Matias Ahola

Pilvipalvelut

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

8.4.2018

Metropolia

Tekijä Otsikko Sivumäärä Aika	Matias Ahola Pilvipalvelut 29 sivua 8.4.2018
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Lehtori Tapio Wikström

Insinöörityön tarkoituksena on tutustua pilvipalveluiden keskeisimpiin ominaisuuksiin, palvelumalleihin ja pilvimalleihin. Pilvipalvelut ovat internetin välityksellä esimerkiksi tiedonkäsittelyssä ja -siirrossa käytettäviä tietotekniikkapalveluita, joita voivat käyttää sekä yksityiset henkilöt että yritykset.

Pilvipalveluiden perusajatuksena on, että palveluiden käyttäjä tarvitsee vain toimivan verkkoyhteyden ja verkkoselaimen käyttääkseen pilvipalveluita. Koska pilvipalvelut toimivat internetin välityksellä, on aiheellista tarkastella pilvipalveluiden tietoturvaa sekä yleisimpiä uhkia. Yleisesti pilvipalvelut jaetaan IaaS-, PaaS- sekä SaaS-palveluihin eli infrastruktuuripalveluihin, sovelluskehitysalustoihin ja sovelluksiin.

Insinöörityöhön sisältyy myös käytännön osuus, jossa luodaan virtuaalikone VMware Workstation 14 -virtualisointialustan avulla. Luotu virtuaalikone siirretään cold migration -menetelmällä Amazon Web Services-pilvipalveluun.

Virtuaalikoneen siirron toteutus Amazon Web Services-pilvipalveluun onnistui hyvin. Cold migration -menetelmä vaati mittavat alkutoimenpiteet, mutta ne helpottivat seuraavien vaiheiden toteutusta. Käytännönosuuden tekemisessä oli ajoittain ongelmia, jotka johtuivat muun muassa oppaiden monimutkaisuudesta. Käytännönosuudessa havainnollistettua virtuaalikoneen siirtoa voivat hyödyntää esimerkiksi yritykset, jotka tarvitsevat puhtaan virtuaalikoneen, jossa on haluttu käyttöjärjestelmä ja tarvittavat palvelut valmiiksi asennettuna.

Avainsanat	Pilvipalvelut, pilvilaskenta, IaaS, PaaS, SaaS, pilvimallit, Amazon Web Services, AWS

Author	Matias Ahola
Title	Cloud computing
Number of Pages	29 pages
Date	8 April 2018
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	Tapio Wikström, Lecturer

The subject of this thesis is to get acquainted with the key features of cloud services, cloud models and service models.

Cloud services are accessible via the Internet, only requirements are a valid internet connection and a web browser. It is appropriate to cover cloud security and the most common threats since cloud services work over the Internet. Cloud services are divided to cloud models that are IaaS, PaaS and SaaS service models, ie Infrastructure as a Service, Platform as a Service and Software as a Service. Cloud services are also divided to cloud models, also known as deployment models. There are four deployment models: private cloud, community cloud, public cloud and hybrid cloud.

The thesis includes a practical part of creating a virtual machine and migrating the virtual machine to the Amazon Web Services. The migration process is done by using cold migration method. The virtual machine is created by using the VMware Workstation 14 virtualization platform.

The migration process of the virtual machine to the Amazon Web Services was successful. The cold migration method required many initial steps but made the following steps easier. There were occasional problems due to complex guides used in the migration process. Companies that need to install clean virtual machines with correct operating system and required services can benefit from illustrated virtual machine migration.

Keywords	Cloud computing, IaaS, PaaS, SaaS, Cloud deployment models, Amazon Web Services, AWS

Sisällys

Lyhenteet

Amazon EC2	*Amazon Elastic Compute Cloud*. Amazonin pilvipalvelussa oleva verkkopalvelu, joka tarjoaa turvallista ja muokattavaa laskentakapasiteettia
Amazon S3	*Amazon Simple Storage Service*. Amazonin pilvipalvelussa oleva skaalautuva tallennuspalvelu, joka tarjoaa käyttäjilleen rajattomasti tallennustilaa.
APT	*Advanced persistent threats*. Kehittyneet pysyvät uhat ovat loismaisia tietoturvahyökkäyksiä, jotka tunkeutuvat hyökkäyksen kohteen järjestelmään, josta ne pyrkivät saamaan jalansijan.
AWS	*Amazon Web Services*. Amazonin tarjoama pilvipalvelu, jota Amazon on tarjonnut vuodesta 2006 alkaen.
Bucket	Amazon S3 -palvelussa oleva looginen tallennusyksikkö, jota käytetään objektien tallentamiseen.
DNS-yhteensopiva nimi	Nimi, joka ei sisällä erikoismerkkejä tai isoja kirjaimia.
DDoS, DoS	*Distributed Denial of Service*. Palvelunestohyökkäys, jolla pyritään estämään verkkosivuston käyttö. Hyökkäys voidaan toteuttaa useasta lähteestä samaan aikaan.
GDPR	*General Data Protection Regulation*, Euroopan unionin tietosuojalainsäädäntö, joka astuu voimaan toukokuussa 2018.
IaaS	*Infrastructure as a Service*, infrastruktuuri palveluna.
IAM	*Identity and Access Management*. Identiteetinhallinta, eli käyttäjätietokannan, tunnistetietojen ja todennuksen hallinta.

Logging	Lokitus. Tarkoitetaan aikajärjestyksessä kirjattavia tallenteita tapahtumista ja niiden aiheuttajista. Lokitus auttaa palveluiden vianetsinnässä.
Metadata	Metadata on tietoa tiedosta, jolla voidaan kuvata muun muassa tiedoston sisältöä. Esimerkiksi tekstitiedoston omistaja, versio ja julkaisupäivämäärä.
Multi-tenant	Monikäyttäjyys. Samassa palvelussa on useita käyttäjiä, mutta jokainen saa yksilöllisen käyttökokemuksen.
PaaS	*Platform as a Service*, sovellusalusta palveluna.
Pilvi-infrastruktuuri	Pilvi-infrastrukuutri on perusta, josta liiketoiminnan tarvitsemat palvelut, sovellukset ja tiedot tarjotaan.
SaaS	*Software as a Service*, sovellukset palveluna.
Single-tenant	Yksikäyttäjyys. Palvelu tarjotaan yhdelle käyttäjälle.
Tietotekniikkaresurssi	Esimerkiksi tallennustila, muistin määrä, verkon kaistanleveys.
TLS-varmenne	*Transport Layer Security*. Salausprotokolla, jolla suojataan internetsovellusten tietoliikenne. Tunnettiin aiemmin lyhenteellä SSL, *Secure Socket Layer*.
Virtualisointialusta	Virtualisointialusta eli hypervisor on virtualisointikerros, jolla voidaan perustaa ja hallita virtuaalikoneita.

1 Johdanto

Insinöörityön tarkoituksena on tutustua pilvipalveluiden keskeisimpiin ominaisuuksiin ja saada kattava yleiskuva pilvipalveluista. Työn lopussa on käytännön osuus, jossa siirretään olemassa oleva virtuaalikone pilvipalveluun. Käytän työssäni Amazonin *Amazon Web Services (AWS)* -pilvipalvelua.

Pilvipalvelut ovat internetin välityksellä käytettäviä tietotekniikkapalveluita, jotka koostuvat viidestä tärkeästä ominaisuudesta, kolmesta palvelumallista sekä neljästä pilvimallista (Mell & Grance 2011: 2). Keskustelua pilvipalveluista käytiin erityisesti Yhdysvalloista alkaneen maailmanlaajuisen finanssikriisin aikana, vaikka pilvipalveluita oli ollut saatavilla myös aiemmin. Pilvipalvelut mahdollistivat kustannustehokkaan toiminnan perinteisiin palvelinjärjestelmiin verrattuna, sillä yritykset vapautuivat omien palvelinlaitteistojen käyttämisestä. (Salo 2012: 16.)

Pilvipalveluita käsiteltäessä on aiheellista ottaa huomioon myös palveluihin liittyvät tietoturva-asiat, sillä palveluiden toimiessa internetissä kuka tahansa voi tehdä ilkivaltaa. Pilvipalveluita käytettäessä käyttäjän oma vastuu tietoturvasta huolehtimisesta korostuu.

Pilvipalvelut jaetaan palvelumalleihin, joita ovat IaaS-, PaaS- sekä SaaS-palvelut eli infrastruktuuripalvelut, sovelluskehitysalustat ja sovellukset. Palveluiden keskeisimpiä ominaisuuksia ovat skaalautuvuus ja kustannustehokkuus, sillä ne mahdollistavat palveluiden räätälöinnin yksittäisen käyttäjän tarpeisiin sopiviksi. (Salo 2012: 20-21.) Myös virtualisointi on suuressa roolissa pilvipalveluissa, sillä tällä tekniikalla mahdollistetaan pilvipalveluille ominaiset piirteet. Virtualisointia käyttämällä palveluntarjoajat voivat jakaa saman fyysisen laitteiston usean käyttäjän kanssa, jolloin toiminta on kustannustehokasta asiakkaalle. (Sosinsky 2011: 94.)

2 Pilvipalvelut ja niiden rakenne

Pilvipalvelu on malli, joka mahdollistaa vaivattoman pääsyn muunneltaviin tietotekniikkaresursseihin, kuten tietoverkkoihin, palvelimiin, tallennustiloihin ja sovelluksiin milloin ja missä tahansa. Resurssien jakaminen ja muunteleminen onnistuvat helposti ja nopeasti pilvipalveluissa vähäisellä vuorovaikutuksella itse palveluntarjoajan kanssa. (Mell & Grance 2011: 2.)

Pilvipalveluiden yleisistä ominaisuuksista on olemassa useita ohjeistuksia ja määrityksiä siitä, miten voidaan tunnistaa oikea pilvipalvelu. Yhden määritelmän pilvipalveluiden ominaisuuksista antaa Yhdysvaltojen julkishallinnon elinkeinoministeriön alainen virasto, National Institute of Standards and Technology (NIST). NIST:n määritelmän mukaan pilvipalvelut koostuvat viidestä tärkeästä ominaisuudesta, kolmesta palvelumallista sekä neljästä pilvimallista (Mell & Grance 2011: 2).

2.1 Pilvipalveluiden ominaisuudet

Pilvipalveluiden ominaisuuksiin kuuluvat seuraavat asiat.

- Itsepalvelullisuus (On-demand self-service)

Käyttäjät voivat muuttaa tietotekniikkaresursseja, kuten palvelimen aikaa ja verkkotallennustilaa, automaattisesti ilman palveluntarjoajan väliintuloa. Itsepalvelullisuus antaa käyttäjälle vapaat kädet, milloin hän tarvitsee resursseja, kuinka paljon resursseja hän tarvitsee sekä minkälaisia resursseja hän haluaa käyttöönsä. (Mell & Grance 2011: 2.)

- Laaja-alainen pääsy palveluihin (Broad network access)

Toiminnot ovat käytettävissä verkon kautta, ja ne ovat päätelaiteriippumattomia. Pilvipalvelut mukautuvat päätelaitteen mukaan; tällöin käyttäjän ei tarvitse erityisiä laitteita käyttääkseen palveluita. (Mell & Grance 2011: 2.)

- Resurssien yhteiskäyttö (Resource pooling)

Palveluntarjoajan tietotekniikkaresurssit yhdistetään palvelemaan useita käyttäjiä samaan aikaan multi-tenant-mallia hyödyntäen. Multi-tenant-mallissa on erilaisia fyysisiä ja virtuaalisia resursseja, jotka on dynaamisesti määritelty käyttäjien kysynnän mukaan. Käyttäjällä ei ole yleensä kontrollia tai tarkkaa tietoa siitä, missä annetut tietotekniikkaresurssit sijaitsevat, mutta korkeammalla tasolla hän voi määritellä sijainnin maan, osavaltion tai datakeskuksen mukaan. Pilvimallista riippuen yksittäiset fyysiset laitteistot voivat olla ainoastaan yhden käyttäjän käytettävissä. (Mell & Grance 2011: 2.)

- Nopea skaalautuvuus (Rapid elasticity)

Tietotekniikkaresursseja voidaan joustavasti lisätä tai vähentää käyttäjän tarpeen mukaan automaattisesti ja reaaliaikaisesti, jolloin käyttäjälle syntyy illuusio palveluntarjoajan rajattomasta resurssimäärästä (Mell & Grance 2011: 2).

- Tarkka ja valvottu resurssien käyttö (Measured Service)

Pilvipalvelujärjestelmät kontrolloivat ja optimoivat tietotekniikkaresurssien käyttöä automaattisesti käyttäen apunaan jonkinasteista mittaustapaa, joka vastaa palveluntyyppiä. Mittaustapana voidaan käyttää muun muassa tallennustilaa, kaistanleveyttä tai aktiivisia käyttäjätilejä, jolle palvelun laskutus pohjautuu. Tietotekniikkaresurssien käyttöä voidaan seurata, valvoa ja raportoida, mikä tarjoaa avoimuuden sekä palveluntarjoajalle että käyttäjälle. (Mell & Grance 2011: 2.)

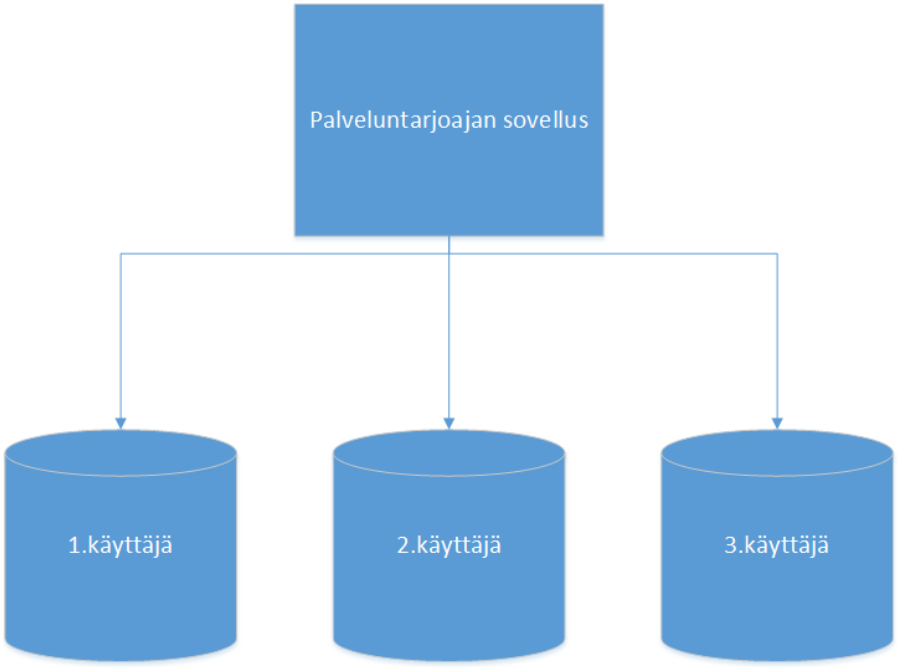
Pilvipalveluiden ominaisuuksien lisäksi pilvipalvelut ovat kustannustehokkaita, helposti ja edullisesti käyttöönotettavia, luotettavia, yksinkertaisia ylläpitää ja päivittää sekä helposti priorisoitavia (Sosinsky 2011: 17-18).

2.2 Palvelumallit

2.2.1 Sovellukset palveluna, SaaS (Software as a service)

SaaS-palvelumallissa käyttäjällä on mahdollisuus käyttää palvelutarjoajan sovelluksia, jotka toimivat palveluntarjoajan pilvi-infrastruktuurissa. Sovelluksia voidaan käyttää useista eri laitteista verkkoselaimen tai sovelluksen käyttöliittymän kautta. Käyttäjä ei hallitse taustalla olevaa pilvi-infrastruktuuria, kuten verkkoa, palvelimia, käyttöjärjestelmiä, tallennustilaa tai yksittäisiä sovellusominaisuuksia. Käyttäjä voi hallita rajoitettuja käyttäjäkohtaisia sovellusasetuksia, kuten valita aikavyöhykkeen tai asettaa sähköpostiviestiin allekirjoituksen. (Mell & Grance 2011: 2.) Lisenssimaksun sijasta käyttäjä maksaa palvelun käytöstä esimerkiksi aikaperusteisesti, käyttäjä- tai konekohtaisesti. Sovellusarkkitehtuuri perustuu monikäyttäjyyteen, mutta käyttäjät saavat kuitenkin yksilöllisen käyttäjäkokemuksen. (Salo 2012: 25-26.) SaaS-palvelumallissa palveluntarjoajan sovelluksesta jaetaan siis jokaiselle käyttäjälle oma instanssi eli istunto.

Google Apps on SaaS-pohjainen pilvipalvelu, jossa Google antaa palvelunkäyttäjälle mahdollisuuden käyttää ilmaiseksi toimistosovelluksia ja sähköpostia tietyin rajoituksin. Esimerkiksi Google Apps -tuoteperheeseen kuuluva palvelu, Google Drive, on ilmainen pilvitallennusratkaisu, jossa tallennustilaa on rajoitettu, mutta lisätallennustilaa voi ostaa kuukausihinnalla.



Kuva 1. Esimerkki SaaS-palvelumallin rakenteesta

2.2.2 Sovellusalusta palveluna, PaaS (Platform as a service)

Ohjelmistokehittäjille suunnatussa PaaS-palvelumallissa palveluntarjoaja tarjoaa ohjelmistokehittäjille sovelluskehitysalustan käyttöönsä. Sovelluskehitysalustan päällä voidaan kehittää, testata sekä ylläpitää sovelluksia. Tämä yksinkertaistaa ja nopeuttaa sovelluskehitystä, sillä kehittäjät voivat keskittyä sovelluskehitykseen ilman huolta infrastruktuurista. Kehitystyöstä tulee nopeampaa, kustannustehokkaampaa ja lopputulos skaalautuu suuriin käyttäjämääriin vaivattomasti. Sovellusalustaan voidaan lisätä lisätoimintoja valmiina moduuleina tai ohjelmointirajapintoina. Palveluntarjoajan vastuulla ovat toimintavarmuus, skaalautuvuus, alustan ylläpito ja päivitykset. Tällöin käyttäjän vastuulle jää vain koodin tuottaminen. (Salo 2012: 24-25.)

PaaS-palvelumalli antaa käyttäjälle mahdollisuuden julkaista pilvi-infrastruktuurin itse luotuja tai hankkimia sovelluksia, jotka on luotu ohjelmointikielillä, kirjastoilla, palveluilla ja työkalujen avulla. Käyttäjä ei hallitse taustalla olevaa pilvi-infrastruktuuria, kuten verkkoa, palvelimia, käyttöjärjestelmiä tai tallennustilaa. Mutta käyttäjä hallitsee sen sijaan julkaistuja sovelluksia ja mahdollisia isäntäympäristön kokoonpanoasetuksia. (Mell & Grance 2011: 2-3.)

2.2.3 Infrastruktuuri palveluna, IaaS (Infrastructure as a service)

Palveluntarjoaja tarjoaa asiakkaalle virtuaalista palvelinkeskusta, jonka kautta käyttäjä voi itse perustaa tarvitsemansa infrastruktuurin. Käyttäjä ei hallitse taustalla olevaa pilvi-infrastruktuuria, mutta hallitsee käyttöjärjestelmiä, tallennustilaa, käytettyjä sovelluksia ja mahdollisesti myös rajoitettuja valvontatoimintoja tietyissä verkko-osissa, kuten palomuureissa (Mell & Grance 2011: 3).

IaaS-pilvimalli tarjoaa kustannustehokkaan ratkaisun infrastruktuurin uudistumiseen ja kehittämiseen myymällä palveluntarjoajan laitteiston resurssit käyttäjän käyttöön. IaaS-palvelumalleissa 70 % IT-investoinneista menee VMwaren mukaan olemassa olevan infrastruktuurin ylläpitoon. Palveluntarjoajan resurssit on virtualisoitu, jonka lisäksi skaalautuminen ja ylläpito on automatisoitu. (Salo 2012: 22-23.)

2.2.4 Muita palvelumalleja

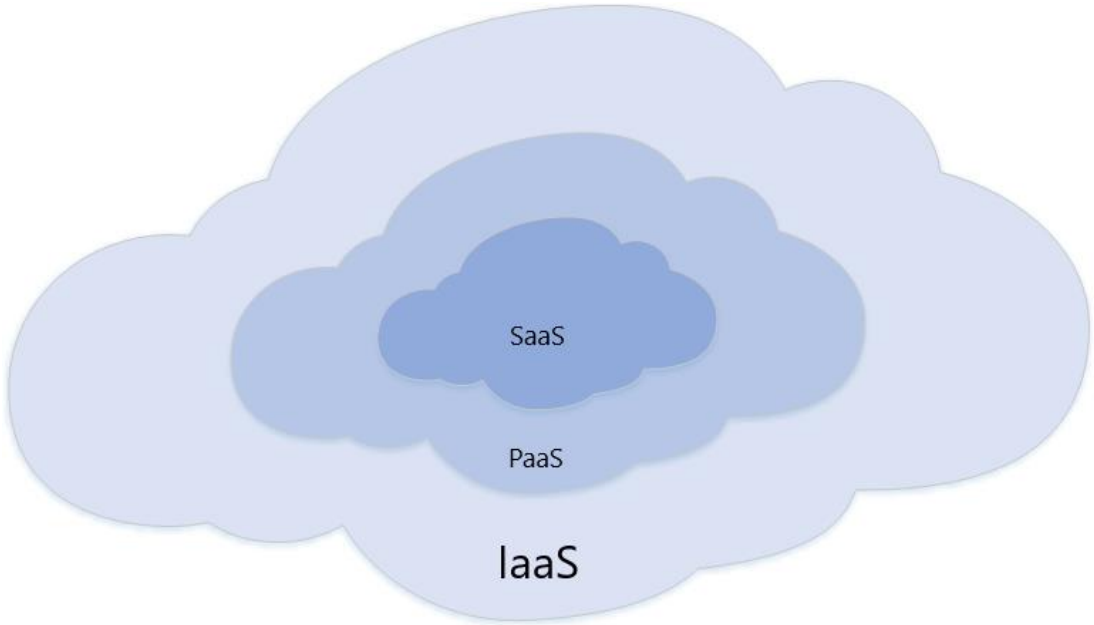
Yleisten palvelumallien pohjalta markkinoille on syntynyt palvelumalleja, jotka ovat erikoistuneet tuottamaan tietynlaisia palveluita. Yksi näistä malleista on tietoturva palveluna, SECaaS (Security as a Service).

SECaaS on toimintamalli, jossa palveluntarjoaja integroi oman tietoturvapalvelunsa osaksi yrityksen infrastruktuuria. Tällaiseen palveluun sisältyy muun muassa yritystoiminnan jatkumisen takaaminen ja palauttaminen (Business Continuity and Disaster Recovery), jatkuva järjestelmävalvonta (Continuous Monitoring), identiteetinhallinta eli käyttäjätietokannan ja todennuksen hallinta (Identity and Access Management) sekä tunkeutumisen havaitseminen (Intrusion Management). (Cloud Security Alliance 2016: 5-6.)

SECaasS toimii SaaS-, PaaS- sekä SaaS-tasolla. SaaS-tasolla SECaaS suojaa käyttäjän tietoja ja palveluntarjoajan sovellusta. PaaS-tasolla pilvimalli tarjoaa suojaa käyttäjän sovelluksille ja palveluntarjoajan sovellusalustalle. IaaS-tasolla palvelu suojaa käyttäjän virtuaalikoneita ja palveluntarjoajan omaa infrastruktuuria. (Hussain & Abdulsalam 2011: 2.)

2.2.5 Palvelumallien arkkitehtuuri

Helpoin tapa lähestyä palvelumallien arkkitehtuuria on, että niiden kuvitellaan kasaantuvan kerroksittain toistensa päälle. Alimmaisena kerroksena on IaaS, sillä sen tietotekniikkaresurssit antavat perustan muille palvelumalleille. Keskimmäinen kerros on PaaS, joka antaa välineet muun muassa IaaS-resurssien hyödyntämiseen, kuten sovelluskehitykseen. Päällimmäisin kerros on loppukäyttäjien näkemä sovelluskerros, SaaS.



Kuva 2. Palvelumallien arkkitehtuuri

2.3 Pilvimallit

2.3.1 Yksityinen pilvi

Pilvi-infrastruktuuri on suunnattu yksittäiselle organisaatiolle, jossa palveluntarjoajan tietotekniikkaresurssit ovat vain yhden organisaation käytössä. Organisaatio omistaa pilvi-infrastruktuurin, jota se voi hallinnoida ja operoida itse. Yksityisen pilvimallin osa-alueet voidaan ulkoistaa kokonaan tai osittain, jolloin toimija vain omistaa pilvi-infrastruktuurin. Yksityinen pilvimalli voi sijaita organisaation omissa tiloissa tai ulkopuolisen tiloissa. (Mell & Grance 2011: 3.)

Yksityinen pilvimalli perustuu yksikäyttäjyyteen, jossa palveluntarjoajan tietotekniikkaresurssit ovat yhden toimijan käytettävissä. Pilvimallin etuna ovat rajattoman kontrolloinnin mahdollisuus ja resurssien muuttaminen. Haittapuolina ovat nopean joustavuuden, resurssien yhteiskäytön sekä käytön mukaan maksamisen menettäminen. (Kavis 2014: 20.)

2.3.2 Julkinen pilvi

Pilvi-infrastruktuuri on avoin kaikille; yritykset, akateemiset laitokset tai julkishallinto voivat omistaa ja hallinnoida pilvi-infrastruktuuria. Palvelu sijaitsee ainoastaan palveluntarjoajan omissa tiloissa. (Mell & Grance 2011: 3.)

Julkinen pilvimalli perustuu monikäyttäjyyteen, jossa loppukäyttäjä maksaa käyttämistään resursseista jaetussa ympäristössä. Loppukäyttäjällä ei ole tarkkaa tietoa käyttämänsä ohjelman maantieteellisestä sijainnista. Pilvimallin etuina ovat käyttökustannukset ja skaalautuvuus; palveluista maksetaan käytön mukaan ja palveluun voidaan liittää ja ottaa pois ominaisuuksia tarpeen mukaan. Pilvimallin haittapuolina ovat hallinnan puute, sääntelykysymykset sekä rajallinen määrä määritelmien muuttamista. (Kavis 2014: 18-20.)

2.3.3 Yhteisöpilvi

Pilvi-infrastruktuuri on jaettu usean toimijan kesken, ja sen tarkoituksena on palvella yhteisöä, joilla on yhteisiä käytäntöjä, vaatimuksia sekä tarpeita. Esimerkiksi julkishallinto voisi hyödyntää yhteisöpilveä. Organisaatio voi omistaa, hallinnoida sekä operoida pilvi-infrastruktuuria itse, mutta tarpeen mukaan se voidaan myös ulkoistaa kolmannelle osapuolelle joko kokonaan tai osittain. Palvelu voi sijaita organisaation omissa tiloissa tai kolmannen osapuolen tiloissa. (Mell & Grance 2011: 3.)

2.3.4 Hybridipilvi

Pilvi-infrastruktuuri koostuu kahdesta tai useammasta eri pilvimallin yhdistelmästä, jossa pilvimallit toimivat omilla käyttötarkoituksillaan, mutta ovat teknisesti toisiinsa sidottuina. (Mell & Grance 2011: 3.) Käytännössä tämä tarkoittaa esimerkiksi sitä, että yrityksellä

on oma yksityinen pilvi, jossa on yritykselle tärkeimmät ja tarkinta tietoturvaa vaativat järjestelmät. Tämän lisäksi yrityksellä on julkisen pilven kautta tallennuskapasiteettia.

2.3.5 Muut pilvimallit

Intercloud

Intercloud on malli, jossa yksittäiset pilvet sulautuvat yhdeksi suureksi saumattomaksi pilveksi eli niin kutsutuksi pilvien pilveksi. Yksittäinen pilvi voisi tarpeen vaatiessa käyttää toisen pilven resursseja, jotka olisivat muuten tavoittamattomissa. Termin intercloud esitti vuonna 2007 Wired-lehden toimittaja Kevin Kelly. (Heino 2010: 56-57.)

Multicloud

Multicloudissa käytetään useampaa samanlaista pilvimallia eri palveluntarjoajalta, kuten kahta tai useampaa yksityistä pilveä. Multicloud eroaa hybridipilvestä siinä, että multicloudissa on useampi samanlainen pilvi eri palveluntarjoajalta. (Redhat n.d.)

Kuva 3. Pilvipalveluiden kokonaisuus

3 Pilvipalveluiden tietoturva

Cloud Security Alliance (CSA) on maailman johtava organisaatio, jonka tarkoituksena on määritellä ja lisätä tietoisuutta parhaista käytännöistä varmistaakseen turvallisen pilvipalveluympäristön. (Cloud Security Alliance n.d.) CSA on listannut pilvipalveluiden 12 suurinta tietoturvauhkaa ja suosituksia niiden välttämiseksi.

3.1 Tietovuodot

Tietovuodot ovat tapauksia, joissa arkaluontoista, salattua tai salassa pidettävää tietoa julkaistaan, varastetaan tai käytetään luvattomasti. Tietovuoto voi olla verkkohyökkäyksen pääasiallinen kohde, tai se voi johtua inhimillisestä erehdyksestä, sovelluksen haavoittuvuudesta tai huonoista tietoturvakäytännöistä. Tietovuodot sisältävät sellaista tietoa, jota ei ole tarkoitettu julkisuuteen, kuten yksityishenkilön terveystiedot tai yrityksen liikesalaisuudet. (Cloud Security Alliance 2016: 8.)

Pilvessä oleva data kiinnostaa eri osapuolia eri syistä. Esimerkiksi rikollisjärjestöt etsivät usein taloudellisia tietoja, terveys- tai henkilötietoja, jotta he voivat suorittaa petoksia, kun taas aktivistit haluavat paljastaa tietoja, jotka voivat aiheuttaa vahinkoa tai häpeää. Palveluntarjoajilla on usein hyvä tietoturva ympäristössään, josta he ovat vastuussa, mutta viime kädessä käyttäjät ovat itse vastuussa tietojensa suojaamisessa pilvipalveluissa. Paras suojaus tietovuotoja vastaan on tehokas tietoturvaohjelma, jonka lisäksi monitasoinen todentaminen (multi-factor authentication) sekä tietojensalaus (encryption) ennaltaehkäisevät tietovuotoja. (Cloud Security Alliance 2016: 8-9.)

3.2 Identiteetinhallinta

Identiteetinhallinnalla tarkoitetaan käyttäjätietokannan, tunnistetietojen ja todennuksen hallintaa. Tietovuodot ja tietohyökkäykset voivat johtua skaalautuvan identiteetinhallintajärjestelmän puutteesta, monitasoisen todentamisen käytön puutteesta, heikon salasanan käytöstä tai automaattisen salausavainten, salasanojen ja varmenteiden kierrättämisen puutteesta. (Cloud Security Alliance 2016: 11.)

Tunnistetietoja tai salausavaimia ei saa sisällyttää lähdekoodiin tai jakaa julkiseen tietolähteeseen (repository), kuten GitHubiin, koska mahdollisuus näiden löytymiselle ja väärinkäyttämiselle on olemassa. Salausavainten on oltava asianmukaisesti turvattu sekä julkisten avainten hallintajärjestelmä (PKI) tulee olla läsnä varmistamassa asianmukainen toiminta. (Cloud Security Alliance 2016: 11.)

Identiteetinhallintajärjestelmät ovat yhä useammin yhteydessä toisiinsa. Identiteetin yhdistäminen pilvipalvelutarjoajan kanssa ovat yleistymässä entisestään käyttäjähallinnan taakan keventämiseksi. Palveluntarjoajalta ja käyttäjältä vaaditaan monitasoisia todentamisjärjestelmiä, kuten älykortti, kertakäyttöinen salasana (OTP) ja puhelintodentaminen. Tämän kaltaiset todentamistavat ennaltaehkäisevät salasanavarkauksia ja estävät palvelujen luvattoman käytön. Vanhemmissa järjestelmissä tulee turvakäytännöissä huolehtia salasanan vahvuudesta ja riittävän tiheästä salasanan vaihtovälistä. (Cloud Security Alliance 2016: 11.)

Salausavaimet, mukaan lukien TLS-varmenteet, tietojen suojaamiseen käytettävät avaimet sekä salasanojen suojaamiseen käytettävät avaimet on kierrätettävä määräajoin. Kierrättämällä edellä mainittuja avaimia voidaan puuttua avainten luvattomaan käyttöön. Kierron puuttuminen voi merkittävästi kasvattaa hyökkäyksen vakavuutta ja sen kestoa, jos hyökkääjällä on salausavain. (Cloud Security Alliance 2016: 11.)

Jokainen keskitetty tallennusmekanismi, joka sisältää tietosalaisuuksia, kuten salasanat ja yksityiset avaimet, on erittäin arvokas kohde hyökkääjille. Salasanojen ja avainten keskittäminen on kompromissi, jota jokaisen organisaation on mietittävä. (Cloud Security Alliance 2016: 11-12.)

3.3 Suojaamattomat käyttöliittymät ja rajapinnat

Pilvipalveluiden tarjoajat paljastavat osan ohjelmiston käyttöliittymästä (UI) tai ohjelmointirajapinnasta (API), joita käyttäjät käyttävät vuorovaikutuksessa pilvipalveluiden kanssa. Näiden avulla voidaan esimerkiksi hallita ja valvoa pilvipalveluita. Yleisten pilvipalveluiden ominaisuuksien turvallisuus ja saatavuus ovat riippuvaisia näiden rajapintojen turvallisuudesta. Rajapinnat on suunniteltava suojamaan sekä vahingollisilta että haitallisilta pyrkimyksiltä kiertää turvakäytäntöjä. Organisaatiot sekä kolmannet osapuolet voi-

vat kehittää rajapintoja hyväksi käyttäen lisäarvoa tuovia palveluja. Tämä voi lisätä tietoturvariskiä, sillä organisaatio voi joutua luovuttamaan käyttäjätunnuksiaan kolmansille osapuolille. (Cloud Security Alliance 2016: 14.)

Ohjelmointirajapinnat ja käyttöliittymät ovat yleisesti kaikista avoin osa järjestelmästä, sillä ne ovat kenties ainoa osa järjestelmästä, jossa IP-osoite on luotettavan organisaation ulkopuolella. Nämä osat ovat sen takia alttiita raskaille hyökkäyksille, jolloin niihin tulee kohdentaa riittävää valvontaa ja suojausta. (Cloud Security Alliance 2016: 14.)

3.4 Järjestelmän haavoittuvuudet

Järjestelmän haavoittuvuudet ovat hyödynnettäviä ohjelmointivirheitä, joita hyökkääjä voi käyttää tunkeutuessaan tietokonejärjestelmään tietojen varastamista, järjestelmän hallinnoimista tai palvelutoimintojen häiritsemistä varten. Käyttöjärjestelmän komponenttien, kuten ytimen, järjestelmäkirjastojen ja sovellustyökalujen, haavoittuvuudet asettavat kaikki palvelut ja tiedot huomattavaan riskiin. Tällainen uhka ei ole uusi, mutta pilvipalvelujen monikäyttäjyyden seurauksena hyökkääjillä on uusi hyökkäyspinta, jota he voivat käyttää. (Cloud Security Alliance 2016: 16.)

Säännöllisillä haavoittuvuustarkistuksilla, järjestelmäuhkien raportoinnilla ja tietoturvapäivityksien asentamisella voidaan sulkea haavoittuvuuden luomia tietoturva-aukkoja. Hyökkääjän mahdollisuutta ottaa koko tietojärjestelmä haltuun voidaan rajoittaa käyttäjien käyttöoikeuksilla. (Cloud Security Alliance 2016: 16)

3.5 Käyttäjätilien ja palvelujen kaappaaminen

Hyökkäysmetodit, kuten tietojenkalastelu, erilaiset petokset ja ohjelmien haavoittuvuuksien hyödyntäminen tuottavat edelleen tulosta. Samoja käyttäjätunnuksia ja salasanoja käytetään usein, mikä vahvistaa edellä mainittujen hyökkäyksien vakavuutta. Pilvipalvelut tuovat esiin uuden uhan. Jos hyökkääjä saa kaapattua käyttäjätunnukset, hän voi niiden avulla tarkkailla kyseisen käyttäjän toimintaa, manipuloida dataa, antaa käyttäjälle väärennettyä tietoa tai jopa ohjata käyttäjän väärennetyille verkkosivuille. Kaapatusta tilistä tai palvelusta voi tulla hyökkääjän toiminnan perusta. (Cloud Security Alliance 2016: 18.)

Organisaatioiden tulisi välttää käyttäjätunnuksien jakamista käyttäjien ja palveluiden kesken ja hyödyntää mahdollisuuksien mukaan kaksivaiheista todennusta. Kaikkia tilejä ja tilitapahtumia on pystyttävä valvomaan ja jäljittämään tilinomistaja. (Cloud Security Alliance 2016: 18.)

3.6 Sisäpiirin uhka

Sisäpiirin uhan voi aiheuttaa joku organisaation entinen tai nykyinen työntekijä, urakoitsija tai muu liikekumppani, jolla on ollut pääsy organisaation verkkoon, järjestelmään tai tietoihin. Tällainen henkilö saattaa tai on saattanut väärinkäyttää pääsyä järjestelmään, mikä voi vaikuttaa kielteisesti luottamuksellisuuteen, eheyteen tai organisaation tietojen ja tietojärjestelmien saatavuuteen. (Cloud Security Alliance 2016: 20.)

Sisäpiirin uhkaa voidaan rajoittaa muun muassa valvomalla salausprosessia ja avaimia itse, minimoimalla pääsyä järjestelmiin rooleilla, tehokkaalla lokituksella (logging) ja ylläpitäjien toimien seurannalla. (Cloud Security Alliance 2016: 20.)

3.7 Kehittyneet pysyvät uhat

Kehittyneet pysyvät uhat (Advanced persistent threats, APT) ovat loismaisia tietoturvahyökkäyksiä, jotka tunkeutuvat hyökkäyksen kohteen järjestelmään, josta ne pyrkivät saamaan jalansijan. APT:t pyrkivät salaa viemään yrityksen tietoja ja aineetonta omaisuutta. APT:t pyrkivät tavoitteeseensa huomaamattomasti pitkällä aikavälillä ja ne mukautuvat usein niitä vastaan asetettuihin turvatoimiin. (Cloud Security Alliance 2016: 22.)

Tietojenkalastelu, suorat hakkerointijärjestelmät, hyökkäyskoodin toimittaminen USB-laitteiden kautta, kumppaniverkostojen kautta tunkeutuminen sekä turvattomien verkkojen käyttäminen ovat menetelmiä, joilla APT:t pääsevät leviämään. Kun APT:t ovat päässeet järjestelmään sisälle, pystyvät ne leviämään järjestelmän sisällä tavallisen verkkoliikenteen seassa saavuttaakseen tavoitteensa. (Cloud Security Alliance 2016: 22.)

Tällainen uhka voidaan ennaltaehkäistä esimerkiksi tiedottamalla ja kouluttamalla käyttäjiä tunnistamaan ja toimimaan haavoittuvuuksia vastaan, sillä monet näistä haavoittuvuuksista edellyttävät käyttäjän toimia. Käyttäjiä tulisi ohjeistaa harkitsemaan kahdesti ennen liitteen avaamista tai linkin painamista. (Cloud Security Alliance 2016: 22.)

3.8 Tietojen pysyvä häviäminen

Pilvipalveluun tallennettu tieto voi hävitä muistakin syistä kuin tietohyökkäyksen seurauksena. Pilvipalveluntarjoajan vahingossa tapahtuva poisto tai pahempi fyysinen katastrofi, kuten tulipalo tai maanjäristys, voi aiheuttaa asiakastiedon pysyvän menetyksen. Palveluntarjoajan tai käyttäjän tulee ryhtyä riittäviin toimenpiteisiin, kuten varmuuskopioimaan tietoja ja noudattamaan yritystoiminnan jatkumisen takaamisen ja palauttamisen (Business continuity and disaster recovery) -mallia. Pilvipalveluntarjoaja ei ole vastuussa tietojen häviämisestä, jos käyttäjä salaa tietonsa ennen pilvipalveluun siirtoa ja hävittää salausavaimen. Käyttäjän tulisi tutustua pilvipalveluntarjoajan käyttöehtoihin ja -sopimukseen. (Cloud Security Alliance 2016: 24.)

3.9 Asianmukaisen huolellisuuden laiminlyönti

Organisaatio, joka pyrkii omaksumaan pilviteknologioita tekemättä huolellista taustatutkimusta pilvipalveluidentarjoajista, altistaa itsensä lukemattomiin kaupallisiin-, taloudellisiin-, teknillisiin-, laillisiin- ja yhteensopivuusriskeihin, jotka vaarantavat menestysmahdollisuudet (insufficient due diligence.) Esimerkiksi organisaation käytössä olevan sovelluksen siirtäminen pilvipalveluun, joka on ollut riippuvainen organisaation sisäisestä tietosuojatasosta, on vaarallinen, kun sitä hallinnoivat toiminnot häviävät. Hyvän etenemissuunnitelman ja muistilistan huolellinen suunnitteleminen on välttämätön onnistumisen kannalta. Tämä koskee niin pilveen siirtyvää kuin jo pilvessä olevaa organisaatiota. (Cloud Security Alliance 2016: 26-27.)

3.10 Pilvipalveluiden väärinkäyttö

Huonosti suojatut pilvipalvelut, ilmaiset kokeilujaksot ja vilpilliset rekisteröitymiset maksupetoksien avulla altistavat pilvipalvelut haitalliselle toiminnalle. Haitalliset toimijat voivat hyödyntää pilvipalveluiden resursseja suunnatakseen hyökkäyksensä käyttäjiä, organisaatioita tai muita pilvipalveluntarjoajia vastaan. Palvelunestohyökkäykset (Distributed Denial of Service), roskapostien lähettäminen ja tietojenkalastelu ovat esimerkkejä pilvipalveluiden väärinkäytöstä. (Cloud Security Alliance 2016: 29.)

Palveluntarjoajan tulee tunnistaa maksutapahtumapetokset ja pilvipalvelujen väärinkäyttö, mukaan lukien lähtevät ja saapuvat palvelunestohyökkäykset, jotta palveluiden väärinkäyttöä voidaan hillitä. Palveluntarjoajalla on oltava tapauskohtaiset toimintamallit resurssien väärinkäytön käsittelemiseksi sekä keino, jolla käyttäjät voivat ilmoittaa palveluntarjoajalta peräisin olevista väärinkäytöksistä. (Cloud Security Alliance 2016: 29.)

3.11 Palvelunestohyökkäykset

Palvelunestohyökkäyksien tarkoituksena on estää palvelunkäyttäjien pääsy omaan dataan ja sovelluksiin. Palvelunestohyökkäyksessä hyökkäyksen kohteena olevan palveluntarjoajan rajallisia järjestelmäresursseja, kuten prosessorin tehoa, muistia, levytilaa tai verkon kaistanleveyttä, kuormitetaan, jolloin tämä aiheuttaa järjestelmänhidastumisen ja jättävät palvelunkäyttäjät ihmettelemään, miksi palvelu on hidas eikä vastaa. (Cloud Security Alliance 2016: 31.)

3.12 Jaetun teknologian ongelmat

Pilvipalvelujentarjoajien käyttämien palvelinten komponenttien infrastruktuuria, kuten prosessorien välimuistia tai näytönohjaimia, ei ole kuitenkaan suunniteltu niin, että se tarjoaisi vahvoja eristysominaisuuksia. Tämä voi johtaa jaetun teknologian ongelmiin, joita voidaan mahdollisesti hyväksikäyttää jokaisessa palvelumallissa. Tältä suojautumiseksi vaaditaan tarkkaa tietoturvastrategiaa, jossa huomioidaan muun muassa prosessointi, käyttäjien ja sovellusten toimien seuranta sekä tietoverkot. Tärkeintä on huomioida, että yksittäinen haavoittuvuus tai virheellinen määritys voi johtaa koko pilvipalvelun kompromissiin. Palveluntarjoaja voi ennaltaehkäistä jaetun teknologian tietomurtoja käyttämällä monitasoista tunnistautumista jokaisella isäntäkoneella, isäntäpohjaista tunkeilijan havaitsemisjärjestelmää (HIDS) sekä verkkopohjaista tunkeilijan havaitsemisjärjestelmää (NIDS). (Cloud Security Alliance 2016: 33.)

4 Tietosuojalainsäädäntö

Vuonna 2018 voimaan tuleva Euroopan unionin laajuinen tietosuojalainsäädäntö GDPR (General Data Protection Regulation) yhdenmukaistaa tietosuojalainsäädäntöä EU:n alueella. Tietosuojalainsäädännön tavoitteena on suojella jokaista EU:n kansalaista tietovuodoilta ja -murroilta sekä vahvistaa kansalaisten yksityisyyttä. Jokainen EU -alueella toimiva yritys, joka käsittelee henkilötietoja, joutuu noudattamaan uutta lainsäädäntöä. Jokaisesta rikkomuksesta sakotetaan; suurin mahdollinen sakko on 4 % vuotuisesta liikevaihdosta tai 20 miljoonaa euroa riippuen siitä, kumpi niistä on suurempi. Uusi tietosuojalainsäädäntö vaatii yrityksiä yksinkertaistamaan käyttöoikeusehtoja ymmärrettävämpään muotoon. (EUGDPR n.d.)

Tietosuojavaltuutetun toimisto (2016) on tiivistänyt lainsäädännön tärkeimmät asiat seuraavasti:

• Oikeus tulla unohdetuksi: Kun käyttäjä ei enää halua, että hänen tietojaan käsitellään, tiedot poistetaan, paitsi jos on olemassa jokin laillinen peruste säilyttää ne. Tarkoitus on taata kansalaisten yksityisyydensuoja, ei hävittää menneitä tapahtumia tai rajoittaa lehdistönvapautta.

• Tiedonsaanti helpottuu: Ihmiset saavat tietoa siitä, miten heidän tietojaan käsitellään, ja tämä tieto on annettava heille selkeällä ja ymmärrettävällä tavalla. Oikeus siirtää omat tietonsa tietojärjestelmästä toiseen helpottaa henkilötietojen siirtämistä palveluntarjoajalta toiselle.

• Oikeus saada tieto tietoturvaloukkauksesta: Yritysten ja organisaatioiden on raportoitava kansalliselle tietosuojaviranomaiselle tietoturvaloukkauksista. Käyttäjille on ilmoitettava vakavista loukkauksista mahdollisimman pian, jotta nämä voivat ryhtyä tarvittaviin toimiin.

• Sisäänrakennettu ja oletusarvoinen tietosuoja: Tietosuojatakeet otetaan huomioon tuotteissa ja palveluissa jo suunnitteluvaiheessa, ja yksityisyydensuojaa edistävät oletusarvot (asetukset) ovat automaattisesti käytössä esimerkiksi sosiaalisessa mediassa ja mobiilisovelluksissa.

• Tiukemmat seuraukset rikkomuksista: tietosuojaviranomaiset voivat antaa EU-sääntöjä rikkovalle yritykselle sakon, joka on jopa neljä prosenttia yhtiön maailmanlaajuisesta liikevaihdosta. (Tietosuojavaltuutetun toimisto 2016.)

5 Virtuaalikone pilvipalvelussa

5.1 Amazon Web Services (AWS)

Amazon Web Services (AWS) on Amazonin pilvipalvelu, jota Amazon on tarjonnut yrityksille jo vuodesta 2006 alkaen. Amazonin AWS:n valikoimassa on monipuolisesti erilaisia valmiita pilvipalveluita erilaisiin tarkoituksiin kustannustehokkaasti, joustavasti ja turvallisesti. (Amazon About AWS n.d.)

Amazon Elastic Compute Cloud (Amazon EC2) on Amazonin pilvipalvelussa oleva verkkopalvelu, joka tarjoaa turvallista ja muokattavaa laskentakapasiteettia (compute capacity). Amazon EC2:n yksinkertainen käyttöliittymä mahdollistaa kapasiteetin hankkimisen ja määrittämisen vaivattomasti ja antaa täydellisen hallinnan tietotekniikkaresursseihin. Amazon EC2 lyhentää aikaa, joka kuluu uusien palvelimien käyttöönotossa. Tietotekniikkaresursseja voidaan skaalata tarpeiden mukaan. Amazon EC2:ssa maksetaan vain käytettävän kapasiteetin määrästä. Palvelu on yhteensopiva muiden Amazonin tuotteiden kanssa. Amazon EC2 -palvelua käyttävät muun muassa Netflix, NASA/JPL sekä Airbnb. (Amazon EC2 n.d.)

Amazon Simple Storage Solution (Amazon S3) on Amazonin pilvipalvelussa oleva skaalautuva tallennuspalvelu, joka tarjoaa käyttäjilleen rajattomasti tallennustilaa. Amazon S3:lla on yksinkertainen käyttöliittymä, jonka avulla voidaan tallentaa tai hakea dataa rajattomasti mistä ja milloin tahansa. Amazon S3 tarjoaa kattavat turvallisuus- ja yhteensopivuusominaisuudet, jotka täyttävät jopa tiukimmat sääntelyvaatimukset sekä sisältää laajan kyselyominaisuuden (query), jolla voidaan analysoida tallennettu dataa. Amazon S3:sta maksetaan käyttäjän datan määrän mukaan. Palvelu on yhteensopiva muiden Amazonin tuotteiden kanssa. Amazon S3 -palvelua käyttävät muun muassa Netflix, Airbnb sekä Thomson Reuters. (Amazon S3 n.d.)

5.2 Virtuaalikoneen siirtäminen pilvipalveluun

5.2.1 Yleisesti

Insinöörityön käytännönosuudessa luodaan virtuaalikone käyttäen VMwaren virtualisointialustaa ja siirretään luotu virtuaalikone Amazon Web Service -palveluun Amazon

Machine Image (AMI) -levykuvaksi. AMI-levykuvaa voidaan hyödyntää uusien instanssien luomisessa EC2-palvelussa. Virtuaalikoneen siirto toteutetaan cold migration -siirtotavalla, jossa siirrettävä virtuaalikone on sammutettuna. Cold migration -siirtotavassa virtuaalikoneen sisältämät palvelut ovat poissa käytöstä siirron ajan. Siirrossa käytetään apuna Amazonin AWS Import/Export -työkalua. Käytännönosuuden tukena on käytetty Amazon AWS:n VM Import/Export User Guide-, AWS Command Line Interface User Guide-, Amazon Simple Storage Service Developer Guide-, Amazon Web Services General Reference -käyttöoppaita.

Käytännönosuudessa asennettava virtualisointisovellus VMware Workstation 14 sekä käyttöjärjestelmä Microsoft Windows Server 2016 ladataan Metropolia Ammattikorkeakoulun Microsoft- ja VMware-storesta. Virtuaalikoneelle asennettava käyttöjärjestelmä asennetaan perusasetuksin. Käyttöjärjestelmän asennuksen aikana luodun käyttäjätilin nimi ja salasana pitää pitää tallessa, sillä niitä tarvitaan myöhemmin tämän työn aikana.

5.2.2 Siirron alkutoimenpiteet

Ennen siirtoa käyttäjän tulee rekisteröityä Amazonin AWS -palveluun (https://aws.amazon.com/), luoda käyttäjätili ja antaa käyttäjätilille riittävät käyttöoikeudet, luoda käyttäjäntilin pääsyavaimet (Access Key ID) ja IAM Service Role, luoda Amazon S3 -palveluun bucket sekä asentaa siirron mahdollistavat sovellukset.

Amazonin AWS -palveluun rekisteröityminen on yksinkertaista; se vaatii sähköpostiosoitteen, salasanan ja käyttäjänimen. Tilin tyypiksi voi valita työ- tai yrityskäyttöön tarkoitetun *Professional*-version tai henkilökohtaiseen käyttöön tarkoitetun *Personal*-version. Rekisteröitymiseen vaaditaan luottokortin tiedot. Tämän jälkeen Amazon suorittaa puhelinvarmistuksen, jolla varmistetaan annettujen tietojen paikkansapitävyys. Amazonin AWS palvelu soittaa annettuun puhelinnumeroon ja pyytää syöttämään verkkoselaimeen ilmestyneen nelinumeroisen koodin puhelimeen. Viimeisessä vaiheessa valitaan haluttu AWS tukipalvelujen palvelutaso. Palvelutasoja ovat *Basic plan, Developer plan, Business plan* sekä *Enterprise level support.* Palvelutasoista *Basic plan* on ilmainen, joka sisältyy automaattisesti kaikkiin tileihin.

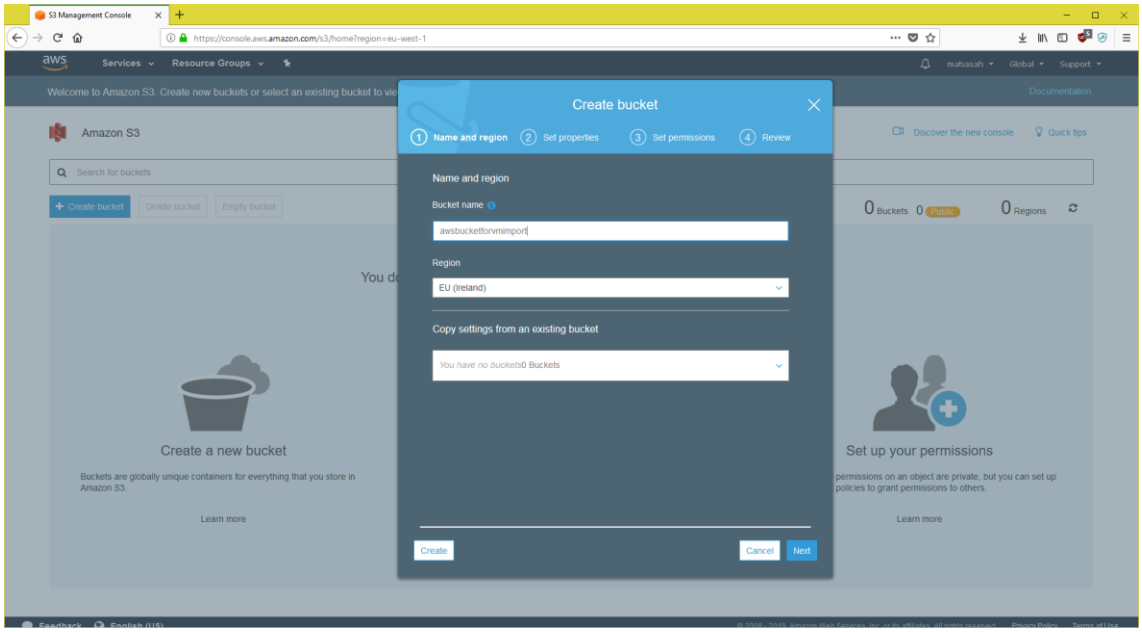
Rekisteröitymisen jälkeen käyttäjätilille luodaan uusi käyttäjä, jolle annetaan riittävät oikeudet suorittaa virtuaalikoneen siirtäminen. Sisäänkirjautumisen jälkeen päänäkymän

ylälaidassa on Services-vetovalikko, josta valitaan IAM. Aukeavan verkkosivun vasemmasta laidasta valitaan Users-välilehti ja painetaan Add User -painiketta. Annetaan uudelle käyttäjälle nimi ja annetaan käyttäjälle Programmatic access -pääsytyyppi. Tätä pääsytyyppiä tarvitaan, koska se mahdollistaa virtuaalikoneen siirtämisen AWS-palveluun. Tämä luo Access Key ID -pääsyavaimen, joka täytyy asettaa tietokoneelle, jolta virtuaalikone siirretään. Access Key ID -pääsyavaimen salasana kannattaa tallentaa turvalliseen paikkaan, sillä jos salasanan unohtaa tai hukkaa, niin sitä ei voi enää palauttaa. Tällöin joudutaan luomaan uusi Access Key ID Amazonin AWS konsolinäkymän IAM Users -sivulta.

Tätä työtä varten käyttäjätilille annetaan täydet oikeudet tehdä mitä vain, eli annetaan Amazonin valmiiksi luotu AdministratorAccess-rooli Attach existing policies directly -välilehden alta. Tätä roolia ei kannata antaa jokaiselle käyttäjälle, koska silloin käyttäjä pääsee tekemään muutoksia ilman muiden hyväksyntää. Käyttöoikeusrooleja, joilla voi rajata käyttäjätilien pääsyä eri palveluihin, voidaan luoda itse. Käyttäjätiliä voi tarkastella ennen sen luomista, jolloin tarvittavat muutokset voidaan tehdä, jos jotain on mennyt väärin. Käyttäjätilien asetuksia voidaan myös myöhemmin muuttaa.

S3 bucketteja käytetään objektien tallentamiseen, jotka sisältävät sekä dataa että metadataa. Bucketeilla on useita käyttötarkoituksia, sillä ne esimerkiksi tunnistavat käyttäjätilin, joka on vastuussa tallennus- ja tiedonsiirtomaksuista. (Amazon Simple Storage Service 2018: 3.) AWS S3 -palvelujen käyttäjien tulee luoda bucket ennen kuin he voivat tallentaa dataa Amazonin julkiseen pilveen. Bucketiin voidaan myös liittää käyttöoikeuksia.

S3 bucket luodaan Amazonin konsolinäkymässä. Avautuvalla hallintasivulla valitaan *Create bucket*, joka avaa ponnahdusikkunan. Avautuvassa ponnahdusikkunassa pyydetään bucketin nimeä, jonka tulee olla DNS-yhteensopiva, sekä maantieteellistä aluetta, mihin kyseinen bucket halutaan luoda. DNS-yhteensopiva nimi ei sisällä isoja kirjaimia eikä erikoismerkkejä. Tässä työssä bucketille on annettu nimi *awsbucketforvmimport*. Jos on aiemmin luonut bucketin, niin sen asetukset voidaan tuoda uudelle bucketille. Seuraavassa välilehdessä annetaan tarvittavat ominaisuudet, kuten versiointi, lokitustapa ja salausmuoto. Seuraavaksi asetetaan oikeuksia; mitä kukin saa tehdä tämän bucketin sisällön kanssa. Seuraavaksi hyväksytään valitut määritykset, minkä jälkeen bucket on luotu.



Kuva 4. S3 bucketin luominen Amazon AWS -palvelussa.

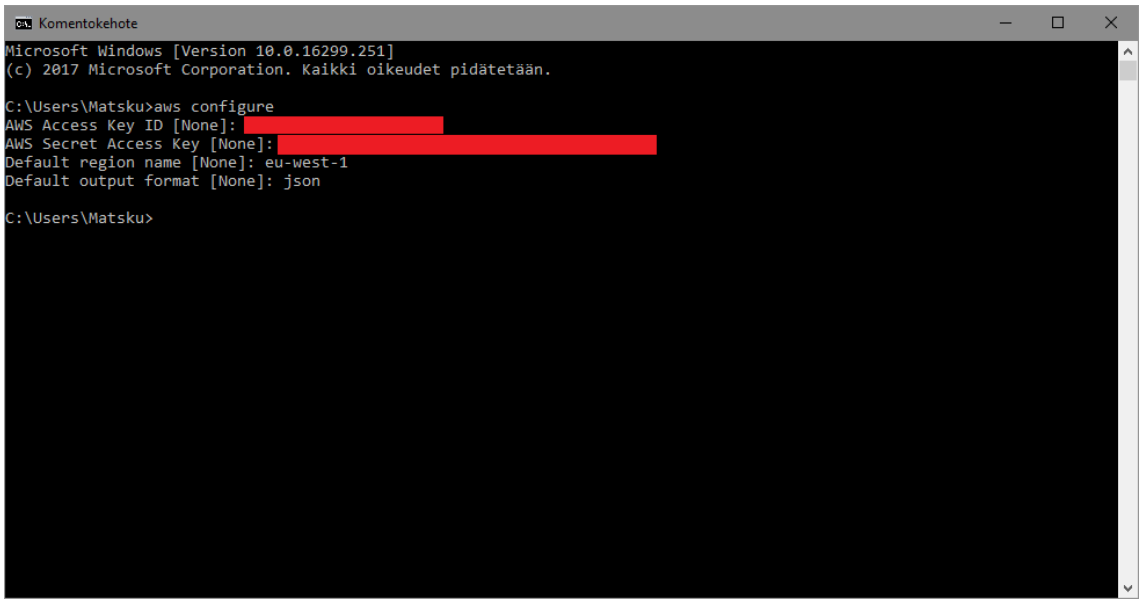
Virtuaalikoneen siirrossa käytetään apuna AWS Import/Export-työkalua, AWS CLI-käyttöliittymää, VMware Open Virtualization Format Tool 3.5.0 -sovellusta sekä Python-ohjelmointikieltä. AWS Import/Export -työkalu ei tue UEFI/EFI -muotoisia käyttöjärjestelmiä. Käyttöjärjestelmä tulee olla GPT-muodossa, jotta siirto on mahdollista AWS Import/Export -työkalun avulla. VMwaren Workstation 14 -virtualisointialustan oma Export-työkalu luo virtuaalikoneen ovf-tiedostomuotoon, mutta AWS AMI ei tue tätä muotoa. Tiedostomuoto tulee muuttaa ova -päätteiseksi, ja se onnistuu VMware Open Virtualization Format Tool 3.5.0 -sovelluksella, jonka voi ladata ja asentaa VMwaren verkkosivuilta. Sovelluksen lataaminen vaatii rekisteröitymisen, joka on ilmainen. Python asennetaan Pythonin kotisivuilta ja siitä löytyy eri versioita eri käyttöjärjestelmille. Python tulee asentaa tietokoneelle järjestelmänvalvojana ja asennusvaiheessa tulee valita PATH-vaihtoehto. Tämä varmistaa, että Python asentuu oikein eikä jatkossa tule ongelmia.

Kun Python on asennettu, asennetaan komentorivin kautta AWS CLI, joka mahdollistaa komentojen syöttämisen Amazonin AWS-palveluun omalta työasemalta. AWS CLI on komentorivipohjainen käyttöliittymä, jonka avulla pääsee käsiksi Amazonin AWS-palveluun. AWS CLI asennetaan seuraavilla komennoilla:

```
python --version
pip --version
pip install awscli
aws --version
```

From <https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-windows.html#awscli-install-windows-pip>

AWS CLI tulee konfiguroida käyttämään luodun käyttäjätilin Access Key ID:tä, joka löytyy Amazonin konsolinäkymästä. Avataan komentokehote ja annetaan komento *aws configure*. Tässä pyydetään Access Key ID -pääsyavaimen ID ja salasana. Regioniksi (maa-alue) tulee valita sama, johon S3 bucket on luotu. Default output -formaatiksi valitaan json.



Kuva 5. Access Key ID:n tiedot syötetään AWS CLI -konfiguraatioon.

Virtuaalikoneen siirtämiseksi S3 bucketista Amazonin EC2 -palveluun tarvitaan IAM Service Rolea. IAM Service Role on tässä työssä nimetty *vmimportiksi.* Tiedosto luodaan tekstieditorilla ja voidaan tallentaa mihin vain. Roolia varten luodaan trust-policy.json- ja role-policy.json-tiedostot. Seuraavisssa kuvissa esitetään näiden tiedostojen luominen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
            }
         }
      }
   ]
}
```

From <https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

Koodi 1. trust-policy.json

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::awsbucketforvmimport",
            "arn:aws:s3:::awsbucketforvmimport/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
         ],
         "Resource":"*"
      }
   ]
}
```

From <https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

Koodi 2. role-policy.json. *Awsbucketforvmimport* korvataan oman bucketin nimellä.

Json-tiedostojen luomisen jälkeen komentorivillä mennään kohdehakemistoon, jossa luodut json-tiedostot sijaitsevat. Annetaan seuraavat komennot:

```
aws iam create-role --role-name vmimport --assume-role-policy-document
file://trust-policy.json
```

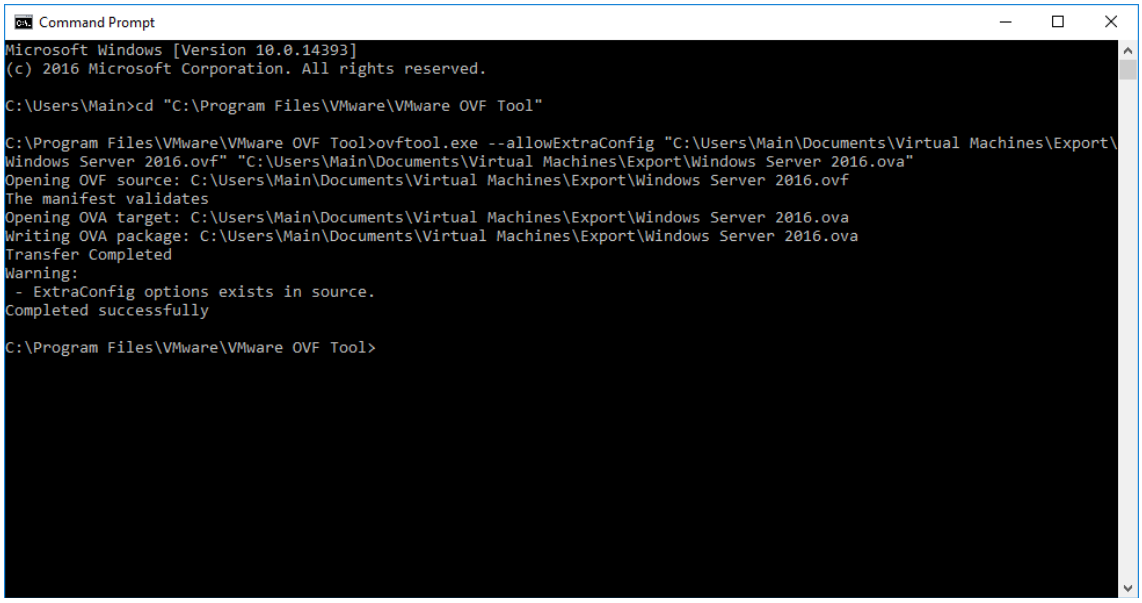
```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --
policy-document file://role-policy.json
```

5.2.3 Virtuaalikoneen siirtäminen

Alkutoimenpiteiden jälkeen virtuaalikone ja AWS ovat valmiina siirtoa varten. Virtualisointialustasta (VMware Workstation 14) varmistetaan, että siirrettävä virtuaalikone on sammutettu. Avataan siirrettävän virtuaalikoneen välilehti ja valitaan ylävalikosta *File -> Export to OVF*. Valitaan kohdekansio, johon virtuaalikoneen levykuva viedään. Tällä toiminnolla luodaan siirtoon tarvittava levykuva. Amazonin AWS Import/Export -työkalu ei kuitenkaan tue ovf -tiedostomuotoa, joten se täytyy muuttaa. Avataan komentokehote ja vaihdetaan hakemistoksi hakemisto, johon VMware OVF Tool on asennettu.

Seuraavalla komennolla muutetaan tiedostomuoto sellaiseksi, jonka Amazon AWS tunnistaa eli ova-päätteiseksi.

```
ovftool.exe --allowExtraConfig "C:\Users\Main\Documents\Virtual Machines\Ex-
port\Windows Server 2016.ovf" "C:\Users\Main\Documents\Virtual Machines\Ex-
port\Windows Server 2016.ova"
```



Kuva 6. Ovf -tiedoston muuntaminen ova -tiedostoksi VMware OVF Tool -sovelluksen avulla.

Seuraavaksi siirretään ova-päätteiseksi muutettu tiedosto S3 bucketiin seuraavilla komennoilla.

```
aws s3 ls
aws s3 cp "Windows Server 2016.ova" s3://awsbucketforvmimport/
aws s3 ls s3://awsbucketforvmimport/
```

Virtuaalikone tulee siirtää S3-palvelusta EC2-palveluun, jotta sitä voidaan käyttää. Tätä varten tulee luoda *containers.json*-tiedosto. Tiedoston voi tallentaa mihin vain.

```
{
    "Description": "Windows Server 2016",
    "Format": "ova",
    "UserBucket": {
        "S3Bucket": "awsbucketforvmimport",
        "S3Key": "Windows Server 2016.ova"
    }
}
```

Koodi 3. containers.json.

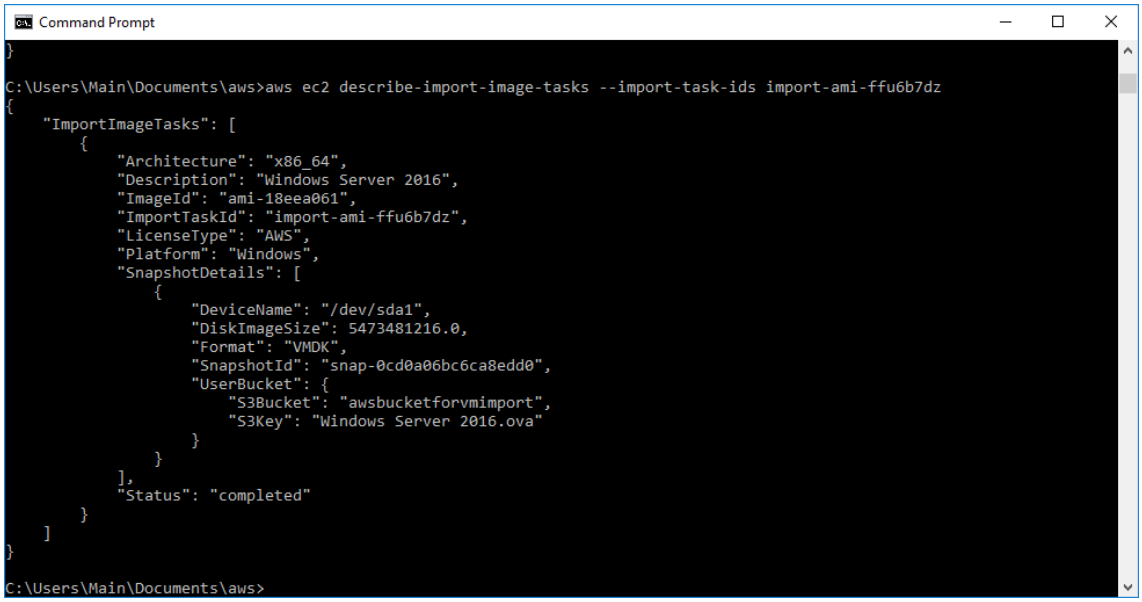
Siirto EC2-palveluun aloitetaan komennolla:

```
aws ec2 import-image --description "Windows Server 2016" --disk-containers
file://containers.json
```

Komento täytyy suorittaa samassa kansiossa, jossa *containers.json*-tiedosto sijaitsee. Komento luo siirrolle ID-numeron, joka tässä tapauksessa on *ffu6b7dz*. ID-numeron avulla siirron etenemistä voi seurata syöttämällä seuraava komento:

```
aws ec2 describe-import-image-tasks --import-task-ids import-ami-ffu6b7dz
```

Virtuaalikoneen siirto on onnistunut, kun yllä oleva komento antaa siirron tilaksi *completed.* Menemällä AWS konsolinäkymän verkkosivuille ja navigoimalla EC2:n Images-välilehden alla olevaan AMIs-kohtaan, tulisi siellä näkyä siirretyn virtuaalikoneen levykuva.

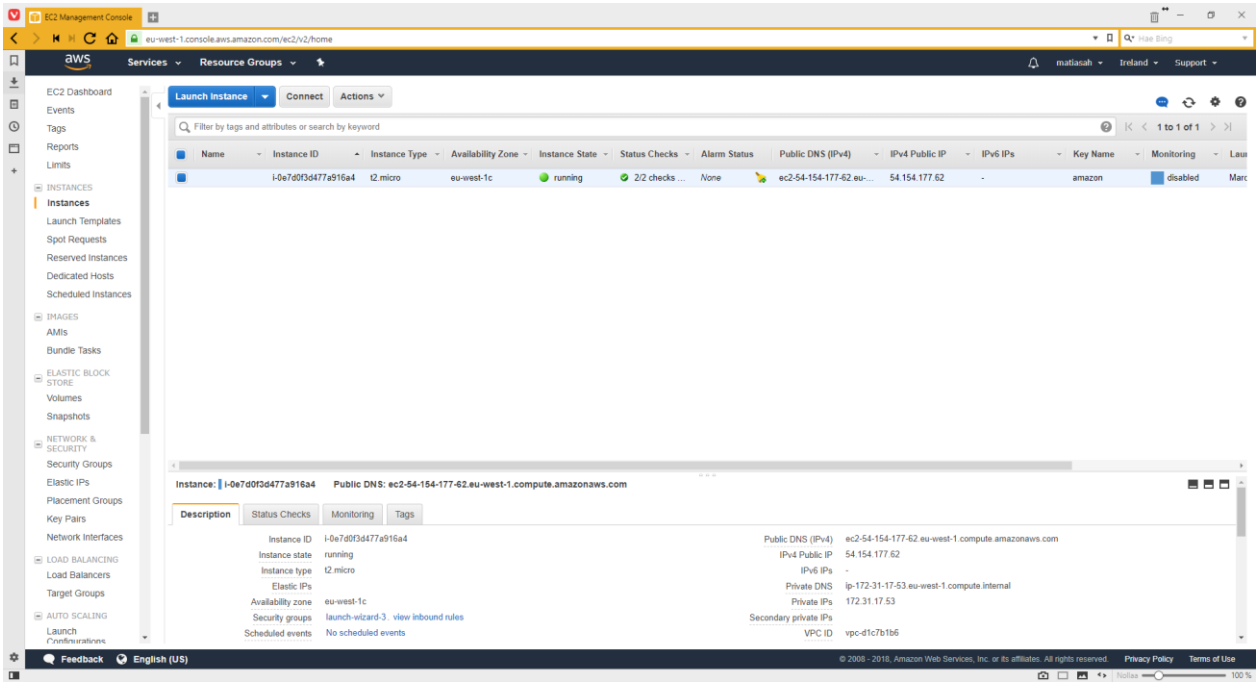


Kuva 7. Levykuvan siirtäminen S3-palvelusta EC2:een.

5.2.4 Instanssin käyttöönotto

Virtuaalikoneen levykuva on siirretty onnistuneesti Amazonin pilvipalveluun. Amazonin EC2-palveluun tulee perustaa instanssi, jotta siirrettyä levykuvaa voidaan käyttää.

Instanssin perustamiseksi klikataan AMIs-valikosta löytyvää levykuvaa hiiren oikealla painikkeella ja valitaan *Launch,* jolloin siirrytään instanssin luomiseen. Aluksi valitaan instanssityyppi eli millaiset laitteisto-ominaisuudet halutaan. Instanssiin voidaan halutta-essa konfiguroida esimerkiksi yksityiskohtaiset palomuuri- ja tietoturva-asetukset sekä vaihtaa halutut IP-osoitteet. Jos ei halua konfiguroida instanssia ollenkaan, vaan mennä oletusasetuksilla, valitaan *Review and launch.* Instanssia varten luodaan avainpari, joilla kirjaudutaan instanssiin. Samaa avainparia voidaan käyttää useampaan instanssiin.



Kuva 8. Valmis instanssi Amazon EC2 -palvelussa.

Luotua instanssia käytetään etäyhteydellä. Yhteys muodostetaan lataamalla ja avaa-malla instanssin rdp-tiedosto. Sisäänkirjauduttaessa käytetään samaa käyttäjätunnusta ja salasanaa kuin ennen siirtoa.

5.2.5 Yhteenveto

Käytännönosuuden tarkoituksena oli siirtää olemassa oleva virtuaalikone pilvipalveluun Amazon AWS -palvelun avulla. Lopputuloksena siirto onnistui hyvin. Virtuaalikoneen siirtäminen cold migration -menetelmällä oli kuitenkin ensimmäisellä kerralla työläs, koska se vaati monivaiheiset alkutoimenpiteet. Siirtovaiheessa eri oppaiden ohjeiden tulkitsemisessa oli välillä vaikeuksia useiden monimutkaisten vaiheiden vuoksi, mikä teki käytännönosuuden työstämisestä ajoin hidasta ja vaivalloista. Toivon, että tämän insinöörityön käytännönosuuden vaihe vaiheelta etenevien työskentelyohjeiden avulla vastaavan työn tekeminen onnistuu jatkossa yksinkertaisemmin.

Insinöörityössä havainnollistettua virtuaalikoneen siirtoa pilvipalveluun voivat hyödyntää esimerkiksi yritykset, jotka tarvitsevat aina saatavilla olevan, puhtaan virtuaalikoneen, jossa on haluttu käyttöjärjestelmä ja tarvittavat palvelut. Tällainen virtuaalikone voidaan siirtää pilvipalveluun AMI-levykuvaksi, josta voidaan asentaa uusia instansseja yhä uudelleen ilman, että virtuaalikoneen asennusprosessia tarvitsisi aloittaa alusta.

Työtä voisi jatkaa siirtämällä virtuaalikoneen pilvipalveluun toisella siirtomenetelmällä, esimerkiksi Amazon Server Migration Services -palvelulla. Tällöin virtuaalikone kahdennettaisiin pilvipalveluun, ja siirto olisi reaaliaikainen.

Lähteet

Amazon Web Services. 2018. Amazon Simple Storage Service: Developer Guide. Verkkoaineisto. <https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-dg.pdf>. Luettu 13.3.2018.

Amazon Web Services. 2018. AWS Command Line Interface User Guide. Verkkoaineisto. <https://docs.aws.amazon.com/cli/latest/userguide/aws-cli.pdf#awscli-install-windows>. Luettu 13.3.2018.

Amazon Web Services. 2018. General Reference. Verkkoaineisto. <https://docs.aws.amazon.com/general/latest/gr/aws-general.pdf>. Luettu 13.3.2018.

Amazon Web Services. 2018. VM Import/Export: User Guide. Verkkoaineisto. <https://docs.aws.amazon.com/vm-import/latest/userguide/vm-import-ug.pdf>. Luettu 15.3.2018.

Amazon Web Services. About AWS. Verkkoaineisto. <https://aws.amazon.com/about-aws/>. Luettu 14.3.2018.

Amazon Web Services. Amazon EC2. Verkkoaineisto. <https://aws.amazon.com/ec2/?nc2=h_l3_c>. Luettu 20.3.2018.

Amazon Web Services. Amazon S3. Verkkoaineisto. <https://aws.amazon.com/s3/?nc2=h_l3_sc>. Luettu 20.3.2018.

Cloud Security Alliance. 2016. Security as a Service: Defined categories of Security as a Service (preview) – Continuous monitoring as a Service. Verkkoaineisto. <https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categories-securities-prep.pdf>. Luettu 13.2.2018.

Cloud Security Alliance. 2016. The Treacherous 12: Cloud Computing Top Threats in 2016. Verkkoaineisto. <https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf>. Luettu 13.2.2018.

Cloud Security Alliance. About. Verkkoaineisto. <https://cloudsecurityalliance.org/about/>. Luettu 4.10.2017.

EU GDPR. GDPR Key Changes. Verkkoaineisto. <https://www.eugdpr.org/key-changes.html>. Luettu 23.3.2018.

Heino, Petteri. 2010. Pilvipalvelut. Hämeenlinna: Talentum Media Oy.

Hussain, Mohammed – Abdulsalam, Hanady. 2011. SECaaS: Security as a Service for cloud-based applications. Verkkoaineisto. <https://www.researchgate.net/publication/254004357_SECaaS_security_as_a_service_for_cloud-based_applications>. Luettu 13.3.2018.

Kavis, Michael. 2014. Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS). New Jersey: John Wiley & Sons, Inc.

Mell, Peter – Grance, Timothy. 2011. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Verkkoaineisto. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Luettu 4.10.2017.

Red Hat. Cloud Computing: What is multicloud? Verkkoaineisto. <https://www.redhat.com/en/topics/cloud-computing/what-is-multicloud>. Luettu 10.10.2017.

Salo, Immo. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo.

Sosinsky, Barrie. 2011. Cloud Computing Bible. Indianapolis: Wiley Publishing, Inc.

Tietosuojavaltuutetun toimisto. 2016. Kysymyksiä ja vastauksia tietosuojauudistuksesta. Verkkoaineisto. <http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html>. 5.4.2016. Luettu 23.3.2018.