KARELIA-AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

Teemu Lyttä

SAAS-VIRTUAALIPALVELINYMPÄRISTÖN PYSTYTYS AWS-ALUSTALLE

Opinnäytetyö
Huhtikuu 2019

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Huhtikuu 2019
Tietojenkäsittelyn koulutusohjelma

Tikkarinne 9
80200 JOENSUU
+358 13 260 600 (vaihde)

Tekijä(t)
Teemu Lyttä

Nimeke
SaaS-virtuaalipalvelinympäristön pystytys AWS-alustalle

Toimeksiantaja
Metalliteollisuusalan yritys

Tiivistelmä

Tämän opinnäytetyön tarkoitus oli rakentaa opinnäytetyön toimeksiantajalle toimiva SaaS-palvelinympäristö. Palvelinympäristö rakennettiin Amazon Web Services -palvelun-tarjoajan pilvipalvelinalustalle.

Opinnäytetyö oli toiminnallinen, joten se ei sisällä tietoperustaa lukuun ottamatta tutkimus-tietoa. Vaiheet palvelinympäristön rakentamiseksi on selostettu tarkasti, jotta toimeksian-taja voi käyttää tätä opinnäytetyötä käyttöohjeena uusien palvelinympäristöjen pystyttä-mistä varten.

Työn tuloksena toimeksiantajalle rakentui toimiva palvelinympäristö. Toimeksiantaja voi käyttää tätä ympäristöä testiasennusten sekä erilaisten testitoimenpiteiden suorittamiseen ohjelmistolla, jota se tarjoaa asiakkailleen SaaS-palveluna.

Kieli	Sivuja	33
suomi	Liitteet	1
	Liitesivumäärä	1

Asiasanat
SaaS, Software as a service, palvelinympäristö, pilvipalvelu, AWS

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
April 2019
Degree programme in Business Information technology

Tikkarinne 9
80200 JOENSUU
FINLAND
+ 358 13 260 600 (switchboard)

Author (s)
Teemu Lyttä

Title
Setting up a SaaS Virtual Server Environment on the AWS Platform

Commissioned by
A metal industry company

Abstract

The purpose of this thesis was to build a functional server environment for the commissioner of the thesis. The server environment was to be built in the Amazon Web Services hosted cloud computing environment.

The thesis is action-oriented, which means that the thesis does not have much research information, excluding the materials collected for the knowledge basis. The steps for building the server environment have been explained in depth, and the thesis will work as a user guide for the commissioner.

The result of the thesis was a functional server environment for the commissioner. The commissioner can use the environment to conduct test installations and different test procedures for the software which it offers to the customers as a SaaS service.

Language
Finnish

Pages	33
Appendices	1
Pages of Appendices	1

Keywords
SaaS, Software as a service, server environment, cloud hosting service, AWS

Sisältö

Liitteet

Lyhenteet

AMI	Amazon Machine Image, Amazon levykuva.
AWS	Amazon Web Services, Amazonin pilvilaskenta-alusta.
CSV	Comma-separated Values, tekstitiedosto, jonka arvot ovat eroteltu toisistaan pilkuilla sekä rivinvaihdoilla.
EC2	Elastic Compute Cloud, Amazonin virtuaalipalvelininstansseja tarjoava palvelu.
HTTPS	Hypertext Transfer Protocol Secure, hypertekstin siirtoprotokolla, joka on salattu.
IAM	Identity and Access Management, identiteetin- ja kulunhallinta.
IP	Internet Protocol, internetprotokolla, jonka tarkoitus on IP-tietoliikennepakettien toimittaminen.
IT	Information technology, informaatioteknologia.
MFA	Multi Factor Authentication, monivaiheinen tunnistautuminen.
QR code	Quick Response Code, ruutukoodi, johon on sisällytetty dataa.
RDS	Relational Database Service, relaatiotietokantapalvelu.
S3	Simple Storage Service, Amazonin tallennusjärjestelmä.
SaaS	Software as a Service, ohjelmisto palveluna.
SOAP	Simple Object Access Protocol, tietoliikenneprotokolla, joka suorittaa proseduurien etäkutsuja.
SQL	Structured Query Language, kyselykieli, jota voidaan käyttää relaatiotietokantaan tehtävien toimenpiteiden suorittamiseen.
SQS	Simple Queue Service, Amazonin viestienkäsittelyyn käytettävä väliohjelmisto.
SSL	Secure Sockets Layer, salausprotokolla, jota käytetään tietoliikenteen suojaamiseen.
TCP	Transmission Control Protocol, tietoliikenneprotokolla tietokoneiden välisten yhteyksien luomista varten.
XML	Extensible Markup Language, yläkäsite tai standardi tietynlaisille merkintäkielille.

1 Johdanto

Yrityksillä on yhä enenevissä määrin erilaisia ohjelmistoja tukemassa yrityksen liiketoimintaa. Tämä edellyttää usein sitä, että yrityksellä on myös näitä ohjelmistoja varten rakennettu oma tietohallinto, joka vastaa asentamisesta, päivittämisestä sekä myös mahdollisesti kehittämisestä. Ohjelmistot vaativat asennuksen joko palvelimelle tai asiakaspäätteelle. Hyvin organisoitu tietohallinto luo yritykselle huomattavaa kilpailuetua markkinoilla.

Tietohallinnon perustaminen sekä ylläpito voivat vaatia yritykseltä paljon resursseja. Erityisesti pienyrityksissä tietohallinto käsitteenä ja sen merkitys voi olla vieras. (Jaakkola 2012.) Tämä voi johtaa yrityksen ulkoistamaan tietohallintonsa tai hankkimaan tarvittavat ohjelmistot palveluna. Ohjelmistosta, joka hankitaan palveluna, käytetään myös lyhennettä *SaaS.*

SaaS-palveluntarjoaja tarjoaa asiakkaalleen ohjelmiston pilvipalveluna. Palvelu mahdollistaa sen, että asiakkaan ei tarvitse asentaa ohjelmistoa omalle asiakaspäätteelleen tai palvelimille, eikä hänen tarvitse huolehtia sovellukseen kohdistuvista päivitys- ja huoltotoimenpiteistä. Useissa tapauksissa tällainen palvelu välitetään verkkoselaimen kautta. (Pilvi 2019.)

Opinnäytetyössä kuvataan, kuinka *SaaS*-virtuaalipalvelinympäristö pystytetään toimeksiantajan asettamien vaatimusten mukaisesti. Opinnäytetyön toimeksiantaja on Suomessa toimiva metalliteollisuusalan yritys. Kyseinen palvelinympäristö on yrityksen sisäiseen testikäyttöön pystytettävä palvelinympäristö, jonka on tarkoitus toimia tukena yrityksen sisäisille IT-toimijoille. Ympäristöä käytetään yrityksen asiakkailleen tarjoaman SaaS-ohjelmiston testikäyttöä varten. Palvelinympäristö rakennetaan pilvipalvelualustalle, jonka tarjoaa *AWS* (*Amazon Web Services)*.

Opinnäytetyö suoritetaan toiminnallisena opinnäytetyönä. Tarkoituksena on dokumentoida työn eri vaiheet tarkalla tasolla. Kyseistä dokumentaatiota voidaan

jatkossa hyödyntää, kun yrityksellä on tarpeen pystyttää uusia *SaaS*-palvelinympäristöjä. Työn ohessa tuotettavaa materiaalia voidaan jatkossa käyttää tukimateriaalina uusien työntekijöiden perehdytyksessä. Työ kuvataan palvelinympäristön pystyttäjän näkökulmasta, ja työn lopputuloksena toimeksiantajalle on pystytetty toimiva *SaaS*-palvelinympäristö, jota toimeksiantaja voi käyttää tarjoamiensa ohjelmistojen testaamiseen. Työn teknisen osuuden suorittamisessa hyödynnetään jo työelämässä sekä Karelia-ammattikorkeakoulussa opittuja taitoja. Toimeksiantajan toivomuksesta opinnäytetyöstä on poistettu kaikki sellainen tieto, joka voi paljastaa toimeksiantajan identiteetin.

2 Toimeksiantaja sekä kulunhallintaohjelmisto

Tässä luvussa esitellään toimeksiantaja, sekä sen asiakkailleen tarjoama ohjelmisto yleisellä tasolla. Palvelinympäristöön käyttöön tulevien palvelimien tarkemmat järjestelmävaatimukset löytyvät liitteestä 1.

Kulunhallintaohjelmistolla tarkoitetaan elektronista järjestelmää, jota käytetään tietoliikenneverkon kautta. Tästä syystä ohjelmistoon kuuluvien komponenttien täytyy olla yhdistettynä verkkoon, johon ohjelmisto on asennettuna. Ohjelmisto tunnistaa käyttäjän, sekä antaa kulkuoikeuden käyttäjälle, mikäli se on myönnettynä hänelle ohjelmiston kautta. Tämänlainen ohjelmisto on joustava, avausoikeutta ei enää myönnetä pelkän mekaanisen aukaisuoikeuden avulla, vaan avauksen mahdollistamiseksi komponentilla tulee olla myös elektroninen aukaisuoikeus. (Elprocus 2019.)

2.1 Toimeksiantaja

Toimeksiantajana opinnäytetyölle toimii metalliteollisuusalan yritys. Yrityksellä on käytössään kulunhallinnan harjoittamiseen käytettävä ohjelmisto, jota yritys tarjoaa asiakkailleen *SaaS*-palveluna.

Jotta yritys voi tarjota asiakkailleen palvelua, tulee yrityksellä olla osaava IT-henkilöstö, joka osaa käyttää, asentaa sekä suorittaa erilaisia huoltotoimenpiteitä ohjelmistoa varten. Tätä varten yrityksellä on herännyt tarve saada käyttöön kyseiselle kulunhallintaohjelmistolle erillinen testiympäristö, jossa henkilöstö voi harjoitella ohjelmiston asennusta sekä tehdä erilaisia ongelmanratkaisutoimenpiteitä tuotantoympäristöillä ilmenneiden ongelmien ratkaisemiseksi.

2.2 Kulunhallintaohjelmiston ominaisuudet

Kulunhallintaohjelmisto, jota toimeksiantaja tarjoaa asiakkailleen *SaaS*-palveluna, on asiakkaan verkkoselaimen kautta käytettävä ohjelmisto. Ohjelmistolla hallinnoidaan asiakasyrityksen elektromekaanisten avainten sekä lukkojen aukaisuoikeuksia.

Elektromekaanisella komponentilla tarkoitetaan yleisesti avainta tai lukkoa, joka sisältää myös mekaanisen jyrsintiedon lisäksi elektronisen aukaisuoikeustiedon. Avauksen mahdollistamiseksi avaimen tulee sopia lukkoon mekaanisesti, ja sillä tulee olla myönnettynä erillisen ohjelmiston kautta aukaisuoikeus. (Turvakolmio 2017.)

Vaikka ohjelmistoa käytetäänkin asiakkaan toimesta verkkoselaimen kautta, tulee palvelua tarjoavan yrityksen suorittaa ohjelmiston asennus omille palvelimilleen. Asiakas ottaa omalta asiakaspäätteeltään verkkoselaimen kautta verkkoyhteyden palvelua tarjoavan yrityksen palvelimelle, jossa ohjelmisto sijaitsee. Tämän yhteyden muodostamiseen asiakkaalla tulee olla erillinen *SSL-sertifikaattitiedosto*[1] asennettuna verkkoselaimeen. Asiakkaalla tulee myös olla hallussaan palvelua tarjoavan yrityksen asiakkaalle myöntämä erillinen tunnistekomponentti, joka on suojattu *PIN*-koodilla. Tällä komponentilla sekä sertifikaattitiedostolla asiakas voidaan identifioida palveluntarjoajan palvelimella, ja samalla

[1] SSL-sertifikaattitiedostolla luodaan suojattu yhteys kahden tietokoneen välille. Sertifikaatin tarkoitus on luoda allekirjoitus palvelimelle, joka toimii suojatun SSL-yhteyden takaajana ja varmenteena siitä, että yhteys on muodostettu tarkoitettuun tietokoneeseen. (Aitoa 2019.)

asiakkaalle valikoituu käytettäväkseen vain asiakkaan omat tiedot palvelinympäristön tietokannasta. Kyseinen asiakas ei pääse näillä tiedoilla käsiksi muiden palvelinympäristöllä sijaitsevien asiakkaiden tietoihin.

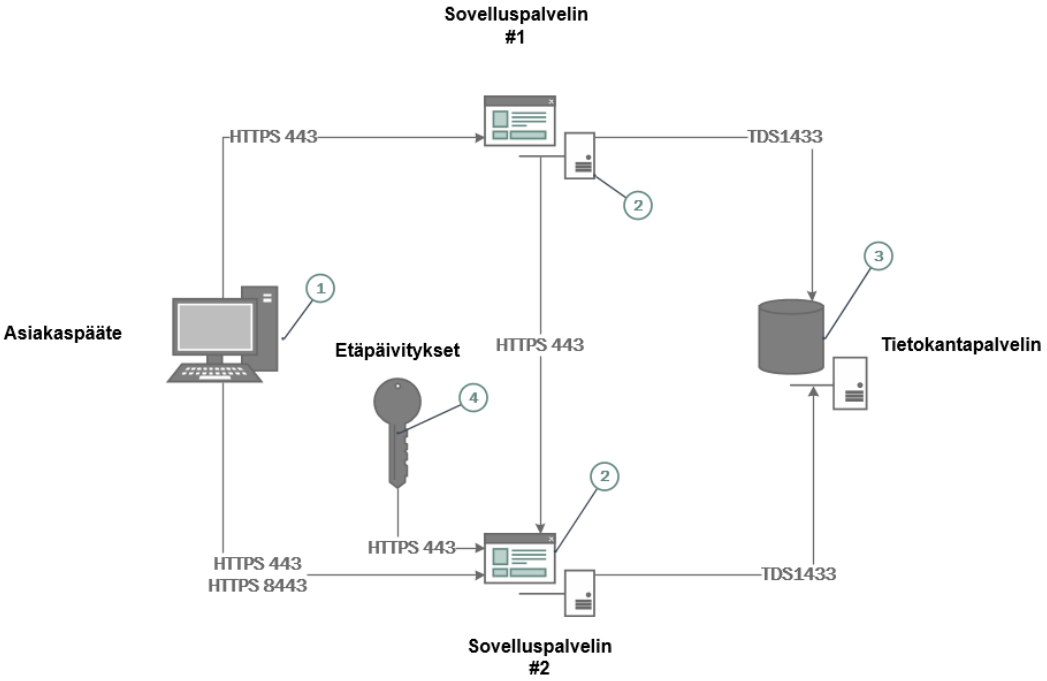
Ohjelmistossa asiakas voi hallinnoida elektromekaanisten komponenttien avausoikeuksia, sekä hallinnoida komponentteja käyttävien henkilöiden tietoja. Avaimia voidaan jakaa työntekijöille, niille voidaan ohjelmoida erilaisia voimassaoloasetuksia ja niitä varten voidaan tarvittaessa luoda erillisiä kieltotehtäviä, esimerkiksi tilanteessa, jossa avain sattuisi katoamaan.

Avaimia on mahdollista päivittää joko selaimen kautta paikallisesti asiakaspäätteeseen liitetyn ohjelmointilaitteen avulla, tai erilaisilla etäohjelmointiyksiköillä, joita asiakas on voinut tarpeensa mukaan asentaa maantieteellisesti eri sijainteihin avainpäivitysten saatavuuden helpottamiseksi. Näillä etäohjelmointiyksiköillä tulee olla muodostettuna internetyhteys palveluntarjoajan palvelimelle.

2.3 Kulunhallintaohjelmiston palvelinympäristön kuvaus

Ohjelmisto asennetaan palvelinympäristöön, joka koostuu kolmesta palvelimesta: kahdesta sovelluspalvelimesta sekä yhdestä tietokantapalvelimesta. Kyseiset palvelimet voivat olla joko fyysisiä tai virtuaalisia palvelimia. Toimeksiantajan tarjoamien järjestelmävaatimusten mukaan (liite 1) ohjelmisto tukee vain *Windows Server* -palvelintyyppiä.

Palvelimien tulee voida muodostaa verkkoyhteys toisiinsa. Tästä syystä tietoliikenneyhteydet palvelimien välillä tulee olla sallittuna palomuurissa kuvion 1 mukaisesti.



Kuvio 1. Toimeksiantajan ohjelmiston tietoliikennekuvaus (mukaillen ohjelmiston tietoliikennekuvaus 2019).

1. Asiakaspäätettä käytetään asiakkaan toimesta ohjelmistoon kirjautumiseen verkkoselaimen kautta.
2. Sovelluspalvelimille asennetaan ohjelmisto palveluntarjoajan toimesta. sovelluspalvelimista palvelin #1 suorittaa ohjelmiston käyttöliittymää ja #2 hallinnoi suoritettavia etäpäivityksiä.
3. Tietokantapalvelin sisältää molempien sovelluspalvelimien tietokannat.
4. Etäpäivitysyksiköt ovat yhteydessä siihen sovelluspalvelimeen, joka suorittaa etäpäivitystehtäviä (Sovelluspalvelin #2).

Näiden palvelimien lisäksi on myös suositeltavaa tilata erillinen hallinnointipalvelin (ns. hyppypalvelin), jota käytetään sovelluspalvelimille sekä tietokantapalvelimelle kirjautumiseen. Kyseistä palvelinta ei ole esitetty kuviossa 1, sillä sitä ei tulla käyttämään *SaaS*-palvelua käyttävän asiakkaan toimesta.

3 SaaS

SaaS on liiketoimintamalli, jossa asiakas maksaa ohjelmistosta, joka tarjotaan hänelle palveluna. Ohjelmisto sijaitsee palveluntarjoajan palvelimilla, ja asiakas pääsee siihen käsiksi esimerkiksi verkkoselaimen kautta. Nykyään *SaaS*-liiketoimintamallista käytetään myös termiä *Cloud Computing* (Techopedia 2019). *Cloud computing* -malleja ovat *SaaS*-palvelun lisäksi myös *IaaS (Infrastructure as a service)* sekä *PaaS (Platform as a service).*

PaaS-palvelu tarjoaa valmiita pilvipohjaisia ympäristöjä, joita käytetään esimerkiksi sovelluskehityksessä. *PaaS*-ympäristö tekee sovellusten kehittämisestä, testaamisesta sekä julkaisusta nopeaa, helppoa sekä kustannustehokasta. *PaaS* tarjoaa erilaisia palveluun sisäänrakennettuja työkaluja, joiden avulla sovelluksia voidaan kehittää. (Apprenda 2019.)

IaaS-palvelu on itsepalvelumalli palvelinkeskusten infrastruktuurien, kuten levytila ja verkkoasetukset, käsittelyä, monitorointia sekä hallintaa varten. Sen sijaan, että käyttäjä tilaisi laitteistot suoraan palveluntarjoajalta, käyttäjä tilaa *IaaS*-ympäristön ja maksaa ympäristöstä vain sen mukaan, paljonko ympäristön resursseja on käytetty. (Apprenda 2019.)

Ensimmäinen ***SaaS***-ympäristö perustettiin 1960-luvulla. Tuolloin palvelu kulki nimellä *Time sharing system*. Näppäimistöt sekä monitorit, joissa ei ollut omaa prosessoria, yhdistettiin keskusyksikköön tai pientietokoneeseen. Sovellukset sekä niiden tarvitsema ja käyttämä data sijaitsivat keskusyksikössä. Pääteaseman näppäimistön kautta annettiin syöte keskusyksikölle, jonka jälkeen tämä antoi tulosteen oikealle päätemonitorille. Tämä oli varhainen tapa yhdistää tietokoneet toisiinsa – eli toisin sanoen palvelu nimeltään Internet. (Hur 2019.)

Tämä toimintamalli pätee edelleen *SaaS*-palvelun osalta, tosin tapa muodostaa yhteys palveluntarjoajan ohjelmistoon on hieman monimutkaisempi. Nykyään asiakas tarvitsee ohjelmiston käyttämistä varten oman asiakaspäätteen (*Client*),

jotta hän voi muodostaa yhteyden Internetin kautta ohjelmistoon, joka sijaitsee palveluntarjoajan palvelimella.

On yleistä, että *SaaS*-palvelussa ostetaan käyttöoikeus palveluntarjoajan ohjelmistoon. Käyttöoikeutta voidaan rajata erilaisilla lisensseillä, jotka määrittävät esimerkiksi ohjelmiston käyttäjien maksimimäärän, vasteajan tukipyyntöihin sekä ohjelmiston versiopäivityksen. Lisenssejä hankitaankin siis lisää sitä mukaa, kun ohjelmiston käyttötarve kasvaa. (Mäkilä 2011, 7.)

Hankkimalla ohjelmiston *SaaS*-palveluna asiakkaan on mahdollista resursoida tietohallintoon kohdistuvia kuluja tehokkaammin. Tietohallinto voi olla yritykselle kallista, ja useille yrityksille tietohallinto käsitteenä voi olla täysin uusi. Kun asiakas ostaa *SaaS*-palvelun, asiakkaan ei tarvitse huolehtia ohjelmiston asentamisesta, versiopäivityksistä tai ohjelmistoon kohdistuvasta kehitystyöstä. Palvelu on myös nopea ottaa käyttöön, ja asiakas maksaa palvelusta lähtökohtaisesti käyttöasteen mukaan.

4 AWS

AWS (*Amazon Web Services*) on pilvipalvelualusta, jonka tarjoaa *Amazon. Amazon EC2* (*Elastic Compute Cloud*) ja *Amazon S3* (*Simple Storage Service*) ovat tunnetuimpia sekä käytetyimpiä *AWS*:n tarjoamia palveluita.

AWS-palvelun suunnittelu aloitettiin vuonna 2002. Tällöin palvelun nimi oli *Amazon.com Web Service*, ja se tarjosi *SOAP* (*Simple Object Access Protocol*) ja *XML* (*Extensible Markup Language*) -rajapintoja Amazonin tuotekatalogiin. Myöhemmin yritys alkoi kehittämään teknologiaa, jossa infrastruktuurin hallintapalvelujen sekä kehittäjätyökalujen yhdistelmä olisi *Pseudo*[2]-käyttöjärjestelmä Internetiä varten. Eristämällä eri infrastruktuurin osia (suorituskyky, muisti, tietokanta) käyttöjärjestelmän komponenteiksi ja omistamalla kehittäjäystävällisiä työkaluja

[2] Pseudokoodi tarkoittaa ohjelmointikielen tapaista koodia, joka kuvaa mitä tietokoneohjelman tai algoritmin tulee suorittaa. Ohjelmointikielen sijasta pseudokoodissa käytetään tavallista tekstiä. (Rouse 2019).

niiden hallintaa varten oli mahdollista luoda automatisoitu sekä standardisoitu infrastruktuuri, jolle pystytään kohdistamaan tarvittaessa lisää resursseja.

Vuonna 2004 yrityksen ensimmäinen julkinen blogipostaus *AWS*:tä paljasti, että palvelua ollaan kehittämässä. *AWS* julkaistiin virallisesti 19.3.2006, ja julkaisun yhteydessä se tarjosi *S3*, *EC2* sekä *SQS* (*Simple Queue Service*) -palveluita. Euroopassa *EC2* ja *S3* -palvelut julkaistiin vuonna 2009. *AWS*:in tarjoama palvelu herätti pilvipalveluvalmiiden yritysten mielenkiinnon, jonka seurauksena yhteistyötä alettiin harjoittamaan suuryritysten, kuten *Netflix*, *Dropbox* sekä *Reddit,* kanssa. (Rojas 2017.)

4.1 Palvelinympäristöä pystytettäessä käytettävät AWS-palvelut

EC2 on *AWS*:in palvelu, jonka kautta tilataan virtuaalipalvelininstansseja. Yksi palvelun eduista on, että käyttäjän ei tarvitse tehdä investointeja fyysisiä palvelimia varten etukäteen, vaan käyttäjä voi tilata palvelimen virtuaalisena, sekä määrittää sille halutut resurssit, kuten muistit sekä käyttöjärjestelmän. Palvelussa tilatut instanssit ovat helposti skaalautuvia, niille on mahdollista tilata tarvittaessa lisää resursseja, ja niitä on myös mahdollista hallinnoida AWS-hallinnointikonsolin kautta. Tämä auttaa esimerkiksi tilanteissa, joissa tarjottavan palvelun kysyntä tai suosio kasvaa, ja tämän seurauksena palvelinympäristöön kohdistuu suurempi kuorma. (Amazon 2019a.)

EC2 tarjoaa myös mahdollisuuden muokata palvelinympäristön palomuurin asetuksia turvallisuusryhmien (*Security groups*) avulla. Palvelun käyttäjä voi esimerkiksi sallia tietoliikenteen tietystä *IP*-osoitteesta palvelimelle, määrittelemällä turvallisuusryhmälle tietoliikenneyhteyteen käytettävän yhteyskäytännön sekä käytettävän portin. (Amazon 2019b.)

Palvelininstanssilla tarkoitetaan Amazonin *EC2*-palvelussa käytettävää virtuaalipalvelinta. Instanssityyppejä on erilaisia, ja niillä on omat ominaisuudet, esimerkiksi prosessorin teho sekä muistien määrät.

Amazon VPC (Amazon Virtual Private Cloud) mahdollistaa *AWS*-resurssien käyttämisen itse määritetyssä virtuaalisessa verkossa. Tämä verkko toimii samalla tavalla kuin tavallisen palvelinkeskuksen verkko. Tällainen verkko on loogisesti eristetty[3] muista *AWS*-palvelussa käytössä olevista virtuaalisista verkoista. Tähän verkkoon on mahdollista julkaista *AWS*-resursseja, kuten *EC2*-palvelussa luotuja palvelininstansseja. (Amazon 2019c.)

Amazon RDS (Relational database service) on *AWS*:in tarjoama relaatiotietokantapalvelu. Relaatiotietokanta koostuu monesta eri taulukoista, jotka sisältävät erilaista dataa, eli yksi tieto tallennetaan vain yhteen paikkaan. Relaatiotietokannassa nämä tiedot yhdistyvät toisiinsa, ja tietokanta itsessään sisältää tiedon siitä, miten tiedot ovat yhdistettynä taulukoiden välillä. (Sarja 2006.)

RDS-palvelu on helppo ottaa käyttöön, siihen on mahdollista tilata nopeasti lisää resursseja sekä erilaiset hallinnointitehtävät, kuten palvelinten päivitykset sekä varmuuskopioiden talteen ottaminen, suoritetaan automaattisesti. Palvelu on mahdollista ottaa käyttöön *Amazon Aurora*, *PostgreSQL*, *MySQL*, *MariaDB*, *Oracle Database* sekä *SQL Server* -tietokantamoottoreilla. (Amazon 2019d.)

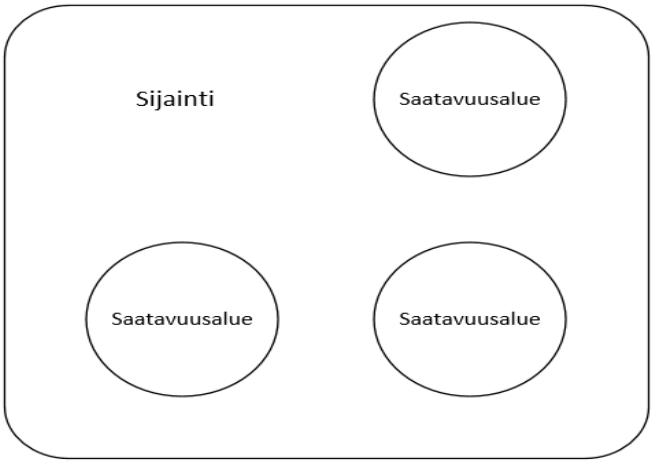
AWS Identity and Access Management (IAM) -palvelun avulla hallinnoidaan käyttäjien pääsyä *AWS*:in palveluihin sekä resursseihin. *IAM*:in avulla voidaan luoda uusia käyttäjiä hallinnointikonsolia varten, sekä hallinnoida heidän pääsyään *AWS*-resursseihin. (Amazon 2019e.)

4.2 Amazon-palvelinkeskukset

AWS tarjoaa palveluitaan maailmanlaajuisesti hajautetuilta palvelinkeskuksiltaan. Palvelinkeskuksia sijaitsee maailmalla 20:ssä maantieteellisessä sijainnissa, ja näihin alueisiin on sijoitettuna 61 toisistaan eristettyä saatavuusaluetta. Saatavuusalueella tarkoitetaan maantieteellisellä alueella sijaitsevia, toisistaan eristettyjä alueita.

[3] Looginen eristäminen on asetus, joka estää laitteita, jotka käyttävät samaa fyysistä verkostoa, kommunikoimasta keskenään (Peterson 2017).

Euroopassa palvelua on tarjolla viidessä eri maantieteellisessä sijainnissa. Jokaisessa sijainnissa on kolme saatavuusaluetta kuvion 2 mukaisesti. Taulukko 1 kuvaa, missä maantieteellisissä sijainneissa AWS-palvelua on saatavilla.



Kuvio 2. *Regions and Availability zone concepts* -kuviota mukaillen (Amazon 2019f).

Taulukko 1. *AWS*-palvelun saatavuus Euroopassa (Amazon 2019f).

SIJAINTI	FRANKFURT	IRLANTI	LONTOO	PARIISI	TUKHOLMA
SAATAVUUS-ALUEET	3	3	3	3	3

5 Palvelinympäristön pystytys

Toimeksiantajan testikäyttöön tarkoitettu palvelinympäristö pystytettiin *AWS*-pilvipalvelualustalle. *AWS* valittiin palveluntarjoajaksi, koska se mielletään toimeksiannon antaneen yrityksen sisällä hyväksi pilvipalvelualustan tarjoajaksi, ja sen tarjoamat palvelut toimivat vakaasti. Palveluiden vakaus on nähtävissä ***AWS Service Health Dashboardilta***, joka listaa *AWS*-palveluiden tilan viimeisimmän vuoden ajalta. (Amazon 2019g.)

5.1 Tilattavat palvelimet

Palvelinympäristöön tilattiin neljä palvelinta, jotka toimivat seuraavissa rooleissa:

- kaksi sovelluspalvelinta
- hyppypalvelin
- tietokantapalvelin.

Kyseiset palvelimet pystytettiin samaan *VPC*-virtuaaliverkkoon.

Sovelluspalvelimella tarkoitetaan palvelinta, jolle asennetaan *SaaS*-palvelua varten käytettävä ohjelmisto. Sovelluspalvelimilta avataan tietoliikenneyhteydet sekä toisiaan että tietokantapalvelinta varten kuvion 1 mukaisesti.

Hyppypalvelimella on palvelin, johon on sallittuna etätyöpöytäyhteyden muodostaminen Internetistä. Tältä palvelimelta käyttäjä pääsee hallinnoimaan muita palvelinympäristöön kuuluvia palvelimia. **Tietokantapalvelimeen** otetaan myös yhteys tältä palvelimelta erillisellä *SQL Server Management Studio* -ohjelmistolla.

5.2 AWS-hallinnointitilin perustaminen

AWS-hallinnointitili luotiin *AWS*:in kotisivujen kautta. Kotisivut sekä itse hallinnointiportaali eivät ole saatavilla suomenkielisenä, joten tässä työssä hallinnointiportaalia käytettiin englanninkielisenä.

Palveluun rekisteröitymiseksi annettiin seuraavat tiedot:

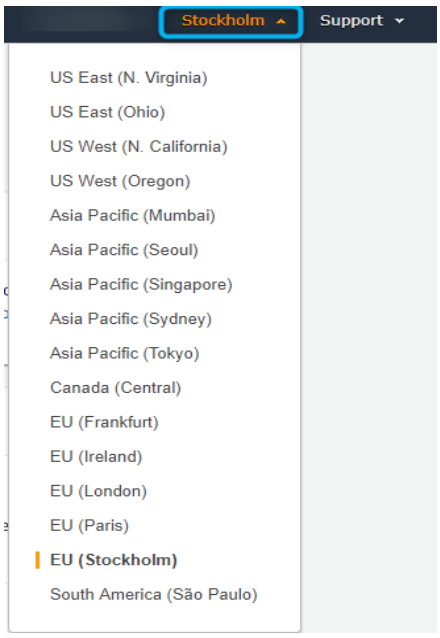
- sähköpostiosoite
- salasana
- etu- ja sukunimi
- puhelinnumero
- osoitetiedot
- pankki- tai luottokortin tiedot (Palvelua on mahdollista käyttää rajallisesti maksutta).

Tämän jälkeen palvelu tarkasti käyttäjän henkilöllisyyden lähettämällä käyttäjän puhelinnumeroon varmistusviestin, joka sisälsi palveluntarjoajan antaman vahvistuskoodin. Vahvistuskoodin syöttämisen jälkeen *AWS*-hallinnointitili oli valmiina käytettäväksi.

Tästä toimenpiteestä muodostui *Root*-tason käyttäjätunnukset. Kyseisellä tunnuksella on pääsy kaikkiin *AWS*-hallinnointitilin palveluihin sekä resursseihin. *AWS* suosittelee, että palvelua ei käytettäisi lähtökohtaisesti näillä tunnuksilla, vaan jokapäiväistä hallinnointia varten luotaisiin Amazonin *IAM*-palvelun avulla käyttäjä. (Amazon 2019h.) Mikäli *Root*-tason käyttäjätunnukset päätyisivät väärin käsiin, tilin väärinkäyttäjä saisi aikaan merkittävää vahinkoa tilillä sijaitseville palvelimille sekä käyttäjille.

5.3 AWS-hallinnointikonsolin palvelinkeskuksen valinta

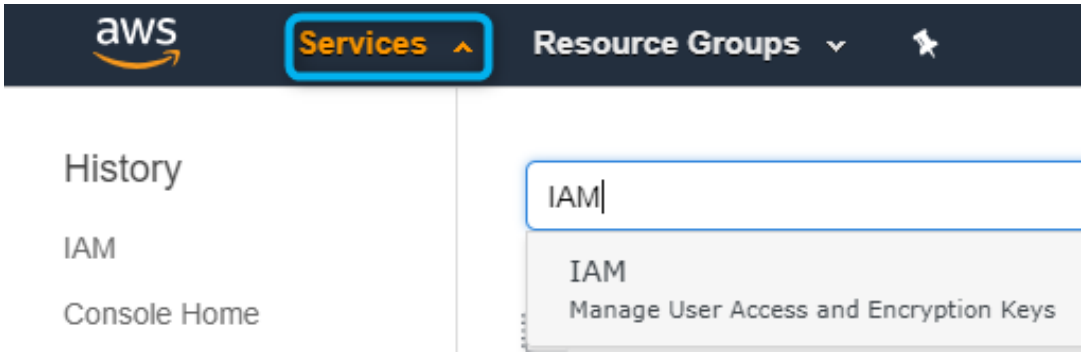
AWS-tilille kirjautumisen jälkeen suoritettiin *AWS*-palvelinkeskuksen sijainnin vaihtaminen toimeksiantajan esittämän toiveen mukaisesti. Palvelinkeskus vaihdettiin hallinnointikonsolin oikeassa yläkulmassa sijaitsevasta *Support*-painikkeen vasemmalla puolella sijaitsevasta painikkeesta kuvan 1 mukaisesti.



Kuva 1. Palvelinkeskuksen valinta (Amazon 2019i).

5.4 IAM käyttäjähallinta sekä uusien Admin-käyttäjien lisäys

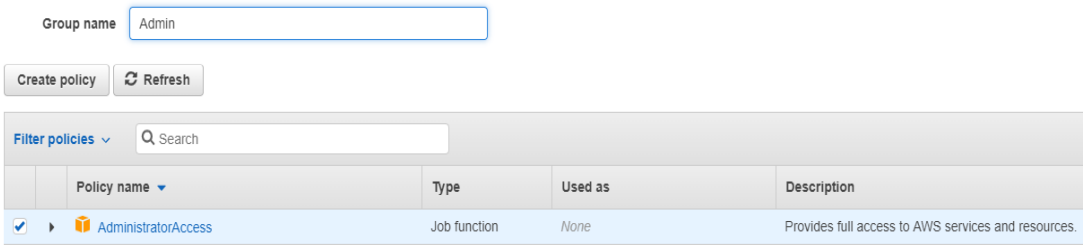
Kuten luvussa 5.2 mainittiin, *Root*-tason käyttäjätunnusta ei suositella käytettäväksi hallinnointikonsolin jokapäiväistä käyttöä varten, joten tätä varten luotiin erilliset *Admin*-tason käyttäjätunnukset *IAM*-palvelun avulla. *IAM*-palveluun pääsee hallinnointikonsolin hakupalvelun avulla. *AWS*:in hakupalveluun pääsee vasemmassa yläkulmassa sijaitsevasta *Services*-painikkeesta kuvan 2 mukaisesti. Tähän hakukenttään syötettiin arvoksi *IAM.*



Kuva 2. *AWS*-hallinnointikonsolin hakupalvelun käyttäminen (Amazon 2019i).

Käyttäjät luotiin *IAM*-palvelin valikosta *Users*. Käyttäjän luominen aloitettiin painikkeella *Add User*, jonka jälkeen syötettiin käyttäjän nimi ja palveluun kirjautumistyyppi. Koska luotava käyttäjä käyttää palvelua hallinnointikonsolin kautta, valittiin kirjautumistyypiksi *AWS Management Console access*. Käyttäjälle asetettiin itse määritelty salasana, *AWS*-palvelun tarjoaman automaattisesti generoidun salasanan sijasta. Salasanan määrittämisen jälkeen siirryttiin käyttöoikeuksien valintaan painamalla *Next: Permissions* -painiketta.

Käyttäjälle lisättiin ryhmä, joka määrittää käyttäjän oikeudet hallinnointikonsolissa. Ryhmän luonti tapahtui painamalla *Create group* -painiketta. Ryhmän nimeksi valittiin *Admin*, sillä nimen haluttiin kuvaavan ryhmän käyttötarkoitusta mahdollisimman tarkasti. Ryhmäkäytänteeksi ryhmälle valittiin *AdministratorAccess*-käytänne kuvan 3 mukaisesti. Tämä tarjoaa käyttäjälle täyden pääsyn *AWS*-palveluihin sekä resursseihin. Ryhmä luotiin painikkeella *Create group*, ja tämän jälkeen siirryttiin seuraavaan valikkoon *Next: Tags* -painikkeella.

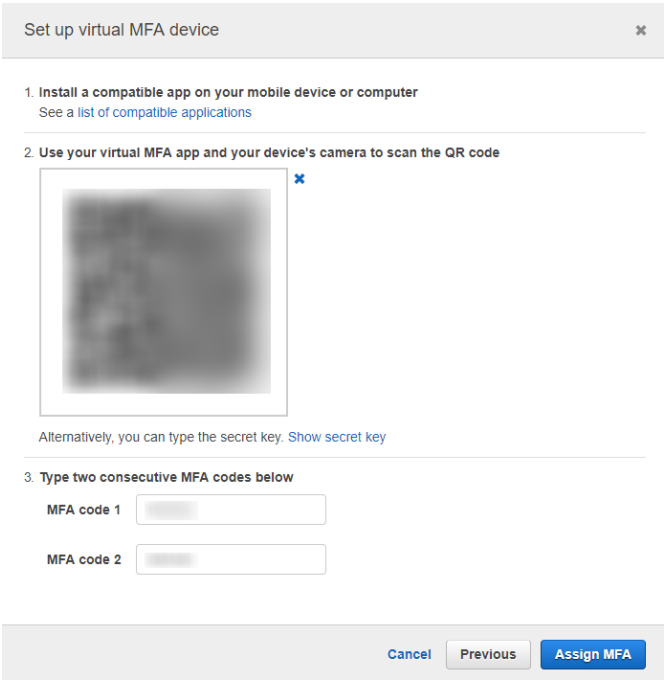


Kuva 3. *Admin*-tason oikeuksien myöntäminen (Amazon 2019i).

Tags-valikossa käyttäjälle on mahdollista lisätä tunnistetieto. Tämä helpottaa käyttäjien hallinnointia *AWS*-hallinnointikonsolissa, mikäli käyttäjiä on useampia. Toimeksiantajan mukaan käyttäjiä ei tule niin montaa, että kyseinen tieto tarvittaisiin.

Yhteenvetonäkymässä on mahdollista tarkastaa syötettyjen käyttäjätietojen oikeellisuus ennen käyttäjän luomista. Tietojen tarkastamisen jälkeen käyttäjä luotiin *Create user* -painikkeella. Tämän jälkeen palvelu ilmoitti, että käyttäjä on nyt onnistuneesti luotu. Tärkeä vaihe tässä kohdassa on, että tältä sivulta ladataan käyttäjän hallinnointikonsoliin kirjautumista varten tiedot sisältävä *CSV*-tiedosto *Download .csv* -painikkeella. Kyseinen tiedosto taltioitiin turvalliseen paikkaan toimeksiantajan tiloihin, sillä tiedoston sisältämillä käyttäjätunnuksella pääsee käsiksi kaikkiin *AWS*-tilin resursseihin sekä palveluihin.

Käyttäjille on suositeltavaa ottaa käyttöön kaksivaiheinen tunnistautuminen. Kun tilillä käytetään kaksivaiheista tunnistautumista, tulee käyttäjän palveluun kirjautumisvaiheessa tunnistautua myös toisen palvelun avulla, pelkän käyttäjätunnuksen ja salasanan lisäksi. Tämä ominaisuus otettiin käyttöön käyttäjän asetuksista, painamalla *Users*-näkymässä käyttäjän nimeä, ja siirtymällä *Security credentials* -välilehdelle. *Assigned MFA Device* -näkymässä painettiin *Manage*-painiketta ja valittiin *Virtual MFA Device*. Tunnistautumiseen käytettävälle laitteelle ladattiin erillinen tunnistautumissovellus, jolla skannattiin palvelun tarjoama, kuvassa 4 esitetty *QR*-koodi tunnistautumiseen käytettävän laitteen kameralla tunnistautumissovelluksen kautta. Lopuksi palveluun syötettiin tunnistautumissovelluksen tarjoamat kaksi peräkkäistä *MFA*-koodia, jonka jälkeen ominaisuus otettiin käyttöön *Assign MFA* -painikeella.



Kuva 4. *MFA*-asetusten määrittäminen (Amazon 2019i).

5.5 VPC-asetusten määritys ja turvallisuusryhmien perustaminen

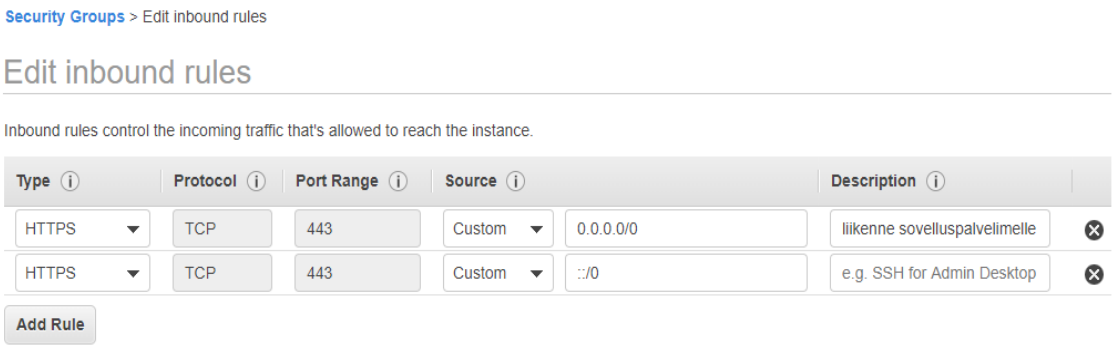
AWS-palvelu luo käyttäjälle automaattisesti oman virtuaaliverkon, kun palvelu otetaan käyttöön. Kyseisen verkon ominaisuuksia pääsee tarkastelemaan hakemalla kuvan 2 hakuvalikosta avainsanalla *VPC*. Tärkeänä tietona tässä näkymässä on *IPv4 CIDR* -tieto, joka kertoo käyttäjälle kyseisen verkon *IP*-osoitteen.

Tietoliikenteen suojaamiseksi on suositeltavaa tehdä verkkoa varten erilliset turvallisuusryhmät. Turvallisuusryhmä toimii virtuaalisena palomuurina palvelininstansseille, kontrolloiden sekä sisään- että ulospäin suuntaavaa liikennettä (Amazon 2019b).

Turvallisuusryhmät luotiin *VPC*-näkymässä vasemmassa valikossa olevan *Security Groups* -painikkeen kautta. Koska palvelininstanssien tarkoitus on toimia samassa virtuaaliverkossa, luotiin ympäristöön palomuuriavaukset, jotka vastaavat kuviota 1. *Security groups* -valikossa turvallisuusryhmä luotiin *Create security group* -painikkeella. Seuraavaksi turvallisuusryhmälle annetiin nimi ja kuvaus,

minkä jälkeen se lisätiin tämän luvun alussa mainittuun virtuaaliverkkoon. Tämän jälkeen ryhmä luotiin *Create*-painikkeella.

Tämän lisäksi ryhmälle määritettiin sisäänpäin suuntaavan liikenteen säännöt. Säännöt määritettiin valitsemalla turvallisuusryhmä, ja valitsemalla alhaalla oleva välilehti *Inbound Rules* (sisäänpäin suunnatun liikenteen säännöt), jonka jälkeen sääntö luotiin *Edit Rules* -painikkeella. Kuvassa 5 on esitetty asetukset säännölle, jossa liikenne sovelluspalvelimelle on sallittuna internetistä *HTTPS*-portin 443 kautta.



Kuva 5. Turvallisuusryhmien sisäänpäin suunnatun liikenteen konfigurointi (Amazon 2019i).

Kyseinen sääntö luotiin molemmille sovelluspalvelimille, sillä niiden pitää olla yhteydessä internettiin, jotta palvelun käyttäjät sekä etäohjelmointiyksiköt voivat muodostaa niihin yhteyden. Etäohjelmointitehtäviä suorittavalle sovelluspalvelimelle määritettiin 443 portin lisäksi myös 8443 *HTTPS*-portti. Turvallisuusryhmät luotiin seuraavia palvelimia varten, kuvion 1 perusteella:

- **sovelluspalvelin #1** (*HTTPS* 443)
- **sovelluspalvelin #2** (*HTTPS* 443, 8443)
- **hyppypalvelin** (*RDP* 3389)
- **tietokantapalvelin** (*TDS* 1433, sallittuna vain palvelimen omasta *VPC*-verkosta).

Jotta etätyöpöytäyhteys on mahdollista muodostaa palvelinympäristön sisäisestä virtuaaliverkosta molemmille sovelluspalvelimille, täytyi tätä varten luoda erillinen

turvallisuusryhmä. Ryhmälle asetettiin yhteyskäytänteeksi (*Protocol*) *RDP* ja portiksi 3389. Turvallisuusryhmän sisäänpäin suunnatun liikenteen asetuksiin määritettiin *Source*-kohtaan palvelinympäristön oman virtuaaliverkon *IPv4*-osoite, joka on esitetty tämän luvun alussa. Näillä asetuksilla etätyöpöytäyhteyden voi muodostaa sovelluspalvelimille vain palvelinympäristön omasta virtuaaliverkosta. Luodut turvallisuusryhmät lisättiin palvelinympäristöön tilattaville palvelininstansseille niiden tilaamisen jälkeen.

5.6 Tietokantapalvelimen tilaaminen

Tietokantapalvelin tilattiin *AWS*-hallinnointiportaalin *RDS*-palvelusta. Palveluun pääsi hakupalvelusta avainsanalla *RDS*. Tietokantaa tilattaessa tuli huomioida, että tilattava tietokantapalvelin vastasi ohjelmiston järjestelmävaatimuksia (liite 1).

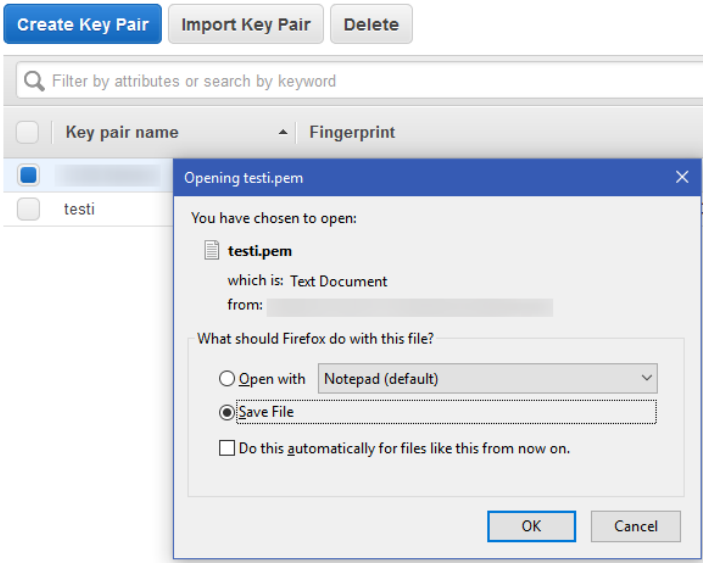
RDS-näkymässä tietokantapalvelimen tilausprosessi aloitettiin painikkeella *Create database*. *Select Engine* -näkymässä tietokantamoottoriksi valittiin *Microsoft SQL Server* sekä *SQL Server Standard Edition*, sillä nämä ovat ohjelmiston tukemat tietokantamoottori-tyypit. Tietokantainstanssin resurssit valittiin siten, että se vastaa tietokantapalvelimelle asetettuja järjestelmävaatimuksia. *Allocated storage* -kohtaan levytilan kooksi valittiin 100 GB, sillä se täyttää ohjelmiston järjestelmävaatimuksen asettamat vaatimukset.

Tietokantainstanssille määritettiin myös tunnistetieto, jolla se voidaan erottaa muista *AWS*-tilillä käytettävistä tietokantainstansseista. Samalla kyseiselle instanssille määritetiin *Master*-tason käyttäjätunnus sekä salasana. Tätä tunnusta käytetään tässä kohdassa luotavalle tietokantapalvelimelle kirjautumiseen.

Seuraavassa valikossa tämä tietokantapalvelin määritettiin toimimaan luvussa 4.1 selostettuun virtuaaliverkkoon *Amazon VPC* -kohdassa. *VPC security groups* -kohdassa valittiin *Choose Existing VPC Security groups* -kohtaan luvussa 5.5 luotu tietokantapalvelimen turvallisuusryhmä. Tietokanta luotiin painamalla sivun alaosasta *Create database* -painiketta.

5.7 Palvelininstanssien tilaaminen EC2-palvelun avulla

Palvelininstanssit tilattiin hallinnointikonsolissa *EC2*-palvelun avulla. Koska tietokantapalvelin tilattiin *Amazon RDS*-palvelun kautta, tarvitsi tämän palvelun kautta tilata vain sovelluspalvelimet sekä hyppypalvelin. Palveluun pääsee hakuvalikosta *EC2*-avainsanalla. Ensimmäisenä palvelimia varten luotiin avainpari[4] *EC2*-valikon vasemmassa laidassa olevasta *Key Pairs* -kohdasta *Create Key Pair* -painikkeella. Avainparille annettiin nimi, jonka jälkeen avainparin luotiin *Create*-painikkeella kuvan 6 mukaisesti. Tästä generoitui avaintiedosto, jota käytettiin kaikissa palvelinympäristöön tilattavissa palvelininstansseissa. Kyseistä tiedostoa käytettiin myös, kun instanssin käyttäjätileille luotiin salasanat.



Kuva 6. Avainparin luominen (Amazon 2019i).

Avainparin luomisen jälkeen tilattiin palvelininstanssit *EC2*-valikon vasemman laidan *Instances* -kohdan kautta *Launch instance* -painikkeella. *AMI*-tietoa valittaessa täytyi varmistaa, että virtuaalipalvelimeksi valittiin sovelluspalvelimen ohjelmiston järjestelmävaatimukset täyttävä virtuaalipalvelin (liite 1). Tämän jälkeen määritettiin, montako kappaletta tämänlaisia instansseja luodaan. Tässä kohti tilattiin kaksi instanssia samanlaisilla asetuksilla, nämä instanssit toimivat ohjel-

[4] Avainparia käytetään kirjautumistietojen salaamiseen sekä salauksen purkamiseen (Amazon 2019j).

miston sovelluspalvelimina. *VPC*-verkoksi valittiin luvussa 5.5 mainittu virtuaaliverkko. Instansseille ei määritetty tässä kohtaa julkista *IP*-osoitetta, joten kohtaan *Auto-assign Public IP* -kohtaan jätettiin oletusarvoisesti arvoksi *Disabled*.

Add Storage -kohdassa palvelininstansseille määritetään levytilan määrä siten, että se vastasi ohjelmiston järjestelmävaatimuksia. *Add Tags* -kohdassa instansseille on mahdollista määrittää tunnistetiedot, jotka helpottavat instanssien hallintaa. Koska instansseja tilatiin vain kolme kappaletta, tunnistetietoja ei tarvinnut luoda.

Configure security group -kohdassa instansseille on mahdollista määrittää luvussa 5.5 niille luodut turvallisuusryhmät. Sovelluspalvelimille nämä turvallisuusryhmät määritettiin jälkeenpäin, koska palvelininstanssille tulee asettaa vain kyseiselle instanssille tarkoitettu turvallisuusryhmä.

Review and Launch-valikossa varmistettiin tilattavien instanssien tiedot, jonka jälkeen instanssit tilattiin *Launch*-painikkeella. *AWS* alkoi tämän jälkeen pystyttämään tilattuja palvelimia, ja palvelimet olivat valmiita käytettäväksi, kun niiden *State*-tieto muuttui *Running*-tilaan.

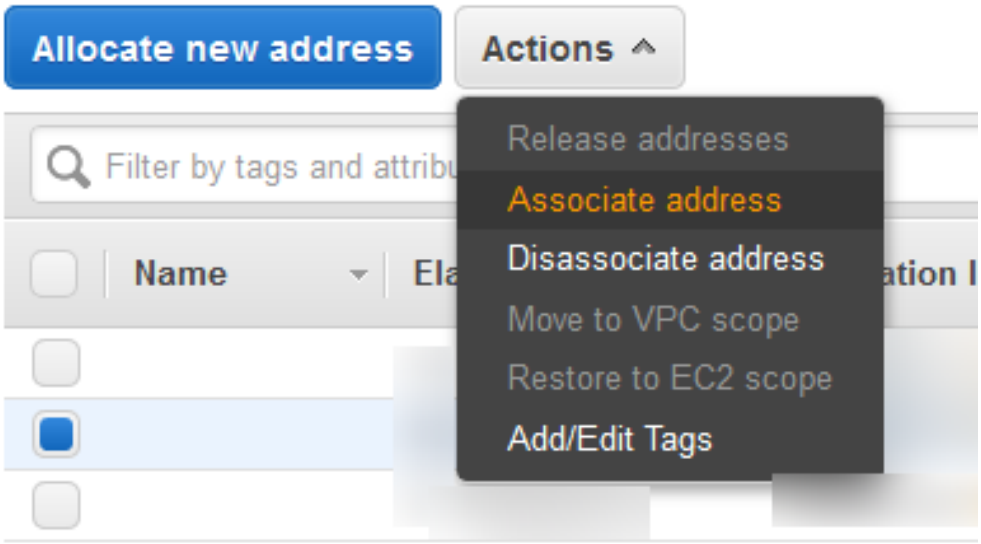
Palvelinympäristöön tilattiin tällä tavalla vielä hyppypalvelin. Hyppypalvelimen järjestelmävaatimuksia ei ole määritettynä, joten tätä varten tilattiin resursseiltaan pienempi palvelininstanssi.

5.8 Elastisen IP-osoitteen määritys

Jotta asiakaspäätteillä sekä etäohjelmointiyksiköillä on mahdollisuus luoda yhteys sovelluspalvelimiin, palvelimella on oltava julkinen *IP*-osoite. Luvussa 5.7 luoduille instansseille ei määritetty niiden tilausvaiheessa julkista *IP*-osoitetta. Tämä tieto määritettiin *EC2*-palvelun avulla elastisella *IP*-osoitteella. Elastisen *IP*-osoitteen etuna on sen käytettävyys: palvelimen äkillisen kaatumisen voi peittää tarvittaessa ohjaamalla liikenne toisen palvelimen käyttöön (Amazon 2019k). Elastinen *IP*-osoite on mahdollista määrittää mille tahansa *AWS*-tilin instanssille.

Elastinen *IP*-osoite luotiin *EC2*-näkymän vasemmassa reunassa olevasta valikosta *Elastic IPs. Allocate new address* -painikkeella luotiin uusi osoite, joka vahvistettiin *Allocate*-painikkeella. Tämä loi elastisen *IP*-osoitteen, joka voidaan määrittää halutulle palvelininstanssille.

Elastinen *IP*-osoite luotiin hyppypalvelimelle ja molemmille sovelluspalvelimille, jotta niihin voidaan muodostaa yhteys internetistä. Se määritettiin instanssille kuvan 7 mukaisesti, *Associate address* -painikkeella.



Kuva 7. Elastisen *IP*-osoitteen asettaminen instanssille (Amazon 2019i).

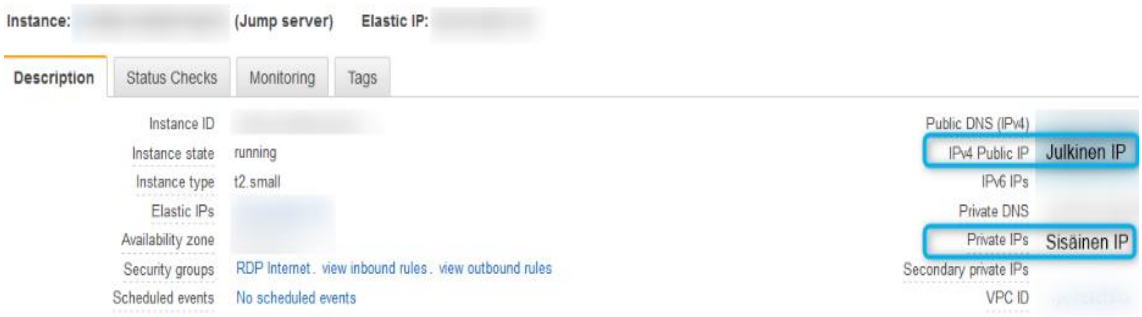
6 Virtuaalipalvelimien toimivuuden testaus

Tämä luku kuvaa toimenpiteet tilattujen palvelimien testaamista varten. Palvelimille tulee kyetä muodostamaan etätyöpöytäyhteys, sekä tietokantayhteyden tulee toimia hyppypalvelimelta tietokantapalvelimelle.

6.1 Etätyöpöytäyhteys

AWS-palvelusta tilattujen palvelimien toimivuus testattiin muodostamalla niihin etätyöpöytäyhteys. Tämä tehtiin hakemalla Windowsin haun[5] kautta palvelu nimeltä *Etätyöpöytäyhteys* (englanniksi *Remote Desktop Connection*). Koska suora etätyöpöytäyhteys internetistä sallittiin vain hyppypalvelimelle, muodostettiin etätyöpöytäyhteys ensimmäiseksi tähän palvelimeen.

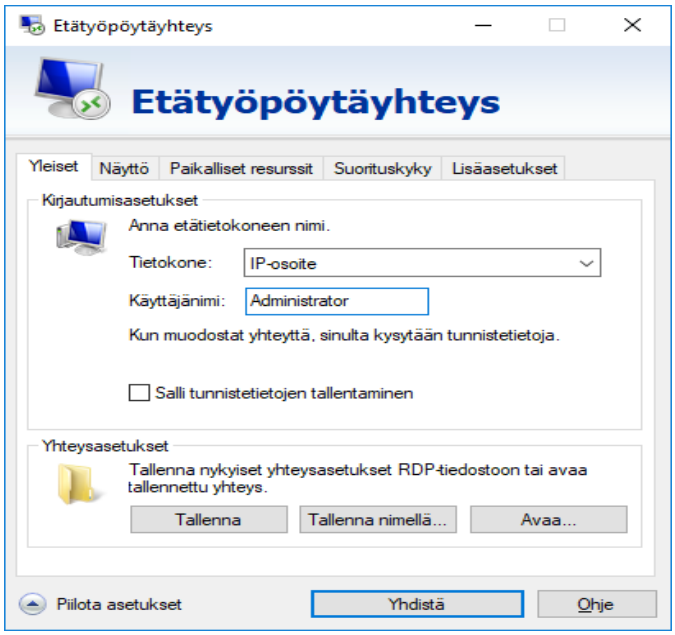
Yhteyden muodostamista varten tarvitaan joko tietokoneen nimi tai *IP*-osoite. Koska Internet ei tunne kyseistä tietokonetta nimellä, muodostettiin etätyöpöytäyhteys luvussa 5.8 luotuun hyppypalvelimen elastiseen *IP*-osoitteeseen. Hyppypalvelimen *IP*-osoitteen sai noudettua *AWS*-hallinnointikonsolin *EC2*-valikosta, *Instances*-välilehdeltä. Kun hyppypalvelin on valittuna, tieto löytyy *Description*-näkymän *Public IP*-kohdasta, kuvan 8 mukaisesti.



Kuva 8. Palvelininstanssin julkinen sekä sisäinen *IP*-osoite (Amazon 2019i).

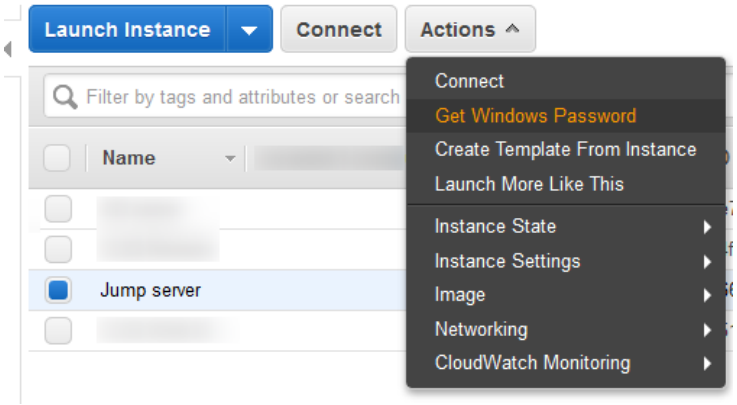
Kyseinen *IP*-osoite syötettiin Windowsin etätyöpöytäyhteys-palveluun, Tietokone-kohtaan. Käyttäjänimi oli AWS:in oletusarvoisesti määrittämä *Administrator*. Kuvassa 9 on esitetty, kuinka tiedot syötetään etätyöpöytäyhteys-palveluun.

[5] Windowsin haun saa päälle klikkaamalla työpöydän vasemmasta alakulmasta suurennuslasikuvaketta (Windows 10), ja kirjoittamalla tähän näkymään tekstiä



Kuva 9. Palvelimelle kirjautumiseen käytettävä etätyöpöytäyhteys.

Yhdistämisen jälkeen palvelu kysyi käyttäjätilin salasanaa. Salasana muodostettiin *AWS*-hallinnointikonsolissa *EC2*-valikossa valitsemalla hyppypalvelin, ja tämän jälkeen *Actions*-valikosta *Get Windows Password* -painikkeella kuvan 10 mukaisesti.



Kuva 10. Salasanan luominen palvelininstanssia varten (Amazon 2019i).

Tämän jälkeen palvelu pyysi valitsemaan luvussa 5.7 muodostetun avaintiedoston salasanan purkamista varten. Avaintiedoston valinnan jälkeen valittiin vaihtoehto *Decrypt Password*. Tästä *Administrator*-tilille generoitui salasana, jota käytetään palveluun kirjautumiseen. (Amazon 2019l.)

Salasanan etätyöpöytäpalveluun syöttämisen jälkeen palvelu antoi varoituksen ”*Etätietokoneen identiteettiä ei voi vahvistaa. Haluatko muodostaa yhteyden siitä huolimatta?”*. Tässä kohtaa valittiin *kyllä*, ja tämän jälkeen etätyöpöytäyhteys hyppypalvelimelle onnistui. Hyvien käytänteiden mukaisesti tämä *AWS*:in tarjoama oletusarvoinen salasana tulee muuttaa kirjautumisen jälkeen. (Amazon 2019l.)

Hyppypalvelimelta täytyi vielä testata etätyöpöytäyhteyksien muodostaminen palvelinympäristön sovelluspalvelimiin. Yhteys muodostettiin samalla tapaa kuin hyppypalvelimelle, tosin julkisen *IP*-tiedon sijasta tällä kertaa etätyöpöytäyhteyspalveluun syötettiin palvelimen sisäinen *IP*-osoite. Kyseinen tieto saatiin *AWS*-hallinnointikonsolista, samasta valikosta kuin palvelimien julkinen *IP*-osoite. Palvelimen sisäinen *IP*-osoite on nähtävillä *Private IPs*-kohdassa. Sovelluspalvelimille luotiin myös salasana samalla tapaa kuin hyppypalvelimelle, *AWS*-hallinnointikonsolin kautta.

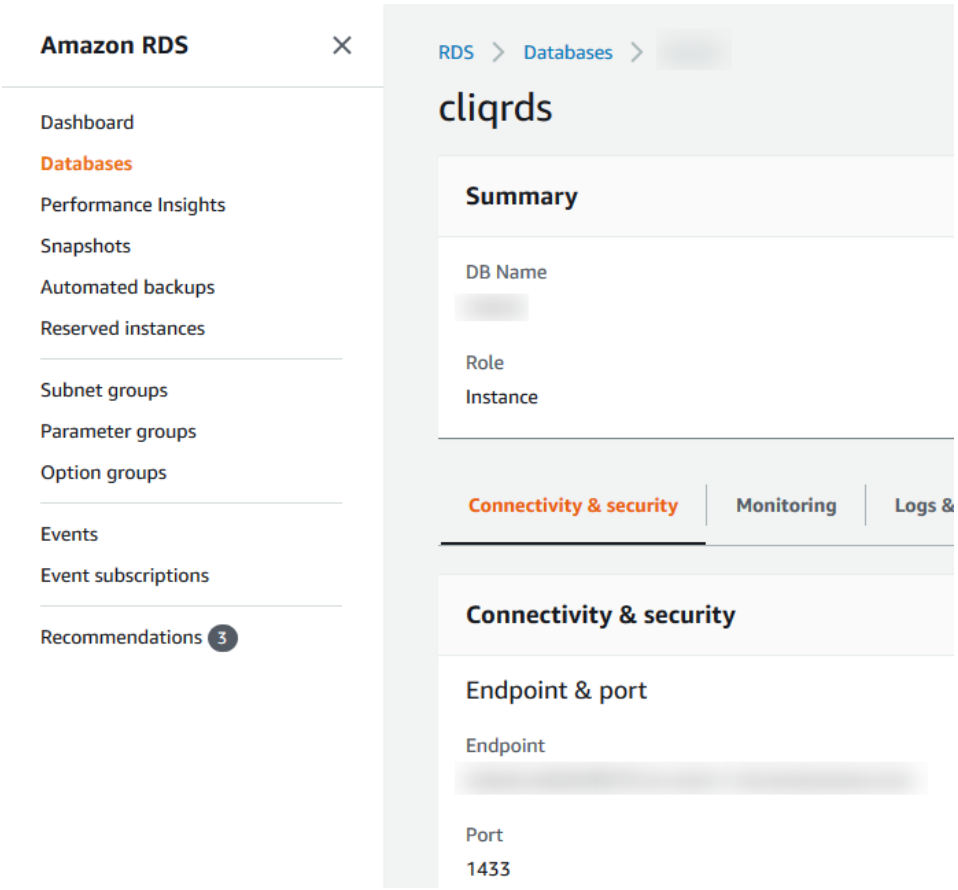
6.2 Tietokantapalvelinyhteys

Lopuksi täytyi tarkastaa, että yhteys tietokantapalvelimeen toimii. Tätä varten hyppypalvelimelle ladattiin sekä asennettiin *SQL Server Management Studio* -ohjelmisto. Ohjelmistolla otetaan yhteys tietokantapalvelimeen, joka tilattiin *AWS*:iltä luvussa 5.6. Ohjelmisto on maksuton, ja sen saa ladattua Microsoftin verkkosivuilta.

Ohjelmiston asennuksen jälkeen ohjelmisto käynnistettiin hakemalla se nimellä Windowsin haun kautta. Ohjelmisto kysyi tämän jälkeen seuraavia tietoja:

- **palvelimen nimi** (*Server name*) saatiin *AWS*-hallinnointikonsolin kautta *RDS*-valikosta *Databases*-välilehdeltä valitsemalla luvussa 5.6 tilattu tietokantapalvelin. Palvelimen nimi -kenttään syötettiin tämän tietokantapalvelininstanssin *Endpoint*-tieto, joka on esitetty kuvassa 11

- **tunnistautuminen** (*Authentication*) -kohtaan valittiin *SQL Server Authentication*, sillä kirjautumiseen käytetään luvussa 5.6 luotuja *Master*-tason käyttäjätunnuksia
- **kirjautumistunnus** (*Login*) sekä **salasana** (*Password*) -kenttiin syötettiin käyttäjätunnukseksi luvussa 5.6 luotu *Master*-tason käyttäjätunnus.



Kuva 11. Tietokantapalvelimen *Endpoint*-tiedon hakeminen (Amazon 2019i).

Etätyöpöytäyhteyksien sekä tietokantapalvelimelle kirjautumisen onnistuttua voitiin todeta, että palvelinympäristön tietoliikenneyhteydet toimivat, ja seuraavaksi palvelimille voi alkaa asentamaan toimeksiantajan asiakkailleen tarjoamaa *SaaS*-palvelua.

7 Työn tulokset

Edellä kuvattujen työvaiheiden jälkeen toimeksiantajalle rakentui toimiva palvelinympäristö, johon voidaan asentaa toimeksiantajan asiakkailleen tarjoama ohjelmisto. Toimeksiantajan toimihenkilöt voivat suorittaa ohjelmiston testiasennuksen palvelimille.

Tässä opinnäytetyössä tehty toiminnallinen osuus toimii myös käyttöohjeena toimeksiantajalle, mikäli toimeksiantaja kokee tarpeelliseksi pystyttää uusia palvelinympäristöjä. Tässä työssä tuotettua ohjeistusta on myös mahdollista käyttää muidenkin kuin toimeksiantajan toimesta, sillä se kuvaa yleisellä tasolla, kuinka palvelinympäristön voi pystyttää *AWS*-palveluun.

Opinnäytetyön aihealueeseen ei kuulunut asiakkaan *SaaS*-palveluna tarjottavan ohjelmiston asennus ja testaus. Koska virtuaalipalvelimet tilattiin *AWS*:iltä toimeksiantajan käyttämän ohjelmiston järjestelmävaatimuksia noudattaen, ei ohjelmiston asennuksen ja käytön osalta pitäisi ilmetä ongelmia. Toimeksiantajan tulee vielä huomioida palvelinten tietoturva sekä käyttäjänhallinta omana kokonaisuutenaan.

Toimeksiantajalla on nyt käytössä opinnäytetyössä pystytetty palvelinympäristö *Saas*-palveluna tarjottavan ohjelmiston testikäyttöä varten. Täten opinnäytetyölle asetetut vaatimukset täyttyivät.

8 Pohdinta

Aikataulu opinnäytetyön valmistumiselle oli toukokuu 2019. Sain työn päätökseen reilusti ennen alkuperäistä aikataulua. Tämän mahdollisti se, että sain järjestettyä työlle tarpeeksi aikaa sekä tarvittavat resurssit toimeksiantajalta. Aikataulua laatiessani huomioin mahdolliset riskit, kuten muiden samanaikaisesti suoritettavien kurssien aiheuttamat kiireet ja toimeksiantajan aikataulumuutokset.

Kokonaisuutena tämä aihe oli erittäin opettavainen, sillä minulla ei ollut aikaisempaa kokemusta virtuaalipalvelinympäristöjen pystyttämisestä. Suurin osa opinnäytetyössäni käsitellyistä aiheista oli itselleni uutta, joten työn teknistä osuutta suorittaessani minulla kului paljon aikaa termien sekä erilaisten teknologioiden ominaisuuksien oppimiseen.

Amazonilla on saatavilla paljon materiaaleja pilvipalvelinympäristöjen ylläpidon helpottamiseksi, ja näistä oli suuri apu työn teknistä osuutta suoritettaessa. Toimeksiantajan IT-henkilöstö osasi myös tarjota tukea palvelinympäristöihin kohdistuneissa, hankalimmissa ongelmanratkaisutilanteissa.

Palvelinympäristön jatkokehitystä ajatellen palvelimille olisi hyvä ottaa käyttöön edistyneempi käyttäjänhallintajärjestelmä, esimerkiksi *Windowsin Active Directory* -palvelu. Tämän avulla palvelinympäristön käyttäjiä on helpompi hallinnoida, ja niille voidaan tarvittaessa asentaa erilaisia käyttöoikeuksien rajoituksia, mikäli esimerkiksi käyttäjien ei haluta voivan tehdä muutoksia palvelimien tärkeimpiin ominaisuuksiin. Samaten palvelimet voisi liittää myös käyttämään samaa toimialuetta palvelimien hallinnoinnin helpottamiseksi. Tämä on mahdollista, sillä ne sijaitsevat samassa virtuaaliverkossa.

Haastavinta opinnäytetyön suorittamisessa oli aiheenvalinta ja -rajaus. Aiheenvalinnassa kesti pitkään, mutta onnistuin löytämään aiheen, joka kiinnosti minua, ja jolla oli potentiaalia kasvattaa ammatillista osaamistani huomattavasti. Työtä tehdessä huomasin, että aihealue oli liian laaja, eikä kokonaisuus vaikuttanut kovinkaan helppolukuiselta tai järkevästi toteutettavalta. Onnistuin kuitenkin rajaamaan aiheen ja lopputuloksesta saatiin selkeä kokonaisuus.

Opinnäytetyön suorittamisen jälkeen koen omaavani riittävän osaamisen tason palvelinympäristön pystyttämiseksi *AWS*-pilvipalvelualustalle ja opin paljon uutta *SaaS*-palvelumallista. Samalla myös raportin laadintataitoni kehittyivät huomattavasti. Pääsin hyödyntämään Karelia AMK:ssa ja työelämässä opittuja taitoja, tämän ansiosta työn toteuttaminen ei tuntunut missään vaiheessa liian raskaalta.

Lähteet

Aitoa. 2019. Mikä on SSL-sertifikaatti, mikä https on ja miksi. https://www.aitoa.fi/ssl-sertifikaatti-mika-on-ja-miksi. 17.3.2019.

Amazon. 2019a. Amazon EC2. https://aws.amazon.com/ec2/. 6.2.2019.

Amazon. 2019b. Security Groups for your VPC. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html. 14.3.2019.

Amazon. 2019c. Amazon Virtual Private Cloud. https://aws.amazon.com/vpc/. 7.2.2019.

Amazon. 2019d. Amazon Relational Database Service (RDS). https://aws.amazon.com/rds/. 14.2.2019.

Amazon. 2019e. AWS Identity and Access Management (IAM). https://aws.amazon.com/iam/. 14.2.2019.

Amazon. 2019f. AWS Global Infrastructure. https://aws.amazon.com/about-aws/global-infrastructure/. 8.3.2019.

Amazon. 2019g. AWS Service Health Dashboard. https://status.aws.amazon.com/govcloud. 8.3.2019.

Amazon. 2019h. The AWS Account Root User. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html. 8.3.2019.

Amazon. 2019i. Amazon Management Console. https://aws.amazon.com/console/. 14.3.2019.

Amazon. 2019j. Amazon EC2 Key Pairs. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html. 17.3.2019.

Amazon. 2019k. Elastic IP Addresses. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-eips.html. 17.3.2019.

Amazon. 2019l. Connecting to your Windows Instance. https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/connecting_to_windows_instance.html. 17.3.2019.

Apprenda. 2019. Iaas, Paas, Saas (Explained and Compared). https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/. 20.3.2019.

Elprocus. 2019. Know about Access Control Systems and Their Types with Features. https://www.elprocus.com/understanding-about-types-of-access-control-systems/. 17.3.2019.

Hur, J. 2019. The History of SaaS. Bebusinessed. https://bebusinessed.com/history/the-history-of-saas/. 9.4.2019.

Jaakkola, I. 2012. Pieni tietohallinto pieneen tarpeeseen. Tivi. https://www.tivi.fi/Arkisto/2012-05-31/Pieni-tietohallinto-pieneen-tarpeeseen-3192212.html. 9.4.2019.

Mäkilä, T. 2011. Pilviohjelmistot – Pienyrityksen opas. Turku: Turku Science Park.

Peterson, J. 2017. What does “logical isolation” in computer networking actually mean. Quora. https://www.quora.com/What-does-logical-isolation-in-computer-networking-actually-mean. 9.4.2019.

Pilvi. 2019. Mikä on SaaS-palvelu. https://www.pilvi.com/fi/mika-on-saas-palvelu/. 18.3.2019.

Rojas, A. 2017. A Brief History of AWS. Mediatemple. https://mediatemple.net/blog/news/brief-history-aws/. 9.4.2019.

Rouse, M. 2005. pseudocode. Whatis. https://whatis.techtarget.com/definition/pseudocode. 9.4.2019.

Sarja, J. 2006. Relaatiotietokanta. Verkkopedagogi. https://verkkopedagogi.net/vanhat/fi/sisalto/materiaalit/access2003/luku0375c6.html?C:D=419702&selres=419702. 9.4.2019.
Techopedia. 2019. Software as a Service (SaaS). https://www.techopedia.com/definition/155/software-as-a-service-saas. 14.2.2019.
Toimeksiantaja. 2019. Ohjelmiston tietoliikenteen kuvaus.
Turvakolmio. 2017. Mikä on elektromekaaninen lukitus. https://turvakolmio.fi/news/2017/10/19/mit-on-elektromekaaninen-lukitus. 9.4.2019.

Ohjelmiston järjestelmävaatimukset

Sovelluspalvelimet

Palvelin:	Windows Server 2012 tai uudempi
Prosessori:	64 bittinen, 2 GHz, 4 ydintä
Keskusmuisti:	8 GB
Levytila:	20 GB

Tietokantapalvelin

Palvelin:	Windows Server 2012 tai uudempi
Tietokanta:	SQL Server 2012 Std 64 bittinen tai uudempi, SQL Server Express -versio ei ole tuettu
Prosessori:	64 bittinen, 2 GHz, 4 ydintä
Keskusmuisti:	8 GB
Levytila:	100 GB

Asiakaspääte

Käyttöjärjestelmä:	Windows Vista Windows 7 Pro/Ent/Ult (32 tai 64 bittinen) Windows 8 (64 bittinen) Windows 10 (64 bittinen)
Prosessori:	Kykenevä suorittamaan yllä mainittuja käyttöjärjestelmiä yhteensopivan internetselaimen kanssa
Keskusmuisti:	Kykenevä suorittamaan yllä mainittuja käyttöjärjestelmiä yhteensopivan internetselaimen kanssa
Internetselain:	Internet explorer 11 (32 bittinen) Firefox 60.0.1 tai uudempi (32 bittinen) Firefox 60 ESR tai uudempi (32 bittinen) Edge