Pauli Vuolle-Apiala

Finanssialan tekoälysovelluksen tuotannollistaminen ja operointi pilviympäristössä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

29.04.2025

Tiivistelmä

Tekijä:	Pauli Vuolle-Apiala
Otsikko:	Finanssialan tekoälysovelluksen tuotannollistaminen ja operointi pilviympäristössä
Sivumäärä:	57 sivua
Aika:	29.04.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Ohjelmistotuotanto
Ohjaajat:	Simo Silander, FM Kari Nousiainen, TkT

Insinöörityössä tutkittiin LähiTapiola Palvelut Oy:n toimeksiannosta erään tekoälysovelluksen tuotannollistamista ja käyttöönottoa Microsoft Azure -pilviympäristössä. Työn tavoitteena oli mahdollistaa tekoälysovelluksen tuotantokäyttö sekä varmistaa, että sovellus toimi sille asetettujen toiminnallisten ja tietoturvavaatimusten mukaisesti. Lisäksi ratkaisun tuli mahdollistaa tekoälysovelluksen jatkokehittäminen sekä siirtäminen eri ympäristöihin automaattisen koonnin putkien avulla.

Työn aikana kehitettiin Azure DevOps -ympäristöön automaattisen koonnin putket, jotka rakensivat tekoälysovelluksen vaatiman infrastruktuurin ja julkaisivat tekoälysovelluksen kehitys- ja tuotantoympäristöihin. Infrastruktuuri verkkoeriytettiin virtuaaliverkkojen avulla, ja sen määrittely toteutettiin infrastruktuuri koodina -periaatteen mukaisesti Bicep-kielellä.

Insinöörityön tuloksena syntyi malli tekoälysovellusten tuotannollistamiseen ja käyttöönottoon Azure-pilviympäristössä. Toteutettu ratkaisu täytti sille asetetut vaatimukset, ja se on osoittautunut toimivaksi ja luotettavaksi tavaksi saattaa tekoälysovellus tuotantokäyttöön.

Avainsanat: Azure, DevOps, Prompt Flow, OpenAI, Bicep, Infrastructure as Code, Virtuaaliverkko, Private Link, Tekoäly

---

Abstract

Author:	Pauli Vuolle-Apiala
Title:	Production Deployment and Operation of Cloud AI Application in Financial Sector
Number of Pages:	57 pages
Date:	29 April 2025
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Software Engineering
Supervisors:	Simo Silander, M.Sc Kari Nousiainen, D.Sc. (Tech.)

This thesis introduces the production deployment and operation of an AI application in the Microsoft Azure cloud environment. The main objective of the study was to ensure that the AI application could reliably be used in production, while meeting both the practical and security requirements set to it. The second objective was to implement the solution in a way that enables both the future development of the application, as well as the deployment of the application to different environments through automated deployment pipelines.

During the study, automated pipelines were created using Azure DevOps. These pipelines built the infrastructure needed by the AI application and deployed the application to both development and production environments. The infrastructure was secured using virtual networks, and all configurations were defined using the Bicep language, following Infrastructure as Code principles.

The result of the study is a practical solution for deploying AI applications to production in Azure cloud environments. The developed solution met all the requirements set to it and proved to be an effective and reliable method for deploying AI applications to production.

Keywords: Azure, DevOps, Prompt Flow, OpenAI, Bicep, Infrastructure as Code, Virtual Network, Private Link, AI

Sisällys

Lyhenteet

CI/CD: *Continuous Integration/Continuous Development.* Automaattisen koonnin putket, jotka mahdollistavat muutosten integroimisen sovelluksiin.

CLI: *Command Line Interface.* Komentoliittymä, joka mahdollistaa kommunikoinnin tietokoneohjelman kanssa komentoriviä käyttäen.

IAC: *Infrastructure as Code*. Infrastruktuurin rakentaminen ja hallinnointi koodipohjaisesti määritystiedostojen avulla, joka mahdollistaa esimerkiksi versionhallinnan.

ADO: *Azure DevOps*. Azuren tarjoama ympäristö, joka toimii muun muassa versionhallinnan sekä automaattisen koonnin putkien alustana.

YAML: *Yet Another Markup Language.* Merkintäkieli, joka on helposti luettava ja ymmärrettävä. Käytetään muun muassa ADO:n automattisen koonnin putkien konfiguraatiotiedostona.

JSON: *JavaScript Object Notation*. Avain-arvo-pareihin perustuva tiedostomuoto.

GHAZDO: *GitHub Advanced Security for Azure DevOps*. Tietoturvatyökalu, jonka avulla ohjelmistojen haavoittuvuuksia voidaan tarkkailla automatisoidusti.

1 Johdanto

Insinöörityössä tutkitaan erään tekoälysovelluksen tietoturvallista käyttöönottoa ja operointia modernissa pilviympäristössä. Käyttöönotto tapahtui Azure-pilviympäristössä, jonne sovellus koottiin automaattisen koonnin putkien (lyh. CI/CD) avulla. Käyttöönoton jokaisen vaiheen täytyi tapahtua koodipohjaisesti, jotta ratkaisu täytti tuotanto-operoinnin vaatimukset. Insinöörityön aikana tekoälysovellukselle ja sen käyttöönoton toteutukselle tehtiin vaatimusmäärittely. Sovellukselle luotiin vaatimusmäärittelyn mukaiset, tuotantokelpoisen prosessin muodostavat skriptit tietoturvallisen infrastruktuurin luomiseen sekä tekoälysovelluksen kokoamiseen ja julkaisuun.

Työ toteutettiin LähiTapiola Palvelut Oy:lle. Käyttöönotettu tekoälysovellus automatisoi liiketoimintaan liittyvää prosessia. Käyttötapaus oli tekoälysovellukselle otollinen, sillä prosessi on rutiininomaista ja tarkkaa työtä. Tekoälysovelluksen tuotannollistaminen loi toistettavan ja tuotantokelpoisen prosessin tulevien tekoälysovellusten kehittämiselle ja operoinnille tuotantokäytössä.

Tekoälysovelluksen käyttöönoton prosessin keskeiset vaiheet olivat infrastruktuurin luonti sekä sovelluksen ohjelmakoodin kokoaminen ja julkaiseminen. Infrastruktuurin luovat koodipohjaiset määrittelyt toteutettiin Microsoftin kehittämällä Bicep-kielellä. Koodipohjaiset määrittelyt mahdollistivat tekoälysovelluksen vaatimien resurssien ohjelmallisen rakentamisen Azure-pilviympäristöön. Sovelluksen ohjelmakoodi koottiin ja julkaistiin käyttäen Azuren tarjoamia työkaluja.

Tekoälysovelluksen käyttöönotossa täytyi huomioida erityisesti tietoturvaa. Liiketoiminnan prosessin käyttämät tiedot saattoivat sisältää henkilötietoja, joten tietoliikenteen tuli tapahtua kokonaan yksityisen verkon sisällä. Insinöörityössä huomioidaan tietoturvavaatimuksia erityisesti infrastruktuurin koodipohjaisessa määrittelyssä sekä Azure DevOps -ympäristön toteutuksessa ja määrittelyssä.

Insinöörityön ensimmäisessä luvussa määritellään työn tavoitteet ja taustoitetaan aihetta. Toisessa luvussa tarkastellaan Microsoft Azure -pilviympäristön keskeisiä käsitteitä, kuten esimerkiksi resurssiryhmiä sekä tilauksia. Kolmannessa luvussa käsitellään Azure-pilviympäristön verkkoeriytystä virtuaaliverkkojen ja Private Link -palvelun avulla. Neljäs luku keskittyy koneoppimisresursseihin, ja niiden käyttöön tekoälysovelluksen julkaisuprosessissa. Viidennessä luvussa tarkastellaan infrastruktuuri koodina -periaatteen mukaista toteutusta Bicep-kielellä. Kuudes luku käsittelee Azure DevOps ympäristöä ja esittelee insinöörityön aikana kehitetyt automaattisen koonnin putket, jotka loivat tekoälysovelluksen vaatiman infrastruktuurin sekä kokosivat ja julkaisivat tekoälysovelluksen pilviympäristöön.

2 Tavoitteet

Insinöörityön tavoite oli toteuttaa erään tekoälysovelluksen tuotannollistaminen ja käyttöönotto pilviympäristössä. Tekoälysovellus kehitettiin LähiTapiola Palvelut Oy:n toimesta, ja insinöörityön tekijä osallistui sen kehitystyöhön. Insinöörityössä ei esitellä tekoälysovellusta tai sen toimintaa tarkemmin, sillä ne ovat liiketoiminnan kannalta sensitiivistä tietoa. Tekoälysovellus on insinöörityön kirjoittamisen hetkellä tuotantokäytössä.

Tuotannollistetun ratkaisun tuli mahdollistaa sovelluksen jatkokehittäminen ja kokoaminen eri ympäristöihin automaattisen koonnin putkien avulla. Lisäksi automaattisen koonnin putkien tuli varmistaa, että sovelluksen toiminta on sille asetettujen toiminnallisten vaatimusten mukaista.

Toiminnallisten vaatimusten lisäksi ratkaisun tuli täyttää sille asetetut tietoturvavaatimukset. Valmiin sovelluksen tuli olla täysin verkkoeriytetty siten, että yhteyden muodostaminen sovelluksen rajapintaan oli mahdollista vain keskitetyn rajapintahallintajärjestelmän kautta. Rajapintahallintajärjestelmää tai sen toimintaa

ei esitellä insinöörityössä tarkemmin, sillä ne eivät ole työn tavoitteiden tai sisällön kannalta oleellisia.

Tekoälysovelluksen infrastruktuurin muodostavien Azure-resurssien tuli olla julkiselta verkolta piilotettuja. Lisäksi sovelluksen rajapinnan käytölle sekä sovelluksen versionhallinnalle ja Azure-resursseille asetettiin tiukat käyttöoikeusvaatimukset, jotta pääsy- ja käyttöoikeus voitiin sallia vain hyväksytyille käyttäjille.

Insinöörityön lopputulokset, kuten esimerkiksi Azure-resurssit, sovelluksen ohjelmakoodi sekä automattisen koonnin putket ovat nähtävillä Azure DevOps -ympäristössä sekä Azure-pilvipalvelussa. Insinöörityön tavoitteita voidaan tarkastella yksityiskohtaisemmin jakamalla ne näihin kahteen osa-alueeseen.

2.1 Azure DevOps (ADO)

2.1.1 Automaattisen koonnin putket

Insinöörityön yhtenä keskeisimmistä tavoitteista oli automaattisen koonnin putkien kehittäminen Azure DevOps -ympäristössä. Putket mahdollistivat tekoälysovelluksen ohjelmakoodin automatisoidun kokoamisen ja julkaisun Azure-pilviympäristöön. Automaattisen koonnin putket kehitettiin sekä sovelluksen ohjelmakoodin kokoamiseen että sovelluksen vaatiman Azure-infrastruktuurin rakentamiseen. Putkien tuli olla parametrisoitavia ja ympäristöstä riippumattomia kokonaisuuksia, jotka ajettaessa mahdollistavat tekoälysovelluksen käyttöönoton halutussa Azure-pilviympäristössä.

Infrastruktuurin rakentava automaattisen koonnin putki ajoi Bicep-kielellä kirjoitetun määrittelytiedostot, joiden suoritusta parametrisoitiin JSON-konfiguraatiotiedoston avulla. Tiedostoissa määriteltiin luotavat resurssit sekä niiden halutut ominaisuudet. Konfiguraatiotiedosto sisälsi tiedon käytettävästä ympäristöstä, jonne määrittelytiedostot loivat resurssit. Resurssien ominaisuuksia muokattiin käytettävän ympäristön mukaan, käyttäen esimerkiksi laadukkaampaa datan varmuuskopiointia vain tuotantoympäristössä.

Infrastruktuurin rakentavan putken ajoja ei tarvinnut ajastaa tai automatisoida, sillä kehitys- ja tuotantoympäristöjen resurssit luotiin vain silloin, kun sovellus haluttiin ottaa käyttöön uudessa ympäristössä. Työn aikana tekoälysovelluksen kehitys- ja tuotantoympäristöjen resurssit eroteltiin toisistaan resurssiryhmien avulla. Jatkokehityksessä tavoitteena on eristää tuotantoympäristö omaan tilaukseensa, joka mahdollistaa tiukemman käyttöoikeuksien valvonnan sekä tietoturvan.

Sovelluksen ohjelmakoodin kokoava automaattisen koonnin putki kokosi koodin viimeisimmän version ja loi sille rajapinnan infrastruktuuriputken luomaan koneoppimistyötilaan (engl. *Machine learning workspace*). Lisäksi ohjelmakoodin kokoamisen putki loi resurssit, joita koneoppimistyötila tarvitsee toimiakseen.

Automaattisen koonnin putkien tuli olla parametrisoitavia ja itsenäisesti ajettavia työprosesseja. Ne mahdollistivat tekoälysovelluksen siirtämisen ja monistamisen eri Azure-tilausten tai ympäristöjen välillä parametrejä muuttamalla.

2.1.2 Tietoturva

Insinöörityön aikana toteutetun ratkaisun tuli olla tietoturvallinen. Tietoturvan toteutus Azure DevOps -ympäristössä oli jaettavissa kolmeen osa-alueeseen, jotka olivat yhteys verkkoeriytettyyn Azure-ympäristöön, käyttöoikeuksien valvonta sekä koodin haavoittuvuuksien tunnistaminen.

Yhteyden muodostaminen verkkoeriytettyyn ympäristöön tapahtui Azuren virtuaaliverkkojen kautta. Yhteys muodostettiin virtuaaliverkossa sijainneeseen virtuaalikoneeseen, jolle asennettiin Microsoftin julkaisema agenttiohjelmisto, joka mahdollisti virtuaalikoneen rekisteröimisen DevOps-agentiksi. Automaattisen koonnin putket suoritettiin DevOps-agentilla, jolloin prosessi suoritettiin tietoturvallisesti virtuaaliverkon sisällä julkiverkolta piilossa.

Käyttöoikeuksia valvottiin Azure DevOps -ympäristön tarjoaman käyttöoikeushallinnan avulla. Käyttöoikeuksia annettiin ja rajattiin käyttäjän roolin mukaan.

Vain sallituilla henkilöillä oli oikeus muokata versionhallinasta löytyvää ohjelmistokoodia ja automaattisen koonnin putkien konfigurointitiedostoja. Myös automaattisen koonnin putkien ajo-oikeuksia rajattiin.

Python-ohjelmistokoodin haavoittuvuuksia tunnistettiin *GitHub Advanced Security for Azure DevOps* -palvelun (lyh. *GHAZDO*) avulla, jota ajettiin automatisoidusti viikon välein. Työkalu tunnisti mahdolliset haavoittuvuudet Python-pakettien versioissa. Tunnistettu haavoittuvuus korjattiin joko päivittämällä tai korvaamalla paketti.

2.2 Azure-pilvipalvelu

2.2.1 Infrastruktuuri

Tekoälysovelluksen vaatiman infrastruktuurin tietoturvallisuus ja skaalautuvuus olivat keskeisiä luotettavan tuotantokäytön takaamiseksi. Infrastruktuuri koodina -periaatteen mukaiset määrittelyt mahdollistivat toistettavan ympäristöjen luomisen, vähentäen samalla virheiden riskiä. Määrittelyt sisälsivät tarkat konfiguraatiot resursseille, mikä paransi ympäristön hallittavuutta ja mahdollisti sen versionhallinnan. Määrittelyt toimivat tekoälysovelluksen infrastruktuurin palautumissuunnitelmana, joka mahdollisti ympäristön nopean uudelleen rakentamisen.

2.2.2 Tietoturva

Luotettava ja aukoton tietoturva Azuressa oli insinöörityön eräs keskeisimmistä tavoitteista. Insinöörityön aikana toteutettu tietoturva koostui verkkoeriytyksestä, käyttöoikeuksienhallinnasta sekä Entra ID -pohjaisesta tunnistautumisesta.

Verkkoeriytys toteutettiin Private Link -palvelulla. Tekoälysovelluksen tietoliikenteen tuli olla salattua ja julkiverkolta piilossa, sillä sovellus saattoi vastaanottaa arkaluontoista syötetietoa. Tekoälysovelluksen vaatimat resurssit verkkoeriytettiin virtuaaliverkkojen avulla. Virtuaaliverkon avulla resurssit oli mahdollista

piilottaa julkiverkolta niin, että niiden sisältämät resurssit pystyivät kuitenkin kommunikoimaan keskenään käyttäen yksityisiä IP-osoitteita virtuaaliverkon sisällä. Virtuaaliverkosta oli mahdollista avata yhteys rajapintahallintajärjestelmään palomuuriavausten avulla, jolloin tuotantoprosessien oli mahdollista lähettää pyyntöjä tekoälysovelluksen rajapinnalle.

Tekoälysovellukselle luotujen resurssien käyttöoikeuksien valvonta toteutettiin Azuren *Role Based Access Control* -palvelun (lyh. *RBAC)* avulla. RBAC-palvelu mahdollisti resurssien käyttöoikeuksien rajaamisen Microsoft Entra -palvelua käyttäen. Resurssien käyttöoikeuksien tuli olla tarkkaan rajattu niin, että vain hyväksytyt henkilöt pystyivät näkemään resurssien ominaisuuksia, tekemään niihin muutoksia tai käyttämään niitä.

3 Microsoft Azure -pilviympäristö

Microsoft Azure on LähiTapiolan ensisijainen pilviympäristö. Insinöörityössä tuotannollistettava ja käyttöönotettava tekoälysovellus on kehitetty ja viety tuotantoon kyseisessä pilviympäristössä. Insinöörityössä perehdyttiin erityisesti tekoälyn, koneoppimisen sekä verkkoeriyttämisen resursseihin, jotka muodostivat tekoälysovelluksen vaatiman pilvi-infrastruktuurin. Infrastruktuurin avulla määriteltiin ja toteutettiin skaalautuva sekä toimintavarma alusta, joka täytti LähiTapiolan tietoturvavaatimusten asettamat kriteerit tekoälysovelluksen tuotantokäytölle.

3.1 Pilviympäristöt

Pilviympäristöt ovat moderni vaihtoehto perinteisille palvelinkeskuksille. Ne tarjoavat perinteisiä palvelinkeskuksia korkeamman skaalautuvuuden ja kustannustehokkaamman käytön. Pilviympäristöt ovat yleensä toimittajan tarjoamia ja ylläpitämiä, mikä säästää pilviympäristöä käyttävältä asiakasyritykseltä sekä ajallisia että rahallisia resursseja. (Collier & Shahan 2015: 17.) Tunnettuja pilviympäristöjä ovat esimerkiksi *Microsoft Azure*, *Amazon Web Services* sekä *Google Cloud*.

Perinteiset palvelinkeskukset edellyttävät yrityksiltä merkittäviä sijoituksia esimerkiksi tietoliikenneverkkoihin, laitteistoihin sekä niiden konfigurointeihin. Palvelinkeskusten hallinta ja ylläpito jäävät tällöin yrityksen vastuulle, mikä aiheuttaa jatkuvia kustannuksia. Lisäksi perinteisten palvelinkeskusten skaalautuvuus on usein rajallista, sillä laitteisto, joka muodostaa palvelinkeskuksen kapasiteetin, on hankittava etukäteen. Tämän seurauksena kapasiteetin kasvattaminen myöhemmässä vaiheessa voi vaatia merkittäviä lisäsijoituksia, kun taas käyttämättömän kapasiteetin ylläpito voi aiheuttaa tarpeettomia, jatkuvia kustannuksia. (Collier & Shahan 2015: 17-18.)

Pilviympäristöjä on erilaisia riippuen niiden käyttötarkoituksista ja teknisistä vaatimuksista. Esimerkiksi julkiset pilviympäristöt (engl. *public cloud*), jollainen Microsoft Azure -pilviympäristö on, tarjoavat merkittäviä etuja perinteisiin palvelinkeskuksiin verrattuna. Julkisen pilviympäristön tarjoaja on vastuussa laitteiston hankinnasta ja konfiguroinneista, ympäristön pystyttämisestä sekä ympäristön jatkuvan toimivuuden takaamisesta asiakkaan käytössä. Lisäksi ympäristössä tarjotaan usein erilaisia valmiita palveluita tai sovelluksia, joita asiakas voi ottaa käyttöönsä. (Collier & Shahan 2015: 17-18.)

Julkisissa pilviympäristöissä hyödynnetään usein kulutuspohjaista hinnoittelumallia, jossa asiakasyritys maksaa pilviympäristön tarjoajalle vain käyttämistään resursseista, kuten esimerkiksi palveluista, sovelluksista, laskentatehosta tai tietovarastoinnista. Pilviympäristön tarjoaja voi laskuttaa asiakasta tämän käyttämistä resursseista kiinteän summan esimerkiksi kuukausittain, tai vaihtoehtoisesti laskuttaa käytetyistä resursseista tuntipohjaisesti, mikä kuvaa resurssien todellista käyttöastetta. (Collier & Shahan 2015: 17-18.) Insinöörityössä käytetyistä resursseista maksettiin pääsääntöisesti tuntiperusteisen hinnoittelun mukaisesti, mikä ei välttämättä ole kustannustehokasta. Kiinteän hinnoittelun malli olisi todennäköisesti ollut edullisempi, jos resurssien käyttöasteita olisi pystytty ennakoimaan etukäteen.

Julkisten pilviympäristöjen lisäksi vaihtoehtoina ovat myös yksityiset pilviympäristöt (engl. *private cloud*) sekä näiden yhdistelmänä toteutetut hybridiympäristöt

(engl. *hybrid cloud*). Yksityisessä pilviympäristössä asiakas toteuttaa ja ylläpitää pilviympäristön laitteistoa omassa palvelinkeskuksessaan, jolloin ympäristön hallinta ja ylläpitovastuu ovat kokonaan asiakkaalla. Hybridiympäristössä julkinen ja yksityinen pilviympäristö yhdistyvät siten, että resursseja voidaan hyödyntää molemmista ympäristöistä käyttötarpeen mukaan. Esimerkiksi hybridiympäristössä asiakas voi tarjota verkkopalvelua julkisen pilven kautta ja ylläpitää sen käyttämää tietokantaa yksityisessä pilviympäristössä. (Collier & Shahan 2015: 18.)

Insinöörityössä toteutettu ratkaisu käytti Azuressa hybridipilviympäristöä, josta oli mahdollista muodostaa yhteys LähiTapiolan sisäverkkoon. Tämä mahdollisti tekoälysovelluksen rajapinnan kutsumisen LähiTapiolan sisäverkosta käsin, jolloin sovellusta hyödyntävien prosessien oli mahdollista käyttämään rajapintaa tietoturvallisesti.

3.2 Yleinen katsaus Microsoft Azure -pilviympäristöön

Microsoft Azure -pilviympäristö tarjoaa käyttäjille laajan valikoiman palveluita ja työkaluja. Azuren käyttäjät voivat luoda ja hyödyntää pilviresursseja tarpeidensa mukaan. Käyttäjät voivat esimerkiksi rakentaa Azuren tarjoamien resurssien avulla sovelluksilleen niiden tarvitseman infrastruktuurin. Azure veloittaa käytetyistä resursseista niiden käyttöasteen mukaan, tyypillisesti tuntipohjaisesti.

3.2.1 Datakeskukset

Microsoft Azure on toteutettu maailmanlaajuisten datakeskusten avulla, mikä takaa palvelun korkean saatavuuden eri puolilla maailmaa. Maailmanlaajuiset datakeskukset hyödyntävät myös Azuren käyttäjiä, sillä ne mahdollistavat käyttäjien rakentamien sovellusten ja palveluiden tarjonnan ympäri maailmaa. (Collier & Shahan 2015: 18.) Lisäksi datakeskukset mahdollistavat käyttäjien resurssien monistuksen (engl. *redundancy*). Monistus mahdollistaa käyttäjien resurssien tai datan monistamisen eri datakeskuksiin, mikä lisää Azuren palveluiden vikasietoisuutta. Esimerkiksi tietokannat ja Storage Account -resurssit tukevat

monistamista Azuressa. (Collier & Shahan 2015: 106.) Insinöörityössä monistustoiminnallisuutta hyödynnettiin erityisesti tuotantoympäristön resursseissa.

3.2.2 Pilvipalvelumallit

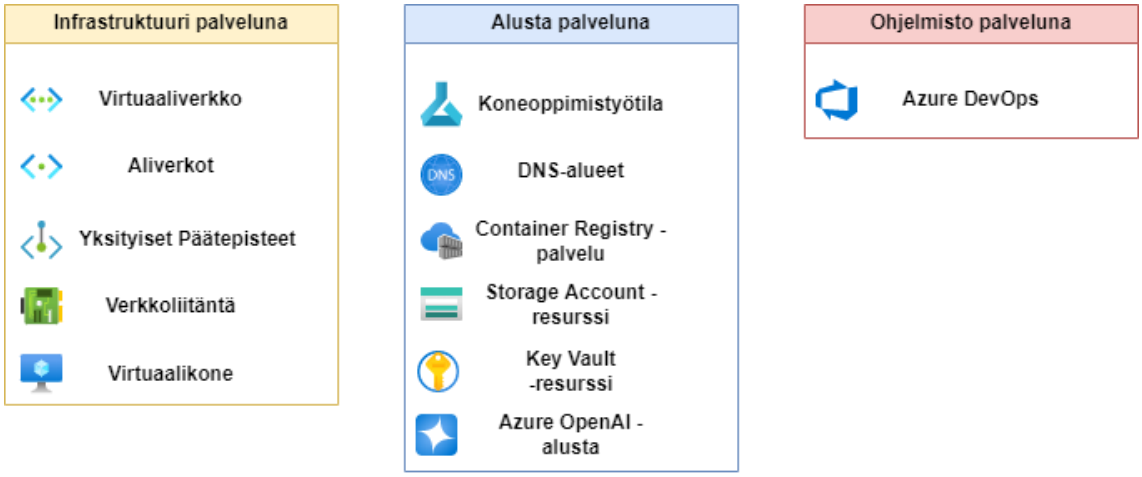
Azuren tarjoamat resurssit ja palvelut ovat luokiteltavissa erilaisiin pilvipalvelumalleihin. Jos käyttäjällä on esimerkiksi tarve perustaa oma palvelin, voi hän luoda virtuaalikoneresurssin. Käyttäjä voi hallita virtuaalikoneen käyttöjärjestelmää, samalla, kun Azure vastaa fyysisen laitteiston ylläpidosta. Virtuaalikone edustaa infrastruktuuri palveluna -mallia (engl. *Infrastructure as a Service*, lyh. *IaaS*). (Collier & Shahan 2015: 19.)

Infrastruktuuri palveluna -mallissa pilvipalvelun tarjoaja ylläpitää palvelinkeskusta eli infrastruktuuria, jonne käyttäjä voi luoda esimerkiksi virtuaalikoneen. Käyttäjä saa virtuaalikoneelle laajan hallintaoikeuden esimerkiksi käyttöjärjestelmän ja ohjelmistojen asentamista varten. Palvelumallissa virtuaalikoneen ylläpito jää käyttäjän vastuulle, ja tämän on huolehdittava esimerkiksi käyttöjärjestelmän päivityksistä. Palvelumallin nimen mukaisesti käyttäjä siis vain vuokraa palvelinkeskuksen infrastruktuuria palveluntarjoajalta. Muita infrastruktuuri palveluna -mallin mukaisia tuotteita Azuressa ovat esimerkiksi virtuaalikoneet sekä virtuaaliverkot, joita kumpaakin hyödynnettiin insinöörityössä toteutetussa verkkoeriytyksessä. (Collier & Shahan 2015: 19.)

Alusta palveluna -mallissa pilvipalvelun tarjoaja ylläpitää sovellusten ajamiseen tarvittavaa alustaa ja siihen liittyvää infrastruktuuria. Alustan käyttäjät voivat esimerkiksi suorittaa sovelluksiaan tällä alustalla ilman, että heidän tarvitsee hallinnoida alustan infrastruktuuria. Pilvipalvelun tarjoaja päivittää ja ylläpitää alustan muodostavaa infrastruktuuria, tarjoten käyttäjille valmiin ja ylläpidetyn alustan sovelluksille. (Collier & Shahan 2015: 19.) Esimerkki alusta palveluna -mallin tuotteista Azuressa on *Azure OpenAI* -alusta, jota insinöörityössä tuotannollistettava tekoälysovellus käytti. Alustalla julkaistiin (engl. *Deploy*) tekoälymalleja, jotka olivat alustan ylläpitämiä ja joista maksettiin käyttöasteen mukaan.

Infrastruktuuri palveluna- ja alusta palveluna -mallien lisäksi kolmas yleisesti käytetty malli on ohjelmisto palveluna -malli (engl. *Software as a Service*, lyh. *SaaS*). Ohjelmisto palveluna -mallissa pilvipalvelun tarjoaja ylläpitää sekä sovellusta että sen vaatimaa infrastruktuuria käyttäjän puolesta. Käyttäjät voivat käyttää valmista ohjelmistoa niin, että pilvipalvelun tarjoaja vastaa täysin sen ylläpidosta sekä saatavuudesta. Esimerkiksi Azure DevOps -ympäristö on ohjelmisto palveluna -mallin mukainen tuote, joka toimi insinöörityössä kehitettyjen automaattisen koonnin putkien ajoympäristönä. Tyypillisesti ohjelmisto palveluna -mallin tuotteita tarjotaan jatkuvana kuukausi- tai vuosipohjaisena tilauksena. (Collier & Shahan 2015: 19.)

Insinöörityössä hyödynnettyjen resurssien ja palveluiden voidaan katsoa edustavan kaikkia kolmea palvelumallia. Käytettyjen resurssien ja palveluiden voidaan katsoa jakautuvan palvelumalleihin kuvan 1 mukaisesti. Kuvassa tehty luokittelu ei kuitenkaan ole ehdoton, ja osan resursseista ja palveluista voisi katsoa kuuluvan useampaan kuin yhteen palvelumalliin. Esimerkiksi Storage Account -resurssin voisi tulkita sekä infrastruktuuri palveluna- että alusta palveluna -palvelumallin mukaiseksi resurssiksi.



Kuva 1. Insinöörityössä hyödynnytetyt Azure-resurssit pilvipalvelumalleittain.

Insinöörityössä keskeisenä filosofiana oli hyödyntää mahdollisimman paljon valmiita alustoja ja hallinnoituja palveluita. Tällä pyrittiin vähentämään tuotantoratkaisun ylläpidon tarvetta.

3.2.3 Käyttöoikeudet (RBAC)

Käyttöoikeuksien hallinta toteutetaan Azuressa RBAC -palvelulla (*Role Based Access Control*). Sen avulla hallitaan käyttäjien, ryhmien tai sovellusten käyttöoikeuksia Azure-resursseihin. Järjestelmä perustuu roolimääritelmiin (engl. *role definition)*, käyttäjiin sekä roolimäärityksiin (engl. *role assignment)*. Käyttäjille voidaan määrittää rooleja, jotka antavat oikeudet esimerkiksi hallita resursseja tai suorittaa niillä tiettyjä toimintoja. Käyttäjät voivat olla joko yksittäisiä käyttäjiä, käyttäjäryhmiä tai erilaisia sovellusten tunnistautumiseen liittyviä palveluita ja yhteyksiä. (Rajendran 2023.)

Sovellusten valtuutusta ja tunnistautumista varten Azure tarjoaa esimerkiksi palvelukäyttäjiä (engl. *Service Principal*) sekä hallittuja identiteettejä (engl. *Managed Identity*). Palvelukäyttäjät ovat keskeinen osa sovellusten tunnistautumista, ja niiden avulla sovelluksille voidaan määrittää käyttöoikeuksia ilman varsinaisten käyttäjätilien luomista. Hallitut identiteetit voidaan ajatella eräänlaisina palvelukäyttäjinä, jotka joko Azure tai käyttäjä voi luoda ja kiinnittää resursseihin. Esimerkiksi virtuaalikoneresurssi voi hallitun identiteetin avulla tunnistautua ja käyttää muita Azure-resursseja, jos identiteetille määritetyt RBAC-roolit sen sallivat. (Rajendran 2023.)

RBAC-roolit muodostavat oikeudet, jotka määrittelevät, mitä toimintoja käyttäjä tai resurssi voi Azuressa suorittaa. Oikeuksia on mahdollista rajata laajuuksien (engl. *scope*) avulla. Mahdollisia laajuuksia ovat esimerkiksi resurssiryhmät, yksittäiset resurssit tai kokonaiset tilaukset (engl. *subscription*). (Rajendran 2023.) Tekoälysovelluksen käyttöoikeuksien hallinta toteutettiin RBAC-roolien avulla.

Azure tarjoaa laajan valikoiman valmiiksi määriteltyjä RBAC-rooleja. Lisäksi käyttäjien on mahdollista määritellä omia, räätöityjä roolejaan. Roolien

räätälöinti on suotavaa esimerkiksi silloin, kun valmiit RBAC-roolit sisältävät liian laajoja oikeuksia käyttötapaukseen nähden. Insinöörityössä tuotannollistetun tekoälysovelluksen käyttäjille määriteltiin räätälöity RBAC-rooli, joka sisälsi vain tarvittavat käyttöoikeudet tekoälysovelluksen rajapinnan kutsumiseen. Räätälöity rooli määritettiin palvelukäyttäjälle, joka oli luotu tekoälysovelluksen tuotantokäyttöä varten.

3.2.4 Tilaukset ja hallintaryhmät

Azuren palveluiden käyttäminen edellyttää tilausta (engl. *subscription*). Tilaus on looginen yksikkö, joka tarjoaa todennetun pääsyn Azuren palveluihin ja mahdollistaa resurssien luonnin ja hallinnan. Tilaukset toimivat Azuressa rajaamisenkeinoina. Ne toimivat laskutusrajauksena, jolloin Azuresta syntyviä kustannuksia voidaan seurata tilauskohtaisesti, sekä käyttöoikeusrajauksena, jolloin käyttäjille tai käyttäjäryhmille voidaan antaa pääsy tietyille tilauksille. Ne mahdollistavat myös resurssien loogisen rajaamisen, kuten esimerkiksi kehitys- ja tuotantoympäristöjen resurssien erottelun resurssiryhmää ylemmällä tasolla. (Tank 2023.)

Hallintaryhmät (engl. *management groups*) helpottavat Azure-tilausten hallintaa. Azure-tilaukset kuuluvat hallintoryhmiin, mikä mahdollistaa keskitetyn hallinnan sekä hierarkkisen rakenteen muodostamisen. Hallintaryhmiin on mahdollista asettaa linjauksia, jotka voivat esimerkiksi rajoittaa Azuren toiminnallisuuksia toivotulla tavalla. Hallintaryhmään määritetyt linjaukset ja käyttöoikeudet periytyvät hallintaryhmään kuuluville tilauksille, mikä helpottaa linjausten ja käyttöoikeuksien hallintaa. (Tank 2023.) Hallintaryhmien asettamiin linjauksiin ja rajoitteisiin on mahdollista pyytää poikkeuslupaa.

Insinöörityössä tuotannollistettava tekoälysovellus kehitettiin eräällä LähiTapiolan Azure-tilauksella, missä se on kirjoittamisen hetkellä tuotantokäytössä. Tilauksen hallintaryhmä asettaa tilaukselle monia linjauksia ja rajoitteita, kuten esimerkiksi rajoitteen resurssien maantieteelliselle sijainnille. Rajoitteet huomioitiin insinöörityön aikana toteutetussa tuotannollistamisen ratkaisussa. Niitä

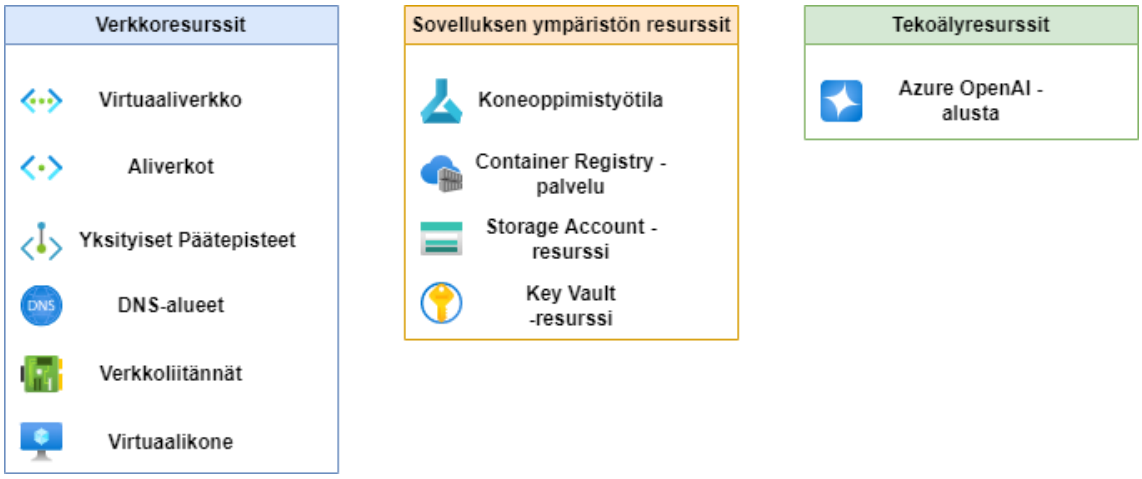
noudatettiin lukuun ottamatta rajoitetta resurssien maantieteelliselle sijainnille, johon haettiin poikkeuslupaa AI-resurssien osalta.

3.2.5 Resurssiryhmät

Insinöörityön aikana tekoälysovellukselle luotiin Azuren tarjoamien resurssien avulla ympäristö, jonka tuli olla tarkkaan valvottavissa. Ympäristöä varten luotiin oma *resurssiryhmä* (engl. *Resource group*), johon kaikki tekoälysovelluksen ympäristön muodostavat resurssit sijoitettiin. Resurssiryhmän käyttöoikeudet rajattiin tarkkaan RBAC-rooleilla ympäristön turvallisuuden varmistamiseksi.

Resurssiryhmät ovat Azuren resurssienhallinnan eräs keskeisimmistä käsitteistä. Ne tarjoavat loogisen tavan järjestää ja hallita resursseja, mahdollistaen resurssien ryhmittelyn niiden käyttötarkoituksen mukaan. Ne mahdollistavat myös resurssien käsittelyn yhtenä kokonaisuutena, mikä helpottaa esimerkiksi infrastruktuurin hallintaa sekä käyttöoikeusrajauksien toteuttamista. Esimerkiksi kuluja on mahdollista tarkastella resurssiryhmätasolla, mikä helpottaa tekoälysovelluksen käyttämien resurssien juoksevien kulujen seurantaa. (What is Azure Resource Manager? 2025.)

Insinöörityössä määriteltiin kolme eri resurssiryhmää eri käyttötarkoituksia varten. Kuva 2 esittää resurssien jakautumista resurssiryhmittäin. Resurssiryhmien jakoon päädyttiin, sillä resurssit olivat selkeästi jaettavissa käyttötarkoitustensa mukaan. Ensimmäinen resurssiryhmä sisälsi toteutetun ratkaisun verkkoresurssit, kuten esimerkiksi virtuaaliverkon sekä Private DNS -alueet. Toinen resurssiryhmä sisälsi Azure OpenAI -alustan. Kolmanteen resurssiryhmään sijoitettiin tekoälysovelluksen ympäristön muodostavat resurssit, kuten esimerkiksi koneoppimistyötila.



Kuva 2. Insinöörityön aikana muodostetut resurssiryhmät. Verkkoresurssit, ympäristön muodostavat resurssit sekä tekoälyresurssit ovat eriytettynä omiin resurssiryhmiinsä.

Erityisesti Azure OpenAI -alustan eriyttäminen omaan resurssiryhmäänsä osoittautui hyödylliseksi. Kyseiseen resurssiryhmään täytyi tilata poikkeuslupa luoda resursseja muihin kuin sallittuihin sijainteihin, sillä alusta ei tarjonnut kaikkia tarvittuja ominaisuuksia Länsi- ja Pohjois-Euroopan sijainneilla, jotka ovat ainoat hallintaryhmän linjauksissa sallitut sijainnit.

3.3 Azure CLI -komentorivityökalu

Azure CLI (*Command Line Interface*) on resurssien hallintaan tarkoitettu komentorivityökalu. Työkalu mahdollistaa resurssien hallinnan suorittamalla komentoja komentoriviltä tai skripteistä, ja se tukee Windows-, Linux- ja macOS-ympäristöjä. Sen komennot ovat syntaksiltaan yksinkertaisia ja helposti luettavia. (What is Azure CLI? 2025.) Työkalua voidaan laajentaa useilla eri lisäosilla, kuten esimerkiksi koneoppimisen resursseihin keskittyvällä ML-laajennuksella, mikä mahdollistaa komentorivityökalun soveltamisen moniin eri käyttötarkoituksiin Azuressa.

Azure-pilviympäristön resursseja on mahdollista luoda useilla eri tavoilla, kuten esimerkiksi Azure CLI -komentorivityökalulla sekä Bicep- ja Terraform-kielillä. Resurssien luonti on mahdollista myös *portaalista* käsin, joka on Azure-

pilviympäristön verkkopohjainen käyttöliittymä. Resurssien luominen portaalin kautta ei kuitenkaan jätä toistettavia jälkiä, minkä vuoksi insinöörityössä ratkaisun toteuttamisessa edellytettiin, että resurssit luodaan Bicep-määrittelytiedostojen tai Azure CLI -komentorivityökalun avulla.

Insinöörityössä Azure CLI -komentorivityökalua, ja erityisesti sen ML-laajennusta, hyödynnettiin automaattisen koonnin putkissa MLOps-sapluunoiden kautta. Tekoälysovelluksen koneoppimistyötilan sisäiset komponentit luotiin komentorivityökalua käyttäen.

3.4 Azure LähiTapiolassa

Azure on LähiTapiolan pääpilviympäristö. LähiTapiolalla on useita linjauksia ja rajoitteita, joita tuotantokäytössä olevien pilviympäristöjen tulee noudattaa. Linjauksien ja rajoitteiden noudattamista valvotaan esimerkiksi hallintaryhmien avulla.

Linjaukset ja rajoitteet ohjaavat esimerkiksi resurssien luomista Azure-ympäristöissä. Keskeisiä linjauksia ja rajoitteita resurssien luomiselle ovat esimerkiksi rajoite resurssien maantieteelliselle sijainnille, jonka tulee olla joko Länsi- tai Pohjois-Eurooppa. Linjaukseen on mahdollista pyytää poikkeuslupaa, mikä sallii resurssien luomisen muilla maantieteellisillä sijainneilla. Lisäksi Azuren virtuaalikoneresurssien luomista julkisilla IP-osoitteilla on rajoitettu, mikä pienentää virheen riskiä resurssia luodessa.

LähiTapiolan linjaukset määräävät, että tuotantokäytön sovelluksille tulee olla tuotantokäyttöä varten osoitettu Azure-tilauksensa. Tällä pyritään erottamaan tuotantoresurssit muista ympäristöistä, mikä helpottaa tuotantoympäristön resurssien valvontaa ja hallintaa. Lisäksi tilausten eriyttäminen helpottaa esimerkiksi laskutuksen seurantaa sekä käyttöoikeuksien hallintaa.

Insinöörityön aikana monet linjauksista vaikuttivat tekoälysovelluksen tuotannollistamisen prosessiin. Yksi keskeisistä linjauksista oli kielto käyttää

esikatselutilassa olevia työkaluja tai palveluja tuotantosovelluksissa. Kehittäjien vastuulla oli valvoa tämän linjauksen noudattamista. Linjaus aiheutti insinöörityön aikana haasteita, sillä useat tekoälyresurssit ja niiden ohjelmointikirjastot olivat insinöörityön aikaan esikatselutilassa. Linjausta kuitenkin noudatettiin, eikä tekoälysovellus tai sen tuotannollistamisen ratkaisu hyödynnä esikatselutilassa olevia työkaluja tai palveluita. Muita insinöörityön kannalta keskeisiä linjauksia olivat vaaditut infrastruktuuri koodina -periaatteen mukaiset määrittelyt tuotannon pilviratkaisuille sekä Entra ID -tunnistautumismekanismin käyttö aina, kun se oli mahdollista.

4 Verkkoeriytys Azuressa

Verkkoeriytys on keskeinen osa turvallisen pilviympäristön suunnittelua. Insinöörityössä tuotannollistetulle tekoälysovellukselle lähetettävä data saattoi sisältää arkaluontoisia tietoja. Tekoälysovelluksen oli täten oltava piilossa julkiverkolta, jolloin yhteyden muodostaminen sovellukseen oli mahdollista vain LähiTapiolan sisäverkosta.

Azure tarjoaa verkkoeriyttämiseen useita työkaluja, kuten esimerkiksi virtuaaliverkot (engl. *virtual network*) sekä yksityiset päätepisteet (engl. *private endpoints*). Verkkoeriyttäminen oli merkittävä ja tärkeä osa insinöörityötä, ja se toteutettiin Microsoftin parhaiden käytänteiden mukaisesti.

4.1 Virtuaaliverkot

Virtuaaliverkot ovat loogisia verkkorakenteita, joiden avulla voidaan eristää ja yhdistää Azure-pilviympäristössä toimivia resursseja. Ne toimivat pilviympäristön sisäisinä lähiverkkoina, jotka mahdollistavat resurssien välisen kommunikoinnin hallinnan. Virtuaaliverkot mahdollistavat turvallisten yhteyksien luonnin Azuren ulkopuolisiin verkkoihin, kuten esimerkiksi internetiin tai yrityksen sisäverkkoon. (What is Azure Virtual Network? 2025.)

Virtuaaliverkkoja tarvitaan turvallisen ja hallittavan Azure-pilviympäristön rakentamiseen. Niiden avulla voidaan estää luvattomat yhteydet, ohjata verkkoliikennettä sekä varmistaa, että vain tietyillä resursseilla on mahdollisuus kommunikoida keskenään tai ulkoisten verkkojen kanssa. (What is Azure Virtual Network? 2025.) Yhteyksien hallinta oli erityisen tärkeää tekoälysovelluksen tuotantoympäristössä, josta sallittiin yhteys vain keskitettyyn rajapintahallintajärjestelmään.

Virtuaaliverkko määritellään Azure-pilviympäristössä IP-osoiteavaruuden avulla, jonka IP-osoitteet varataan vain virtuaaliverkon käyttöön. Osoiteavaruus on mahdollista jakaa aliverkkoihin, jotka tarjoavat keinon jakaa osoiteavaruus eri käyttötarkoitusten mukaan. Resurssit liitetään näihin aliverkkoihin, ja niiden välistä liikennettä virtuaaliverkon sisällä voidaan hallita esimerkiksi verkon suojausryhmien (engl. *Network security group*), reititystaulukoiden (engl. *Routing table*) sekä yksityisten päätepisteiden avulla. Kokonaisia virtuaaliverkkoja voidaan yhdistää toisiinsa virtuaaliverkkoliitosten (engl. *Virtual network peering*) avulla, jolloin eri verkkojen resurssit voivat kommunikoida keskenään turvallisesti. (What is Azure Virtual Network? 2025.)

Verkon suojausryhmät ja reititystaulut mahdollistavat virtuaaliverkon ja sen aliverkkojen turvaamisen ohjaamalla ja rajoittamalla niihin saapuvaa liikennettä. Verkon suojausryhmät mahdollistavat erityisesti tietoliikenteen hallinnan. Niihin määritellään sääntöjä, jotka joko sallivat tai estävät liikennettä esimerkiksi IP-osoitteen, portin tai tietoliikenneprotokollan perusteella. (Network security groups 2025.) Reititystaulut taas määrittävät, miten verkon tietoliikenne reititetään eri kohteisiin. Reitityssäännöt sisältävät osoiteavaruuden ja seuraavan verkkokohteen, kuten esimerkiksi virtuaaliverkon tai palomuurin, johon tuleva tietoliikenne reititetään. (Virtual network traffic routing 2025.)

Insinöörityössä tuotannollistettua tekoälysovellusta varten luotiin oma virtuaaliverkkonsa. Virtuaaliverkko pilkottiin kolmeen aliverkkoon käyttötarkoitusten mukaan, jotka olivat kehitys, tuotanto ja integraatio. Kokonaisuudet oli eriytettävä toisistaan hallittavuuden takaamiseksi.

Kehitysaliverkkoa käytettiin sovelluksen ja infrastruktuurin kehitystyöhön sekä automaattisen koonnin putkien testaamiseen. Tuotantoaliverkko toimi sovelluksen tuotantoympäristön verkkona, johon sovellus ja sen vaatima infrastruktuuri koottiin automaattisen koonnin putkien avulla. Integraatioaliverkko sisälsi erityisesti integraatiotarkoituksiin tarkoitettuja resursseja, kuten Azure DevOps -agentin käyttämän virtuaalikoneen, jonka toimintaa kuvataan tarkemmin insinöörityön myöhemmässä luvussa.

Aliverkoille määriteltiin verkon suojausryhmä sekä reititystaulu, joiden avulla virtuaaliverkkoon pääsy sallittiin vain tietyistä IP-osoiteavaruuksista. Kaikkiin aliverkkoihin sallittiin HTTP-protokollaan perustuva liikenne portin 443 kautta, jonka lisäksi integraatioaliverkkoon sallittiin TCP-protokollan mukainen liikenne portilta 22. Tämä mahdollisti SSH-yhteyden muodostamisen virtuaaliverkon sisältä integraatioaliverkossa sijainneisiin virtuaalikoneisiin.

4.2 Private Link

Azure Private Link -palvelu mahdollistaa yksityisten ja suojattujen yhteyksien muodostamisen virtuaaliverkossa Azure-resurssien ja palveluiden välillä. Yhteys kulkee yksityisten päätepisteiden kautta, jolloin verkkoliikenne ohjautuu Microsoftin taustaverkon (engl. *Backbone network*) kautta ja pysyy näin julkiverkolta piilossa. Tämä mahdollistaa resurssien eristämisen julkiverkosta, mikä taas mahdollistaa turvallisen verkkoliikenteen tuotantoympäristössä. (What is Azure Private Link? 2025.) Yksityinen päätepiste liitetään suoraan resurssiin, minkä seurauksena resurssiin kiinnitetään verkkoliitäntä (engl. *Network interface*), joka määrittää resurssille yksityisen IP-osoitteen virtuaaliverkon osoiteavaruudesta.

Private Link -palvelun käyttö on tärkeää, kun halutaan varmistaa, että sovelluksen tai palvelun liikenne pysyy kokonaan piilossa julkiverkolta. Private Link -palvelu mahdollistaa myös palveluiden ja -resurssien käytön tietoturvallisesti on prem -ympäristöistä käsin ilman, että liikenne kulkee julkiverkon kautta. (What is Azure Private Link? 2025.)

Private Link -palvelu otetaan käyttöön luomalla yksityinen päätepiste virtuaaliverkkoon ja liittämällä se haluttuun resurssiin, mikä mahdollistaa suojatun yhteyden muodostamisen resurssiin virtuaaliverkon sisältä. Päätepisteen luonnin yhteydessä määritellään tarvittavat ominaisuudet, kuten mihin aliverkkoon päätepiste kiinnitetään sekä sen käyttämät DNS- eli nimenselvennyspalvelut (*Domain Name System*). (What is a private endpoint? 2025.)

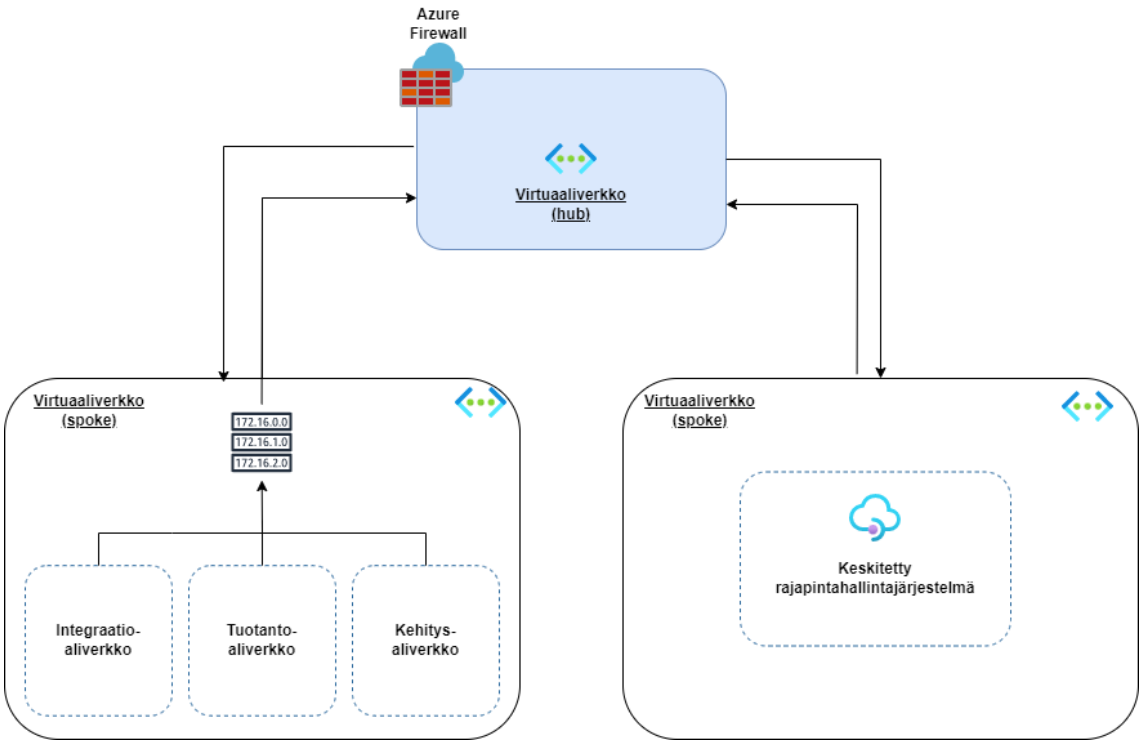
Private Link -palvelu oli keskeinen osa insinöörityössä tuotannollistetun tekoälysovelluksen arkkitehtuuria. Tekoälysovellus hyödynsi useita erilaisia resursseja, kuten esimerkiksi koneoppimis- sekä tekoälyresursseja. Private Link -palvelu mahdollisti näiden resurssien tietoturvallisen kommunikoinnin virtuaaliverkossa piilottaen tekoälysovelluksen tietoliikenteen julkiverkolta.

4.3 Hub-and-spoke-verkkotopologia

Hub-and-spoke-arkkitehtuuri on eräs Azuren suosittelemista verkkotopologioista. Topologian keskeiset osat ovat spoke-verkot sekä keskitetty hub-verkko, johon useat spoke-verkot liitetään. Azuren hub-and-spoke-verkkotopologiassa hub- ja spoke-verkot ovat toisiinsa liitettyjä virtuaaliverkkoja. Hub-verkko sisältää keskitetyt palvelut, kuten esimerkiksi DNS-palvelun, palomuurin ja yhteydet sisäverkkoihin, ja toimii tietoliikenteen väylänä spoke-verkkojen välillä. Spoke-verkkojen välinen tietoliikenne kulkee hub-verkon kautta. Hub-and-spoke-verkkotopologia soveltuu Azure-pilviympäristöihin erityisesti skaalautuvuutensa ansiosta. (Hub-spoke network topology in Azure 2025.)

Hub-and-spoke-verkkotopologia sopii erityisesti käytettäväksi verkkoihin, joissa halutaan yhdistää keskitetty hallinta ja verkkojen eriyttäminen. Topologia tukee esimerkiksi erilaisten ympäristöjen verkkojen hallintaa, mahdollistaen samalla yhteiset ja keskitetyt palvelut. Keskitetty arkkitehtuuri yksinkertaistaa reititystä spoke-verkkojen välillä, lisää verkon turvallisuutta ja selkeyttää verkon valvontaa. Lisäksi hub-verkko voi toimia keskitettynä yhdyskäytävänä sisäverkkojen sekä Azuren verkkojen välillä, mikä mahdollistaa hybridiratkaisut. (Hub-spoke network topology in Azure 2025.)

Insinöörityön aikana luotiin virtuaaliverkko, johon tekoälysovelluksen kehitys- ja tuotantoympäristö sijoitettiin. Luotu virtuaaliverkko toimi spoke-verkkona hub-and-spoke-mallin mukaisesti. Virtuaaliverkkoa varten luotiin reititystaulu, joka ohjasi tietoliikenteen hub-verkon palomuurille. Kuva 3 havainnollistaa toteutetun verkkoratkaisun rakennetta.



Kuva 3. Toteutetun verkkoratkaisun rakenne. Aliverkoista lähtevä liikenne ohjataan hub-verkolle reititystaulujen avulla.

Tekoälysovelluksen tuotantokäyttöä varten tilattiin palomuuriavaus, mikä mahdollisti tietoliikenteen tekoälysovelluksen käyttämän virtuaaliverkon ja LähiTapiolan keskitetyn rajapintahallintajärjestelmän välillä. Palomuuriavauksella sallittiin liikenne rajapintajärjestelmästä tekoälysovelluksen käyttämän virtuaaliverkon IP-osoiteavaruuteen.

4.4 DNS-palvelut

Azure Private DNS -palvelu on valmis nimenselvennyspalvelu (engl. *Domain Name System*, lyh. *DNS*), joka mahdollistaa nimenselvennyksen

virtuaaliverkoissa ilman erillistä DNS-ratkaisua. Palvelu muodostuu yksityisistä DNS-alueista (engl. *DNS zones*), johon DNS-tietueet (engl. *DNS records*) sijoitetaan. Yksityiset DNS-alueet voidaan liittää virtuaaliverkkoihin, joiden halutaan käyttävän nimenselvennyksessä kyseisiä DNS-alueita. Yksityiset DNS-alueet eivät ole selvennettävissä internetistä käsin, jolloin nimenselvennys niitä vasten on mahdollista vain niihin liitetyistä virtuaaliverkoista käsin. Azure Private DNS -palvelu tukee useita yleisiä DNS-tietuetyyppejä, kuten esimerkiksi A-, AAAA- sekä CNAME-tietueita. (What is an Azure Private DNS zone? 2023.)

Azure Private DNS -palvelu parantaa virtuaaliverkon tietoturvaa sekä yksinkertaistaa DNS-tietueiden hallintaa. Yksityiset DNS-alueet rajoittavat nimenselvennyksen yksityiseen verkkoon, estäen niiden näkyvyyden julkiverkosta, mikä parantaa virtuaaliverkon tietoturvaa. (What is an Azure Private DNS zone? 2023.)

Azure Private DNS -palvelua voidaan käyttää luomalla yksityiset DNS-alueet ja liittämällä ne haluttuun virtuaaliverkkoon, joka käyttää liittämisen jälkeen yksityisiä DNS-alueita nimikyselyissään. DNS-alueet voidaan liittää useampaan kuin yhteen virtuaaliverkkoon. (What is an Azure Private DNS zone? 2023.) DNS-tietueet sijoitetaan yksityisiin DNS-alueisiin yksityisten päätepisteiden luonnin yhteydessä, jonka jälkeen virtuaaliverkko voi nimikyselyllä selvittää päätepisteiden IP-osoitteet virtuaaliverkossa. (What is a private endpoint? 2025.)

Insinöörityön aikana rakennettu tekoälysovelluksen infrastruktuuri käytti Azure Private DNS -palvelua osana verkkoratkaisuaan. Yksityisiä DNS-alueita oli useita, sillä eri resurssityypeille määriteltiin omat DNS-alueensa. Resurssin luonnin yhteydessä resurssille luotiin yksityinen päätepiste, jonka DNS-tietue sijoitettiin kyseisen resurssityypin DNS-alueeseen. Yksityiset DNS-alueet liitettiin tekoälysovelluksen käyttämään virtuaaliverkkoon, jolloin DNS-tietueita olivat hyödynnettävissä virtuaaliverkon sisäisessä tietoliikenteessä. Tuotannollistetun tekoälysovelluksen rajapinnan DNS-tietue tuotiin osaksi keskitetyn rajapintahallintajärjestelmän nimenselvennyspalvelua, jolloin virtuaaliverkossa sijaitsevaa rajapintaa oli mahdollista kutsua rajapintahallintajärjestelmästä käsin.

5 Koneoppiminen ja tekoäly Azuressa

Azure tarjoaa monia erilaisia työkaluja ja resursseja koneoppimis- sekä tekoälysovellusten kehittämiseen. Insinöörityössä keskeisin resurssi oli koneoppimistyötila (engl. *Machine Learning Workspace*), jossa tekoälysovellus kehitettiin ja tuotannollistettiin. Koneoppimistyötila toimii tekoälysovelluksen varsinaisena käyttöympäristönä. Se tarjoaa erilaisia toimintoja esimerkiksi mallien ja datan rekisteröintiin sekä versiointiin.

Insinöörityössä tekoälysovelluksen ohjelmakoodi koottiin malliksi, joka rekisteröitiin koneoppimistyötilaan. Rekisteröidyn mallin pohjalta koottiin julkaisu (engl. *Deployment*), joka sijoitetaan koneoppimistyötilassa luotuun hallittuun päätepisteeseen (engl. *Managed online endpoint*). Päätepiste toimii tekoälysovelluksen reaaliaikaisesti kutsuttavana REST-rajapintana, johon tuotannon palvelukäyttäjä voi lähettää kutsuja keskitetyn rajapintajärjestelmän kautta.

5.1 Koneoppimistyötila ja sen resurssit

Koneoppimistyötila on ympäristö, joka mahdollistaa koneoppimis- ja tekoälymallien keskitetyn kehittämisen, käyttöönoton ja hallinnan. Koneoppimistyötila toimii alustana, jossa kehittäjät voivat hallitusti versioida työtään, kuten esimerkiksi kehitettyjä malleja sekä niiden tarvitsemia tietoaineistoja. (What is an Azure Machine Learning workspace? 2025.)

Työtilassa voidaan suorittaa erilaisia koneoppimiseen liittyviä ajoja, kuten mallien koulutusta ja testausta. Tällaiset ajot suoritetaan tyypillisesti *jobeina*, jotka ovat yksittäisiä ajoja, joiden tuloksia voidaan vertailla ja versioida työtilassa. Ajoja varten työtilaan on luotava virtuaalikoneita tai -klustereita (engl. *Compute Instance, Compute cluster*), joilla ajot suoritetaan. (What is an Azure Machine Learning workspace? 2025.) Koneoppimistyötila tarjoaa myös generatiivisten tekoälysovellusten kehittämiseen tarkoitetun Prompt Flow -työkalun, jolla insinöörityössä tuotannollistettava tekoälysovellus on toteutettu. (What is Azure Machine learning prompt flow? 2024.)

Koneoppimistyötila tarvitsee toimiakseen erilaisia resursseja, joista keskeisimmät ovat *Storage Account-, Container Registry- ja Key Vault* -resurssit. Nämä resurssit ovat Azuren tarjoamia yleisiä resursseja, jotka eivät liity yksinomaan koneoppimistyötilan käyttöön, mutta ovat sen toiminnalle välttämättömiä.

5.1.1 Azure Storage Account

Azure Storage Account -resurssi tarjoaa skaalautuvan ja tehokkaan tavan tallentaa dataa Azure-pilviympäristössä. Storage account -resurssi tarjoaa erilaisia tallennuspalveluja, kuten esimerkiksi *Blob Storage*- sekä *File Storage* -palvelut. (Collier & Shahan 2015: 101.)

Blob Storage -palvelu on tarkoitettu suurten ja rakenteettomien tiedostojen tallentamiseen. Tiedostot tallennetaan *blobeiksi* (*Binary Large Object*), jotka järjestellään kontteihin (engl. *container*). Kontit ovat kansioiden ja hakemistojen kaltaisia organisoimiseen tarkoitettuja rakenteita. File Storage -palvelu mahdollistaa tiedostojen jakamisen SMB-protokollan avulla, mikä tekee palvelusta monikäyttöisen. Storage Account -resurssi tarjoaa myös *Table Storage*- ja *Queue Storage* -palvelut, joita insinöörityössä ei käytetty. (Collier & Shahan 2015: 101-105.)

Storage Account -resurssi tukee erilaisia tunnistautumistapoja, kuten esimerkiksi *Microsoft Entra ID*-, *Shared Key*- sekä *Access Signature (SAS)* -tunnistautumista. Microsoft suosittelee käyttämään Entra ID -tunnistautumista, joka on vaihtoehdoista turvallisin. Se mahdollistaa pääsynhallinnan RBAC-roolien avulla, jolloin salasanoja tai avaimia ei tarvita.

Storage Account -resurssi varmistaa datan saatavuuden monistamalla tallennetun datan automaattisesti. Monistuksen taso tulee valita resurssin luonnin yhteydessä neljästä vaihtoehdosta, jotka ovat *Locally Redundant Storage-, Geo-Redundant Storage-, Read Access Geo-Redundant Storage*- sekä *Zone Redundant Storage* -monistus (lyh. LRS, GRS, RA-GRS, ZRS). Monistuksesta koituu kuluja, jotka määräytyvät monistettavan datan määrän sekä monistuksen

tason mukaan, LRS-monistuksen ollessa tyypillisesti halvin. (Collier & Shahan 2015: 106-107.)

Storage Account -resurssi tukee verkkoeriytystä virtuaaliverkkojen avulla. Resurssille voidaan luoda yksityinen päätepiste, jolloin resurssiin on mahdollista muodostaa yhteys virtuaaliverkosta, jossa yksityinen päätepiste sijaitsee. Yksityinen päätepiste tulee luoda jokaiselle resurssin tarjoamalle palvelulle, jota halutaan käyttää virtuaaliverkosta käsin. Esimerkiksi sekä Blob Storage- että File Storage -palveluja varten tulee luoda oma yksityinen päätepisteensä virtuaaliverkkoon, josta käsin palveluja halutaan käyttää. (Configure Azure Storage firewalls and virtual networks 2024.)

Insinöörityön aikana luotu koneoppimistyötila edellytti Storage Account -resurssin luomista. Työtila tarvitsi resurssin Blob Storage- ja File Storage -palveluja esimerkiksi tiedostojen, lokien sekä koneoppimistyötilan sisäisten tietorakenteiden tallentamiseen. Insinöörityön aikana luotiin verkkoeriytetty Storage Account -resurssi, jota tekoälysovelluksen koneoppimistyötila käytti. Resurssin määrittelyt olivat kehitys- ja tuotantoympäristöjen välillä lähes identtiset. Molempien ympäristöjen Storage Account -resurssiin määriteltiin yksityiset päätepisteet Blob Storage- ja File Storage -palveluille. Tunnistautumismekanismina käytettiin Entra ID -tunnistautumista. Ainoana erona ympäristöjen välillä oli monistuksen taso. Kehitysympäristössä käytettiin LRS-monistusta turhien kulujen välttämiseksi. Tuotantoympäristössä monistuksen tasoksi valittiin GRS.

5.1.2 Azure Container Registry

Azure Container Registry -resurssi on Azuren hallinnoima rekisteripalvelu, joka mahdollistaa Docker-kuvien tallentamisen Azure-pilviympäristössä sijaitsevaan yksityiseen rekisteriin. Rekisteri tukee Entra ID -tunnistusta, ja sen käyttö edellyttää asianmukaista RBAC-roolia. Rekisteriä voidaan käyttää Azure-palveluiden, kuten esimerkiksi koneoppimistyötilojen tai automaattisen koonnin putkien kanssa. (Azure Container Registry 2023.)

Rekisteripalvelu tarjoaa kolme erilaista palvelutasoa, jotka ovat *Basic*-, *Standard*- ja *Premium*-tasot. Basic-palvelutaso tarjoaa minimimäärän tallennustilaa ja suorituskykyä, ja on vaihtoehdoista edullisin. Standard-taso tarjoaa Basic-tasoa enemmän tallennustilaa ja suorituskykyä. Premium-taso tarjoaa korkeimman suorituskyvyn sekä lisäominaisuuksia, kuten esimerkiksi datan monistuksen sekä tuen virtuaaliverkoille. (Azure container registry service tiers 2024.)

Koneoppimistyötila käyttää rekisteripalvelua esimerkiksi ajoympäristöjen (engl. *Environment*) luomista ja versiointia varten. Koneoppimistyötilassa kehittäjät voivat määritellä konttipohjaisia ajoympäristöjä, joissa koneoppimis- ja tekoälysovellukset ajetaan. Ympäristöt rakennetaan Docker-kuviksi, jotka koneoppimistyötila tallentaa käyttämäänsä rekisteripalveluun. (What are Azure Machine Learning Environments? 2024.)

Insinöörityössä koneoppimistyötilalle määriteltiin verkkoeriytetty rekisteripalvelu, johon tekoälysovelluksen ajoympäristön Docker-kuva tallennettiin. Kehitys- ja tuotantoympäristöt käyttivät kumpikin Premium-palvelutason resurssia, sillä verkkoeriyttämistä ei voitu toteuttaa muilla palvelutasoilla. Rekisteripalvelu yhdistettiin ympäristön aliverkkoon yksityisellä päätepisteellä.

5.1.3 Azure Key Vault

Azure Key Vault -resurssi on palvelu, joka mahdollistaa salaisuuksien turvallisen tallennuksen, käytön ja hallinnan Azure-pilviympäristössä. Palvelu tukee Entra ID -tunnistautumista, ja sen käyttö edellyttää RBAC-roolien määrittämistä. Entra ID -tunnistautuminen mahdollistaa hallittujen identiteettien tunnistautumisen Key Vault -palveluun. (Azure Key Vault basic concepts 2025.)

Azure Key Vault -palvelu tukee verkkoeriyttämistä virtuaaliverkoilla. Palvelu voidaan yhdistää virtuaaliverkkoon yksityisellä päätepisteellä, jolloin palvelu on saavutettavissa virtuaaliverkosta käsin. Pääsyä palveluun voidaan rajoittaa palomuurisäännöillä, jolloin palvelu ei ole saavutettavissa julkiverkosta käsin. (Network security for Azure Key Vault 2025.)

Insinöörityön aikana koneoppimistyötilalle luotiin verkkoeriytetty Key Vault -palvelu. Pääsyä palveluun rajoitettiin palomuurisäännöillä, jotka sallivat tietoliikenteen vain virtuaaliverkon sisältä. Key Vault -palvelu oli vain koneoppimistyötilan sisäisessä käytössä, jolloin työtila tallensi sinne salaisuudet, joita se vaati toimiakseen.

5.1.4 Koneoppimistyötilan virtuaaliverkko

Koneoppimistyötila tukee verkkoeriytystä virtuaaliverkkojen avulla. Työtila voidaan turvata käyttämällä yksityisiä päätepisteitä, jolloin työtilan ja sen käyttämien resurssien välinen liikenne liikkuu vain yksityisten IP-osoitteiden kautta. Yksityiset päätepisteet mahdollistavat virtuaaliverkossa olevien resurssien käytön koneoppimistyötilasta käsin. Tällöin työtilaa on mahdollista käyttää tietoturvallisesti virtuaaliverkosta käsin esimerkiksi Azure Bastion -palvelun avulla. Azure Bastion -palvelu toimii hyppypalvelimena (engl. *Jump box*), mikä mahdollistaa koneoppimistyötilan käytön julkiverkosta käsin. (Secure an Azure Machine Learning workspace with virtual networks 2024.)

Koneoppimistyötilan verkkoeriyttäminen perinteisten virtuaaliverkkojen avulla ei kuitenkaan ole ainoa tapa toteuttaa verkkoeriytys. Koneoppimistyötilan verkkoeriyttäminen suositellaan toteutettavan Microsoftin hallitsemien virtuaaliverkkojen (engl. *Managed virtual network*) avulla. Microsoftin hallitsemat virtuaaliverkot tarjoavat käyttäjälle yksinkertaisemman ratkaisun verkkoeriytyksen toteuttamiseen. Kun hallittu virtuaaliverkko otetaan työtilassa käyttöön, Azure luo automaattisesti työtilaan liitetyn erillisen ja sisäisesti hallitun virtuaaliverkon, jolloin käyttäjän ei tarvitse luoda omaa, erillistä virtuaaliverkkoa. Hallittu virtuaaliverkko toimii myös yksityisillä päätepisteillä, ja siihen liitetyt resurssit on mahdollista liittää erilliseen, käyttäjän hallitsemaan virtuaaliverkkoon. Kuten erilliset virtuaaliverkot, myös Microsoftin hallitsemat virtuaaliverkot ovat käyttäjän säädettävissä, jolloin tämä voi esimerkiksi rajoittaa sisään- tai ulospäin suuntautuvaa verkkoliikennettä haluamallaan tavalla. (Workspace Managed Virtual Network Isolation 2025.)

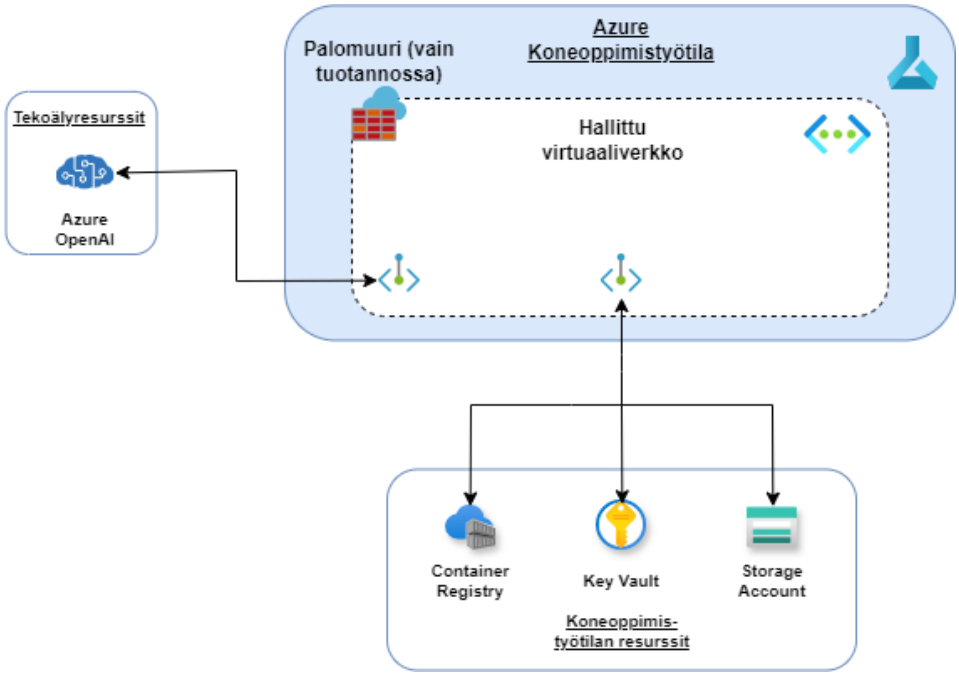
Microsoftin hallitsemien virtuaaliverkkojen hyödyntäminen yksinkertaistaa yksityisten verkko- ja päätepisteiden ratkaisuja, sillä hallittu virtuaaliverkko konfiguroi vaaditut yksityiset päätepisteet työtilan virtuaaliverkkoon automaattisesti, jolloin koneoppimistyötilan verkkoeriytys ei vaadi käyttäjältä kuin vähäistä manuaalista konfigurointia. Microsoft suosittelee hallittujen virtuaaliverkkojen käyttöä koneoppimistyötilan verkkoeriytyksessä. (Workspace Managed Virtual Network Isolation 2025.)

Verkkoliikenteen hallinta on keskeinen osa verkkoeriytyksen suunnittelua. Microsoftin hallitsemat virtuaaliverkot mahdollistavat sekä sisään- että ulospäin suuntautuvan verkkoliikenteen rajoittamisen palomuurisääntöjen avulla. Koneoppimistyötilan hallitun verkon palomuurin voi esimerkiksi konfiguroida sallimaan liikenne ainoastaan virtuaaliverkon sisältä, tai estämään liikenteen koneoppimistilasta julkiverkkoon kokonaan. Koneoppimistyötilasta ulospäin suuntautuvan liikenteen rajoittaminen edellyttää Azure Firewall -palvelun käyttöönottoa. (Workspace Managed Virtual Network Isolation 2025.)

Ulospäin suuntautuvaa liikennettä voidaan hallita lisäämällä työtilan virtuaaliverkkoon ulospäin suuntautuvan liikenteen sääntöjä (engl. *Workspace outbound rule*). Yhteyksiä julkiverkkoon voi esimerkiksi sallia luomalla FQDN-kohtaisia (*Fully Qualified Domain Name*) sääntöjä, jotka sallivat yhteyden työtilasta kyseiseen osoitteeseen. Yhteyksiä hallitun virtuaaliverkon ulkopuolisiin resursseihin, kuten esimerkiksi Azure OpenAI- tai Storage Account -resursseihin, hallitaan myös ulospäin suuntautuvan liikenteen säännöillä. Kun koneoppimistyötilan hallittuun virtuaaliverkkoon lisätään sääntö, joka sallii yhteyden työtilasta resurssille, luodaan resurssia varten yksityinen päätepiste työtilan hallittuun virtuaaliverkkoon. (Workspace Managed Virtual Network Isolation 2025.) Eräs hallittujen virtuaaliverkkojen haittapuolista on se, että käyttäjä ei näe niiden IP-osoiteavaruutta, sillä virtuaaliverkko sijaitsee Microsoftin hallitsemassa infrastruktuurissa. Tämä saattaa tehdä virtuaaliverkon palomuuriavauksista haastavia.

Insinöörityössä tekoälysovelluksen tuotantoympäristöksi rakennettu koneoppimistyötila verkkoeriytettiin käyttäen Microsoftin hallitsemaa virtuaaliverkkoa,

joka konfiguroitiin estämään julkiverkosta tuleva liikenne. Kuva 4 kuvaa koneoppimistyötilan hallittua virtuaaliverkkoa ja siihen liitettyjä resursseja. Hallittuun virtuaaliverkkoon lisättiin ulospäin suuntautuvan liikenteen sääntö Azure OpenAI -resurssiin, jotta yhteyden muodostaminen siihen oli koneoppimistyötilasta käsin mahdollista.



Kuva 4. Koneoppimistyötilan hallitun virtuaaliverkon rakenne. Ulospäin suuntautuvan liikenteen sääntö sallii yhteyden Azure OpenAI -alustalle.

Hallitun virtuaaliverkon konfiguraatio oli kehitys- ja tuotantoympäristöissä palomuuria lukuun ottamatta identtinen. Azure Firewall -palomuuripalvelua ei otettu kehitysympäristössä käyttöön siitä aiheutuvien kulujen takia, jotka olivat noin 800 € kuukaudessa. Palomuuripalvelu otettiin käyttöön vain tuotantoympäristössä, sillä LähiTapiolan tietoturvalinjaukset määräävät, että ulospäin suuntautuvaa liikennettä on kyettävä rajoittamaan ympäristöissä, jotka ovat tuotantokäytössä.

5.2 Prompt Flow

Prompt Flow -työkalu on koneoppimistyötilassa saatavilla oleva kehitystyökalu, joka on suunniteltu helpottamaan generatiivisiin kielimalleihin perustuvien tekoälysovellusten kehittämistä ja käyttöönottoa. Työkalu tarjoaa visuaalisen käyttöliittymän koneoppimistyötilassa, jossa kehittäjät voivat esimerkiksi testata miten muutokset mallin kehotteeseen tai parametreihin vaikuttavat sovelluksen toimintaan. (What is Azure Machine Learning prompt flow? 2024.)

Prompt Flow -työkalu perustuu rakenteeseen, jossa työnkulku (engl. *Flow*) on määritelty selkeästi jäsenneltyihin tiedostoihin ja konfiguraatioihin. Työnkulku koostuu kansiorakenteesta, jota ohjaa YAML-tiedosto nimeltä ”flow.dag.yaml”. YAML-tiedosto kuvaa työnkulun rakenteen, ja määrittelee suoritettavien solmujen (engl. *Node*) järjestyksen, riippuvuudet sekä parametrit. Yksittäiset solmut voivat olla esimerkiksi Python-tiedostoja, Jinja2-tiedostomuodossa olevia kehotteita (engl. *Prompts)* tai Azuren tarjoamia valmiita LLM-solmuja. LLM-solmut muodostavat yhteyden Azure OpenAI -resurssiin, ja käyttävät haluttua mallia saamiensa syötteiden ja konfiguraatioiden mukaisesti. (Develop prompt flow 2024.)

Insinöörityössä tuotannollistettava tekoälysovellus määriteltiin tiedostorakenteisena Prompt Flow -ratkaisuna, joka koostui vain Python-solmuista. Ratkaisu rekisteröitiin koneoppimisympäristöön mallina, joka julkaistaan palvelukäyttäjän kutsuttavaksi hallittuun päätepisteeseen koneoppimistyötilassa.

Alkuperäisen suunnitelman mukaan sovellus oli tarkoitus toteuttaa joko Azure Function App -palvelun avulla tai konttipohjaisena ratkaisuna Azure Container Instances -ympäristössä. Lopulliseksi toteutustavaksi valittiin kuitenkin tiedostorakenteinen Prompt Flow -ratkaisu, joka mahdollisti sovelluksen kehityksen, testauksen ja käyttöönoton koneoppimisympäristön sisällä. Prompt Flow -ratkaisun keskeisenä etuna oli mahdollisuus julkaista se mallina hallittuun päätepisteeseen koneoppimistyötilassa. Hallittu päätepiste tarjoaa julkaisuille muun muassa valmiin Microsoft Entra ID -tunnistautumismekanismin sekä

automaattisesti hallinnoidun infrastruktuurin, mikä parantaa ratkaisun operoitavuutta tuotantoympäristössä.

5.3 Azure OpenAI

Azure OpenAI -resurssi on Azure-ympäristöön integroitava alusta, joka mahdollistaa ohjelmallisen pääsyn OpenAI-yrityksen suuriin kielimalleihin. Alusta mahdollistaa kielimallien tietoturvallisen käytön Azuressa kehitettävissä sovelluksissa. Alustalle voi julkaista (engl. *Deploy*) erilaisia malleja, joita voidaan ohjelmallisesti käyttää REST-rajapinnan tai SDK-kirjastojen kautta. Alusta tarjoaa keinoja asettaa malleille rajoitteita, kuten esimerkiksi maksimirajoitteen tokeneille, joita mallit voivat käyttää minuutissa. Tämä mahdollistaa alustan resurssien jakamisen mallikohtaisesti. (What is Azure OpenAI Service? 2025.)

Alusta tukee virtuaaliverkkojen ja yksityisten päätepisteiden käyttöä, minkä ansiosta se voidaan liittää osaksi verkkoeriytettyä ympäristöä. Lisäksi alustalla on mahdollista käyttää Entra ID -tunnistautumista, ja se tukee hallittuja identiteettejä. (What is Azure OpenAI Service? 2025.)

Alustan julkaisujen tietoturvallinen hyödyntäminen koneoppimistyötilassa edellyttää työtilayhteyden (engl. *Workspace connection*) luomista kyseiseen resurssiin. Yhteyksien avulla koneoppimistyötilasta voidaan tunnistautua ulkoisiin palveluihin, kuten esimerkiksi Azure OpenAI -alustalle. Työtilassa yhteydet voidaan määritellä koko työtilan laajuisiksi tai yksittäisen käyttäjän käyttöön. Työtilayhteyksiin liittyvät salaisuudet, kuten esimerkiksi mahdolliset API-avaimet, tallennetaan koneoppimistyötilan käyttämään Azure Key Vault -palveluun työtilan toimesta. (Connections in prompt flow 2024; Add a new connection using the Azure Machine Learning SDK 2025.)

Työtilan yhteydet voidaan luoda käyttämällä Entra ID -tunnistautumista resursseihin, jota Microsoft suosittelee. Azure OpenAI -alustaan luotu yhteys mahdollistaa kielimallin käytön osana koneoppimistyötilassa kehitettyjä sovelluksia. Prompt Flow -työkalu käyttää työtilayhteyksiä muodostaessaan yhteyden

alustaan. (Connections in prompt flow 2024; Add a new connection using the Azure Machine Learning SDK 2025.)

Tekoälysovelluksen käyttö edellytti yhteyttä Azure OpenAI -alustaan. Azure OpenAI -alusta ja sen sisällä julkaistu suuri kielimalli määriteltiin osana infrastruktuurin koodimäärittelyjä.

Azure OpenAI -alustaa käytettyyn työtilasta työtilayhteyden avulla. Yhteys rekisteröitiin koneoppimistyötilaan, ja verkkoliikenne työtilasta Azure OpenAI -alustalle sallittiin ulospäin suuntautuvan liikenteen säännöllä. Yhteys toteutettiin Entra ID -tunnistautumismekanismilla, mikä edellytti RBAC-roolien asettamista hallitun päätepisteen identiteetille.

5.4 Hallitut päätepisteet ja julkaisut

Koneoppimistyötilassa on mahdollista julkaista malleja hallituissa päätepisteissä. Päätepiste ovat koneoppimistyötilan tarjoama infrastruktuuri, joka toimii muuttumattomana ja kutsuttavana URL-osoitteena ja jossa malleja voidaan julkaista (engl. *Deploy*) HTTP-protokollalla kutsuttavaksi. Julkaisut ovat päätepisteeseen koottuja resurssikokonaisuuksia, jotka sisältävät mallin ajamiseen tarvittavan koodin, ympäristön sekä laskentaresurssin. Yksi päätepiste voi sisältää useita julkaisuja, jotka voivat käyttää erillisiä resursseja sekä eri versioita malleista, tai kokonaan erilaisia malleja. Päätepiste mahdollistaa myös saapuvan liikenteen jakamisen eri julkaisujen välille. Päätepisteet tarjoavat URL-osoitteen lisäksi sekä tunnistautumis- että valtuutusmekanismin (engl. *Authorization*). Päätepiste voi käyttää tunnistautumiseen joko Entra ID -tunnistautumista tai perinteistä API-avain-tunnistautumista. Päätepiste tukee hallittuja identiteettejä, joille tulee määrittää resursseihin Entra ID -tunnistautumista varten tarvittavat RBAC-roolit. (Endpoints for inference in production 2024.)

Koneoppimistyötila tarjoaa hallittujen päätepisteiden lisäksi kahta muuta päätepistetyyppiä. Serverless API -päätepisteet ovat hallittujen päätepisteiden kaltaisia, mutta ne eivät vaadi käyttäjältä osoitettuja laskentaresursseja. Batch-

päätepisteet taas on suunniteltu eräajoihin, joissa päätepisteen ei tarvitse olla reaaliaikaisesti kutsuttava. Tuotannollistettavan tekoälysovelluksen päätepistetyypiksi valittiin hallittu päätepiste, sillä sovelluksen tuli olla reaaliaikaisesti kutsuttavissa ja hallitusti skaalattavissa. (Endpoints for inference in production 2024.)

Hallittujen päätepisteiden skaalautuvuus mahdollistaa resurssien, kuten laskentaresurssien automaattisen lisäämisen tai vähentämisen mallin käyttöasteen perusteella. Skaalaus toteutetaan Azure Monitor -palvelun autoskaalaus-ominaisuuden avulla, joka mahdollistaa sääntöpohjaisen skaalauksen. Automaattinen skaalaus perustuu mittareihin, kuten esimerkiksi prosessorin käyttöasteeseen. Eräs sääntö voisi esimerkiksi määritellä, että jos prosessorin käyttöaste on yli 70 % viiden minuutin ajan, voidaan päätepisteen julkaisun laskentaresursseja lisätä. Vastaavasti jos käyttöaste on alhainen, voidaan laskentaresurssien määrää automaattisesti laskea. Automaattista skaalausta on mahdollista myös aikatauluttaa, ja sitä voidaan toteuttaa julkaisukohtaisesti. (Autoscale online endpoints in Azure Machine Learning 2024.)

Koneoppimistyötilan päätepisteet on mahdollista verkkoeriyttää käyttämällä työtilan hallittua virtuaaliverkkoa. Hallitulle päätepisteelle tuleva tietoliikenne käyttää työtilan yksityistä päätepistettä, jolloin liikenne pysyy julkiselta verkolta piilossa. Ulospäin suuntautuva liikenne kulkee kohteeseensa työtilan virtuaaliverkon ulospäin suuntautuvien sääntöjen avulla, jolloin päätepisteessä oleva julkaisu voi turvallisesti käyttää esimerkiksi muita Azure-resursseja. (Network isolation with managed online endpoints 2024.)

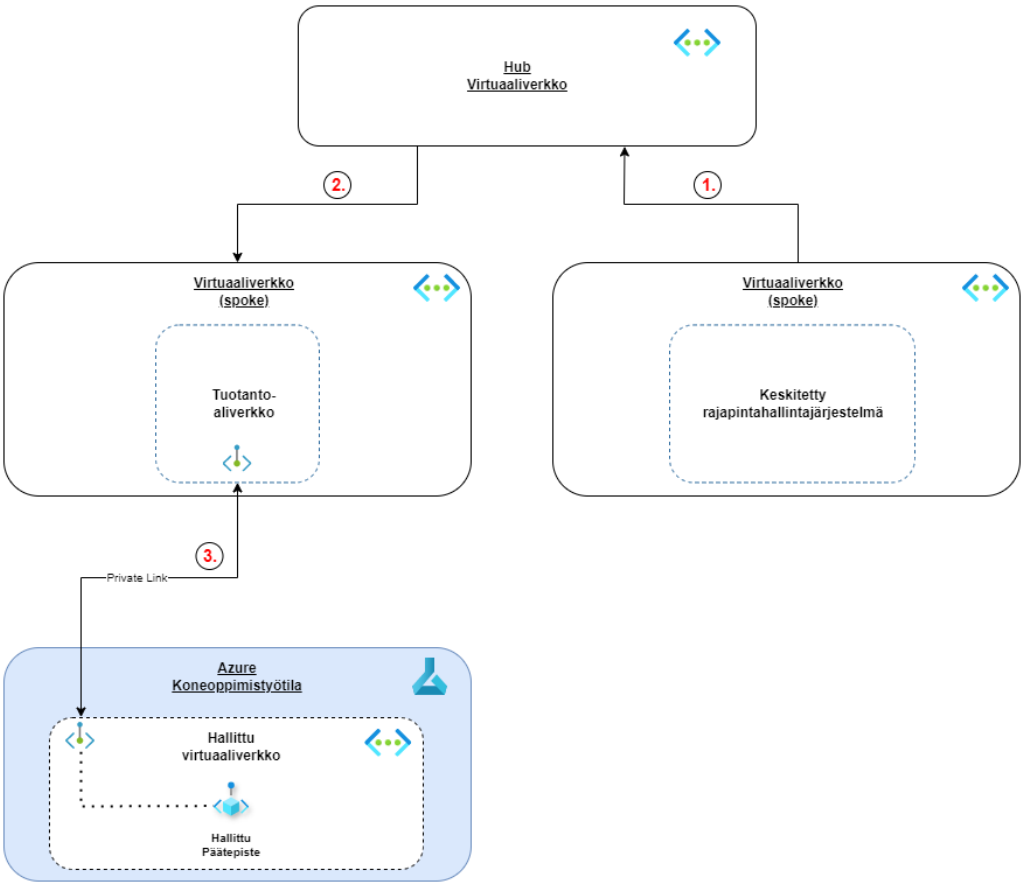
Insinöörityössä tuotannollistettu tekoälysovellus rekisteröitiin koneoppimistyötilaan mallina, joka julkaistiin hallitussa päätepisteessä tuotantokäyttöön. Insinöörityössä päädyttiin käyttämään tuotannossa hallittua päätepistettä, sillä sen tarjoamat edut olivat merkittävät.

Hallittua päätepistettä voitiin skaalata automaattisesti eri metriikoiden mukaan käyttöasteen noustessa, mikä varmisti palvelun saatavuuden tuotantokäytössä.

Automaattinen skaalaus teki ratkaisusta myös kustannustehokkaan, sillä laskentaresurssien määrää oli mahdollista vähentää päätepisteen käytön ollessa vähäistä. Lisäksi päätepisteet tukevat Microsoft Entra ID -tunnistautumismekanismia, mikä helpotti kehitystyötä merkittävästi. Jos tuotantokäytössä olisi esimerkiksi konttipohjainen ratkaisu Azure Container Instances -ympäristössä, tekoälysovelluksen kehittäjien olisi täytynyt ohjelmoida tunnistautumismekanismi osaksi sovelluksen kontin toteutusta. MLOps-näkökulmasta (*Machine Learning Operations*) hallitut päätepisteet ovat erinomainen ratkaisu, sillä ne tarjoavat suoraviivaisen ja minimaalisen tavan julkaisujen hallintaan automaattisen koonnin putkien avulla.

Hallitun päätepisteen kutsumisen tuli olla mahdollista keskitetystä rajapintajärjestelmästä. Tämän toteuttaminen oli insinöörityössä haasteellista, sillä koneoppimistyötila käytti Microsoftin hallitsemaa virtuaaliverkkoa, jolloin virtuaaliverkon IP-osoiteavaruus ei ollut kehittäjien tiedossa, eikä suoran palomuuriavauksen tekeminen rajapintajärjestelmään ollut mahdollista.

Suoran palomuuriavauksen sijaan päätepisteen tietoliikenne tuli ohjata perinteisen virtuaaliverkon kautta yksityisten päätepisteiden avulla. Kuva 5 havainnollistaa tuotannossa toteutettua ratkaisua. Yhteys hallitulle päätepisteelle muodostettiin koneoppimistyötilan yksityisen päätepisteen kautta, joka sijaitsee perinteisessä virtuaaliverkossa.



Kuva 5. Yhteys keskitetystä rajapintajärjestelmästä hallittuun päätepisteeseen, jossa tekoälysovellus on julkaistu. Ympyröidyt numerot kuvaavat liikenteen kulkua.

Kuvan ympyröidyt numerot kuvaavat HTTP-pyynnön reititystä keskitetystä rajapintahallintajärjestelmästä. Kohdassa yksi rajapintahallintajärjestelmästä tuleva pyyntö reititetään Hub-verkolle. Kohdassa kaksi pyyntö reititetään edelleen tekoälysovelluksen ympäristön perinteiselle spoke-virtuaaliverkolle. Koneoppimistyötilan hallittu virtuaaliverkko on yhdistetty tähän virtuaaliverkkoon yksityisellä päätepisteellä, jota pitkin HTTP-pyynnöt kulkeutuvat hallitulle päätepisteelle. Kohdassa kolme HTTP-pyyntö kulkeutuu hallitulle päätepisteelle yksityistä päätepistettä pitkin. Ratkaisu edellyttää, että rajapintahallintajärjestelmä kykenee selventämään hallitun päätepisteen yksityisen IP-osoitteen, mikä edellyttää

hallitun päätepisteen DNS-tietueen tuomista osaksi rajapintahallintajärjestelmän DNS-alueita.

6 Infrastruktuuri koodina -periaate ja Bicep

Insinöörityön aikana tekoälysovelluksen vaatima infrastruktuuri rakennettiin infrastruktuuri koodina -periaatteen (engl. *Infrastructure as Code*) mukaisesti. Infrastruktuuri määriteltiin koodipohjaisesti Microsoftin kehittämällä Bicep-kielellä, mikä mahdollisti infrastruktuurin versiohallinnan sekä julkaisun automatisoinnin.

LähiTapiolan linjaukset määräävät, että Azure-pilviympäristössä toteutettujen tuotantoratkaisujen tulee seurata infrastruktuuri koodina -periaatetta. Insinöörityön aikana linjausta noudatettiin, ja tekoälysovelluksen infrastruktuuri määriteltiin koodipohjaisesti. Infrastruktuurin koodipohjaisesta määrittelystä rajattiin kuitenkin pois koneoppimistyötilan sisäiset resurssit, lukuun ottamatta joitakin virtuaalikoneita ja -klustereita.

Rajaus perustui siihen, että koneoppimistyötilan sisäiset resurssit, kuten esimerkiksi hallittu päätepiste, liittyivät vahvasti tekoälysovelluksen kooditoteutukseen. Tämän vuoksi niiden määrittely ja luonti katsottiin järkevämmäksi sisällyttää osaksi tekoälysovelluksen versionhallintaa ja automaattisen koonnin putkia, eikä osaksi erillistä infrastruktuurin julkaisuputkea.

6.1 Infrastruktuuri koodina -periaate

Infrastruktuuri koodina -periaate (lyh. *IaC*) on DevOps-käytäntöihin kuuluva infrastruktuurin hallintamalli, jossa ympäristön määrittely ja julkaisu toteutetaan komentorivityökalujen tai käyttöliittymien sijaan versioitavalla koodilla. Määrittely tapahtuu esimerkiksi Bicep- tai Terraform-kielellä kirjoitettujen määritystiedostoilla, joiden avulla varmistetaan ympäristön yhtenäinen rakentuminen riippumatta sen lähtötilasta. Tämä helpottaa esimerkiksi muutosten testaamista, sillä ympäristö voidaan testauksen jälkeen palauttaa alkuperäiseen muotoonsa määritystiedostojen avulla. Infrastruktuuri koodina -periaatetta noudattamalla

kehittäjät vähentävät manuaalisen määritystyön tarvetta, mikä vähentää esimerkiksi virheiden todennäköisyyttä. (What is infrastructure as code? 2024.)

IaC-ratkaisut voidaan jakaa kahteen päätyyppiin määrittely- ja toimintatavan mukaan, jotka ovat deklaratiiviset ja imperatiiviset tyypit. Deklaratiivisessa tyypissä määritellään haluttu lopputila, ja järjestelmä huolehtii tarvittavista toimenpiteistä tämän tilan saavuttamiseksi. Kehittäjän ei tarvitse määritellä vaiheittaista etenemistä, vaan ainoastaan lopullinen tila, johon ratkaisulla pyritään. Imperatiivisessa lähestymistavassa kehittäjän taas tulee tarkalleen määritellä, mitkä komennot suoritetaan missä järjestyksessä, jotta lopputila saavutetaan. (Infrastructure as Code (IaC): Comparing the Tools 2022.)

Insinöörityön aikana IaC-periaatetta noudatettiin, ja infrastruktuurin määritystiedostot olivat osa tekoälysovelluksen tuotannollistamisen ratkaisun versiohallintaa. Tekoälysovelluksen kehitys- ja tuotantoympäristöjen resurssit määriteltiin ja luotiin lähes kokonaan IaC-pohjaisesti. Ainoana poikkeuksena olivat virtuaaliverkot, joiden luomista on rajoitettu hallintaryhmätason sääntöjen avulla LähiTapiolan Azure-tilauksissa. Virtuaaliverkot tuli tilata keskitetyltä taholta, millä varmistettiin se, että virtuaaliverkot oli konfiguroitu oikein ja että ne olivat käyttötapaukseen nähden sopivan kokoisia. Verkkoeriytys toteutettiin muilta osin IaC-pohjaisesti.

6.2 Azure Resource Manager

Azure Resource Manager (lyh. ARM) on Azuren hallinta- ja käyttöönottopalvelu, joka hallitsee resurssien luomista, päivittämistä ja poistamista eri työkalujen ja API-rajapintojen kautta. ARM-palvelu tukee Infrastruktuurin hallintaa eri tasoilla, kuten hallintaryhmissä, tilauksissa, resurssiryhmissä sekä yksittäisissä resursseissa. Se huolehtii resurssien luontijärjestyksestä ja hallinnoi niiden välisiä mahdollisia riippuvaisuuksia, ja mahdollistaa infrastruktuurin hallinnan määritystiedostoilla eli JSON-pohjaisilla ARM-mallitiedostoilla (engl. *ARM template*). (What is Azure Resource Manager? 2025.)

ARM-mallitiedosto on JSON-muotoinen määritystiedosto, jolla kuvataan infrastruktuurin haluttu lopputila. Mallitiedostossa määritellään resurssit, niiden ominaisuudet sekä sijainti. ARM-mallitiedostot ovat deklaratiivisia, jolloin kehittäjä määrittää infrastruktuurin lopputilan. (What are ARM templates? 2025.)

Insinöörityössä ei hyödynnetty suoraan JSON-pohjaisia ARM-mallitiedostoja, sillä ARM-mallitiedostot ovat pitkinä JSON-tiedostoina vaikealukuisia, mikä olisi lisännyt virheiden todennäköisyyttä. ARM-mallitiedostot olivat kuitenkin insinöörityössä vaihtoehto, mutta infrastruktuuri päädyttiin määrittelemään Bicep-kielellä.

6.3 Bicep

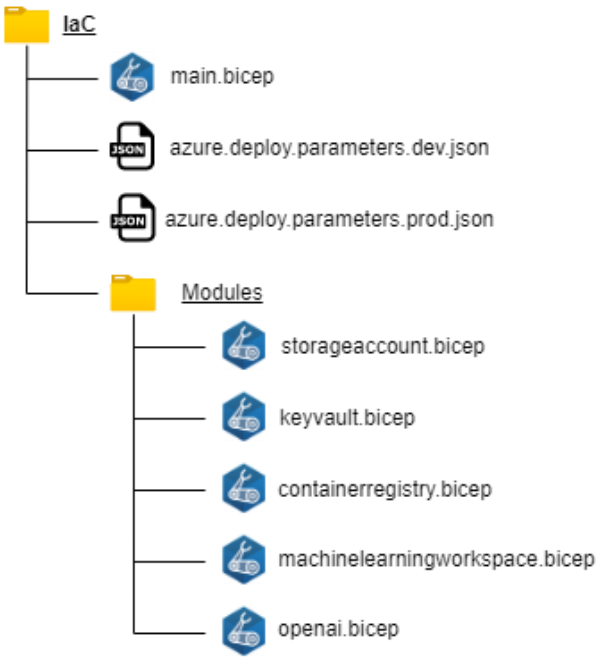
Bicep on Microsoftin kehittämä kieli, joka on suunniteltu Azure-pilviympäristön resurssien määrittelyyn ja julkaisuun IaC-periaatteen mukaisesti. Bicep on tyypiltään deklaratiivinen kieli, jossa kehittäjän täytyy määritellä resurssit halutussa lopputilassa. Azure Resource Manager -palvelu huolehtii resurssien luomisesta oikeassa järjestyksessä. Bicep tarjoaa kehittäjille tavan hallita Azure-resursseja ilman pitkiä komentosarjoja tai manuaalista konfigurointia (What is Bicep? 2025.)

Bicep-tiedostoissa määritellään luotavat resurssit ja niiden ominaisuudet helppolukuisella syntaksilla. Kehittäjä kuvaa halutun lopputilan, ja ARM-palvelu huolehtii resurssien luomisesta ja järjestyksestä. Bicep tukee samoja resurssityyppejä ja API-versioita kuin JSON-pohjaiset ARM-mallitiedostot. (What is Bicep? 2025.)

Bicep-kieli mahdollistaa modulaarisen käsittelyn, jossa käyttäjät voivat jakaa kokonaisuuksia hallittaviin osiin moduulien avulla. Moduuleita käytetään yhdessä päätiedostossa, jonka nimeämiskäytäntö on usein ”main.bicep”. Kun Bicep-tiedosto suoritetaan, käännetään Bicep-tiedostot taustalla automaattisesti ARM-muotoon, jonka jälkeen ne suoritetaan Azure Resource Managerin prosesseissa. (What is Bicep? 2025.)

Bicep-tiedostot ovat parametrisoitavia, jolloin samaa määritystiedostoa voidaan käyttää eri ympäristöjen luontiin ilman koodin rakenteellisia muutoksia. Parametrit luetaan Bicep-tiedostoissa muuttujiin, joita voidaan käyttää esimerkiksi resurssien nimeämiseen. ARM-palvelu asettaa parametrien arvot ennen resurssien luontia. Parametrit voidaan sijoittaa esimerkiksi erilliseen JSON-tiedostoon, joka syötetään ARM-palvelulle Bicep-tiedostojen suorituksen yhteydessä. (Parameters in Bicep 2025.)

Infrastruktuurin koodipohjainen määrittely oli insinöörityön eräs keskeisiä vaiheita, joka edellytti perehtymistä koneoppimisresursseihin sekä verkkoeriyttämiseen. Infrastruktuurin Bicep-määrittelyssä käytettiin modulaarista lähestymistapaa, jossa resurssit ja niiden verkkoeriytyksen komponentit pyrittiin eriyttämään omaan moduulinsa. Kuva 6 havainnollistaa toteutettujen Bicep-määrittelyjen tiedostorakennetta.



Kuva 6. Bicep-määrittelyn rakenne. Moduuleja käytetään sekä kehitys- että tuotantoympäristön rakentamiseen, ja ne sisältävät määritellyn resurssin verkkoeriytyskomponentit.

Kehitys- ja tuotantoympäristö rakennettiin käyttäen yhteisiä Bicep-määrittelyitä, joita parametrisoitiin JSON-tiedostoilla. Kehitys- ja tuotantoympäristöjä varten määriteltiin omat parametritiedostonsa, jotka syötettiin ARM-palvelulle ympäristön rakennuksen yhteydessä automaattisen koonnin putkissa.

Ympäristöjen toteutukset olivat lähes identtiset, pois lukien hallitun virtuaaliverkon palomuuri ja sen FQDN-säännöt sekä Storage Account -resurssin monistuksen kalliimpi taso, jotka olivat tuotantoympäristön määrittelyissä. Poikkeavat määritykset toteutettiin käyttäen ehdollisia lausekkeita, joissa valinta perustui ympäristön tyyppiin, joka määriteltiin parametritiedostoissa. Ympäristöt rakennettiin suorittamalla parametrisoidut Bicep-tiedostot Azure DevOps -ympäristön automaattisen koonnin putkissa.

7 Azure DevOps

Azure DevOps -ympäristö oli insinöörityössä merkittävässä osassa. Sekä tuotannollistettavan tekoälysovelluksen vaatima infrastruktuuri että tekoälysovelluksen kokoaminen ja julkaisu toteutettiin DevOps -ympäristössä automaattisen koonnin putkilla. Automaattisen koonnin putket vastasivat sekä tekoälysovelluksen ohjelmakoodin kokoamisesta että sen julkaisemisesta hallittuun päätepisteeseen tuotantokäyttöä varten. Julkaisuprosessi toteutettiin Azure CLI -komentorivityökalun avulla. Infrastruktuurin Bicep-määritykset suoritettiin erillisessä automaattisen koonnin putkessa.

Automaattisen koonnin putket rakennettiin parametrisoitavaksi ja modulaarisiksi, mikä mahdollisti ratkaisun hallitun julkaisun eri ympäristöihin. Putkien kehittämisessä noudatettiin MLOps-lähestymistapaa, mikä varmisti infrastruktuurin ja tekoälysovelluksen toistettavan ja automatisoidun käyttöönoton. Julkaisuputken toteutuksessa hyödynnettiin Microsoftin MLOps-sapluunoita (engl. *MLOps templates*), jotka tarjosivat valmiiksi testattuja komentoja infrastruktuurin ja mallien julkaisemiseen. Sapluunat nopeuttivat putkien kehitystyötä ja tukivat ratkaisun skaalautuvaa käyttöönottoa eri ympäristöissä.

7.1 Azure DevOps ja automaattisen koonnin putket

Azure DevOps -ympäristö on Microsoftin kehittämä palvelukokonaisuus, joka on suunniteltu tukemaan ohjelmistokehitystyötä. Ympäristöä voi käyttää pilvipalveluna tai paikallisena asennuksena, jolloin se täyttää myös tiukimmat tietoturvavaatimukset. Azure DevOps koostuu useista erilaisista palveluista, kuten esimerkiksi Azure Repos -versionhallinnasta sekä Azure Pipelines -automaatioputkista. (What is Azure DevOps? 2025.)

Azure Repos -palvelu on versionhallintapalvelu, joka tukee sekä Git-versionhallintaa että Team Foundation Version Control -järjestelmää. Versionhallintajärjestelmät mahdollistavat koodimuutosten tallentamisen, seuraamisen ja jakamisen. (What is Azure Repos 2024.) Insinöörityössä käytettiin Git-pohjaista versionhallintaa, sillä Git-pohjaisen versionhallinnan käyttö oli kehittäjille vakiintunut käytäntö.

Azure Pipelines -palvelu automatisoi ohjelmistoprojektien rakentamista, testaamista ja julkaisua automaattisen koonnin putkien avulla. Se yhdistää jatkuvan integroinnin, testauksen ja toimituksen haluttuun ympäristöön. Palvelu tukee useita ohjelmointikieliä ja mahdollistaa sovellusten rakentamisen eri käyttöjärjestelmillä. Se tarjoaa laajan tuen erilaisille ympäristöille ja mahdollistaa julkaisut esimerkiksi virtuaalikoneille, kontteihin ja pilviympäristöihin. Azure Pipelines -palvelu integroituu versionhallinnan ratkaisuihin, kuten esimerkiksi Azure Repos -palveluun. (What is Azure Pipelines? 2024.)

Automaattisen koonnin putket (lyh. *CI/CD*, engl. *Continuous Integration/Continuous Delivery*) ovat olennainen osa modernia datatiede- ja ohjelmistokehitystä. Data-analytiikassa ja koneoppimisen sovelluksissa automaattisen koonnin putket ovat perinteisesti suorittaneet esimerkiksi datan käsittelyä sekä erilaisia koneoppimissovellusten ja -mallien julkaisua. (Azure CI/CD data pipelines 2024.) Putket määritellään YAML-muotoisilla määritystiedostoilla, jotka rakentuvat ennalta määritetyn skeeman mukaisesti. Putket koostuvat tyypillisesti vaiheista (engl. *Stage*), tehtävistä (engl. *Job*) ja askeleista (engl. *Step)*, joiden avulla

monimutkaisiakin prosesseja voidaan jäsennellä hallittaviksi kokonaisuuksiksi. (YAML schema reference for Azure Pipelines 2025.)

Insinöörityössä toteutetussa tuotannollistamisen ratkaisussa hyödynnettiin Azure Repos- ja Azure Pipelines -palveluita. Insinöörityössä käytettiin Git-pohjaista versionhallintaa, jonka avulla hallittiin tekoälysovelluksen ohjelmakoodia, infrastruktuurin määrittelytiedostoja sekä automaattisen koonnin putkien määrittelyjä. Versionhallinta suojattiin käyttöoikeusmäärityksillä, jotka varmistivat, että vain sovelluksen sekä tuotannollistamisen putkien kehittäjillä oli mahdollisuus muokata versionhallinnan sisältöä.

Automaattisen koonnin putket määriteltiin YAML-tiedostoina osana versionhallintaa. Putkiin määriteltiin kaksi vaihetta, joista ensimmäinen vastasi tekoälysovelluksen resurssien, kuten esimerkiksi ajoympäristön sekä tekoälysovelluksen mallin, rekisteröinnistä ja versioinnista. Toinen vaihe kokosi ja julkaisi mallin hallittuun päätepisteeseen ja asetti sille esimerkiksi automaattisen skaalautuvuuden säännöt sekä julkaisukohtaisen liikenteen määrän. Molemmat vaiheet koostuivat useista askelista, jotka suorittivat mallin julkaisemisen toimenpiteitä Azure CLI -komentorivityökalun komentoja käyttäen.

7.2 Tietoturva Azure Pipelines -palvelussa

Azure Pipelines -palvelu tarjoaa kehittäjille työkaluja myös tietoturvan varmistamiseen. Eräs näistä työkaluista on Microsoftin kehittämä GitHub Advanced Security for Azure DevOps (lyh. *GHAZDO*) -tietoturvapalvelu, joka mahdollistaa versionhallinnan tietovarastossa sijaitsevan ohjelmakoodin tarkastamisen. Palvelu automatisoi tietoturvatarkastuksia, jotka tunnistavat ohjelmakoodin haavoittuvuuksia, skannaavat ohjelmakoodia salaisuuksien varalle sekä havaitsevat huonoja koodikäytäntöjä, jotka voivat muodostaa tietoturvariskejä. Palvelu integroituu automaattisen koonnin putkiin, jolloin esimerkiksi haavoittuvuuksien skannauksen voi automatisoida ajettavaksi aina ohjelmakoodin muuttuessa (De paiva, Wesley 2023.)

Tekoälysovelluksen ohjelmakoodia sekä putkien vaatimia Python-paketteja skannattiin GHAZDO-palvelun avulla. Automaattisen koonnin putki, jota palvelu käytti, automatisoitiin ajamaan versionhallinnan tietovaraston muutosten yhteydessä sekä ajastetusti viikoittain. Havaitut haavoittuvuudet korjattiin palvelun tekemillä korjausehdotuksilla.

Azure Pipelines -palvelu mahdollistaa turvallisen tunnistautumisen palveluyhteyksien (engl. *Service connections*) avulla. Palveluyhteydet ovat tunnistautuneita yhteyksiä, joiden avulla Azure Pipelines -palvelu voi suorittaa toimenpiteitä esimerkiksi Azure-tilauksissa tai Docker-rekistereissä. Niitä hyödynnetään esimerkiksi julkaistaessa resursseja Azure-pilviympäristöön, jolloin julkaisu tapahtuu turvallistesti tunnistautuneen yhteyden kautta. Palveluyhteyksille määritellään tarvittavat käyttöoikeudet ja niitä hallitaan Azure DevOps -palvelun projektien tasolla. (Manage service connections 2024.)

Insinöörityössä Azure-tilaukselle tunnistautumiseen käytettiin palveluyhteyttä, joka tilattiin keskitetyltä taholta. Palveluyhteys oli oikeutettu hallinnoimaan resursseja koko tilauksella, sillä toteutettu infrastruktuuri sijaitsi useassa eri resurssiryhmässä. Sekä tekoälysovelluksen että infrastruktuurin julkaisun putket käyttivät tätä palveluyhteyttä.

7.3 Agentit

Agentit ovat laskentaresursseja, joilla Azure Pipelines -palvelun automaattisen koonnin putket suoritetaan. Agentit suorittavat putkissa määritellyt komennot yksi kerrallaan. Azure Pipelines -palvelu tarjoaa erilaisia agenttityyppejä, kuten esimerkiksi Microsoftin hallitsemat agentit (engl. *Microsoft-hosted agents*) sekä itsehallinnoidut agentit (engl. *Self-hosted agents*). Microsoftin hallitsemat agentit ovat Microsoftin alustamia ja ylläpitämiä, jolloin käyttäjä ei ole vastuussa niiden konfiguroinnista tai ylläpidosta. Microsoftin hallitsemilla agenteilla ajettu putki suoritetaan tilapäisellä virtuaalikoneella, joka alustetaan uudelleen putken suorituksen jälkeen. (Azure Pipelines agents 2025.)

Itsehallinoidut agentit asennetaan ja ylläpidetään organisaation omilla palvelimilla tai virtuaalikoneilla. Käyttäjä luo itse laskentaresurssin, jolle itsehallinoidun agentin ohjelmisto asennetaan, jonka jälkeen agentti rekisteröidään haluttuun DevOps -projektiin. Itsehallinoidut agentit tarjoavat joustavuutta esimerkiksi asennettavien ohjelmistojen suhteen, ja ne ovat täysin käyttäjän konfiguroitavissa. (Azure Pipelines agents 2025.)

Microsoftin hallinnoimat agentit tarjoavat suoraviivaisen tavan suorittaa automaattisen koonnin putkia ilman, että käyttäjä on vastuussa agenttien konfiguroinnista tai ylläpidosta. Itse hallinoidut agentit taas ovat käyttäjän konfiguroitavissa, ja ne sopivat esimerkiksi tilanteeseen, jossa agentilla täytyy olla pääsy verkkoeriytettyihin resursseihin. (Azure Pipelines agent 2025.)

Insinöörityössä käytettiin itsehallinoituja agentteja. Agentilla täytyi olla pääsy verkkoeriytettyihin resursseihin tekoälysovelluksen Azure-ympäristöissä. Microsoftin hallinnoimilla agenteilla tämä ei ollut mahdollista, joten insinöörityön aikana konfiguroitiin itsehallinoitu ja verkkoeriytetty agentti.

Agenttia varten luotiin virtuaalikone sekä yksityinen päätepiste integraatioaliverkkoon, mikä mahdollisti agentin pääsyn virtuaaliverkon muissa aliverkoissa sijaitseviin verkkoeriytettyihin resursseihin. Virtuaalikonee luotiin B2ms-kapasiteetilla, joka on suorituskyvyltään kohtuullisen heikko. Insinöörityötä varten ei tarvittu suuria määriä laskentatehoa, joten kapasiteetin valinnalla pyrittiin kustannustehokkuuteen. Virtuaalikoneelle asennettiin DevOps Agent -ohjelmisto, jonka jälkeen kone rekisteröitiin osaksi DevOps -projektia, jossa tekoälysovelluksen versionhallinta sekä automaattisen koonnin putket sijaitsivat. Virtuaalikoneelle luotiin huoltokonfiguraatio (engl. *Maintenance configuration*), joka automaattisesti suoritti virtuaalikoneen päivitykset halutuin väliajoin.

7.4 MLOps ja MLOps-sapluunat

MLOps-käytännöt (*Machine Learning Operations*) pyrkivät yhdistämään koneoppimisen ja ohjelmistokehityksen parhaat käytännöt. Niillä pyritään

automatisoimaan ja hallitsemaan tekoäly- ja koneoppimismallien kehitystä, julkaisemista sekä valvontaa eri ympäristöissä. MLOps-käytännöt ovat DevOps-käytäntöjen kaltaisia, mutta ne pyrkivät huomioimaan koneoppimisen erityispiirteitä, kuten esimerkiksi mallien versiointia. MLOps:in toteutus käytännössä tarkoittaa esimerkiksi koneoppimismallin koko elinkaaren hallinnan automatisointia kehityksestä tuotannon ylläpitoon. (Aditya, Soni 2020.)

Insinöörityössä seurattiin MLOps-käytäntöjä. Tekoälysovelluksen malli, ajoympäristö, kehotteet sekä opetusaineisto versioitiin koneoppimistyötilassa ja versionhallinnassa. Käytäntöjä toteutettiin MLOps-sapluunoiden (engl. *MLOps templates*) avulla. Sapluunat ovat Microsoftin kehittämiä Azure Pipelines -palvelun askelia, jotka suorittavat esimerkiksi Az CLI -komentorivityökalun komentoja. Insinöörityössä käytetyt sapluunat ovat parametrisoitavia YAML-määrittelyitä, joita voidaan tuoda osaksi automaattisen koonnin putkien toteutusta.

Sapluunat suorittavat yhden toimenpiteen, joka voi esimerkiksi olla ajoympäristön rekisteröinti koneoppimistyötilaan. Esimerkkikoodi 1 kuvaa ajoympäristön rekisteröinnin suorittavaa sapluunaa. Sapluuna tukee parametrisointia, ja odottaa parametreinään ympäristön nimeä sekä ympäristön YAML-määrittelytiedostoa.

```
# Copyright (c) Microsoft Corporation. All rights reserved.
# Licensed under the MIT License.

parameters:
- name: environment_name
  type: string
- name: environment_file
  type: string

steps:
  - task: AzureCLI@2
    displayName: Register Azure ML environment
    continueOnError: true
    inputs:
      azureSubscription: $(ado_service_connection_rg)
      scriptType: bash
      workingDirectory: $(System.DefaultWorkingDirectory)
      scriptLocation: inlineScript
      inlineScript: |
        az ml environment create \
          --name ${{ parameters.environment_name }} \
          --file ${{ parameters.environment_file }}
```

Esimerkkikoodi 1. Parametrisoitava MLOps-sapluuna, joka luo koneoppimistyötilaan ajoympäristön.

Sapluuna suorittaa Az CLI -komentorivityökalun komennon, joka rekisteröi määrityksen mukaisen ympäristön koneoppimistyötilaan. Esimerkkikoodi 2 havainnollistaa, kuinka sapluunaa käytetään automaattisen koonnin putkessa. Sapluuna tuodaan osaksi putkea erillisestä versionhallinnan tietovarastosta, jolloin sapluunaan voidaan viitata automaattisen koonnin putkessa tiedostonimellä sekä tietovarastolla.

```
resources:
  repositories:
    -  repository: mlops-templates
       name: mlops-templates
       type: git
       ref: main
…
steps:
    -  template: templates/az-cli-v2/register-env.yaml@mlops-templates
       parameters:
         environment_name: “demo_env”
         environment_file: “mlops/azureml/environments/demo_env.yaml”
```

Esimerkkikoodi 2. MLOps-sapluunan käyttö automaattisen koonnin putkessa. Parametrisoitavaa sapluunaa käytetään keskitetystä versionhallinnan tietovarastosta (”mlops-templates”).

MLOps-sapluunat nopeuttivat kehitystyötä merkittävästi. Ne sijoitettiin omaan keskitettyyn versionhallinnan tietovarastoonsa, jossa ne olivat kaikkien automaattisten putkien käytettävissä. Sapluunoiden keskittäminen omaan tietovarastoonsa mahdollisti sen, että sapluunoiden komentojen päivitykset välittyivät automaattisesti kaikkiin sapluunoita hyödyntäviin automaattisen koonnin putkiin.

7.5 Automaattisen koonnin putkien toteutus

Tekoälysovelluksen automaattisen koonnin putket toteutettiin infrastruktuurille sekä sovelluksen kokoamiselle ja julkaisulle koneoppimistyötilassa. Putket muodostivat varsinaisen tuotannollistamisen ratkaisun, joka mahdollisti tekoälysovelluksen siirtämisen ja julkaisun eri ympäristöihin automatisoidusti. Putkien toteutuksessa seurattiin MLOps-käytäntöjä, jotka versioivat tekoälysovelluksen sekä sen vaatimat koneoppimistyötilan sisäiset resurssit.

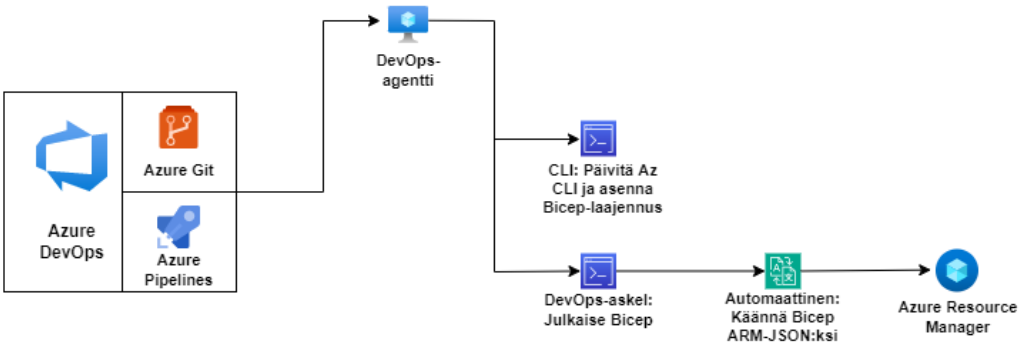
7.5.1 Infrastruktuurin julkaisu

Infrastruktuurin julkaisun putki suoritettiin itsehallinnoidulla agentilla, sillä Bicep-määrittelytiedostojen suorittaminen edellytti yhteyttä virtuaaliverkkoon. Virtuaalikone, jota agentti käytti, sijaitsi virtuaaliverkon integraatioaliverkossa, mikä mahdollisti julkaistujen resurssien verkkoeriyttämisen. Infrastruktuurin putki parametrisoitiin kehitys- ja tuotantotarkoituksiin käyttäen JSON-muotoisia Bicep-parametritiedostoja, jolloin samaa automaattisen koonnin putkea hyödynnettiin kummankin ympäristön julkaisuun. Käytettävän parametritiedoston nimi päätellään putkessa suorituksen aikana valitun ympäristön perusteella.

Infrastruktuurin julkaisun putki oli rakenteeltaan yksinkertainen, ja se koostui kolmesta askeleesta. Ensimmäisessä askeleessa infrastruktuurin Bicep-määrittelytiedostot ladattiin versionhallinnan tietovarastosta agentin virtuaalikoneelle väliaikaiseen hakemistoon. Toisessa askeleessa päivitettiin Az CLI -komentorivityökalu ja sen Bicep-laajennus. Laajennus on tarkoitettu Bicep-määrittelytiedostojen julkaisuun ja hallinnointiin. Kolmannessa askeleessa suoritettiin

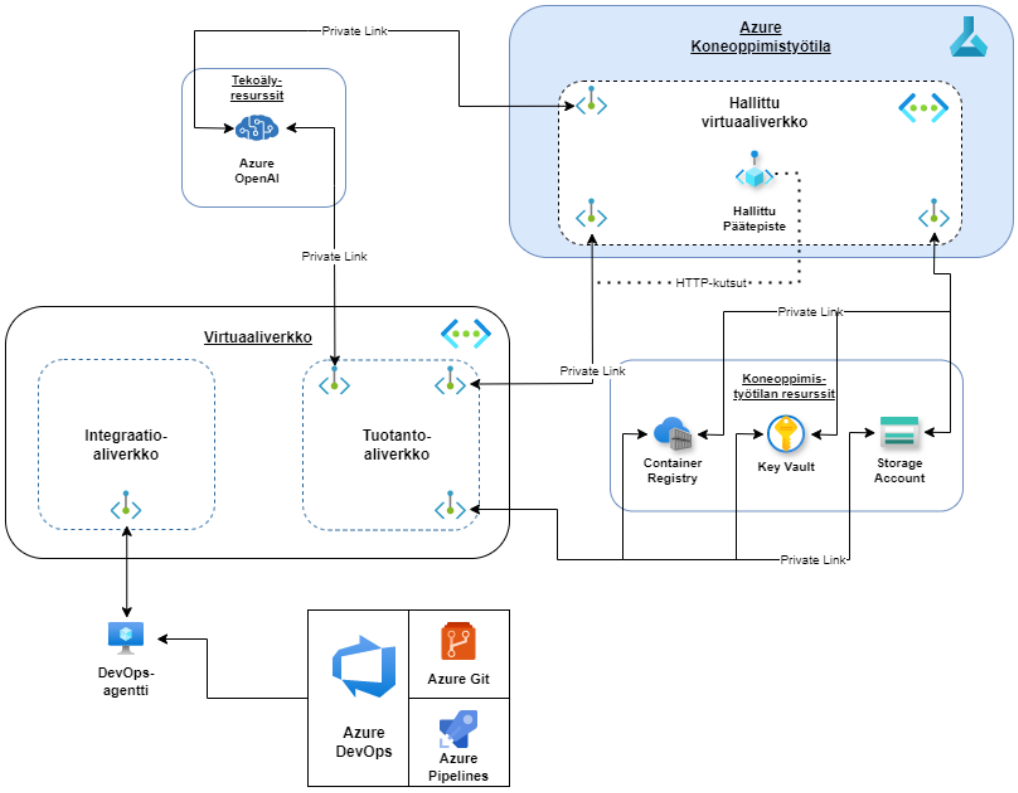
julkaisu hyödyntäen DevOps Pipelines -palvelun tarjoamaa valmista AzureResourceManagerTemplateDeployment@3-askelta.

Julkaisussa käytetty AzureResourceManagerTemplateDeployment@3-askel mahdollistaa määrittelytiedostojen julkaisun eri laajuuksilla, kuten esimerkiksi tilaus- tai resurssiryhmätasolla. Insinöörityössä julkaisut suoritettiin tilaustasolla, sillä määrittelytiedostot loivat resursseja kolmeen eri resurssiryhmään. Vaihtoehtoisesti julkaisut olisi voitu suorittaa käyttäen Azure CLI -komentorivityökalua, mutta insinöörityössä päädyttiin käyttämään valmiiksi määriteltyä askelta. Valmisaskel tarjoaa optimoidun tavan julkaista määrittelytiedostoja, eikä Azure CLI -työkalu tarjoa julkaisuun merkittäviä etuja. Kuva 7 havainnollistaa automaattisen koonnin putken toimintaa ja julkaisun suoritusta.



Kuva 7. Infrastruktuurin julkaisevan automaattisen koonnin putken suoritus. Bicep-määrittelyt julkaistaan ja syötetään ARM-palvelulle.

Määritellyt askeleet suoritetaan järjestyksessä agentin aloittaessa suorituksen. Parametrisoidut Bicep-muotoiset määrittelytiedostot käännetään automaattisesti JSON-muotoisiksi ARM-palvelua varten, joka luo resurssit haluttuun pilviympäristöön. Kuva 8 esittää lopullista resurssirakennetta, jossa Bicep-tiedostoilla määritellyt resurssit on yhdistetty perinteiseen virtuaaliverkkoon.



Kuva 8. Tekoälysovelluksen lopullinen verkkorakenne. Perinteisestä virtuaaliverkosta, ja siihen liitetyistä muista virtuaaliverkoista, on mahdollista muodostaa yhteys hallitussa virtuaaliverkossa sijaitsevaan päätepisteeseen.

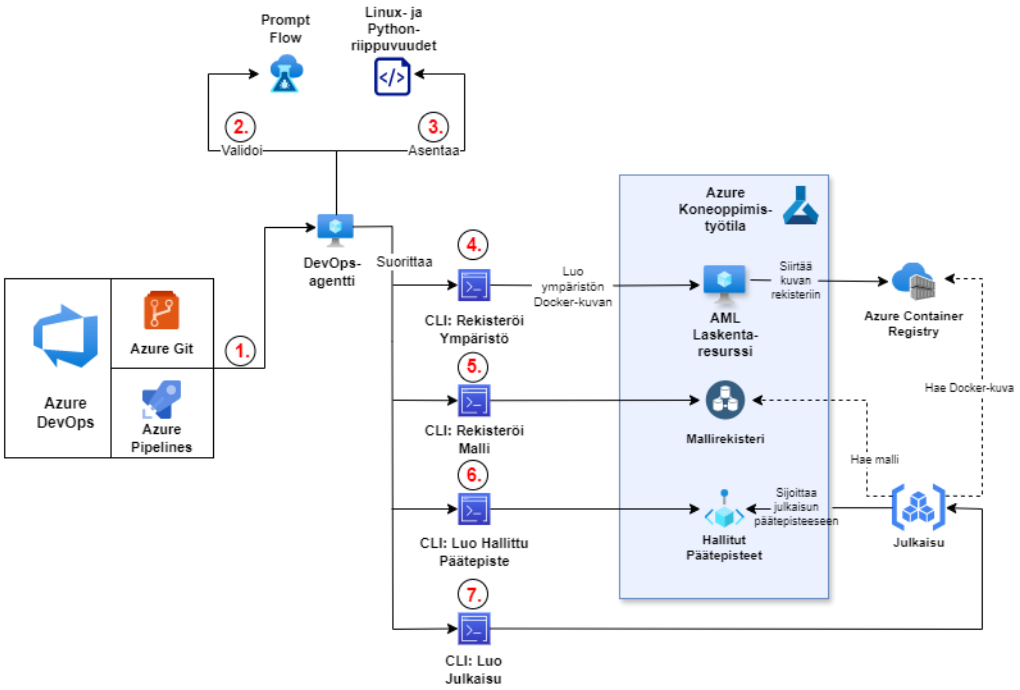
Lopullinen rakenne on verkkoeriytetty eikä yhteyksiä julkiverkon puolelta hyväksytä. Infrastruktuuri mahdollistaa verkkoeriytettyihin resursseihin pääsyn vain virtuaaliverkon sisäpuolelta. Koneoppimistyötilassa sijaitsevaa hallinnoitua päätepistettä voidaan kutsua hub-verkkoon liitetyistä spoke-verkoista, kun päätepisteen DNS-tietue on liitetty DNS-alueeseen, jota kutsujan ympäristö käyttää. Julkaisuja virtuaaliverkkoon kootaan DevOps-agentilla, jonka virtuaalikone on liitetty virtuaaliverkon integraatioaliverkkoon yksityisellä päätepisteellä.

7.5.2 Tekoälysovelluksen julkaisu

Tekoälysovelluksen kokoamisen ja julkaisun automaattisen koonnin putki edellytti myös itsehallinoidun agentin käyttöä, sillä tekoälysovellus koottiin ja julkaistiin verkkoeriytettyyn koneoppimistyötilaan. Putkea ohjattiin YAML-muotoisilla

konfiguraatiotiedostoilla, jotka sisälsivät tiedon käytettävästä palveluyhteydestä sekä tilauksesta, resurssiryhmästä ja koneoppimistyötilasta, johon koottu sovellus julkaistaan. Konfiguraatiotiedosto oli automaattisen koonnin putkessa parametrina, mikä mahdollisti tekoälysovelluksen kokoamisen ja julkaisun automatisoidusti eri ympäristöihin.

Automaattisen koonnin putki määriteltiin kahdessa vaiheessa, jotka kumpikin sisälsivät useita askeleita. Ensimmäisessä vaiheessa tekoälysovelluksen malli ja ajoympäristö koottiin ja versioitiin MLOps-käytäntöjen mukaisesti. Toisessa vaiheessa putki loi koneoppimistyötilaan hallitun päätepisteen, jossa tekoälysovelluksen koottu malli julkaistiin. Lisäksi toisessa vaiheessa määriteltiin, että päätepisteen vastaanottama liikenne ohjataan kokonaisuudessaan uudelle julkaisulle. Seuraavassa kaaviossa (kuva 9) havainnollistetaan tekoälysovelluksen kokoamisen ja julkaisun automaattisen koonnin putken toimintaa.



Kuva 9. Automaattisen koonnin putken suoritusjärjestys sekä toiminnan kuvaus. Ympyröidyt numerot kuvaavat suoritusjärjestystä.

Taulukko 1 kuvaa automaattisen koonnin putken toimintaa yksityiskohtaisesti. Taulukon numerot viittaavat kaavion ympyröityihin numeroihin, jotka kuvaavat putken toimenpiteiden suoritusjärjestystä.

Taulukko 1. Tekoälysovelluksen kokoavan ja julkaisevan putken suoritusjärjestys ja toiminta.

Suoritus-vaihe	**Toiminto**
1.	Automaattisen koonnin putken suoritus alkaa. DevOps-agentti hakee versionhallinnasta viimeisimmän version.
2.	DevOps-agentti varmentaa Prompt Flow -ratkaisun määrittelyn.
3.	DevOps-agentti asentaa Linux- ja Python-riippuvuudet, joita tarvitaan automaattisen koonnin putken suorittamiseen.
4.	DevOps-agentti rekisteröi tekoälysovelluksen ajoympäristön koneoppimistyötilaan Azure CLI -komentorivityökalun avulla. Ympäristön Docker-kuva kootaan koneoppimistilan laskentaresurssilla ja tallennetaan Azure Container Registry -rekisteripalveluun.
5.	DevOps-agentti rekisteröi tekoälysovelluksen ohjelmistokoodin malliksi koneoppimistyötilan mallirekisteriin Azure CLI -komentorivityökalun avulla.
6.	DevOps-agentti luo hallitun päätepisteen Azure CLI -komentorivityökalun avulla.
7.	DevOps-agentti luo julkaisun hallittuun päätepisteeseen Azure CLI -komentorivityökalun avulla. Julkaisu hakee koneoppimistyötilasta ajoympäristön ja mallin, jotka rekisteröitiin aiemmin putkessa.

8 Yhteenveto

Insinöörityön tavoitteena oli toteuttaa erään tekoälysovelluksen tuotannollistaminen ja käyttöönotto Azure-pilviympäristössä. Ratkaisun tuli mahdollistaa sovelluksen automaattinen kokoaminen ja julkaisu eri ympäristöihin. Ympäristöjen tuli olla tietoturvallisia sekä infrastruktuuri koodina -periaatteen mukaisesti määriteltyjä. Työssä kiinnitettiin erityisesti huomiota tietoturvaan, kuten resurssien verkkoeriyttämiseen, käyttöoikeusrajoituksiin ja ohjelmistokoodin haavoittuvuuksien tunnistamiseen. Toteutettu ratkaisu tukee sovelluksen jatkokehittämistä sekä automatisoitua käyttöönottoa eri pilviympäristöissä.

Insinöörityössä kehitetty tekoälysovelluksen tuotannon ja operoinnin ratkaisu täytti sille asetetut vaatimukset. Tekoälysovellus kehitettiin ja tuotannollistettiin insinöörityössä esitellyllä tavalla. Tämä havaittiin toimivaksi käytännöksi. Kirjoittamisen hetkellä tekoälysovellus on ollut useita kuukausia tuotantokäytössä, jossa se on toiminut ongelmitta.

Tekoälysovellusten määrän voidaan odottaa kasvavan tulevaisuudessa, ja insinöörityössä toteutettu ratkaisu tarjoaa toimivan ja tietoturvallisen mallin niiden tuotannollistamiseen. Toteutettu ratkaisu on osoittautunut onnistuneeksi, ja se toimii jatkossa pohjana uusien tekoälysovellusten käyttöönotolle Azure-pilviympäristössä.

Lähteet

Collier, Michael & Shahan, Robin. 2015. Microsoft Azure Essentials - Fundamentals of Azure. E-kirja. Microsoft Press.

Rajendran, Ajith. 2023. Understand the Azure RBAC structure. Verkkoaineisto. Medium. <https://medium.com/@ajithcrajendran/understanding-the-azure-rbac-structure-7666529209ff>. Luettu 06.04.2025.

Tank, Nayan. 2023. Azure Fundamentals (Part 2). Verkkoaineisto. Medium. <https://medium.com/@nayantank/azure-fundamentals-part-2-326bcd3fcaca>. Luettu 06.04.2025.

Add a new connection using the Azure Machine Learning SDK. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/ai-foundry/how-to/develop/connections-add-sdk>. Luettu 22.04.2025.

Authorize access to data in Azure Storage. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/storage/common/authorize-data-access?tabs=blobs>. Luettu 22.04.2025.

Autoscale online endpoints in Azure Machine Learning. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-learning/how-to-autoscale-endpoints?view=azureml-api-2&tabs=cli>. Luettu 23.04.2025.

Azure CI/CD data pipelines. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/devops/pipelines/apps/cd/azure/cicd-data-overview?view=azure-devops>. Luettu 26.4.2025.

Azure Container Registry (ACR). 2023. Verkkoaineisto. Medium. <https://medium.com/@barbieri.santiago/azure-container-registry-acr-1d4dd0eaaaa3>. Luettu 22.04.2025.

Azure Container Registry service tiers. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/container-registry/container-registry-skus>. Luettu 22.04.2025.

Azure Key Vault basic concepts. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts>. Luettu 22.04.2025.

Azure Pipelines agents. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=yaml%2Cbrowser>. Luettu 26.4.2025.

Configure Azure Storage firewalls and virtual networks. 2014. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>. Luettu 22.04.2025.

Connections in prompt flow. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-learning/prompt-flow/concept-connections?view=azureml-api-2>. Luettu 22.04.2025.

Develop prompt flow. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-learning/prompt-flow/how-to-develop-flow?view=azureml-api-2>. Luettu 22.04.2025.

Endpoints for inference in production. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-learning/concept-endpoints?view=azureml-api-2>. Luettu 23.04.2025.

De Paiva, Wesley. GHAzDO: One introduction to GitHub Advanced Security now native in Azure DevOps. 2023. Verkkoaineisto. Medium. <https://blog.devops.dev/ghazdo-one-introduction-to-github-advanced-security-now-native-in-azure-devops-d001cbb96454>. Luettu 27.4.2025.

Hub-spoke network topology in Azure. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/hub-spoke>. Luettu 20.04.2025.

Infrastructure as Code (IaC): Comparing the tools. 2022. Verkkoaineisto. Microsoft. <https://techcommunity.microsoft.com/blog/itopstalkblog/infrastructure-as-code-iac-comparing-the-tools/3205045>. Luettu 25.04.2025.

Manage service connections. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/devops/pipelines/library/service-endpoints?view=azure-devops>. Luettu 26.4.2025.

Soni, Aditya. 2020. MLOps: The Epoch of Productionizing ML Models. Verkkoaineisto. Medium. <https://medium.com/analytics-vidhya/mlops-the-epoch-of-productionizing-ml-models-4eec06d93623>. Luettu 26.4.2025.

Network isolation with managed online endpoints. 2024. Verkkoaineisto. Microsoft. <https://docs.azure.cn/en-us/machine-learning/concept-secure-online-endpoint?view=azureml-api-2&tabs=cli>. Luettu 23.04.2024.

Network security groups. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>. Luettu 20.04.2025.

Network Security for Azure Key Vault. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/key-vault/general/network-security>. Luettu 22.04.2025.

Parameters in Bicep. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/parameters>. Luettu 25.04.2025.

Secure an Azure Machine Learning workspace with virtual networks. 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-

learning/how-to-secure-workspace-vnet?view=azureml-api-2&tabs=requi-red%2Cpe%2Ccli>. Luettu 23.04.2025.

Virtual network traffic routing. 2025. Verkkoaineisto. Microsoft <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>. Luettu 20.04.2025.

What are ARM templates? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/overview>. Luettu 25.04.2025.

What is Azure CLI? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/cli/azure/what-is-azure-cli>. Luettu 26.4.2025.

What is Azure Devops? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/devops/user-guide/what-is-azure-devops?view=azure-devops>. Luettu 26.4.2025

What are Azure Machine Learning Environments? 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-learning/concept-environments?view=azureml-api-2>. Luettu 22.04.2025.

What is Azure Machine Learning prompt flow? 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-learning/prompt-flow/overview-what-is-prompt-flow?view=azureml-api-2>. Luettu 22.04.2025.

What is an Azure Machine Learning Workspace? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/machine-learning/concept-workspace?view=azureml-api>. Luettu 21.04.2024.

What is Azure OpenAI Service? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/ai-services/openai/overview>. Luettu 22.04.2025.

What is Azure Pipelines? 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/devops/pipelines/get-started/what-is-azure-pipelines?view=azure-devops>. Luettu 26.4.2025.

What is Azure Private Link? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/private-link/private-link-overview>. Luettu 13.04.2025.

What is an Azure Private DNS zone? 2023. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/dns/private-dns-privatednszone>. Luettu 20.04.2025.

What is Azure Repos? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/devops/repos/get-started/what-is-repos?view=azure-devops>. Luettu 26.4.2025.

What is Azure Resource Manager? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview>. Luettu 30.3.2025.

What is Azure Virtual network? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>. Luettu 13.04.2025.

What is Bicep? 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/overview?tabs=bicep>. Luettu 25.04.2025.

What is a private endpoint? 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview>. Luettu 13.04.2025.

What is infrastructure as code (IaC)? 2024. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code>. Luettu 24.04.2025.

Workspace Managed Virtual Network Isolation. 2025. Verkkoaineisto. Microsoft <https://learn.microsoft.com/en-us/azure/machine-learning/how-to-managed-network?view=azureml-api-2&tabs=azure-cli>. Luettu 23.04.2025.

YAML schema reference for Azure Pipelines. 2025. Verkkoaineisto. Microsoft. <https://learn.microsoft.com/en-us/azure/devops/pipelines/yaml-schema/?view=azure-pipelines>. Luettu 26.4.2025.