salauksella. Kuvassa 24 esitettynä palomuurin konfigurointi VPN-yhteyttä varten.



Kuva 24. Palomuurin konfigurointi

Lisäksi Azureen määritettiin Site-to-Site IPsec -tunnelin toinen pää sekä lisättiin Google Cloudilla generoitu vahva jaettu avain (PSK) tunnelin molempiin päihin.

Azure VM

Hallintaportaalista provisioitiin Standard B2s -tason CloudVM -niminen virtuaalikone lisälevyllä sekä Windows Server 2016 Datacenter -käyttöjärjestelmällä. Virtuaalikoneen verkkokortille määritettiin hallinnasta yksityinen staattinen IP-osoite 172.20.1.4, sillä Azure varaa neljä ensimmäistä aliverkon osoitetta. Azuressa pääsyylistana toimivasta Network Security Group -moduulista pystyttiin konfiguroimaan inbound/outbound-säännöt, eli esimerkiksi määrittämään mm. RDP:lle auki portti 3389. Tätä ei kuitenkaan tarvittu, sillä Internetiin päin ei tarvittu liikennöidä ja virtuaalikoneen vakiona tuleva julkinen IP-osoite poistettiin. Kuvassa 25 esitettynä Azuren ACL.

65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny	...

Kuva 25. Pääsyylistan hallinta Azuressa

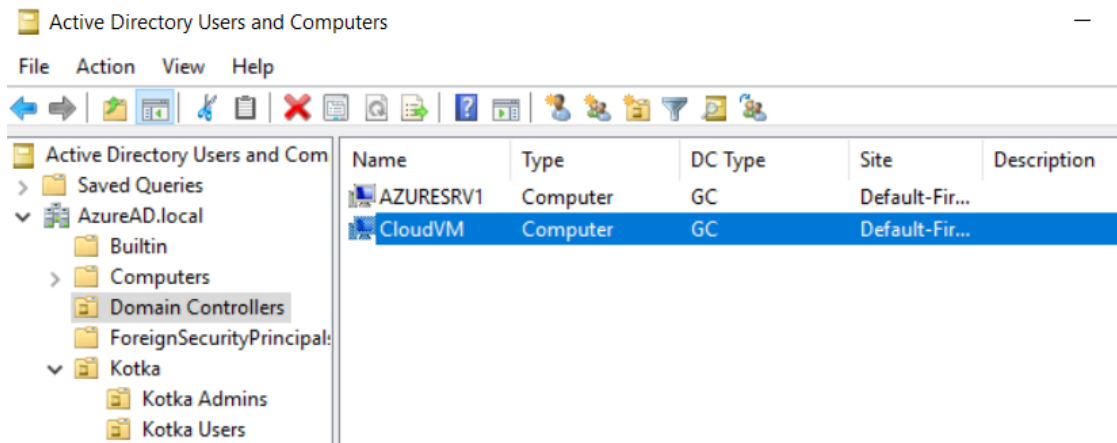
Tämän jälkeen työasemalta otettiin RDP:llä yhteys CloudVM:ään ja määritettiin tälle Active Directory Domain Services muuten perusasetuksin, mutta esimerkiksi SYSVOL määritettiin lisälevylle. CloudVM:lle myös määritettiin paikallisen verkon DNS-palvelimet, jotta tämä osaisi etsiä paikallisen toimialueen. Kuvassa 26 todennettiin nimiresoluution toimivuus perinteisellä pingauksella pilven virtuaalikoneen komentoriviltä.

```
C:\windows\system32>ping azuresrv1

Pinging AzureSrv1.AzureAD.local [192.168.1.10] with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=63ms TTL=125
Reply from 192.168.1.10: bytes=32 time=63ms TTL=125
Reply from 192.168.1.10: bytes=32 time=62ms TTL=125
```

Kuva 26. CloudVM:n komentoriviltä pingaus

CloudVM liitettiin paikalliseen (AzureAD.local) toimialueeseen, jota seurasi tämän korotus toimialueen toiseksi ohjauskoneeksi. Kuvassa alla toimialueen Global Catalog -rooleilla varustetut ohjauskoneet AZURESrv1 ja CloudVM.



Kuva 27. Ohjauskoneet toimialueessa

Tiedonsiirtonopeuksia empiirisesti kokeiltaessa huomattiin, että perus-SKU:n mainostamaan 100 Mbps nopeuteen lähellekään ei ylletty. Microsoftin dokumentaation mukaan VPN:n kaistan nopeuden odotusarvo voidaan laskea jakamalla hitaimman linkkivälin nopeus kahdeksalla. Tämä ei kuitenkaan vaikuta esimerkiksi pilvipohjaisten varmuuskopioiden ottoon, sillä ne menevät julkisen Internetin yli Azuren palvelimille. Azure Backup -palvelu otettiin käyttöön asentamalla paikalliselle palvelimelle MARS agent -sovellus, joka määritettiin ottamaan "system state" -varmuuskopioita säännöllisesti Azureen. Azuren hallintaportaalista näkymä varmuuskopioinnista esitettynä kuvassa 28.

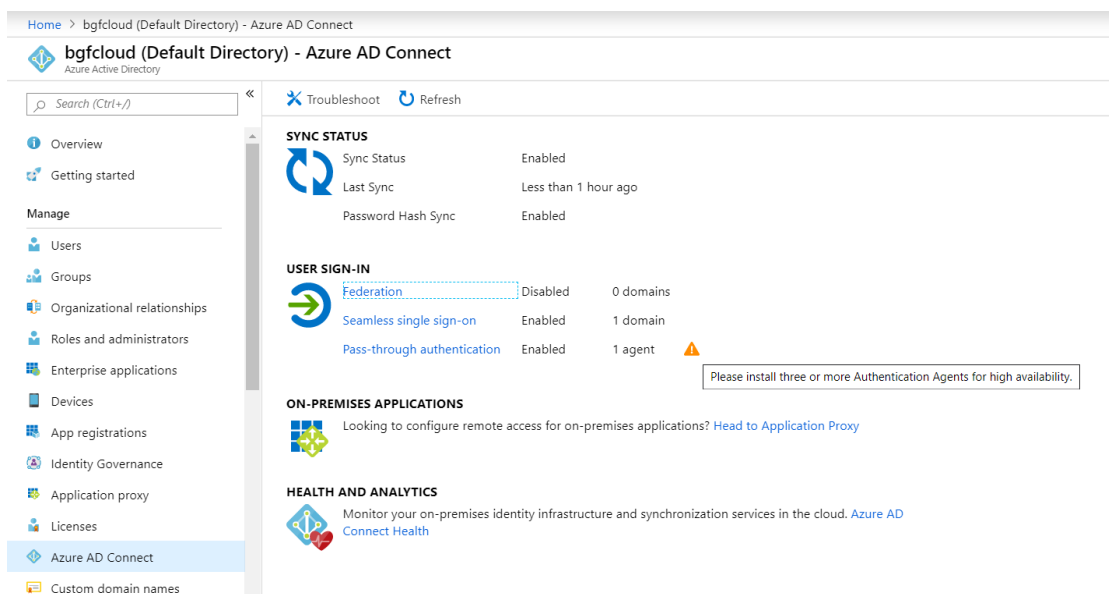
WORKLOAD NAME	OPERATION	STATUS	TYPE	START TIME	DURATION
azuresrv1.azuread.local	Backup	Completed	Files and folders	10/11/2019, 10:51:42 AM	01:43:28

Kuva 28. Azure Backup

Azure Active Directory

Hybriditoimialue toteutettiin liittämällä Azure Active Directory (AAD) paikalliseen toimialueeseen Azure Active Directory Connect -nimisellä ohjelmalla, joka konfiguroitiin hoitamaan käyttäjien identiteetin migraatio, synkronointi ja autentikaatio pilven ja paikallisen infrastruktuurin välillä. Graafisen käyttöliittymän kautta määritettiin service connection point (SCP) toimialueen metsään, jonka avulla toimialueeseen liitetyt laitteet löysivät tarvittavat Azure AD:n tiedot. Azuren ja liittämishjelmiston määrittäykset pystytään suorittamaan GUI:n lisäksi myös esimerkiksi PowerShell-skripteillä. Seamless Single Sign-on (SSSO) konfiguroitiin päästämään Azureen rekisteröityneet käyttäjät paikallisiin resursseihin saumattomasti.

Azure AD:ta varten rekisteröitiin ja liitettiin ”bgfcloud.fi” -niminen verkkotunnus toimimaan reitityskelpoisena UPN-suffiksina sekä luotiin AAD-hakemisto ”bgfcloud”. Tämä UPN-suffiksi myös lisättiin paikallisille käyttäjille .local-päätteen lisäksi. Kuvassa alla näkyvät pass-through-autentikaatio sekä SSSO aktivoituna AAD:n hallintaportaaliassa. Pass-through-autentikaatiossa validaatiopyynnöt menevät paikallisen AD:n kautta.



Kuva 29. Azure AD Connect SSSO:lla ja PTA:lla

Hybrid Azure AD Join

Alustavan työn päätteeksi päästiin lisäämään paikallinen Hyper-V pohjainen Windows 10 -käyttöjärjestelmällä varustettu WinDev1909Eval-virtuaalikone AzureAD.local toimialueeseen, jonka jälkeen virtuaalikoneelle kirjaututtiin Azure AD:ssa luodulla grizzly@bgfcloud.fi tilillä, jolloin koneen status muuttui hybridiliitetyksi toimialueeseen. Tämä varmistettiin katsomalla tila Azuren hallintaportaaliasta. Esitettyä kuvassa 30 alla.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered
<input type="checkbox"/> WinDev1909Eval	✔ Yes	Windows	10.0.18362.0	Hybrid Azure AD join...	N/A	None	N/A	10/31/2019, 3:25:59 PM
<input type="checkbox"/> DESKTOP-TOS3P85	✔ Yes	Windows	10.0.17763.0	Azure AD joined	Niilo Kosol	None	N/A	10/15/2019, 3:25:49 PM
<input type="checkbox"/> DESKTOP-TJKIL9T	✔ Yes	Windows	10.0.17763.0	Azure AD joined	Vieraileva Tahti	None	N/A	2/6/2019, 2:58:42 PM

Kuva 30. Hyper-V pohjainen WinDev1909Eval virtuaalikone hybridiliitettynä toimialueeseen

Tällä metodilla koneelle kirjautuneella käyttäjätillä pystyttiin toimimaan samanaikaisesti sekä paikallisessa ympäristössä että Azuren pilviympäristössä.

8 JOHTOPÄÄTÖS

Pilvipalvelut, joista vielä tarkemmin eriteltynä laaS-palvelut, tarjoavat erityisesti kasvaville yrityksille pätevän ja joustavan alustan skaalata toimintaansa tilanteensa mukaisesti. Pilvipalvelumallin ”avaimet käteen” -konseptin pohjalta tarjotaan valmiiksi paketoituja, ammattimaisesti ylläpidettyjä kokonaisuuksia yrityksen käyttöön, jotka normaalisti saattaisivat olla hyvinkin haastavia toteuttaa omatoimisesti. Tähän kokonaisuuksien joukkoon lukeutuu myös käyttäjän autonomian kasvattaminen esimerkiksi itsepalveluportaaleilla, mikä tuo joustavuutta sekä madaltaa oletusarvoisesti keskitettyä tietoteknistä työtaakkaa. Lähtökohtaisesti uuden järjestelmän optimaalinen hyödyntäminen tapahtuu asteittain, mutta etenkin työssä esitelty laaS-tyypin palvelut ovat luokitelmansa mukaisesti käyttörajapinnan ulkopuolella, joten yleisen käyttäjän näkökulmasta suurempia haasteita ei ilmene siirryttäessä pilvipalveluihin.

Perinteisen paikallisen infrastruktuurin ja palvelinroolien sijoittaminen pilveen on pätevä vaihtoehto silloin, kun tarvitaan nopeaa skaalautuvuutta sekä yksinkertaistusta suhteellisen ylläpitointensivisiin järjestelmiin. Aloittavan yrityksen odotusarvoisen elinkaaren perusteella käyttöperusteinen laskutus on pätevä vaihtoehto, sillä näin saavutetaan madalletun finansiaalisen riskin lisäksi resurssien potentiaalinen vapautus muuhun yritystoimintaan. Yleisimmin pidemmän aikavälin korkein kustannustehokkuus kuitenkin saavutetaan paikallisella järjestelmällä, erityisesti kun osittain karsitaan ”best practice” -standardin mukaisia järjestelmäsuunnittelun sekä ylläpidon toimintatapoja.

Urakkaluonteisen Rendering-as-a-Service-palvelun käytön pohjalta huomattiin trendi, jonka mukaan pilvipalvelut osoittautuvat spesifisissä tapauksissa edullisimmiksi malleiksi valmiin infrastruktuurinsa sekä käyttöperusteisen laskutuksensa vuoksi. Pilvipalvelut sopivat näin ollen myös ennakoitavissa olevien rasisuippujen tueksi, tilapäisen lisäkapasiteetin tarpeen täyttämiseksi sekä kausiluontoiseen käyttöön. Työn aikana myös huomattiin pilvipalveluiden soveltuvan erityisen hyvin tallennus- ja varmennusratkaisuiksi, sillä datan käsittely CSP:n puolelta on parhaimpien käytäntöjen mukaista. Työssä esitettyjen kokonaisuuksien pohjalta voidaan todeta, että pilvipohjaisten palveluiden käyttö tarjoaa useita etuja PK-yrityksille, joita on

syytä harkita järjestelmiä suunniteltaessa. Näin ollen vastaan alkuperäiseen tutkimuskysymykseen sanomalla kyllä, varsinkin aloittavan yrityksen kannattaa hyödyntää pilven tarjoamia mahdollisuuksia.

Amazon Web Services pitää vahvaa markkinajohtajan asemaa ja on enemmän kuin varteenotettava vaihtoehto tarjoamansa mittavan käyttöhistorian omaavan sekä toimivaksi todetun API-kokoelmansa ansiosta. Microsoftin Azure saattaa kuitenkin tuotteidensa yleisyyden sekä lisenssiensä (esim. Windows Server & SQL Server) uusiokäytön takia viedä houkuttelevimman CSP:n aseman PK-yrityksien näkökulmasta. O365:n tilaus sisältää ilmaisia Azuren palveluita, joten tämä on kustannustehokkuuden näkökulmasta vahva etu. Amazonin spot-hinnoittelu kuitenkin tarjoaa vahvan insentiivin käyttää heidän palveluitansa, vaikka muut palvelut hankittaisiinkin esimerkiksi Microsoftilta. On siis täysin mahdollista käyttää rinnakkain useamman CSP:n palveluita.

Soveltuvuusselvityksien teko eri käyttötarkoituksiin, sekä olennaisen dokumentaation lukeminen kulutti huomattavasti aikaa palveluiden yksinkertaisen runsauden ansiosta. Pilvipalvelut eivät olleet ennestään kovinkaan tuttuja, joten aiheeseen orientoituminen vaati oman työnsä. Yhteensä eri palveluita AWS:llä ja Azurella on useita satoja. Tapaustutkimuksen omaisesti suoritettu testiympäristön infrastruktuurin ja luodun toimialueen laajennus Azuren pilveen onnistui melkoisen mutkattomasti, mutta osittainen epävarmuus erityistapauksista hidasti ongelmanratkaisua hieman. Paikalliverkon looginen liitäntä pilveen onnistui suunnitellusti Site-to-Site IPSec VPN -tunnelin avulla, jonka pohjalta saatiin käytännön näkemystä vastaavan järjestelyn toiminnasta. Azure Active Directoryn Pääsääntöisesti ongelmat ratkesivat melkoisen helposti. Yhtenä esimerkkinä mainittakoon tapaus, jossa virtuaalikoneen korottaminen toimialueen ohjauskoneeksi ei ensiksi onnistunut, mutta kävikin ilmi että paikallisen toimialueen uudelleennimeäminen oli kesken, josta päästiin syöttämällä paikallisen palvelimen komentoriville *rendom /end*.

Tehdyn työn pohjalta todettiin pilvipalveluiden kykenevän toimimaan hyväksyttävästi yritystoiminnalle kriittisinä IT-järjestelminä sekä näiden sovellutuksina, kuten käyttäjähallinnan runkona, palvelinalustana ja

varmennusratkaisuna. Opinnäytetyön tavoitteisiin päästiin ja tuloksena syntyi toimiva testiympäristö sekä aiheeseen liittyvä dokumentaatio.

Jatkokehityksenä ehdotan kokonaisuutena pilvipohjaisten virtuaalikoneiden optimaalisiin käyttötarkoituksiin syvempää perehtymistä, sekä datanhallinnan 3-2-1-säännön mukaisesti BCDR- ja varmuuskopiointiratkaisuiden korvaamista tai täydentämistä pilviratkaisuilla.

Toinen esittämäni vahvemmin tietoverkkotekniikkaan nojaava jatkotyömahdollisuus olisi tutkia omavalintaisen pilvipalveluntarjoajan käyttöä useamman toimipisteen yritysverkon "backbonena" implementoimalla CSP:n tukema Software-Defined Wide Area Network -ratkaisu (SD-WAN). Tämä tarjoaisi järeämmän kontrollin ja toiminnan verrattuna perinteiseen VPN-malliin. Azuren tapauksessa yhteydet toimipisteiltä virtualiseen WAN:iin on toteutettu kahdella active/active IPsec -tunnelilla.

LÄHTEET

Ai, Y., Peng, M. & Zhang, K. 2018. Edge Computing Technologies for Internet of Things: a primer. *Digital Communications and Networks* 4 (2), 77–86. WWW-dokumentti. Saatavissa: <https://www.sciencedirect.com/science/article/pii/S2352864817301335> [viitattu 7.4.2019].

Amazon. 2019a. Global Infrastructures Regions and AZs. WWW-dokumentti. Saatavissa: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2 [viitattu 26.8.2019].

Amazon. 2019b. Shared Responsibility Model. WWW-dokumentti. Saatavissa: <https://aws.amazon.com/compliance/shared-responsibility-model/> [viitattu 3.10.2019].

Amazon. 2019c. Introducing Five New Amazon EC2 Bare Metal Instances. WWW-dokumentti. Saatavissa: <https://aws.amazon.com/about-aws/whats-new/2019/02/introducing-five-new-amazon-ec2-bare-metal-instances/> [viitattu 14.7.2019].

Amazon. 2019d. Durability & Data Protection. WWW-dokumentti. Saatavissa: https://aws.amazon.com/s3/faqs/#Durability_.26_Data_Protection [viitattu 18.9.2019].

Amazon. 2019e. What is IAM? WWW-dokumentti. Saatavissa: <https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html> [viitattu 6.10.2019].

Amazon. 2019f. AWS Total Cost of Ownership (TCO) Calculator. Verkkosivu. Saatavissa: <https://awstcocalculator.com/> [viitattu 16.10.2019].

Amazon. 2019g. Autodesk Spot Instances. WWW-dokumentti. Saatavissa: <https://aws.amazon.com/solutions/case-studies/autodesk-spot-instances/> [viitattu 15.8.2019].

Vahteri, M. 2019. Bitgroup Finland OY. WWW-dokumentti. Saatavissa: <https://www.bitgroup.fi/> [viitattu 5.7.2019].

Canalys. 2019. Cloud Market Share Q4 2018 and Full Year 2018. WWW-dokumentti. Saatavissa: <https://www.canalys.com/newsroom/cloud-market-share-q4-2018-and-full-year-2018> [viitattu 6.4.2019].

Cisco. 2015. Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. PDF-dokumentti. Saatavissa: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf [viitattu 7.4.2019].

De Tender, P. 2016. Implementing Operations Management Suite. Berkeley, CA: Apress.

De Tender, P. 2019. Pro Azure Governance and Security. Berkeley, CA: Apress.

DigitalOcean. 2016. What is High Availability? WWW-dokumentti. Saatavissa: <https://www.digitalocean.com/community/tutorials/what-is-high-availability> [viitattu 1.5.2019].

Dube, M. & Dixit, S. 2011. Comprehensive Measurement Framework for Enterprise Architectures. *International Journal of Computer Science & Information Technology* 3 (4), 71-92. PDF-dokumentti. Saatavissa: <https://arxiv.org/ftp/arxiv/papers/1109/1109.1891.pdf> [viitattu 1.5.2019].

Finn, A. 2016. Best Practices for Domain Controller VMs in Azure. WWW-dokumentti. Saatavissa: <https://www.petri.com/best-practices-domain-controller-vms-azure> [viitattu 7.9.2019].

Frankel, S. & Krishnan, S. 2011. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. IETF RFC6071. WWW-dokumentti. Saatavissa: <http://www.hjp.at/doc/rfc/rfc6071.html> [viitattu 4.8.2019].

Freato, R. 2015. Microsoft Azure Security. Birmingham: Packtpub.

Ganguli, S. 2017. Computer Operating Systems: From every palm to the entire cosmos in the 21st Century Lifestyle. *CSI Communications* 40, 5–7. PDF-dokumentti. Saatavissa: http://www.csi-india.org/Communications/CSIC_Feb_2017.pdf [viitattu 19.6.2019].

Ghobakloo, M., Hong, T., Sabouri, M. & Zulkifli, N. 2012. Strategies for Successful Information Technology Adoption in Small and Medium-sized Enterprises. *Information* 2012 3, 36–67. WWW-dokumentti. Saatavissa: <https://doi.org/10.3390/info3010036> [viitattu 8.5.2019].

Hu, Y., Patel, M., Sabella, D., Sprecher, N. & Young, V. 2015. Mobile Edge Computing A key technology towards 5G. ETSI White Paper No.11. PDF-dokumentti. Saatavissa: https://yucianga.info/wp-content/uploads/2015/11/Ref02-2015-09-etsi_wp11_mec_a_key_technology_towards_5g.pdf [viitattu 24.4.2019].

IDC. 2014. DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified. PDF-dokumentti. Saatavissa: <http://www.smalllake.kr/wp-content/uploads/2013/07/DevOps-metrics-Fortune1K.pdf> [viitattu 11.5.2019].

Kananen, J. 2015. Online Research for Preparing Your Thesis. Jyväskylä: JAMK University of Applied Sciences.

Karthikeyan, S. 2018. Practical Microsoft Azure IaaS. Berkeley, CA: Apress.

Lewin, K. 1946 Action Research and Minority Problems. *Journal of Social Issues* 2, 34–46. PDF-dokumentti. Saatavissa: http://www.cscd.osaka-u.ac.jp/user/rosaldo/K_Lewin_Action_research_minority_1946.pdf [viitattu 29.3.2019].

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145. PDF-dokumentti. Saatavissa: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [viitattu 30.3.2019].

Microsoft. 2019a. Microsoft Azure. WWW-dokumentti. Saatavissa: <https://azure.microsoft.com/en-us/> [viitattu 31.3.2019].

Microsoft. 2019b. Azure network architecture. WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-network> [viitattu 11.8.2019].

Microsoft. 2019c. Azure Sentinel. WWW-dokumentti. Saatavissa: <https://azure.microsoft.com/en-us/services/azure-sentinel/> [viitattu 11.8.2019].

Microsoft. 2019d. Windows Virtual Machine Pricing. WWW-dokumentti. Saatavissa: <https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/> [viitattu 11.8.2019].

Microsoft. 2019e. Connect an on-premises network to a Microsoft Azure virtual network. WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/office365/enterprise/connect-an-on-premises-network-to-a-microsoft-azure-virtual-network> [viitattu 6.8.2019].

Microsoft. 2019f. Security. WWW-dokumentti. Saatavissa: <https://azure.microsoft.com/en-us/product-categories/security/> [viitattu 11.8.2019].

Microsoft. 2019g. Azure Active Directory Seamless Single Sign-On. WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ssso> [viitattu 9.9.2019].

Microsoft. 2019h. Domains FAQ. WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/office365/admin/setup/domains-faq?view=o365-worldwide> [viitattu 10.6.2019].

Microsoft. 2019i. Compare Identity Solutions. WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/compare-identity-solutions> [viitattu 20.10.2019].

Microsoft. 2019j. Azure Pricing. WWW-dokumentti. Saatavissa: <https://azure.microsoft.com/en-us/pricing/> [viitattu 10.10.2019].

Microsoft. 2018. Compare Identity Solutions. WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/adds-extend-domain> [viitattu 8.8.2019].

Microsoft. 2017. Configure Multiple VIPs for a cloud service. WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip> [viitattu 1.5.2019].

Nurmi, J. 2016. Implementation of Nested Virtual Laboratory System. Kymenlaakso University of Applied Sciences. Opinnäytetyö. PDF-dokumentti. Saatavissa: <http://urn.fi/URN:NBN:fi:amk-201604204658> [viitattu 6.4.2019].

OpenFog. 2017. OpenFog Reference Architecture for Fog Computing. PDF-dokumentti. Saatavissa: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf [viitattu 5.5.2019].

Oracle. 2019. Dynamic DNS. WWW-dokumentti. Saatavissa: <https://dyn.com/remote-access/> [viitattu 4.8.2019].

Price, J.A., Price, B. & Fenstermacher, S. 2008. Mastering Active Directory for Windows Server 2008. Hoboken: John Wiley & Sons, Incorporated.

Tilastokeskus. 2013. Yritysrekisterin vuositilasto 2012. Helsinki: Edita Publishing OY. PDF-dokumentti. Saatavissa: http://www.stat.fi/til/syr/2012/syr_2012_2013-11-28_fi.pdf [viitattu 7.8.2019].

Tilastokeskus. 2017. Aloittaneet ja lopettaneet yritykset vuonna 2016. Helsinki: Edita Publishing OY. PDF-dokumentti. Saatavissa: http://www.stat.fi/til/aly/2016/aly_2016_2017-10-31_fi.pdf [viitattu 24.11.2019].

Tilastokeskus. 2019. Pienet ja keskisuuret yritykset. WWW-dokumentti. https://www.stat.fi/meta/kas/pienet_ja_keski.html [viitattu 7.4.2019].

Tutunea, M.F. 2014. Smes' Perception on Cloud Computing Solutions. *Procedia Economics and Finance* 15, 514–521. WWW-dokumentti. Saatavissa: [https://doi.org/10.1016/S2212-5671\(14\)00498-5](https://doi.org/10.1016/S2212-5671(14)00498-5) [viitattu 6.9.2019].

Uhl, R. 2015. Disaster Recovery of On-Premises IT Infrastructure with AWS. WWW-dokumentti. Saatavissa: <https://www.slideshare.net/AmazonWebServices/disaster-recovery-of-onpremises-it-infrastructure-with-aws> [viitattu 6.10.2019].

451 Research. 2017. Size and Impact of Fog Computing Market. WWW-dokumentti. Saatavissa: <https://www.openfogconsortium.org/wp-content/uploads/451-Research-report-on-5-year-Market-Sizing-of-Fog-Oct-2017.pdf> [viitattu 6.4.2019].

Liite 1

KUVALUETTELO

Kuva 1. Pilvipalveluiden markkinaosuudet ja kasvu. Canalys. 2019. Cloud Market Share Q4 2018 and Full Year 2018. Saatavissa:

<https://www.canalys.com/newsroom/cloud-market-share-q4-2018-and-full-year-2018> [viitattu 6.4.2019].

Kuva 2. Paikallisen infrastruktuurin ja pilven kustannuksien graafinen esitys. Kodak. 2017. For Print Service Providers, the Sky's the Limit with Cloud Computing. Saatavissa: https://www.kodak.com/gb/en/prinergy-workflow/Blog/Blog_Post/?ContentId=4295002215 [viitattu 6.5.2019].

Kuva 3. Fog-verkon hierarkinen referenssiarkkitehtuuri. OpenFog. 2017. OpenFog Reference Architecture for Fog Computing. Saatavissa: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf [viitattu 5.5.2019].

Kuva 4. http://www.stat.fi/til/aly/2016/aly_2016_2017-10-31_fi.pdf

Kuva 5. Hahmotelma yleisestä verkkotopologiasta pienyrityksessä.

Kuva 6. Esimerkki saatavuuden ja tappion suhteesta. Pisello, T. & Quirk, B. 2004. How to quantify downtime. Saatavissa:

http://www.awarenautics.com/NTi2005/Press_Room/Downtime_Article.pdf [viitattu 8.7.2019].

Kuva 7. Keskimääräinen korjausaika infrastruktuurin vikatilanteessa. IDC. 2014. DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified. Saatavissa: <http://www.smallake.kr/wp-content/uploads/2013/07/DevOps-metrics-Fortune1K.pdf> [viitattu 11.5.2019].

Kuva 8. Päätökseen vaikuttavat tekijät. Strategies for Successful Information Technology Adoption in SME. Ghobakhloo, M., Hong, T., Sabouri, M. & Zulkifili, N. 2012. Saatavissa: <https://www.mdpi.com/2078-2489/3/1/36>

Kuva 9. Konseptuaalinen malli tehokkaaseen IT-järjestelmän käyttöönottoon. Strategies for Successful Information Technology Adoption in SME.

Ghobakhloo, M., Hong, T., Sabouri, M. & Zulkifili, N. 2012. Saatavissa: <https://www.mdpi.com/2078-2489/3/1/36>

Kuva 10. Vastuualuejako asiakkaan ja Amazonin välillä. Amazon. 2019b. Shared Responsibility Model. Saatavissa:

<https://aws.amazon.com/compliance/shared-responsibility-model/> [viitattu 3.10.2019].

Kuva 11. Paikallisen infrastruktuurin heitto komponenteittain pilveen vikatilanteessa. Uhl, R. 2015. Disaster Recovery of On-Premises IT Infrastructure with AWS. WWW-dokumentti. Saatavissa:

<https://www.slideshare.net/AmazonWebServices/disaster-recovery-of-onpremises-it-infrastructure-with-aws> [viitattu 6.10.2019].

Kuva 12. Azure-datakeskusten DLA- ja Q10 Clos verkkotopologiat. Microsoft 2019b. Azure Network Architecture. Saatavissa: <https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-network> [viitattu 11.8.2019].

Kuva 13. D-luokan virtuaalikoneiden hintalistaus. Microsoft. 2019d. Windows Virtual Machine Pricing. Saatavissa: <https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/> [viitattu 11.8.2019].

Kuva 14. Virtuaalikoneen ympäristö Azuren pilvessä. Linkletter, B. 2018. Create a nested virtual machine in a Microsoft Azure Linux VM. Saatavissa: <https://www.brianlinkletter.com/create-a-nested-virtual-machine-in-a-microsoft-azure-linux-vm/> [viitattu 7.8.2019].

Kuva 15. Microsoft 2019. Azure Active Directory Seamless Single Sign-On. Saatavissa: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ssso> [viitattu 9.10.2019].

Kuva 16. Azure Monitorin läpileikkaus. Microsoft. 2019f. Azure Monitor Overview. Saatavissa: <https://docs.microsoft.com/en-us/azure/azure-monitor/overview> [viitattu 26.10.2019].

Kuva 17. Paikallisen toimialueen ja Azuren välinen Kerberos autentikaatio. Microsoft. 2019g. Saatavissa: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ssso> [viitattu 9.9.2019].

Kuva 18. AAD & AAD DS palveluiden vertailu. Microsoft. 2019i. Compare Identity Solutions. Saatavissa: <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/compare-identity-solutions> [viitattu 23.10.2019].

Kuva 19. Azuren TCOS-laskurin suuntaa antava tulos. Microsoft. 2019j. Total Cost of Ownership (TCO) Calculator. Saatavissa: <https://azure.microsoft.com/en-us/pricing/tco/calculator/> [viitattu 15.10.2019].

Kuva 20. Parhaiten parametreihin sopiva EC2-instanssi. Amazon. 2019f. AWS Total Cost of Ownership (TCO) Calculator. Verkkosivu. Saatavissa: <https://awstcocalculator.com/> [viitattu 16.10.2019].

Kuva 21. Testiympäristön verkkotopologia.

Kuva 22. Azuren hallintaportaali & provisoidut resurssit.

Kuva 23. Virtuaalisen oletusyhdyntävän luonti Azuren portaalissa.

Kuva 24. Palomuurin konfigurointi.

Kuva 25. Pääsyylistan hallinta Azuressa.

Kuva 26. CloudVM:n komentoriviltä pingaus.

Kuva 27. Ohjauskoneet toimialueessa.

Kuva 28. Azure Backup

Kuva 29. Azure AD Connect SSSO:lla ja PTA:lla.

Kuva 30. Hyper-V pohjainen WinDev1909Eval virtuaalikone hybridiliitettynä toimialueeseen.