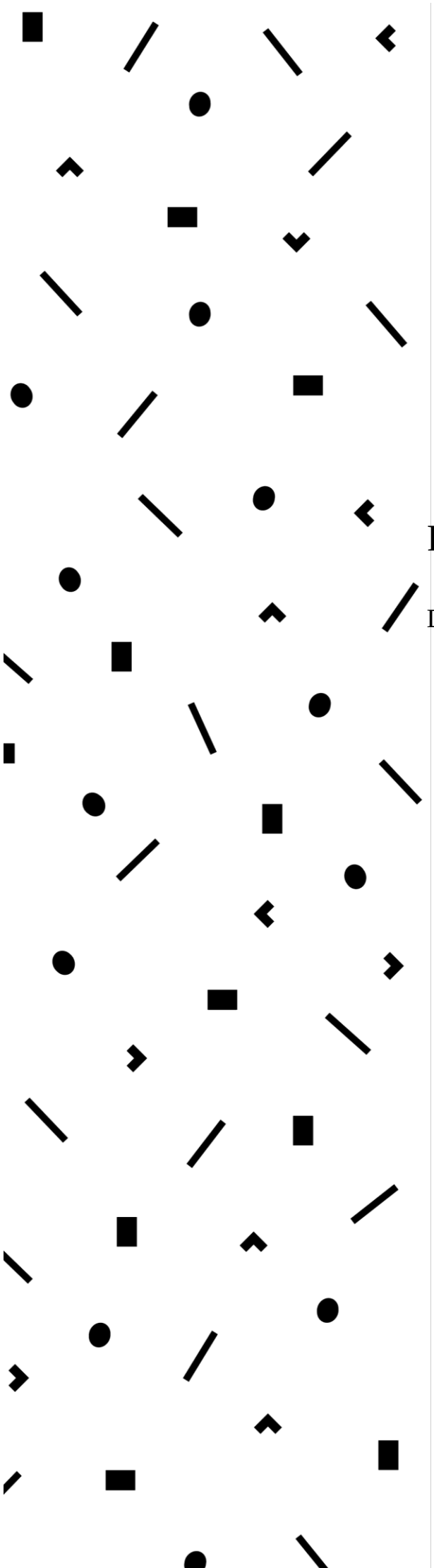


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

# PILVIPALVELUT JA PIENYRITYS

## Domain Controller Microsoft Azuressa

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Saku Lehtimäki

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

LEHTIMÄKI, SAKU: Pilvipalvelut ja pienyritys
Domain Controller Microsoft Azuressa

Tietoliikennetekniikan opinnäytetyö, 39 sivua, 1 liitesivu

Kevät 2015

TIIVISTELMÄ

---

Tämä työ tarkastelee virtualisointia sekä pilvipalveluita ja niiden kustannustehokasta käyttöä pienyrityksen toiminnassa. Työn tavoitteena oli selvittää, mitä virtualisointi ja pilvipalvelut tarkoittavat ja mitkä ovat niiden hyödyt ja mahdolliset riskit. Työn pääpaino oli käytännön toteutuksessa, jossa Microsoft Azure -pilvipalvelusta otettiin käyttöön Active Directory -toimialue pienyritystä varten.

Tietoteknologiassa virtualisoinnilla tarkoitetaan menetelmää, jossa laitteen fyysiset resurssit muutetaan loogisiksi. Tämä mahdollistaa esimerkiksi useiden virtuaalikoneiden käyttämisen yhden fyysisen tietokoneen sisällä. Virtualisoinnin suurimmat hyödyt ovat laitekanna tehokkaampi käyttö, joustavuus ja mukautuvuus sekä keskitetty hallinta. Virtualisoinnin merkkitävimpänä riskinä on virtualisointijärjestelmän hajoaminen, joka poistaa käytöstä kaikki järjestelmän virtualisoimat palvelut.

Virtualisointia on käytetty yrityksissä jo vuosia tehostamaan toimintaa ja laskemaan laitekuluja. Virtualisointijärjestelmien hankinta on kuitenkin pienille yrityksille kallista. Pilvipalvelut antavat yrityksille mahdollisuuden hyötyä virtualisoinnista ilman suuria laitehankintoja. Pilvipalveluiden toiminta perustuu palvelinkeskuksissa tapahtuvaan virtualisointiin, jossa tehokkaiden palvelinklustereiden resurssit jaetaan niistä maksaville asiakkaille.

Pienyritys, joka haluaa käyttää Active Directory -toimialuetta yrityksen koneiden käyttäjätilien hallintaan, voi välttyä laitehankinnoilta perustamalla toimialueen pilveen. Microsoft Azure pilvipalveluun on mahdollista tehdä virtualikoneesta Domain Controller samalla tavoin kuin fyysisestä laitteesta. Virtuaalikone sijaitsee virtuaalisessa verkossa, johon voidaan ottaa yhteys yrityksen verkosta Site-to-Site-menetelmällä tai suoraan koneella Point-to-Site- tai DirectAccess-menetelmillä. Pilvipalvelussa toteutettu toimialue osoittautuu kustannustehokkaaksi ja toimivaksi ratkaisuksi pienyritykselle.

Pilvipalveluiden toimintaan ja rakenteeseen perehtyminen tuo esiin pilvipalveluiden antamat hyödyt yrityksille, tuoden esiin myös sen riskit. Pilvipalveluiden tarjonta monipuolistuu koko ajan ja tuo yrityksille aina erilaisia mahdollisuuksia tehostaa liiketoimintaa.

Asiasanat: virtualisointi, pilvipalvelut, Microsoft Azure, Active Directory

Lahti University of Applied Sciences
Degree Programme in Information Technology

LEHTIMÄKI, SAKU: Cloud computing and a small company Domain Controller in Microsoft Azure

Bachelor's Thesis in telecommunications technology, 39 pages, 1 page of appendice

Spring 2015

ABSTRACT

---

This study examines virtualization and cloud services and their cost-effective use in a small company. The goal of this study was to explain what virtualization and cloud services are and what their benefits and possible risks are. The main focus of this study was on a practical implementation of establishing an Active Directory domain for a small company in Microsoft Azure.

In information technology, virtualization is a process where a device's physical resources are transformed into logical resources. This, for example, enables running multiple virtual machines on a single physical computer. Most notable benefits in using virtualization are efficient use of devices, flexibility and versatility and centralized management. A major risk in virtualization is the failing of the virtualization system, which would stop the functioning of all virtualizated services on that system.

For years virtualization has been used in companies to increase effectiveness and to cut equipment expenses. However, acquiring virtualization systems is expensive for small companies. Cloud services give companies the possibilities to benefit from virtualization without major device purchases. The operation of a cloud service is based on virtualization in data centers with powerful server clusters. Resources from these serverclusters are available to customers for a price.

A small company that wants to use the Active Directory domain for its computer and user account management can avoid device expense by establishing the domain in cloud. It is possible to use a virtual machine in Microsoft Azure cloud services as a Domain Controller in the same way as a physical machine. A connection to the virtual network where this virtual machine is located can be established with a Site-to-Site connection to the company's own network or with a Point-to-Site or DirectAccess connection directly to a computer. A domain implementation in a cloud service turns out to be a cost effective and working solution for a small company.

Cloud services bring benefits for companies, but there are also risks. The supply of cloud services keeps getting more diverse, and which provides companies with ever expanding opportunities to make their business more effective.

Key words: virtualization, cloud services, Microsoft Azure, Active Directory

SISÄLLYS

LYHENNELUETTELO

| | |
|---|---|
| AD DS | Active Directory Domain Services, palvelinrooli |
| ADSI | Active Directory Service Interfaces, hakemistorajapinta |
| BIOS | Basic Input-Output System, järjestelmän alustusohjelma |
| CA | Certificate Authority, digitaalisten sertifikaattien jakelija |
| DC | Domain Controller, toimialueen tunnistuspalvelin |
| DMZ | Demilitarized Zone, aliverkko, joka yhdistää organisaation oman järjestelmän turvattomampaan alueeseen |
| DNS | Domain Name System, nimipalvelujärjestelmä |
| GPO | Group Policy Object, hakemisto-objekti |
| IaaS | Ifrastructure as a Service, pilvipalvelun palvelumalli |
| IP | Internet Protocol, välitysprotokolla |
| IPHTTPS | IP over Hypertext Transfer Protocol Secure, tunnelointiprotokolla |
| LDAP | Lightweight Directory Access Protocol, hakemistopalvelu-verkkoprotokolla |
| NLS | Network Location Server, DirectAccess-komponentti |
| OU | Organizational Unit, hakemisto-objekti |
| PaaS | Platform as a Service, pilvipalvelun palvelumalli |
| SaaS | Software as a Service, pilvipalvelun palvelumalli |
| SDK | Software Development Kit, sovellusten kehitystyökalukokoelma |
| VIP | Virtual IP address, virtuaalinen IP-osoite |
| VLAN | Virtual Local Area Network, virtuaalilähiverkko |
| VPN | Virtual Private Network, virtuaalinen erillisverkko |

# 1 JOHDANTO

Virtualisointi on ollut osana yritysten liiketoimintaa ja tietohallintoa jo melko kauan. Tehokkaan virtualisoinnin mahdollistavien järjestelmien ja laitteiden hankkiminen on voinut olla pienelle yritykselle kuitenkin liian suuri sijoitus. Vuosikymmenen vaihteen jälkeen pilvipalveluiden kehitys ja tarjonta on kuitenkin muuttanut tilannetta. Julkisten pilvipalveluiden tarjoajien yleistyminen, suosion kasvu ja jatkuvasti kiihtyvä kilpailu alalla on kuitenkin mahdollistanut pienten yritysten käyttää hyväksi virtualisoinnista saatuja hyötyjä.

Pilvipalveluita tarjottaessa kaiken taustalla on yleensä virtualisointi, joka mahdollistaa suurien palvelinkeskusten resurssien jakamisen asiakkaiden tarpeiden mukaisesti. Virtualisoinnin eri osa-alueet mahdollistavat palveluiden jakamisen omiin osa-alueisiin tarjoten asiakkaille mahdollisimman tarkkaan vain heidän tarvitsemansa palvelut.

Tämä työ tarkastelee pilvipalvelut mahdollistavaa virtualisointia ja sen hyötyjä, pilvipalveluiden malleja ja rakennetta sekä palveluntarjoajista Microsoft Azurea. Työn käytännön osuuden tavoitteena on selvittää, kuinka pienyritys, jossa työskentelee 1 - 10 työntekijää voi hyödyntää Microsoft Azuren tarjoamia palveluita Active Directory -toimialueen perustamiseen ja sitä millaisia kuluja tästä syntyy.

Työ tehdään ItsPro Oy:n toimeksiantona. Työn tarkoituksena on antaa ohjeet ja perusta uusien palveluiden kehittämiselle sekä käyttäjäkokemus Microsoft Azuresta pilvipalvelu-alustana.

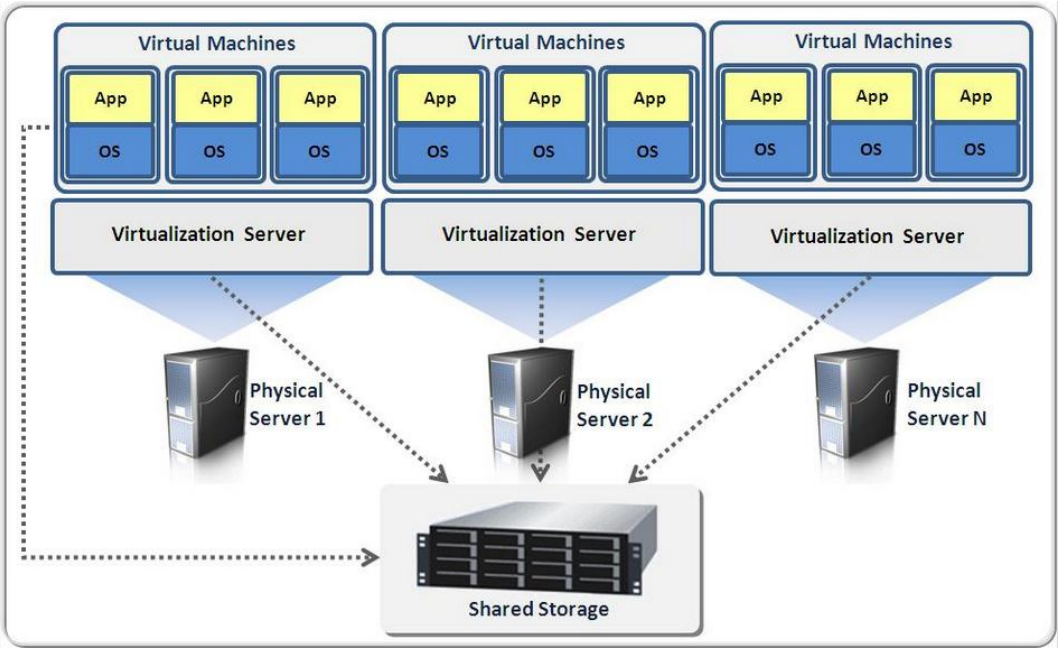
# 2 VIRTUALISOINTI

Tietotekniikassa virtualisoinnilla tarkoitetaan fyysisten resurssien jakamista tai yhdistämistä loogisiksi resursseiksi. Tämä mahdollistaa järjestelmien ja sovellusten käyttää näitä loogisia resursseja tietämättä fyysisten resurssien todellisia ominaisuuksia tai arvoja. Tällä tavoin voidaan jakaa yksi fyysinen resurssi toimimaan useampana loogisena resurssina tai yhdistää useampi fyysinen resurssi toimimaan yhtenä suurempana loogisena resurssina. (Wikia, Inc 2015.)

Virtuaalipalvelimet ja fyysinen palvelinlaitteisto on erotettu toisistaan ohjelmistokerroksella. Ohjelmistokerroksen päällä virtuaalipalvelimia voidaan luoda, poistaa ja siirtää tarvittaessa. Virtualisoinnilla voidaan parantaa fyysisten laitteiden käyttöastetta, nopeuttaa käyttöönottoa, laskea virrankulutusta ja rakentaa vikasietoisempia järjestelmiä. Virtualisointi tuo järjestelmiin joustavuutta, mahdollistamalla esimerkiksi virtualisoidun palvelimen prosessoritehon nostamisen yhdellä asetuksen muutoksella. (Mäntylä 2008.)

## 2.1 Virtualisoinnin osa-alueet

Virtualisointia voidaan käyttää useissa erilaisissa käyttökohteissa ja useisiin eri tarkoituksiin. Virtualisoinnin keskeisimpiin osa-alueisiin kuuluvat palvelin/laitevirtualisointi, tallennusvirtualisointi, sovellusvirtualisointi ja verkkovirtualisointi. (Hiltunen 2010, 3.)




KUVIO 1. Palvelin- ja tallennusvirtualisointi (CommVerge Solutions 2015.)

Palvelinvirtualisoinnissa luodaan virtuaalikone, joka toimii kuin tavallinen fyysinen laite. Yhden laitteen resurssit jaetaan useiden itsenäisesti toimivien virtuaalikoneiden käytettäväksi. Tämä toteutetaan usein hypervisor-hallintasovelluksen avulla. Näin voidaan maksimoidan fyysisen laitteen resurssien käyttöaste ja vapauttaa tai ottaa käyttöön virtualisoitujen koneiden vaatimia resursseja niiden tarpeiden mukaisesti. (Wikimedia Foundation, Inc. 2015e.)

Tallennusvirtualisoinnissa fyysinen tallennustila sijaitsee muualla kuin laitteessa itsessään tai sen lähiverkossa (KUVIO 1). Virtualisoitu tallennustila näkyy käyttäjälle ja järjestelmälle kuten normaali tallennustila. Virtualisoitu tallennennusympäristö mahdollistaa tallennustilan huollon, muutokset ja siirtämisen ilman sitä käyttävien järjestelmien alas ajoa. (Wikia, Inc. 2015.)

Verkkovirtualisoinnilla voidaan verkkoon tehdä loogisia verkkoyhteyksiä, ilman muutoksia fyysiseen verkkoon. Esimerkiksi Virtual Private Network (VPN) -yhteys muodostaa etäyhteyden kahden yksityisen verkon välille tekemättä muutoksia yleiseen verkkoon. (Hiltunen 2010, 4.)

Sovellusvirtualisointi mahdollistaa sovelluksen toiminnan riippumatta sen vaatimasta käyttöjärjestelmästä. Virtualisoidun sovelluksen hyötyinä on muun

muassa päätelaiteriippumattomuus ja ohjelmien välisten yhteensopimattomuuksien välttäminen. (Wikia, Inc. 2015.)

## 2.2 Virtualisoinnin hyödyt ja haasteet

Virtualisoinnin ehkä suurimpina hyötynä on laitteiden tehokkaampi käyttöaste, jolloin säästetään laitekustannuksissa ja pienennetään myös laitekannan kokoa. Yleensä yksi palvelin normaalikäytössä käyttää vain 10 – 15 prosenttia laitteiston suorituskyvystä. Virtualisointi mahdollistaa usean palvelimen käytön yhdellä laitteistolla, jolloin laitteen suorituskyvyn käyttö nousta 70 – 80 prosenttiin. Tämä vähentää laitteiden määrää, ja näin ollen säästetään sähkö- ja ilmastointikuluissa. (Hiltunen 2010, 4 - 5.)

Virtuaalipalvelinten hallinta on yleensä mahdollista tehdä keskitetysti ja etäyhteydellä nopeuttaen ja vähentäen ylläpidon työmäärää. Loogisten resurssien jakaminen ja uudelleen määrittäminen on mahdollista ja onnistuu ilman virtuaalipalvelimen sammuttamista tai uudelleen käynnistämistä. Uuden virtuaalipalvelimen käyttöönotto on helpompaa ja nopeampaa, kuin fyysisen palvelimen, koska voidaan käyttää valmiita levykuvia tai tilannekuvia (snapshot). (Hiltunen 2010, 5.)

Virtualisointi mahdollistaa myös palvelinten helpon siirtämisen ja kahdentamisen. Virtuaalipalvelimesta otettu tilannekuva voidaan hetkessä siirtää verkon yli toiseen fyysiseen palvelimeen ja ottaa käyttöön. Vikatilanteessa virtuaalipalvelin voidaan palauttaa tilannekuvalla toimintakuntoon. (Hiltunen 2010, 5.)

Virtualisoinnin haasteet ovat osittain samat, kuin normaalissa palvelinympäristössä. Vaikka laitteiden määrät saattavat virtualisoinnin avulla laskea, vaaditaan virtualisointi alustalta enemmän prosessointitehoa ja muistikapasiteettia, kuin yksittäiseltä palvelimelta. Virtualisoidussa ympäristössä ohjelmistojen ja käyttöjärjestelmien lisenssimaksut ovat samat kuin fyysisessä. Myös virtualisointiohjelmien lisenssit maksavat. (Himanka 2011, 28 - 29.)

Laiteviat saattavat virtualisoidussa ympäristössä aiheuttaa enemmän vahinkoa kuin erillisissä fyysisissä palvelimissa. Yhden fyysisen palvelimen ylläpitämän

palvelun kaatumisen sijaan voi useita virtualisoituja palvelimia poistua käytöstä isäntälaitteessa ilmenevän laitevian vuoksi. (Himanka 2011, 28 – 29.)

## 2.3 Palvelinvirtualisointi

Palvelinvirtualisoinnissa fyysisen palvelimen laitteiston resurssit muutetaan loogisiksi resursseiksi, joita voidaan käyttää virtuaalipalvelinten resursseina. Virtuaalipalvelimen pystyttämiseen käytetään yleisimmin hypervisor-hallintasovellusta, jonka kautta virtualisoidut laiteresurssit jaetaan virtuaalipalvelimille emuloimalla fyysisiä resursseja. Virtuaalipalvelimen käyttöjärjestelmän asennuksen ja muiden asetusten määrittämisen jälkeen virtuaalipalvelin voidaan liittää yrityksen verkkoon virtuaaliverkkosovittimen kautta.

Hallintasovelluksen kautta virtuaalipalvelimen voi tarvittaessa sammuttaa tai käynnistää, muuttaa palvelimen käyttämiä loogisia resursseja tai ottaa yhteys palvelimeen. Yrityskäyttöön suunnitelluilla hallintasovelluksilla pystytään usein myös hallitsemaan virtualisoituja tallennusjärjestelmiä. Hallintasovellus valvoo loogisten resurssien käyttöä, kirjaa lokitietoihin tapahtumia ja ilmoittaa ongelmista ja vioista. Hallintasovellukseen pystyy myös automatisoimaan toimintoja, kuten varmuuskopiointia ja tilannekuvien ottamista. Monet hallintasovellukset tukevat etäyhteyttä, jolloin ongelmatilanteissa tarvittavat muutokset voidaan tehdä toiselta työasemalta. (Hiltunen 2010, 10.)

### 2.3.1 Palvelinvirtualisoinnin käsitteitä

Palvelinvirtualisoinnissa fyysistä laitetta, jonka resursseja virtuaalikoneet käyttävät ja jonka päällä ne toimivat, kutsutaa isäntäkoneeksi eli Host Machine tai Host System. Virtuaalikoneisiin hypervisorin kautta asennettuja käyttöjärjestelmiä, jotka näkevät vain loogiset resurssit, kutsutaan vieraskäyttöjärjestelmiksi. Vieraskäyttöjärjestelmät eivät tiedosta isäntäkoneen resursseja, vaan havaitsevat ainostaan niille emuloidut resurssit. (Hiltunen 2010, 11.)

Levykuva on tiedosto, johon massamuistin sisältö ja rakenne on tallennettu kokonaisuudessaan. Virtualisointisovelluksen avulla levykuvat näkyvät samalla tavoin kuin alkuperäinen massamuisti, josta levykuva on luotu. Virtuaalipalvelimista voidaan ottaa tilannekuvia (snapshot), joihin palvelimen senhetkinen tila tallentuu. Näitä snaphotteja voidaan käyttää palvelimen tilan palauttamisessa, jos esimerkiksi palvelimeen tehdyissä muutoksissa ilmenee ongelmia. Tilannekuvista voidaan myös luoda uusia virtuaalipalvelimia. (Hiltunen 2010, 11.)

Virtuaalikoneen kovalevy voidaan kapseloida yhden tiedoston sisälle, mikä mahdollistaa kovalevyn helpon kopioimisen tai siirtämisen toiselle isäntäkoneelle. Kapseloitu virtuaalikovalevy toimii kuin levykuva. Virtuaalikoneen siirtämistä isäntäkoneelta toiselle kutsutaan migraatioksi. Virtuaalikoneen pystyy siirtämään isäntäkoneelta toiselle ilman, että virtuaalikonetta sammutetaan välillä. Tätä kutsutaan suoramigraatioksi. Konsolidaatiolla tarkoitetaan virtualisointia hyödyntäen tehtyä palvelinten keskittämistä. Virtuaalikoneet pidetään erillään toisistaan isolaatiolla, jolloin yhden virtuaalikoneen ongelmat eivät vaikuta muihin saman isäntäkoneen virtuaalikoneisiin. Virtuaalikoneet eivät kuitenkaan ole eristettyinä isäntäkoneen ongelmilta, kuten laitevioilta tai kaatumiselta. (Hiltunen 2010, 11.)

Korkea käytettävyys tai saatavuus, eli High Availability, on menettelytapa, jonka tavoitteena on taata järjestelmien jatkuva käytettävyys loppukäyttäjälle. Palvelinvirtualisoinnissa tätä toimintatapaa pyritään ylläpitämään muun muassa suorasiirrolla ja kahdentamalla virtuaalikoneet, jolloin koneen kaatuessa sen toiminta jatkuu toisella koneella ilman loppukäyttäjälle näkyvää häiriötä. (Hiltunen 2010, 11 - 12.)

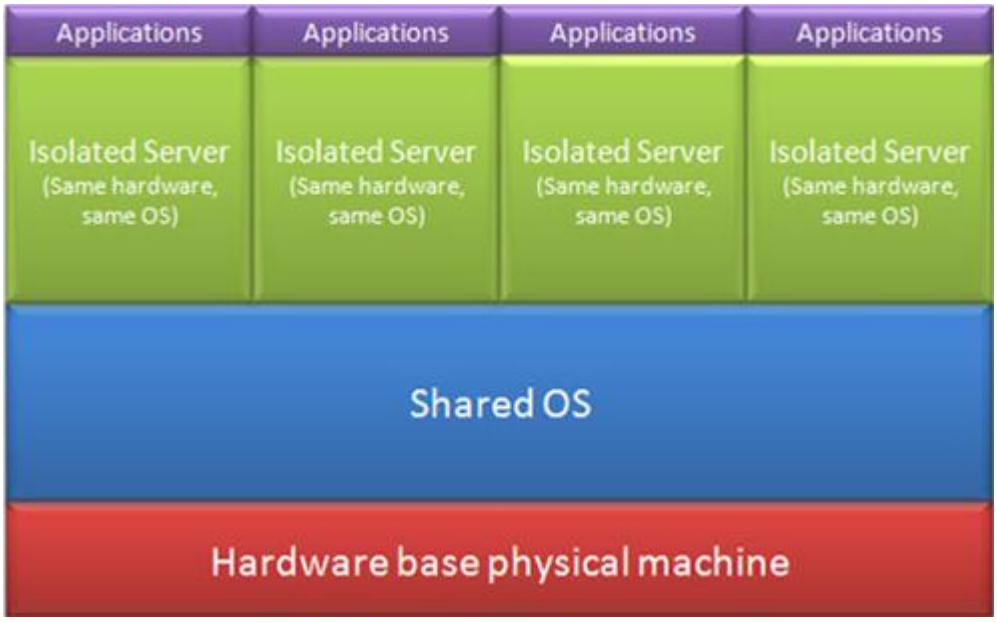
### 2.3.2 Palvelinvirtualisointitekniikat

Täysvirtualisointi, laitteisto-avustettu virtualisointi, käyttöjärjestelmätason virtualisointi ja paravirtualisointi ovat palvelinvirtualisoinnin eri tekniikoita. Virtualisointitekniikaksi on valittava käyttökohteeseen parhaiten sopiva vaihtoehto. (Hiltunen 2010, 12.)

Täysvirtualisoinnissa (englanniksi Full virtualization) isäntäkoneen fyysisten resurssien ja virtualisointitason välillä ei ole ylimääräistä kerrosta, vaan hypervisor emuloi fyysisen laitteiston suoraan virtuaalikoneille. Täysvirtualisointisovellukset eivät aina tarvitse käyttöjärjestelmää alustakseen, vaan asennus tehdään suoraan isäntäkoneelle. Täysvirtualisointi onnistuu vain, jos fyysinen laitteisto ja virtualisointisovellus ovat yhteensopivat. Täysvirtualisoinnin merkittävin hyöty on mahdollisuus ajaa erilaisia käyttöliittymiä erillisille virtuaalikoneille. (Hiltunen 2010, 12.)

Laitteisto-avustetussa virtualisoinnissa (englanniksi Hardware-assisted virtualization) hypervisorin ei tarvitse välittää virtuaalikoneilta tulevia käskyjä fyysiselle laitteistolle. Tämän vuoksi laitteisto-avusteista virtualisointia kutsutaan myös kiihdytetyksi virtualisoinniksi tai natiivivirtualisoinniksi. Laitteisto-avustettua virtualisointia voidaan käyttää yhdessä täys- ja paravirtualisoinnin kanssa, joissa molemmissa laitteisto-avustettu virtualisointi parantaa isäntäkoneen laskentatehon hyödyntämistä. (Hiltunen 2010, 13.)

Käyttöjärjestelmätason virtualisoinnissa (englanniksi Operating system-level virtualization) isäntäkoneen käyttöjärjestelmällä on mahdollista ajaa useampaa samaa käyttöjärjestelmää olevaa vieraskäyttöjärjestelmää samanaikaisesti. Isäntäkoneen sisälle luotu virtuaaliympäristö, eli instanssi, mahdollistaa resurssien käytön ilman emulointia varmistaen resurssien tasaisen jakamisen käyttäjien kesken (KUVIO 2). (Hiltunen 2010, 13.)



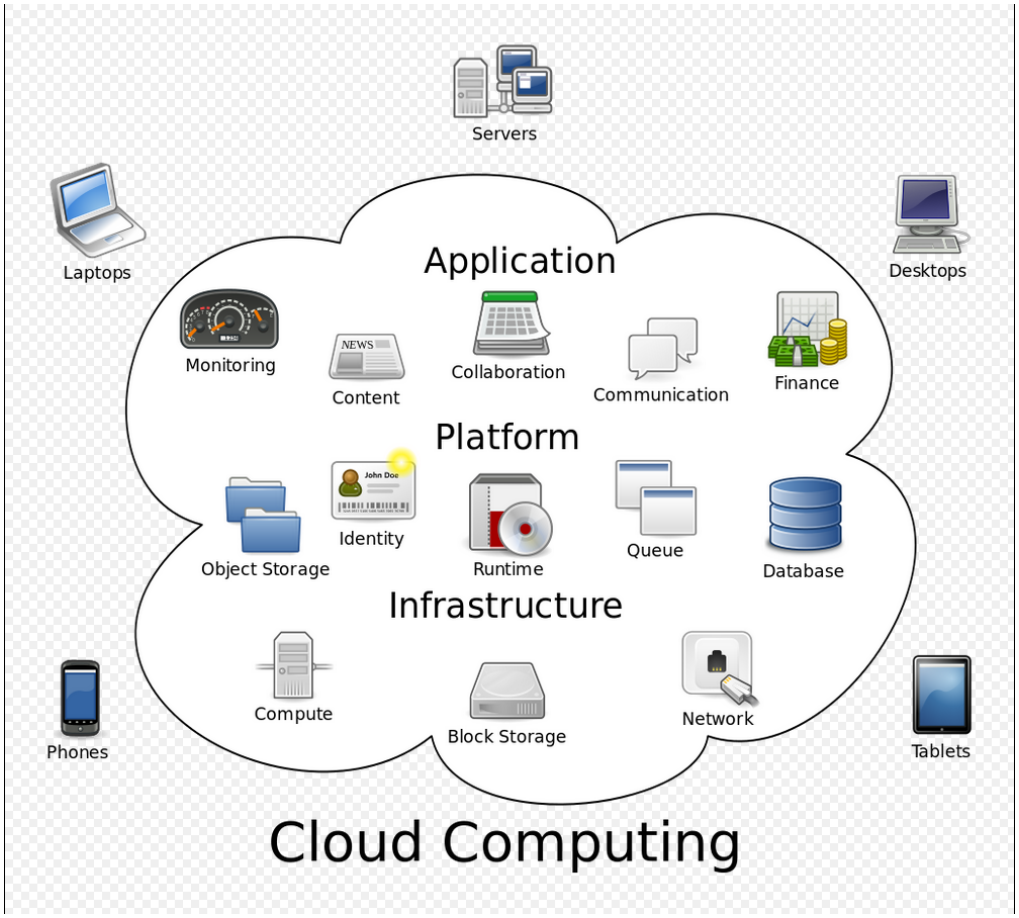

KUVIO 2. Käyttöjärjestelmätason virtualisointi (Microsoft 2009.)

Paravirtualisointi toimii lähes samalla tavoin kuin käyttöjärjestelmätason virtualisointi. Käyttöjärjestelmätason virtualisoinnista eroten paravirtualisoinnissa käyttöjärjestelmän päällä voidaan ajaa myös eri käyttöjärjestelmiä. Tätä varten paravirtualisoituun käyttöjärjestelmään on kuitenkin tehtävä muutoksia. Kaikki käyttöjärjestelmäyhdistelmät eivät ole kuitenkaan tuettuja. Paravirtualisoinnissa hypervisor koordinoi virtuaalikoneiden laiteresurssien käyttöä, laitekannan emuloinnin sijaan. (Hiltunen 2010, 13.)

# 3 PILVIPALVELUT

Pilvilaskennalla ja -palveluilla tarkoitetaan internetissä ja hajautetuissa ympäristöissä tapahtuvaa tietotekniikan kehitystä ja käyttöä. Pilvilaskennassa resurssit jaetaan ja niitä käytetään verkon yli. Kaikki virtualisoinnin yleisimmät osa-alueet ovat usein käytössä pilvilaskennassa ja -palveluissa. Käsitteellä ”pilvi” tarkoitetaan yleensä datakeskuksissa tuotettuja ja internetin yli käytettäviä palveluita (KUVIO 3). (Wikimedia Foundation, Inc. 2015d.)

Pilvilaskennassa resursseja voidaan jakaa useille käyttäjille ja myös niiden käyttökohdetta voidaan vaihtaa dynaamisesti. Esimerkiksi pilvipalveluja tarjoavan yrityksen palvelinsalin koneet voivat toimia osan aikaa vuorokaudesta eurooppalaisten käyttäjien sähköpostipalvelimina ja loppuosan vuorokaudesta amerikkalaisten käyttäjien webpalvelinten resursseina. Tällä toimintatavalla maksimoidaan palvelinten käyttöaste ja näin ollen vähennetään muun muassa toiminnasta syntyviä ympäristöhaittoja. (Wikimedia Foundation, Inc. 2015b.)



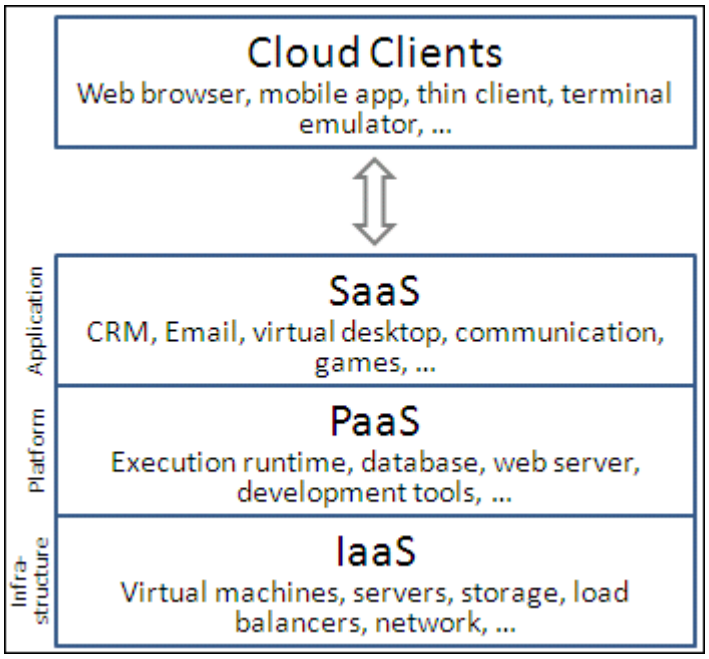

KUVIO 3. Looginen kaavio pilvilaskennasta (Wikimedia Foundation, Inc.

2015b.)

Useat yritykset ovat siirtäneet toimintaansa pilveen välttääkseen laitehankinnoista ja järjestelmien ylläpidosta syntyviä kustannuksia. Pilvipalveluissa toteutetut ratkaisut mahdollistavat myös järjestelmien nopeamman käyttöönoton ja helpon skaalautuvuuden. Nopeiden verkkoyhteyksien, halpojen tietokoneiden ja tallennusjärjestelmien saatavuus sekä virtualisoinnin laajalle levinnyt käyttöönotto on lisännyt pilvipalveluiden tarjontaa. (Wikimedia Foundation, Inc. 2015b.)

## 3.1 Palvelumallit

Pilvipalveluita tarjoavat yritykset jakavat palvelunsa yleensä kolmeen luokkaan: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS). Asiakas pääsee käsiksi tarjottuihin palveluihin verkkoon liitetyn laitteen avulla käyttäen selainta tai erillistä asiakasohjelmistoa (KUVIO 4). (Wikimedia Foundation, Inc. 2015b.)




KUVIO 4. Pilvipalvelumallit (Wikimedia Foundation, Inc. 2015b.)

Infrastructure as a Service on fyysisten tai virtuaalisten tietokoneiden tai muiden resurssien tarjoamista palveluna. IaaS sisältää yleensä verkkoyhteydet, tallennustilan, palvelimet ja niiden ylläpidon. IaaS mahdollistaa palveluiden tuottamisen pilvessä. IaaS-palvelut sisältävät usein myös valmiita

virtuaalikoneiden levykuvia, palomuureja, IP (Internet Protocol) -osoitteita, kuorman tasausta, virtuaalisia lähiverkkoja (VLAN) ja ohjelmistopaketteja. Tässä palvelumallissa käyttäjä vastaa infrastruktuurin käyttöjärjestelmän ja ohjelmistojen asennuksesta, päivittämisestä ja ylläpidosta. IaaS-palveluiden käytön kustannukset muodostuvat yleensä käytetyistä resursseista. (Wikimedia Foundation, Inc. 2015b.)

Platform as a Service -mallissa palveluntarjoaja toimittaa järjestelmäalustan, joka yleensä sisältää käyttöjärjestelmän, ohjelmointiympäristön, tietokannan ja web-palvelimen. Käyttäjät voivat kehittää ja ajaa sovelluksia ympäristössä ilman erillisiä laite- ja ohjelmistohankintoja tai asennuksia. PaaS-mallissa käyttäjän ei tarvitse huolehtia ympäristön skaalautuvuudesta tai tehontarpeesta, koska alustaa on mahdollista laajentaa. (Wikimedia Foundation, Inc. 2015b)

Software as a Service -mallissa asiakkaille tarjotaan ohjelmiston ja tietokantojen käyttöoikeuksia palveluna. Palveluntarjoaja vastaa infrastruktuurista ja sovelluksen toiminnasta. Asiakkaat käyttävät palveluita yleensä internet-selaimella, jolloin ohjelmistoa ei tarvitse asentaa asiakkaan laitteelle. Palvelusta maksetaan yleensä käyttömäärän mukaisesti tai kuukausimaksulla. (Wikimedia Foundation, Inc. 2015b.)

## 3.2 Hankintamallit

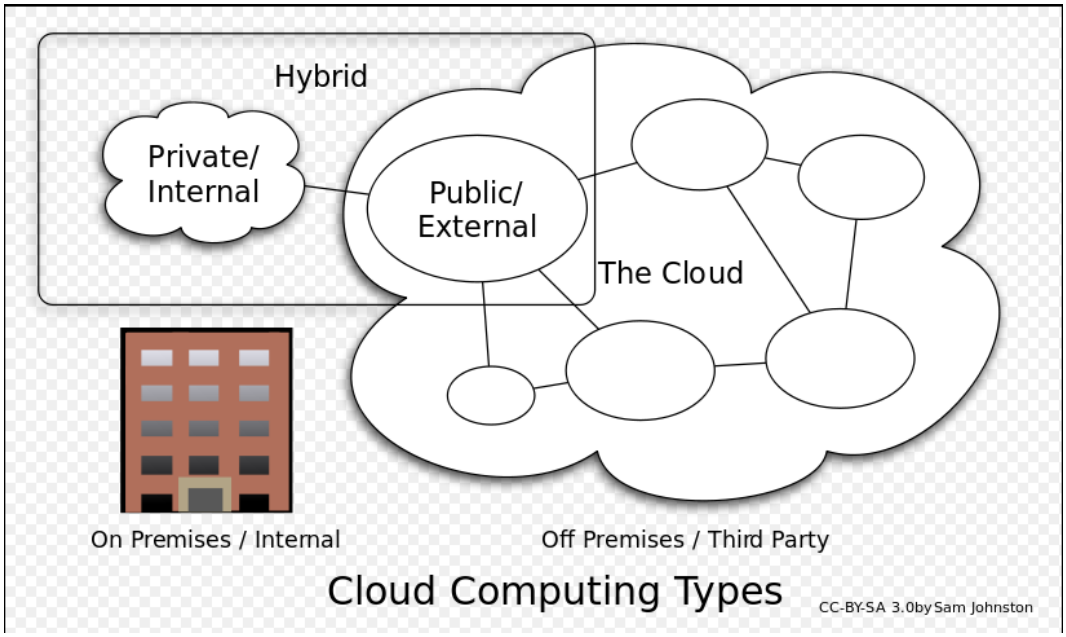
Pilvipalveluiden hankintatapa luokitellaan yleensä käyttäjä- ja omistussuhteiden mukaan. Pilvi voi olla tyypiltään julkinen, yksityinen tai näiden tyyppien sekoitus eli hybridi (KUVIO 5). (Viestintävirasto 2014, 6.)

Yksityinen pilvi tarkoittaa yksittäisen organisaation käytössä olevaa pilveä. Yksityinen pilvi voi silti olla ulkopuolisen organisaation hallinnoima tai ylläpitämä. Yksityisen pilven käyttöönotto vaatii organisaatiolta omistautumista ja yleensä myös huomattavan kertasijoituksen, joten siitä ei saada kaikkia ulkoistetun pilvipalvelun etuja. (Wikimedia Foundation, Inc. 2015b.)

Pilvi on julkinen, jos siinä ylläpidetyt resurssit ja palvelut ovat yleisesti saatavilla. Yksityinen- ja julkinen pilvi voivat olla arkkitehtuuriltaan identtiset, mutta

tietoturvan osalta ne voivat erota suuresti. Yleensä julkisten pilvien ylläpitäjät ovat suuryrityksiä, kuten Google, Microsoft tai Amazon, koska ne vaativat valtavia datakeskuksia ja palvelinsaleja suurten käyttäjämäärien vuoksi. (Wikimedia Foundation, Inc. 2015b.)

Hybridi-pilvessä kaksi tai useampia julkisia tai yksityisiä pilviä jakaa resursseja ja palveluita yhdistetysti. Pilvet toimivat edelleen erillään ja niillä voi olla eri palveluntarjoajat ja ylläpitäjät, esimerkiksi palvelin, joka toimii yrityksen yksityisessä pilvessä, mutta ottaa tarvittaessa käyttöönsä resursseja julkisesta pilvestä tai julkisessa pilvessä ajettu sovellus, joka lukee tietoja yksityisessä pilvessä sijaitsevasta tietokannasta. (Wikimedia Foundation, Inc. 2015b.)




KUVIO 5. Pilvipalveluiden hankintamallit (Wikimedia Foundation, Inc. 2015b.)

## 3.3 Tietoturva

Kaikkiin tietoteknisiin järjestelmiin liittyy omat tietoturvariskinsä. Maailmanlaajuinen Cloud Security Alliance (CSA) -järjestö on omistautunut pilvipalveluihin liittyvien turvallisuusuhkien kartoittamiseen ja niistä tiedottamiseen. Järjestö on vuonna 2010 koonnut listan pilvipalveluiden suurimmista tietoturvariskeistä. (Cloud Security Alliance 2015.)

Pilvipalveluihin pystyy rekisteröitymään kuka tahansa, kenellä on voimassa oleva luottokortti, ja jotkin palveluntarjoajat myös tarjoavat ilmaisia kokeilujaksoja palveluihinsa. Tämä mahdollistaa palveluiden väärinkäytön esimerkiksi roskapostibottien ylläpitoon, haittaohjelmien kirjoittamiseen tai muuhun rikolliseen toimintaa. Väärinkäyttötapauksia voidaan vähentää muun muassa tiukentamalla kirjautumisprosessia ja valvomalla käyttäjien verkkoliikennettä. (Cloud Security Alliance 2010, 8.)

Pilvipalveluiden tarjoajat julkaisevat erilaisia ohjelmisto- ja ohjelmointirajapintoja, joilla asiakkaat käyttävät ja hallitsevat palveluita. Pilvipalvelun turvallisuus ja saatavuus riippuu näiden rajapintojen tietoturvasta. Rajapinnat on suunniteltava turvaamaan käyttäjätunnistus- ja salausjärjestelmät tahallisilta ja vahingossa tehdyiltä ohitusyrityksiltä. Organisaatiot ja kolmannen osapuolen toimijat haluavat usein integroida näitä rajapintoja omiin palveluihinsa. Tämän mahdollistaminen lisää tietoturva-aukkojen syntymistä ja monimutkaistaa rajapinnan kehittämistä. Riskejä voidaan vähentää tutustumalla tarkasti palveluntarjoajan käyttämän rajapinnan tietoturvaan ja käyttäjäntodennusviestien salauksen vahvistamisella. (Cloud Security Alliance 2010, 9.)

Pilvipalveluden käyttäjät eivät yleisesti tiedä, millaiset palkkausperusteet tai taustatarkastukset palveluntarjoajilla on koskien työntekijöitä. Käyttäjät eivät myöskään tiedä, mihin tietoihin työntekijöillä on pääsy. Tietoturvariksi voi siis tulla myös pilvipalveluyrityksen sisältä. Pahantahtoinen tai rikollinen työntekijä voi päästä käsiksi käyttäjien tilitietohin ja muihin yrityksen toimintaan liittyviin kriittisiin tietoihin. (Cloud Security Alliance 2010, 10.)

Varsinkin IaaS-palveluita tarjottaessa ja käytettäessä on otettava huomioon mahdolliset resurssien käyttöoikeuksien rikkomukset. Hypervisorissa tapahtuvan virheen vuoksi virtualisoidulla palvelimella voi olla pääsy resursseihin ja tietoihin, joihin sillä ei ole käyttöoikeutta. Käyttäjillä ei saisi olla minkäänlaisia käyttömahdollisuuksia eikä käyttöoikeutta palveluntarjoajan fyysisiin laitteisiin. Riskiä voidaan vähentää aktiivisella luvattomien ympäristön muutosten valvonnalla, vahvan tunnistautumisen käyttämistä ylläpitäjien

sisäänkirjautumisissa ja haavoittuvuuksien kartoittamisella. (Cloud Security Alliance 2010, 11.)

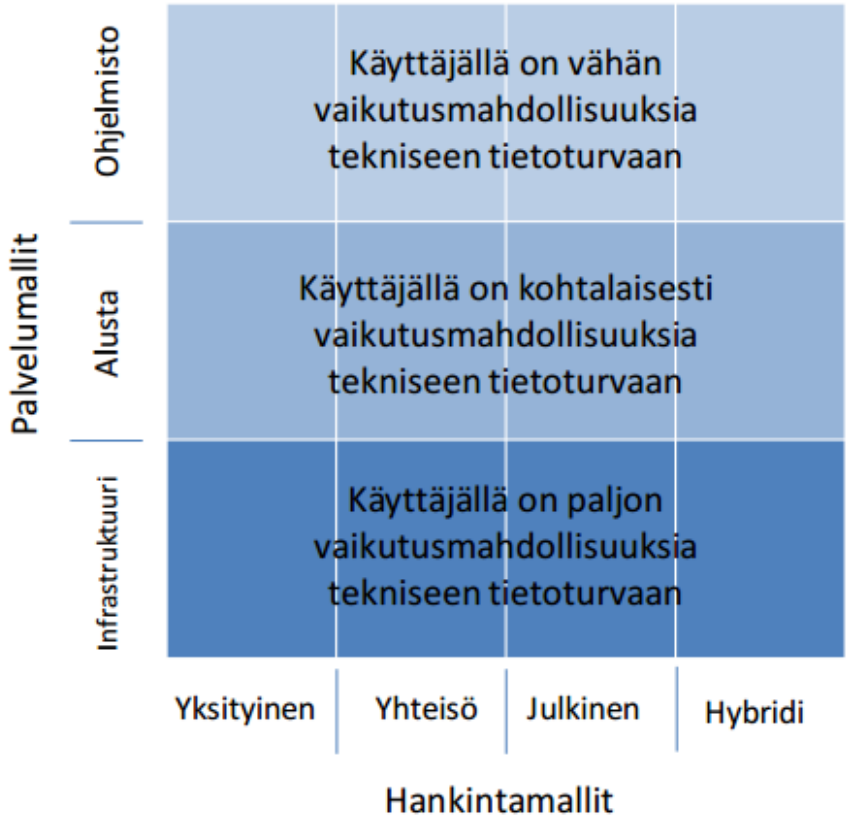
Datan häviäminen tai tuhoutuminen on varsinkin pilvipalveluiden kaltaisissa monimutkaisessa järjestelmissä aina mahdollista. Tallennetun tiedoston poistaminen epähuomiossa ilman varmuuskopiota on valitettavan yleinen virhe. Poistetun tietueviitteen palautus voi olla mahdotonta, tai tallennusjärjestelmä voi korruptoitua täysin yllättäen. Pelkkä salausavaimen häviäminen voi tehdä ympäristöstä käyttökelvottoman. Myöskään ulkopuolisten tahojen ei haluta pääsevän käsiksi arkaluontoisiin tietoihin. Näitä riskejä voidaan vähentää esimerkiksi vahvalla rajapinnan käyttäjienhallinnalla, tiedonsiirtojen salaamisella ja varmistamisella sekä ottamalla käyttöön kestävä salausavainten luonti-, tallennus- ja hallintajärjestelmä. (Cloud Security Alliance 2010, 12.)

Tilien ja palveluiden kaappaus on yleinen riski pilvipalveluiden kaltaisissa järjestelmissä. Käyttäjätunnuksia ja salasanoja voidaan yrittää selvittää phishing-yrityksillä tai ohjelmistojen haavoittuvuuksia hyödyntämällä. Samoja käyttäjätunnuksia ja salasanoja käytetään usein useissa eri palveluissa, mikä saattaa lisätä niiden kaappauksesta aiheutuvaa vahinkoa. Pilvipalvelukäyttäjän tunnuksien kaappaja voi tarkkailla käyttäjän toimintaa, lähettää väärää tietoa käyttäjän nimissä, muutta tietoja tai ottaa tilin kokonaan omaan käyttöönsä. Riskiä voidaan vähentää muun muassa kieltämällä käyttäjänimien jakamisen käyttäjien ja palveluiden välillä, käyttämällä kaksivaiheista tunnistamista mahdollisuuksien mukaan ja aktiivisella kirjautumisien valvonnalla. (Cloud Security Alliance 2010, 13.)

Oman riskinsä pilvipalveluiden käyttöön tuovat sen tarjoajat. Käyttäjät eivät tiedä palveluntarjoajan omista sisäisistä tietoturvaohjeistuksista tai -toimista. Käyttäjillä ei ole tiedossa, mitä kaikkea tietoa heidän toiminnasta tallennetaan tai ketkä käyttävät samoja järjestelmiä heidän kanssaan. (Cloud Security Alliance 2010, 14.)

Viestintäviraston Kyberturvallisuuskeskus on koonnut raportin pilvipalveluiden tietoturvasta. Raportti on tarkoitettu lähinnä yritysten ja muiden organisaatioiden avuksi arvioitaessa pilvipalveluiden turvallisuutta ja valittessa palveluntoimittajaa.

Raportissa havainnoillistetaan käyttäjän mahdollisuutta vaikuttaa tietoturvaan pilven eri palvelu- ja rakennetasoilla. Kuviosta 6 voidaan havaita käyttäjän vaikutusmahdollisuuksia tietoturvaan liittyen vähenevän palvelumallin mukaan. Hankintamallilla ei näytä olevan vaikutusta käyttäjän vaikutusmahdollisuuksiin. (Viestintävirasto 2015, 6.)




KUVIO 6. Käyttäjän vaikutusmahdollisuus tietoturvaan (Viestintävirasto 2014, 6.)

Pilvipalveluihin voi tallentaa miltei rajattomasti ja mitä vain tietoa, kuitenkin huomioon ottaen palveluntarjoajan sopimusehdot. Ennen tiedon tallentamista pilveen on hyvä tehdä riski-hyöty-arvio tallennettavalle tiedolle. Pilvipalveluiden käyttöä sopimusehtojen lisäksi rajoittaa lainsäädäntö. Pilvipalveluiden käyttöönotossa yrityksen on hyvä huomioida myös muut omat sopimusvelvoitteensa. Tietojen siirtämistä ulkomaille on voitu rajoittaa aikaisemmalla sopimuksella. Pilveen siirrettävän aineiston tietoturvaluokitus on otettava myös huomioon. (Viestintävirasto 2014, 11.)

Jos tiedon tallentamiseen ei ole edellämainittuja tai muita ulkoisia esteitä, on palvelun käytön aloitus oman harkinnan ja riskianalyysin varassa. Riskianalyysissä on huomioitava, että pilvipalveluun tallennettu tieto on ulkopuolisen ylläpidettävänä. On harkittava, kuinka suuret riskit tiedon katoamiselle, vääristymiselle, tuhoutumiselle tai kolmannen osapuolen haltuun joutumiselle on ja ovatko palvelun käytöstä saatavat hyödyt riittävät. Tallennettujen tietojen laatu muuttaa riskiarviota, henkilökohtaisten asioiden ja yrityksen liiketoimintaan liittyvien tiedostojen painoarvo voi olla erilainen. (Viestintävirasto 2014, 11.)

Kaikkea yrityksen liiketoimintaan liittyvää dataa ei kannata siirtää ulkopuolisen ylläpidettäväksi, vaan pilveen vietävä data ja laskenta on suunniteltava ja rajattava tarkasti ennen palveluiden käyttöönottoa. Riski-hyöty-arvio auttaa rajaamaan tietoja, jotka on parempi säilyttää yrityksen paikallisilla palvelimilla. (Viestintävirasto 2014, 11.)

## 3.4 Microsoft Azure

Azure on Microsoftin vuonna 2010 julkaisema pilvipalveluympäristö. Azuressa on mahdollista toteuttaa useita erilaisia palvelin- ja sovellusratkaisuja virtualisoituina (KUVIO 7) Microsoftin globaalisti hajautetuissa palvelinsaleissa. Microsoft Azure tarjoaa muun muassa sovellusalustapalveluja (PaaS), virtuaalipalvelimia (IaaS) ja sivustojen isännöintiä sekä tukee useita ohjelmointikieliä ja Microsoftin omia ja kolmannen osapuolen työkaluja. (Wikimedia Foundation, Inc. 2015c.)

Microsoft Azuren perustehtävät pilvipalvelualustana voidaan jakaa kolmeen osaan: virtuaalikoneet, websivujen isännöinti ja Cloud Services -sovellusalusta. Azureen luotavaan virtuaalikoneeseen käyttäjä voi valita levykuvan Microsoftin omasta valikoimasta tai ladata palveluun oman levykuvansa. Virtuaalikoneen koon voi valita laajasta listasta, ja sitä voi myös jälkeenpäin muuttaa. Virtuaalikoneen käyttömaksu koostuu pääosin koneen käyttötunneista. Käyttäjä pystyy kopiomaan Azuressa jo käytössä olevan virtuaalikoneen ja luoda sen levykuvalla uuden. (Boucher 2014.)

Azuren websivustojen isännöinti (Azure Websites) vapauttaa käyttäjän webpalvelimen ylläpidolta. Käyttäjä voi luoda Azureen uuden websivu-sovelluksen tai tuoda olemassa olevan pilveen. Azure Websites tasapainottaa kuormaa luotujen instanssien välillä automaattisesti. Käyttäjä voi itse valita, ajetaanko websivusto omalla palvelimella vai samalla muiden sivustojen kanssa. Palvelimen suorituskykyä voi nostaa tarvittaessa. (Boucher 2014.)

Azure Cloud Services on PaaS-palvelu, joka on suunniteltu samanaikaisesti useiden käyttäjien käytettäväksi, vaatien kuitenkin vain vähäistä ylläpitoa ja on aina käytettävissä. Cloud Services on tehty mahdollisimman hyvin skaalautuvaksi, joustavaksi ja luotettavaksi. Käyttäjä voi luoda minkä tahansa sovelluksen käyttäen esimerkiksi C#- tai Java-ohjelmointikieltä ja ajaa sen Azure Cloud Servicessä Windows palvelimella. Nämä palvelimet kuitenkin eroavat käyttäjien luomista virtuaalikoneista. Azure ylläpitää ja valvoo näitä palvelimia ja huolehtii niiden päivityksistä. (Boucher 2014.)


KUVIO 7. Microsoft Azure pilvipalvelut. (Boucher 2014.)

Microsoftin datakeskuksissa sijaitsevat klusterit, jotka hallitsevat pilven tallennus- ja laskentaresurssien jakamisen Azuren päällä ajettaville sovelluksille, käyttävät erikoiskäyttöjärjestelmää ”tuotekerroksen” ajamiseen. Klusterit sisältävät 1800-2500 palvelinta, jotka käyttävät Windows Server 2008 -käyttöjärjestelmää ja muokattua Hyper-V-virtualisointiohjelmistoa virtualisointipalvelujen tarjoamiseksi. Microsoft Azure Fabric Controller ohjaa palvelujen skaalautuvuutta ja luotettavuutta ja mahdollistaa palvelujen ja ympäristöjen jatkuvan käytön, vaikka palvelin datakeskuksen sisällä kaatuisikin, sekä mahdollistaa käyttäjien

verkkosovellusten, tallennusresurssien ja kuormantasauksen hallinnan. (Wikimedia Foundation, Inc. 2015c.)

Microsoftin datakeskukset sijaitsevat ympäri maailmaa ja ovat Azuren asiakkaiden käytettävissä riippuen asiakkaan sijainnista ja internet-operaattorista. Pohjois-Amerikassa sijaitsee viisi datakeskusta, Etelä-Amerikassa yksi, Aasiassa neljä, Euroopassa kaksi, Japanissa kaksi ja Oseaniassa kaksi. (Wikimedia Foundation, Inc. 2015c.)

# 4 ACTIVE DIRECTORY DOMAIN SERVICES

Active Directory (AD) on Microsoftin kehittämä hakemistopalvelu Windows-palvelinten toimialueen käyttäjien ja koneiden hallintaan. Active Directoryllä voidaan muun muassa hallita käyttäjätilien ja koneiden käyttöoikeuksia, asetuksia, turvallisuusmäärityksiä ja ohjelmistojen asennuksia ja päivittämistä. Active Directoryn toiminta vaatii Domain Controller (DC) -palvelimen, joka vastaa pääasiallisesti käyttäjätilien kirjautumisten oikeellisuuden tarkistamisesta ja käyttäjäryhmän käytäntölistojen jakamisesta. (Wikimedia Foundation, Inc. 2015a.)

Active Directory palvelinrooli esiteltiin ensikertaa Windows 2000 Server -käyttöjärjestelmässä vuonna 1999, ja sen ominaisuuksia on kehitetty ja paranneltu jokaisessa Windows-palvelinkäyttöjärjestelmässä siitä lähtien. Active Directory -palvelinroolista käytettiin aikaisemmin nimitystä domain controller, mutta Windows Server 2008 R2 -käyttöjärjestelmästä lähtien roolia on kutsuttu nimellä Active Directory Domain Services (AD DS). (Wikimedia Foundation, Inc. 2015a.)

## 4.1 Active Directoryn looginen rakenne

Active Directoryn toiminta hakemistopalveluna perustuu tietokantaan ja sitä vastaavaan suoritettavaan koodiin, jonka vastuulla ovat tietokannan haut ja ylläpito. Active Directory suoritettava osa, jota kutsutaan Directory System Agentiksi, on kokoelma Windows-palveluita ja -prosesseja. Active Directoryn tietokannan objekteihin pääsee käsiksi LDAP (Lightweight Directory Access Protocol) -protokollalla, ADSI- (Active Directory Service Interfaces) ja viestirajapinnoilla sekä Security Accounts Manager -palveluilla. (Wikimedia Foundation, Inc. 2015a.)

Objektit, joiden tiedoista Active Directoryn rakenne koostuu, voidaan jakaa karkesti kahteen ryhmään: resurssit (esimerkiksi printterit) ja turvallisuusvaltuudet (käyttäjä- ja konetilit sekä ryhmät). Jokaiselle turvallisuusvaltuudelle annetaan yksilöllinen turvallisuustunniste. (Wikimedia Foundation, Inc. 2015a.)

Jokainen objekti kuvaa yksittäistä itsenäistä kokonaisuutta ja sen ominaisuuksia. Objektit voivat pitää sisällään toisia objekteja. Tietokantamalli määrittää objektin nimen ja ominaisuudet, joista objekti voidaan tunnistaa, sekä sen, millaisia objekteja Active Directoryyn voidaan tallentaa. Tietokantamallilla on myös oma objektinsa, jota voidaan muokata tarvittaessa. Malliobjektit ovat keskeisessä osassa Active Directoryn toimintaa, joten niiden muokkaaminen tai deaktivointi saattaa aiheuttaa vääristymisiä ja muita ongelmia Active Directoryn käyttöönotossa. Luotua objektia ei voi poistaa, ainoastaan deaktivoida. (Wikimedia Foundation, Inc. 2015a.)

Active Directory -verkkoa voidaan tarkastella metsän, puun ja toimialueen tasolla. Active Directory -toteutuksen sisällä objektit on ryhmitelty toimialueisiin. Yhden toimialueen objektit on tallennettu yksittäiseen tietokantaan. Toimialueet voidaan tunnistaa niiden DNS (Domain Name System) -nimen, eli nimiavaruuden, rakenteesta. Looginen ryhmä verkko-objekteja, kuten tietokoneita ja käyttäjiä, jotka jakavat saman hakemistotietokannan, muodostavat toimialueen. (Wikimedia Foundation, Inc. 2015a.)

Puu on yhden tai useamman toimialueen kokoelma, jolla on yhtenäinen nimiavaruus ja jonka luottamushierarkia on transitiivinen. Metsä on kokoelma puita, joilla on yhteiset jaetut hakemistomallit, loogiset rakenteet sekä hakemistoasetukset. Metsä toimii käyttäjien, koneiden, ryhmien ja muiden objektien oikeuksien turvallisuusrajana. (Wikimedia Foundation, Inc. 2015a.)

Järjestelysolut (Organizational units, OU) mahdollistavat toimialueen objektien jakamisen ryhmiin. Järjestelysolut antavat toimialueelle hierarkian, helpottavat ylläpitoa sekä voivat muistuttaa yrityksen oikeaa rakennetta esimerkiksi maantietellisten määritysten mukaan. Microsoft suosittelee järjestelysolujen käyttöä toimialueiden sijasta käytäntötapojen toimeenpanossa ja ylläpidossa. Group Policy Object (GPO) on Active Directory -objekti, jolla hakemiston käytäntötavat määritellään. GPOn vaikutusalueeksi suositellaan järjestelysolua, mutta ne voidaan määrittää toimimaan myös toimialueen tai -paikan tasolla. Ylläpito-oikeudet määritetään usein juuri järjestelysolutasolla. (Wikimedia Foudation, Inc. 2015a.)

## 4.2 Active Directory Domain Servicesin ominaisuuksia

Active Directoryssä on sisäänrakennettu kirjautumistodennus, jolla hakemiston resurssien käyttöoikeudet todennetaan. Ylläpitäjät pääsevät yhdellä sisäänkirjautumisella hallitsemaan hakemistoa ja organisaatiota. Oikeutetut organisaation jäsenet pääsevät kirjautuessaan toimialueeseen kuuluvaan koneeseen käyttämään heille jaettuja resursseja. Käytäntötapoihin perustuva ylläpito helpottaa monimutkaisen verkon hallintaa. (Microsoft 2007.)

Globaali luettelo pitää sisällään kaikkien hakemiston objektien tiedot. Käyttäjät ja ylläpitäjät voivat hakea luettelosta hakemiston tietoja, riippumatta siitä missä toimialueessa data oikeasti sijaitsee. Kysely- ja indeksimekanismi mahdollistaa objektien ja niiden ominaisuuksien julkaisemisen ja luonnin käyttäjien tai sovellusten toimesta. (Microsoft 2007.)

Kahdennuspalvelu levittää hakemiston dataa organisaatioon verkossa. Kaikki toimialueen domain controllerit osallistuvat kahdentamiseen ja pitävät myös itse täydellisen kopion koko hakemiston tiedoista. Muutokset yhdessä domain controllerissa kopioidaan näin muihin toimialueen domain controllereihin. Domain controller voi toimia toimintojen isäntäroolissa, jolloin tietyt toiminnot suoritetaan vain isännällä, hakemiston tietojen yhdenmukaisuuden ja ristiriitaisuuksien välttämiseksi. (Microsoft 2007.)

# 5 ACTIVE DIRECTORY DOMAIN CONTROLLER AZURESSA

Azure -pilvipalvelussa toteutetulla Domain Controllerilla pyritään hyödyntämään virtuaalipalvelimen kustannustehokkuutta verrattuna fyysisen palvelimen ylläpito- ja hankintakustannuksiin. Tämän vuoksi toteutuksessa käytetään edullisinta Azuressa saatavilla olevaa virtuaalipalvelinta. Palvelin täyttää Active Directoryn vähimmäislaitevaatimukset.

Active Directory -toimialueen toteutus Azure -pilvipalvelussa vaatii vähintään yhden virtuaalipalvelimen, joka sijaitsee virtuaaliverkossa ja josta on yhteys yrityksen verkkoon tai suoraan toimialueeseen liittyvään koneeseen. Virtuaalipalvelin toimii Domain Controllerina, joka hallitsee toimialueen koneiden ja käyttäjätilien käyttöoikeus- ja käyttöasetuksia.

Yhteys Azuressa sijaitsevan virtuaaliverkon ja yrityksen verkon tai koneiden välillä muodostetaan VPN-yhteydellä. Yrityksen verkkoon yhteys muodostetaan yrityksen verkon laidalla (Demilitarized Zone, DMZ) sijaitsevan verkkolaitteen avulla. Yrityksen verkon ulkopuolelta yksittäinen kone muodostaa yhteyden virtuaaliverkkoon VPN-asiakasohjelman tai DirectAccess-yhteyden avulla.

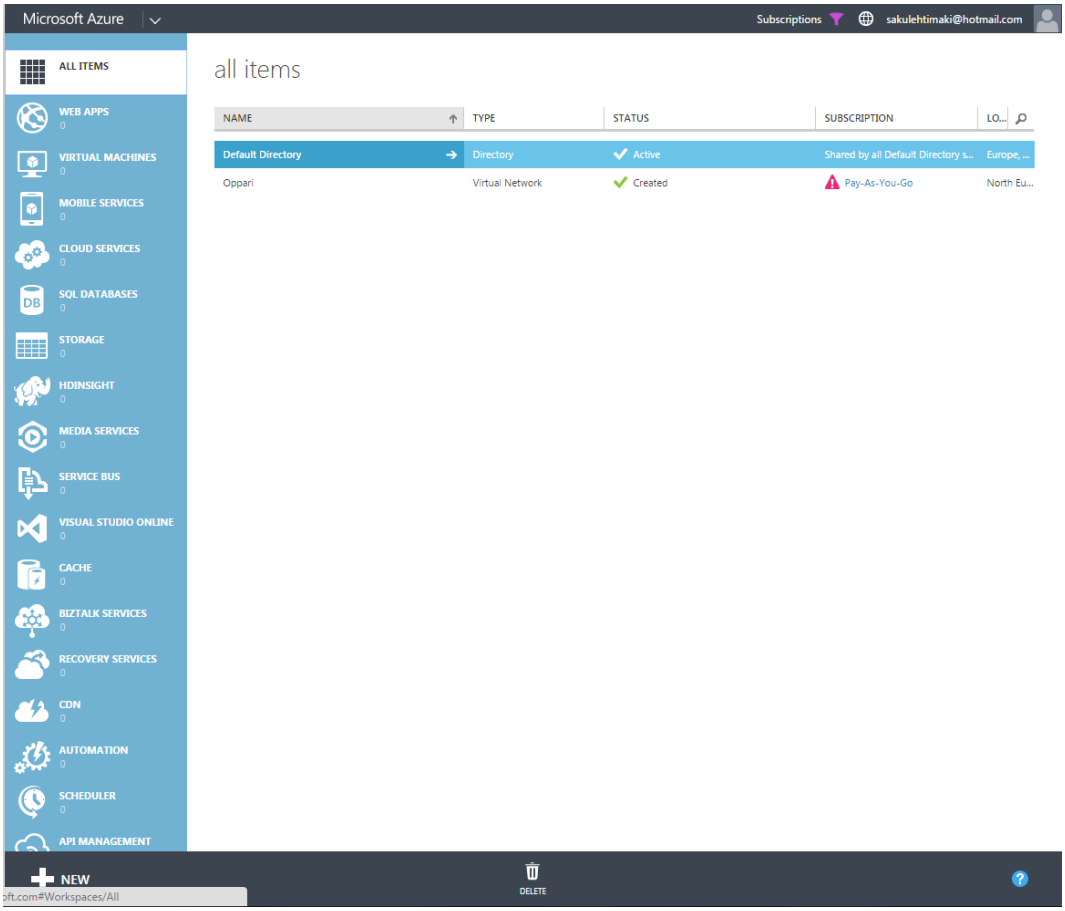
Microsoftin Azure -palvelun käyttö vaatii käyttäjätilin luonnin palveluun. Käyttäjätilinä voidaan käyttää jo olemassa olevaa Microsoft -käyttäjätiliä. Palveluun kirjautumisen jälkeen toimialueen perustaminen voidaan aloittaa.

## 5.1 Domain Controller -palvelimen valmistelu

Azureen kirjautuminen avaa Management Portal -näkymän (KUVIO 8) josta eri virtuaalipalveluita voidaan luoda ja hallita. Sivupalkissa on lueteltuna eri palvelut. Klikkaamalla haluttua palvelua päästään tarkastelemaan kyseisen palvelun olemassa olevia kohteita ja luomaan uusia.

Domain Controllerin asennus Azure -pilveen eroaa hieman paikallisesti tehtävästä asennuksesta. DC:n staattisen IP-osoitteen asettaminen täytyy tehdä erillisen PowerShell -komennon avulla, DNS-palvelin täytyy määrittää virtuaaliverkon asetuksiin ja oletustallennussijainti ei saa olla C-asema.

Azuressa toteutettava AD-toimialue vaatii Domain Controllerin sijoittamista virtuaaliverkkoon. Virtuaaliverkon luomiseksi valitaan Management Portalin sivupalkista kohta NETWORKS. Uuden virtuaaliverkon voi luoda joko pikaluontina Azuren asettamilla asetuksilla, joita voi muokata myöhemmin tai luoda itse mukautetun verkon. Pikaluontina verkolle määritetään nimi, osoiteavaruus, virtuaalikoneiden maksimimäärä, se missä palvelinkeskuksessa verkko sijaitsee, ja DNS-palvelin. Mukautettuna määritetään näiden lisäksi myös se, luodaanko verkkoon VPN-yhteys point-to-site- vai site-to-site –menetelmällä, ja jaetaan halutut aliverkot annetusta osoiteavaruudesta. Active Directory -toimialuetta varten luodaan uusi mukautettu verkko, jolle annetaan nimeksi Oppari, sijainniksi North Europe ja asetetaan aliverkoksi 10.0.0.0/24. DNS- ja VPN-määritykset jätetään vielä asettamatta.




KUVIO 8. Azuren Management Portalin aloitusnäkymä

Virtuaaliverkon luonnin jälkeen voidaan luoda virtuaalikone, joka toimii Domain Controllerina. Management Portalin sivupalkista valitaan kohta VIRTUAL

MACHINES. Uutta virtuaalikonetta luotaessa voidaan jälleen valita joko pikaluontina Azuren määrittämillä asetuksilla luotu kone tai määrittää tarkemmat asetukset itse. Pikaluontina koneelle asetetaan julkinen DNS-nimi, jolle tulee toimialuepääte cloudapp.net, valitaan levykuva, koneen koko, käyttäjätunnus ja salasana, jolla koneeseen kirjaudutaan, ja sijainti. Tarkempia asetuksia varten voidaan määrittää seuraavat kohdat:

- levykuva galleriasta ja levykuvan versio julkaisupäivämäärän mukaan
- koneen nimi, palvelun taso ja koneen koko
- käyttäjätunnus ja salasana
- uusi tai olemassaoleva pilvipalvelu konetta varten
- julkinen DNS-nimi ja koneen sijainti
- uusi tai olemassaoleva tiedontallennustili ja saatavuusryhmä
- liitäntäpisteet
- asennettavia lisäosia.

Domain Controlleria varten valitaan galleriasta levykuvaksi Windows Server 2012 R2 Datacenter ja sen uusin saatavilla oleva versio ja annetaan nimeksi OppariDCAD. Palvelun tasoksi asetetaan STANDARD ja valitaan A0 (shared core, 768 memory) koko. Konetta varten luodaan uusi pilvipalvelu, DNS-nimeksi asetetaan OppariDCAD.cloudapp.net, valitaan virtuaaliverkoksi aiemmin luotu Oppari -verkko ja aliverkko 10.0.0.0/24. Tallennustilinä käytetään automaattisesti tehtyä tiedontallennustiliä. Muut asetukset jätetään oletusasetuksiin.

Domain Controllerina toimivaan koneeseen täytyy lisätä ylimääräinen tallennuslevy, johon palvelin tallentaa AD tietokannan, logit ja System Volume -kansion. Levy lisätään valitsemalla Management Portalista VIRTUAL MACHINES kohdasta kone ja alapalkista kohta ATTACH. Koneeseen valitaan liitettäväksi tyhjä levy, jonka kooksi asetetaan 25 GB. Muut asetukset jätetään oletusasetuksiin. Lisätty levy täytyy alustaa ennen palvelimen AD -roolin asennusta.

Virtuaalikoneen tilan voi nähdä Management Portalin VIRTUAL MACHINES -kohdasta. Luodun koneen tilan ollessa Running koneeseen voidaan ottaa yhteys

Windowsin etätyöpöytä-työkalun Remote Desktop Connectionin avulla. Etätyöpöytäyhteyden voi ottaa itse määrittämällä Remote Desktop Connection -asetuksiin koneen DNS-nimen ja rdp-yhteyttä varten luodun liitäntäpisteen portin tai valitsemalla Management Portalista virtuaalikoneen kohdalta CONNECT. Tämä lataa suoritettavan rdp-tiedoston, jossa edellä mainitut asetukset ovat valmiina. Etätyöpöytäyhteyttä muodostettaessa käytetään koneen luonnin aikana määritettyä käyttäjätunnusta.

## 5.2 Active Directory -toimialueen perustaminen

Ennen Active Direcory Domain Services (AD DS) -palvelinroolin asennusta varmistetaan, että käyttöjärjestelmän kaikki saatavilla olevat päivitykset on asennettu käyttämällä Windows Update -työkalua.

Palvelimelle on asetettava staattinen IP-osoite, koska DC toimii myös verkon DNS-palvelimena. Azuressa staattinen IP-osoite määritetään PowerShell-komennon avulla (KUVIO 9). Komento käynnistää koneen uudelleen, minkä jälkeen staattinen IP-osoite on toiminnassa.

```
Get-AzureVM -ServiceName <Cloud Servicen nimi> -Name
<Virtuaalikoneen nimi> | Set-AzureStaticVNetIP -IPAddress <IP-
osoite virtuaaliverkosta esim. 10.0.0.10> | Update-AzureVM
```

KUVIO 9. Staattisen IP:n määrittäminen

AD DS-palvelinroolin asentaminen aloitetaan avaamalla Server Manager ikkunasta Add roles and features-asennusavustaja ja valitsemalla asennustyypiksi Role-based or feature-based installation. Palvelinlistasta valitaan asennuskohteeksi palvelin, johon asennusta suoritetaan, ja Server Roles -listasta valitaan asennettaviksi rooleiksi Active Directory Domain Services sekä DNS Server. Hyväksytään asennettavaksi oletuksena valitut lisätoiminnot. Tarkistetaan, että kaikki tarvittavat roolit ja toiminnot näkyvät asennuslistassa ja käynnistetään asennus.

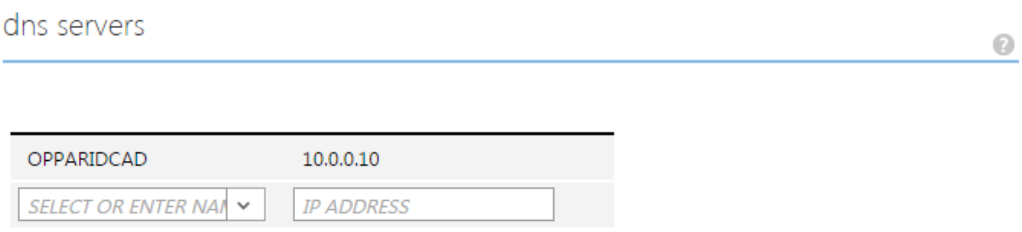
Asennuksen valmistuttua Server Manager ilmoittaa AD DS-roolin tarvitsevan lisäkonfiguraatioita. Avataan Active Directory Domain Services Installation -

asennusavustaja ja Deployment Configuration -sivulta valitaan luotavaksi uusi metsä ja syötetään toimialueen haluttu DNS-nimi. Metsän ja toimialueen toimintatasot asetetaan halutulle tasolle ja määritetään DC toimimaan DNS-palvelimena. NetBIOS-nimi jätetään oletukseksi. Vaihdetaan tietokannan, lokitietojen ja SYSVOL-kansion polut osoittamaan virtuaalikoneeseen lisättyyn levyyn, joka on alustettu levyosioksi F:. Tarkistetaan, että määritetyt asetukset ovat oikein, ja ajetaan asennusedellytysten tarkistus. Kun tarkistus on suoritettu onnistuneesti, asennus voidaan käynnistää. Palvelin käynnistyy uudelleen asennuksen valmistuttua.

## 5.3 Yhdistäminen toimialueeseen

Toimialueeseen yhdistäminen voidaan toteuttaa kahdella tavalla: Point-to-Site tai Site-to-Site. Point-to-Site-menetelmässä yksittäinen asiakaskone liittyy toimialueeseen VPN-asiakasohjelman avulla. Site-to-Site-menetelmässä yrityksen paikallinen verkko yhdistetään toimialueeseen VPN-laitteen avulla.

Active Directory Domain Services- ja DNS-palvelinroolien asennuttua voidaan määrittää palvelin virtuaaliverkon DNS-palvelimeksi (KUVIO 10). Azuren Management Portalin NETWORKS -sivulta valitaan luotu virtuaaliverkko ja CONFIGURE -välilehden alle lisätään palvelin DNS SERVER kohtaa, ja määritetään IP-osoitteeksi staattisesti määritelty osoite.




KUVIO 10. DNS-palvelimen määrittäminen

### 5.3.1 Point-to-Site VPN

Luodun virtuaaliverkon CONFIGURE -välilehden alta täytetään Configure Point-to-Site Connectivity -valintaruutu ja määritetään osoiteavaruus, josta verkkoon

liittyville koneille jaetaan IP-osoitteet. Aiemmin luotuun virtuaaliverkkoon on lisättävä yhdyskäytävä painamalla Add gateway subnet -painiketta. Tallennetaan asetukset Management Portalin alapalkista. Tallennuksen jälkeen siirrytään virtuaaliverkon DASHBOARD -välilehteen ja luodaan uusi dynaamisesti reitittävä yhdyskäytävä valitsemalla Create Gateway -sivun alapalkista.

Point-to-Site käyttää sertifikaatteja käyttäjien yhteyksien todentamiseen. Yhteys vaatii itse allekirjoitetun juurisertifikaatin ja juurisertifikaatista luotuja asiakassertifikaatteja.

Juurisertifikaatti luodaan käyttäen Certificate Creation Tool (makecert.exe) -ohjelmaa, joka löytyy Microsoft Visual Studio Express 2013 -ohjelmistosta tai osana Windows 8.1 SDK -pakettia. Käynnistetään komentokehote Visual Studio Tools -kansiosta ja syötetään kuvion 11 mukainen komento.

```
makecert -sky exchange -r -n "CN=RootSertifikaatti" -pe -a sha1 -
len 2048 -ss My "RootSertifikaatti.cer"
```

KUVIO 11. Juurisertifikaatin luonti

Komento luo sertifikaatin nimeltä RootSertifikaatti ja sitä vastaavan .cer-tiedoston. Tämä .cer-tiedosto ladataan Management Portaliin virtuaaliverkon CERTIFICATES välilehdestä.

Juurisertifikaatista luodaan asiakassertifikaatteja käyttäen samaa komentokehotetta kuin juurisertifikaattia luodessa ja antamalla kuvion 12 mukainen komento.

```
makecert.exe -n "CN=ClientSertifikaatti" -pe -sky exchange -m 96 -
ss My -in "RootSertifikaatti" -is my -a sha1
```

KUVIO 12. Asiakassertifikaatin luonti

Kaikki luodut sertifikaatit löytyvät koneen, jolla sertifikaatit on luotu, sertifikaattikannasta. Tämän voi tarkistaa certmgr.msc-työkalulla. Jokaiselle asiakaskoneelle on hyvä luoda oma asiakassertifikaatti.

Asiakassertifikaatista on tehtävä siirrettävä versio käyttämällä certmgr.msc-työkalua valitsemalla siirrettävä sertifikaatti, avaamalla Action -valikko,

valitsemalla All tasks ja Export. Viedään sertifikaatti yksityisen avaimen kanssa. Tämä luo .pfx-tiedoston, joka kopioidaan ja siirretään asiakaskoneelle. Sertifikaatti asennetaan avaamalla tiedosto ja syöttämällä määritetty salasana. Asennussijaintina käytetään oletussijaintia. VPN-yhteyden toiminnan varmistamiseksi on hyvä siirtää myös juurisertifikaatti asiakaskoneelle samalla toimintaperiaatteella.

VPN-asiakasohjelma ladataan Azure Management Portalista valitsemalla virtuaaliverkko, johon yhteys muodostetaan, ja valitsemalla DASHBOARD -välilehdestä asiakaskoneella käytettävää käyttöjärjestelmää vastaava VPN-paketti.

Ladattu paketti kopioidaan asiakaskoneelle ja suoritetaan asennus. Ohjelman asennuttua siirrytään koneen verkkoyhteys asetuksiin ja käynnistetään juuri luotu VPN-yhteys. Valitsemalla Connect avautuneesta ikkunasta ohjelma muodostaa yhteyden virtuaaliverkkoon. Yhteyden onnistumisen voi varmistaa suorittamalla komentorivillä komennon *ipconfig/all* ja tarkistamalla, onko asiakaskone saanut VPN-yhteydelle IP-osoitteen virtuaaliverkon asetuksissa määritellystä aliverkosta.

Asiakaskone liitetään osaksi toimialuetta samalla periaatteella, kuin paikalliseen toimialueeseen. Koneen SYSTEM PROPERTIES -asetuksista vaihdetaan toimialue tai työryhmä, johon kone kuuluu, toimialueeseen, joka Azure -virtuaaliverkossa sijaitsevalla DC-palvelimella luotiin. Toimialueen nimi on DC-palvelimeen määritetty DNS-nimi Active Directory -toimialueelle. Ennen koneen liittämistä toimialueeseen on Active Directoryyn luotava käyttäjätili, jolla on oikeus liittää kone toimialueeseen. Tämän käyttäjätili on myös koneen pääasiallinen käyttäjä.

Toimialueeseen liittämisen jälkeen kone käynnistetään uudelleen. Kirjautuessa koneelle käyttäen AD-käyttäjätiliä käyttäjäoikeuksia ei tarkisteta palvelimelta, koska VPN-yhteys täytyy muodostaa manuaalisesti kirjautumisen jälkeen. Tämän vuoksi käyttäjätili, jolla kone liitettiin toimialueeseen, on koneen pääasiallinen käyttäjätili, koska kirjautumistiedot säilyvät koneen muistissa. Sisäänkirjautumisen jälkeen asennetaan VPN-yhteyden vaatimat sertifikaatit ja VPN-yhteyspaketti uudelle käyttäjälle, avataan VPN-yhteys ja tarkistetaan yhteyden onnistuminen.

### 5.3.2 Site-to-Site VPN

VPN-yhteyden Site-to-Site-toteutus määritetään virtuaaliverkkoa luotaessa valitsemalla luonti-ikkunan VPN CONNECTIVITY kohdassa Configure site-to-site VPN. Tätä varten luodaan myös uusi Local Network -objekti joka edustaa paikallista verkkoa. Local Network -objektille määritetään nimi ja syötetään VPN-laitteen, jolla yhteys Azure -verkkoon muodostetaan, julkinen IP-osoite. Määritetään osoiteavaruus, johon lähetetty IP-paketti kuljetetaan VPN-yhteyden yli. Virtuaaliverkko luodaan käyttäen samoja toimintaperiaatteita, kuin Domain Controller-palvelimen valmisteluvaiheessa. DC-palvelimen toteuttaminen tässä virtuaaliverkossa ei vaadi muutoksia.

Virtuaaliverkkoon luodaan yhdyskäytävä, kuten point-to-site-toteutuksessa. Yhdyskäytävää luotaessa on otettava huomioon, tukeeko paikallinen VPN-laite staattista tai dynaamista reititystä ja halutaanko virtuaaliverkkoon yhdistää myös point-to-site-menetelmällä.

Yhdyskäytävän valmistuttua kerätään tarvittavat tiedot VPN-laitteen konfiguroimista varten. Virtuaaliverkon DASHBOARD -välilehdeltä löytyy yhdyskäytävän IP-osoite ja jaettu avain, jonka voi kopioida leikepöydälle valitsemalla sivun alapalkista Manage key. Download VPN Device Script -kohdasta ladataan VPN-laitetta vastaava komentosarjamalli. Tehdään tarvittavat määritykset VPN-laitteeseen. Määritysten jälkeen virtuaaliverkon DASHBOARD -välilehdeltä voidaan tarkastella yhteyden päivitettyjä tietoja.

Asiakaskone liitetään osaksi toimialuetta samalla periaatteella, kuin paikalliseen toimialueeseen. Ennen koneen liittämistä toimialueeseen on Active Directoryyn luotava käyttäjätili, jolla on oikeus liittää kone toimialueeseen. Käyttäjän kirjautuessa koneelle voidaan käyttää mitä tahansa luotua AD-käyttäjätiliä, jos kone on yhteydessä paikalliseen verkkoon ja VPN-yhteys VPN-laitteen ja Azure -virtuaaliverkon välillä on toiminnassa.

### 5.3.3 DirectAccess

Azure ei virallisesti tue DirectAccess-yhteyden käyttämistä, joten kaikki DirectAccess-ominaisuudet eivät ole käytössä, mutta yhteys Domain Controlleriin voidaan myös toteuttaa DirectAccess-yhteyden avulla. Windows Server 2012 -palvelimen Remote Access Service -toiminto mahdollistaa DirectAccess-asetusten jakamisen Active Directory -käyttäjäryhmälle, jolloin käyttäjät saavat yhteyden toimialueeseen automaattisesti IPHTTPS-tunneloinnin avulla ilman erillisen VPN-yhteyden avaamista. Asiakaskoneen käyttöjärjestelmän on oltava Windows 8/8.1 Enterprise tai Windows 7 Enterprise tukeakseen DirectAccessia.

Azuressa toteutettavassa AD-ympäristössä tämä mahdollistaa yhdyskäytävän käytöstä poiston, joka vähentää virtuaalitoteutuksen kuluja. Asiakaskoneelle täytyy tehdä yhteydetön liittyminen toimialueeseen, jos kone ei ole ollut yhteydessä Domain Controlleriin, eikä näin ollen ole saanut DirectAccess asetuksia.

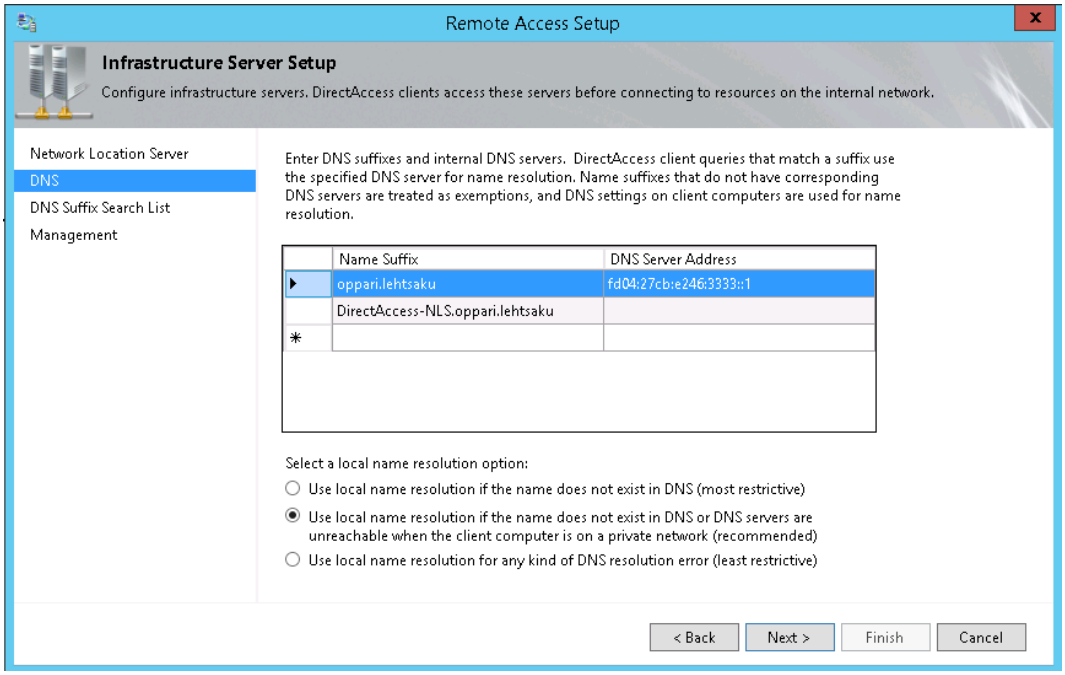
DirectAccess toteutusta varten palvelimelle täytyy asentaa Certificate Authority -rooli (CA), joka jakaa sertifikaatit käyttäjille ja DirectAccess-palvelulle. Pyydetään *certmgr.msc*-työkalun avulla CA:lta palvelimelle sertifikaatti, jonka nimi on sama kuin palvelimen julkinen nimi. Active Directoryyn luodaan ryhmä DirectAccess-asiakkaille.

Asennetaan palvelimelle Remote Access -rooli ja DirectAccess and VPN-ominaisuus Server Manager -käyttöliittymän kautta. Roolin asennuttua käynnistetään Remote Access management konsoli ja valitaan kohta Run the Remote Access Setup Wizard. Asennusohjelma varoittaa staattisen IP:n puuttumisesta. Ohjelma ei tunnista Azuressa tehtyä dynaamisen IP:n varausta staattiseksi osoitteeksi, joten varoituksen voi jättää huomioimatta. Käynnistetään palvelimessa Windows Remote Management -palvelu antamalla komentokehotteeseen komento *winrm quickconfig.* Tämä poistaa ohjelman ilmoittaman virheen. Tarkistetaan vaatimukset uudelleen ja tarkistuksen jälkeen siirrytään seuraavaan kohtaan valitsemalla Next.

Remote Access -asetusten määrittämistä jatketaan kohdasta DirectAccess Client Setup. Deployment scenariona käytetään full DirectAccess for client access and remote managent. Valitaan ryhmäksi käyttäjäryhmä, joka sisältää konetilit DirectAccess-käyttäjiä varten. Loput asetukset jätetään oletusasetuksiin.

Remote Access Server Setup -ikkunasta valitaan palvelimen topologiaksi Behind an edge device (with a single network adapter) ja syötetään palvelimen julkinen nimi, esimerkiksi PALVELIN.cloudapp.net. Verkkokorttina käytetään oletuksena olevaa palvelimen ainoaa verkkokorttia. Selataan sertifikaattilistasta CA:n myöntämä sertifikaatti, jolla on palvelimen julkinen nimi. Seuraavassa kohdassa valitaan käyttäjien autentikointitavaksi AD-tunnukset, merkitään käytettäväksi konesertifikaatteja ja selataan sertifikaattilistasta CA:n juurisertifikaatti.

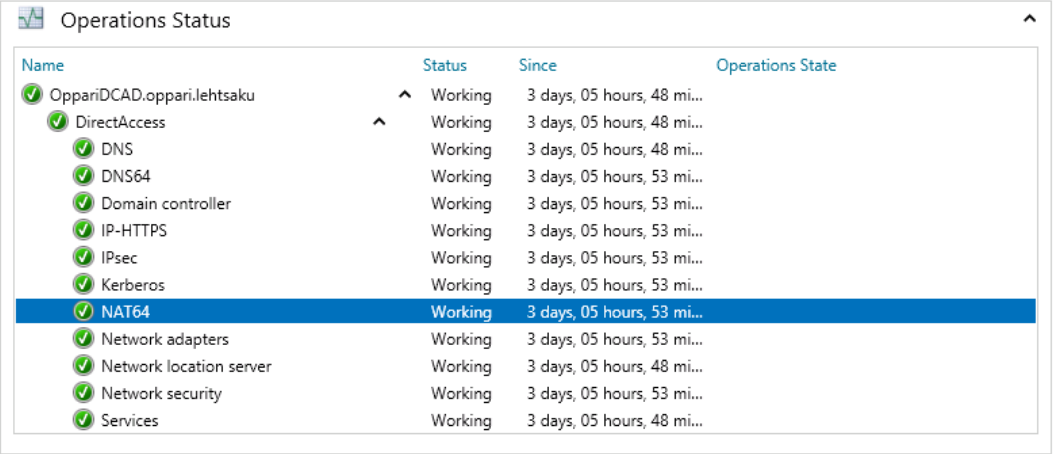
Infrastructure Server Setup -ikkunassa voidaan valita NLS-palvelimen sijainniksi Remote Access -palvelin ja käyttää itse allekirjoitettua sertifikaattia. Todetaan, että DNS-palvelimen nimi ja IP-osoite on oikein ja käytetään suositeltuja asetuksia (katso KUVIO 13.).




KUVIO 13. DirectAccessin käyttämän DNS-palvelimen määrittäminen

Seuraavassa kohdassa asennusohjelma hakee automaattisesti luotetut toimialueet. Siirretään haluttu toimialue käytettävien listaan. Viimeisessä kohdassa voidaan määrittä hallintapalvelimet, jos sellaisia on.

Valitaan Remote Access Management -konsolista Finish. DirectAccess luo uudet Group Policy Objektit jaettaviksi DA-asiakkaille ja palvelimelle ja määrittää tarvittavat asetukset. Tarkistetaan Operation Status -listasta, että kaikki kohdat ovat kunnossa (KUVIO 14).




KUVIO 14. Remote Access Managerin Operation Status näkymä

Viimeiseksi lisätään virtuaalipalvelimeen endpoint IPHTTPS-yhteyttä varten. Azuren Management Portalissa valitaan virtuaalikone, siirrytään ENDPOINTS -välilehteen ja luodaan uusi itsenäinen HTTPS endpoint oletusasetuksilla.

Asiakaskoneet voivat nyt käyttää DirectAccess-yhteyttä. Tarvittavat Group Policy -asetukset ja sertifikaatit on jaettu automaattisesti, jos DirectAcces-käyttäjäryhmään kuuluva kone on ollut yhteydessä Domain Controlleriin.

Asiakaskoneella, joka ei ole ollut yhteydessä Domain Controlleriin ja jolla yhteys halutaan toteuttaa ainoastaan DirectAccessin avulla, tehdään yhteydetön toimialueeseen liittyminen. Tämä tehdään käyttäen Djoin.exe-ohjelmaa. Ensin luodaan konetili DirectAccess-käyttäjäryhmän alle ja provisioidaan konetili Active Directory -palvelimella antamalla komentokehotteeseen kuvion 15 mukainen komento.

```
Djoin /provision /domain <toimialueen nimi> /machine
<asiakaskoneen nimi> /policynames <DA Client GPO:n nimi>
/rootcacerts /savefile c:\files\provision.txt /reuse
```

KUVIO 15. Konetilin provisiointi

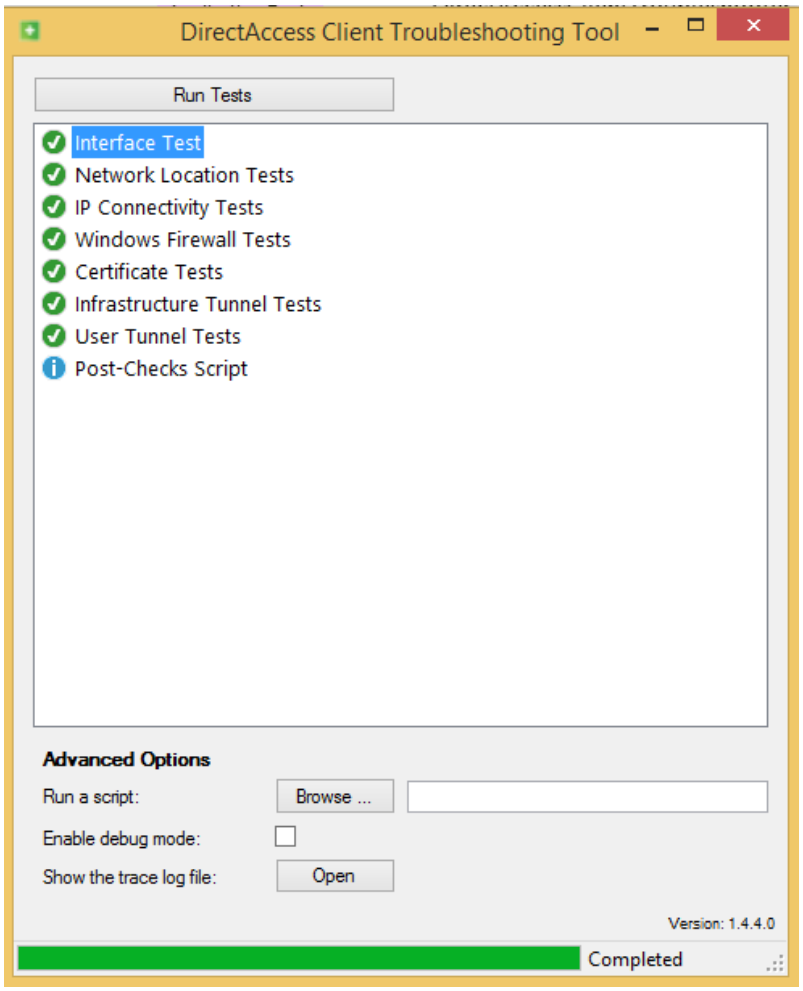
Komento luo tekstitiedoston, joka kopioidaan asiakaskoneelle. Tekstitiedoston kopioimisen jälkeen asiakaskoneella annetaan komentokehotteeseen kuvion 16 mukainen komento.

```
Djoin /requestodj /loadfile C:\provision\provision.txt
/windowspath %windir% /localos
```

KUVIO 16. Yhteydetön liittyminen toimialueeseen

Käynnistetään kone uudelleen, minkä jälkeen kone kuuluu toimialueeseen. Sisäänkirjautumisen jälkeen varmistetaan *certmgr.msc*-työkalulla, että käyttäjällä on tarvittavat sertifikaatit. Siirretään tarvittavat sertifikaatit manuaalisesti koneelle, jos puutteita havaitaan.

DirectAccess-yhteyden tilan voi tarkistaa koneen Networks-asetuksista. Ongelmatilanteissa käytetään DirectAccessClientTroubleshooter -ohjelmaa, joka ladataan asiakaskoneelle. Ohjelma tarkistaa yhteyden ja ilmoittaa mahdollisista ongelmista (KUVIO 17).




KUVIO 17. Asiakaskoneen DirectAccess ongelmanhakutyökalu

Azuressa toteutettavassa DirectAccess-palvelimen käytössä on otettava huomioon Azuren määrittämä VIP (Virtual IP) -osoite, joka vaihtuu, jos virtuaalikoneen resurssit jaetaan uudelleen. Palvelimen voi sammuttaa ja käynnistää uudelleen normaalisti käyttäjärjestelmän kautta, mutta Azure Management Portalin kautta annettu Shutdown-komento jakaa palvelimen käyttämät resurssit uudelleen.

## 5.4 Toteutuksen kustannukset

Azuressa toteutetun Active Directory -toimialueen kustannukset muodostuvat pääosin virtuaalikoneen vuokrasta, yhdyskäytävän käytöstä sekä tallennustilasta ja sen käytöstä. Kustannuksissa ei oteta huomioon asiakaskoneita ja niihin liittyviä kuluja, kuten käyttöjärjestelmälisenssit.

Usage Charges

| Name | Type | Resource | Region | Consumed | Included | Billable | Rate | Value |
|---|---|---|---|---|---|---|---|---|
| Storage | Geo Redundant | Standard IO - Page Blob/Disk (GB) | | 30.6292 | 0.0000 | 30.6292 | 0.0707 | 2.17 |
| Virtual Machines | A1 VM (Windows) | Compute Hours | EU North | 144.0720 | 0.0000 | 144.0720 | 0.0670 | 9.66 |
| Data Management | | Storage Transactions (in 10,000s) | | 504.1638 | 0.0000 | 504.1638 | 0.0003 | 0.14 |
| Networking | | Data Transfer Out (GB) | Zone 1 | 0.0349 | 0.0000 | 0.0349 | 0.0648 | 0.00 |
| Networking | Virtual Network | Gateway Hours | | 274.0833 | 0.0000 | 274.0833 | 0.0268 | 7.35 |

| | |
|---|---|
| Sub-Total | 19.32 |
| **Grand Total** | **19.32** EUR |

KUVIO 18. Laskuerittely kuukauden käytöstä

Laskusta (KUVIO 18) voidaan todeta, että vaikka virtuaalikoneen kooksi on määritetty A0, laskutus tapahtuu A1-koon mukaisella tuntimaksulla. Laskusta ei ilmene, tasoitetaanko kulut esimerkiksi käyttötuntien mukaan vastaamaan A0:n käyttökuluja.

Suurin osa kuluista syntyy yhdyskäytävän ylläpidosta ja virtuaalikoneen käyttötunneista. Domain Controllerin käytössä tallennustilan aktiivikäyttö ja verkkoliikenne eivät aiheuta suuria kuluja, koska palvelin ei joudu jatkuvasti kirjoittamaan ja lukemaan dataa  levyltä eikä verkon yli siirretä suuria data-määriä. Virtuaalikoneen käyttötunteina laskutetaan aika, jolloin kone käyttää sille jaettuja resursseja.

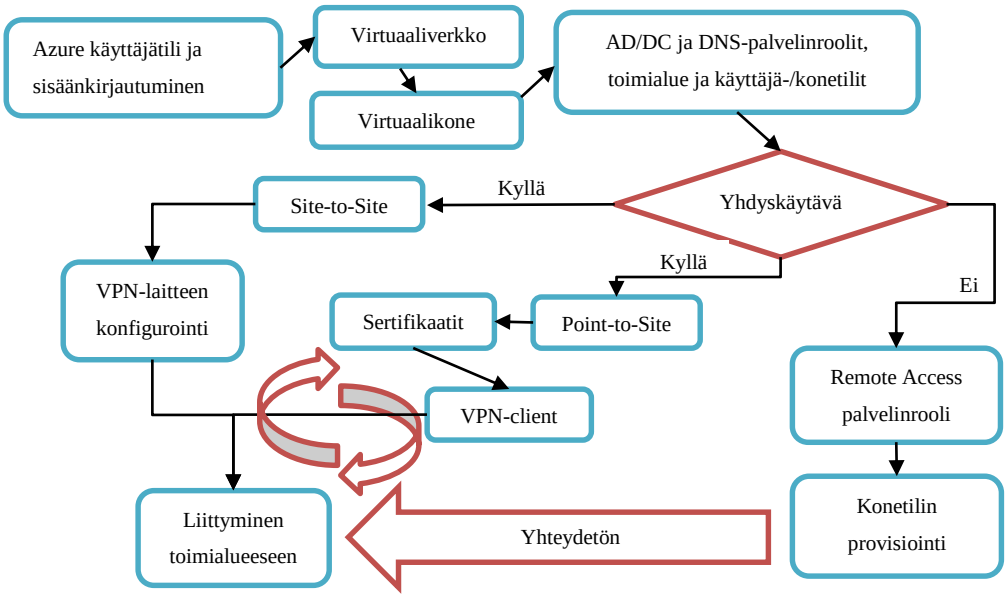
Käyttäen A0-koneen käyttöhintaa site-to-site-toteutuksen kuluiksi voidaan laskea 720 yhdyskäytävän ylläpitotuntia, virtuaalikoneen aktiivikäytöksi 528 tuntia. Azuresta syntyy näin ollen kuluja noin 27 euroa. Tähän on lisättävä paikallinen VPN-laite ja siihen liittyvät kulut, kuten julkinen IP-osoite. Point-to-site-menetelmän kulut ovat Azuren kannalta yhtä suuret, mutta erillistä VPN-laitetta ei tarvita. DirectAccess-toteutuksen kustannuksista voidaan poistaa yhdyskäytävän kulut, jolloin käyttökustannukset ovat noin 8 euroa.

Toteutusten kustannusten jäädessä näin alhaisiksi voidaan suositella käyttämään vähintään A1-koon virtuaalikonetta, jolloin VPN-toteutusten (Site-to-Site ja Point-to-Site) Azuren synnyttämiksi kuluiksi tulee noin 55 euroa. DirectAccess-toteutuksen kustannukset ovat noin 32 euroa.

## 5.5 Toteutuksen tulokset

Kaikki toteutusvaihtoehdot ovat käyttökelpoisia, mutta jokaisessa toteutuksessa on heikkoutensa (katso LIITE 1.). Point-to-Site- ja DirectAccess-toteutukset ovat kuluiltaan pienimmät, mutta vaativat eniten työtä käyttöönotossa. DirectAccess-ratkaisu vie myös laiteresursseja Active Directoryn toiminnalta, jos Remote access -palvelin ja Domain Controller ovat sama kone. Point-to-Site- ja DirectAccess-toteutusten ehdottomana etuna on mahdollisuus toteuttaa ratkaisut, vaikka yrityksellä ei olisi omaa toimitilaa.

Käyttöönoton ja käyttäjäystävällisyyden kannalta paras toteutusvaihtoehto on Site-to-Site-ratkaisu (KUVIO 19) (LIITE 1). Site-to-Site-ratkaisun negatiivisena puolena toteutus vaatii toimitilan ja erillisen VPN-laitteen.




KUVIO 19. Toteutuksen prosessikaavio

DirectAccess-toteutuksessa voidaan suositella käyttämään kahta virtuaalikonetta, joista toinen toimii Domain Controllerina ja toinen Remote Access -palvelimena. Kattavimpana ratkaisuna voidaan pitää site-to-site- ja DirectAccess-toteutuksen yhdistämistä ja toteuttamista kahdella A0-koon virtuaalikoneella, jolloin kustannukset olisivat arviolta 35 euroa. Tähän on lisättävä VPN-laitteen hankintakustannukset ja internet-yhteyden kulut.

# 6 YHTEENVETO

Pilvipalveluiden yleistyminen ja virtualisointi mahdollistavat pienyrityksille samat palvelinratkaisut, kuin suuremmille yrityksille, ilman suuria alkusijoituksia. Pilvipalveluiden tarjoaminen on yritystoimintana melko uusi ja kokoajan kasvava ala. Kilpailun kiihtyessä tarjottavat palvelut monipuolistuvat ja niiden räätälöinti asiakkaan tarpeisiin yleistyy. Pilvipalvelu-ohjelmistojen kehitys antaa yrityksille myös hyvät työkalut omien yksityisten pilvien perustamiseen, jos omistautumista ja rahoitusta toimintaan löytyy.

Pilvipalveluna Microsoft Azure on pääasiallisesti helppokäyttöinen ja toimintojen dokumentointi on hyvä. Asiakaspalvelun valmius yllättää positiivisesti; Azure-tilin luontia seuraavana päivänä Microsoftin asiakaspalvelusta tulee puhelu, jossa tiedustellaan Azuren palveluiden käyttökohdetta ja annetaan käyttökohteeseen perehtyneen henkilön yhteystiedot. Negatiivisena huomiona voidaan mainita laskutettavien palveluiden ja palvelukokonaisuuksien hintojen tarkastelu, joka ei ole niin suoraviivaista, kuin aluksi näyttää.

Pienyrityksen Active Directory on mahdollista toteuttaa Azure-pilvipalvelussa. Toteutus kuitenkin saattaa vaatia suuremman työmäärän ylläpitäjältä, kuin paikallisesti toteutettu ratkaisu. Käyttäjän kannalta helpoin ratkaisu on Site-to-site- tai DirectAccess-menetelmällä. Kustannusten minimoimiseksi valittu A0-kokoisen virtuaalikoneen vähäiset resurssit ilmenevät graafisen käyttöliittymän kankeutena, muitakin ongelmia saattaa ilmetä, jos palvelinta kuormitetaan.

DirectAccess-menetelmän hyötynä on yhdyskäytävän poiston vähentämät kustannussäästöt, mutta yhteydetön toimialueeseen liittäminen vaatii lisää työtä. Koska Azure ei virallisesti tue DirectAccessia, ongelmien ilmetessä virallista tukea ei ole saatavilla ja palvelussa saattaa ilmetä myös tuntemattomia vikoja. Toteutettaessa DirectAccess-palvelu samalla palvelimella, joka toimi myös Domain Controllerina, palvelun viemät palvelinresurssit ovat pois Active Directoryn normaalikäytöstä, mikä saattaa aiheuttaa ongelmia.

Pilvipalvelut ovat asiakasyritysten kannalta varteenotettava ratkaisu perinteisten toteutusten sijasta. Tulevaisuudessa todennäköisesti monien niin pienten kuin suurempienkin yritysten tietoliikennepalvelut ja sovellukset toteutetaan pilvessä.

LÄHTEET

Cloud Security Alliance. 2010. Top Threats to Cloud Computing v1.0 [viitattu 20.3.2015]. Saatavissa: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Security Alliance. 2015. About [viitattu 20.3.2015]. Saatavissa: https://cloudsecurityalliance.org/about/

CommVerge Solutions. 2015. Virtualization –artikkelikuva [viitattu 20.3.2015]. Saatavissa: http://www.commverge.com/LinkClick.aspx?link=images%2Fb.+data+center+-+virtualization+v3.jpg&tabid=192&mid=1845

Hiltunen, J. 2010. Palvelimen virtualisointi. Lahti: Lahden ammattikorkeakoulu, Tekniikan ala [viitattu 20.3.2015]. AMK-opinnäytetyö. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/24102/Hiltunen_Jukka.pdf?sequence=1

Boucher, Rob Jr. 2014. Introducing Microsoft Azure. Microsoft [viitattu 20.3.2015]. Saatavissa: http://azure.microsoft.com/en-us/documentation/articles/fundamentals-introduction-to-azure/

Microsoft. 2007. Active Directory Domain Services Overiview. [viitattu 20.3.2015]. Saatavissa: https://technet.microsoft.com/en-us/library/9a5cba91-7153-4265-adda-c70df2321982

Microsoft. 2009. Mapping application to the Cloud. Operating system-level virtualization –artikkelikuva [viitattu 20.3.2015]. Saatavissa: https://msdn.microsoft.com/en-us/library/dd430340.aspx

Mäntylä, J.-H. 2008. Virtualisointi mullistaa tietotekniikan. Talentum: Tivi [viitattu 20.3.2015]. Saatavissa: http://www.tivi.fi/CIO/2008-11-30/Virtualisointi-mullistaa-tietotekniikan-3158514.html

Viestintävirasto. 2014. Kyberturvallisuuskeskus. Pilvipalveluiden turvallisuus [viitattu 20.3.2015]. Saatavissa:

https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Wikia, Inc. 2015. VirtualisointiWiki: Virtualisointi [viitattu 20.3.2015]. Saatavissa: http://fi.laovirtualisointi.wikia.com/wiki/Luokka:Virtualisointi

Wikimedia Foundation, Inc. 2015a. Active Directory [viitattu 20.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Active_Directory

Wikimedia Foundation, Inc. 2015b. Cloud computing [viitattu 20.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Cloud_computing

Wikimedia Foundation, Inc. 2015c. Microsoft Azure [viitattu 20.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Microsoft_Azure

Wikimedia Foundation, Inc. 2015d. Pilvilaskenta [viitattu 20.3.2015]. Saatavissa: http://fi.wikipedia.org/wiki/Pilvilaskenta

Wikimedia Foundation, Inc. 2015e. Virtualization [viitattu 20.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Virtualization

Ylä-Himanka, S. 2011. Virtualisointi – Microsoft Hyper-V. Oulun seudun ammattikorkeakoulu [viitattu 20.3.2015]. AMK-opinnäytetyö. Saatavissa: https://publications.theseus.fi/bitstream/handle/10024/27427/Yla-Himanka_Susanna.pdf?sequence=1

LIITTEET

LIITE 1. TOTEUTUSVERTAILU

| | Point-to-Site | Site-to-Site | DirectAccess |
|---|---|---|---|
| Kustannukset | 27€(A0) / 55€(A1) | 27€(A0)/55€(A1) + VPN-laite | 8€(A0) / 32€(A1) |
| Käyttöönotto | - Sertifikaatit<br>- Jokaiselle käyttäjälle erillinen käyttöönotto | - VPN laitteen konfigurointi<br>+ Toimialueeseen liittyminen | - Yhteydetön liittyminen<br>- Jokaiselle käyttäjälle erillinen käyttöönotto |
| Ylläpito | AD:n ylläpito yrityksellä | VPN-laitteen ja AD:n ylläpito ja huolto yrityksellä | AD:n ja DA:n ylläpito yrityksellä |
| Muut | + Ei vaadi toimitiloja<br>+ Yhteys mistä tahansa<br>- Kirjautuessa ei yhteyttä palvelimeen<br>- Hankala automatisoida | + ”Jatkuva” yhteys<br>- Yrityksellä oltava toimitila<br>- Ei etäyhteyttä | + Ei vaadi toimitiloja<br>+ Yhteys mistä tahansa<br>+ Automaattinen yhteyden avaus<br>- Ei täyttä tukea<br>- Vie resursseja DC:ltä |