**Janita Tokola**

# PALVELINYMPÄRISTÖN VALINTA

**Opinnäytetyö**
**CENTRIA-AMMATTIKORKEAKOULU**
**Tieto- ja viestintätekniikan koulutusohjelma**
**Joulukuu 2021**

**TIIVISTELMÄ OPINNÄYTETYÖSTÄ**

| | | |
|---|---|---|
| **Centria-ammattikorkeakoulu** | **Aika**<br>Joulukuu 2021 | **Tekijä/tekijät**<br>Janita Tokola |
| **Koulutus**<br>Tieto- ja viestintätekniikka | | ☒ AMK<br>☐ YAMK |
| **Työn nimi**<br>PALVELINYMPÄRISTÖN VALINTA | | |
| **Työn ohjaaja**<br>Sakari Männistö | | **Sivumäärä**<br>50 |
| **Työelämäohjaaja** | | |


Opinnäytetyön tavoitteena oli opastaa lukijaa palvelinympäristön valinnassa. Tarkoituksena oli perustella pilvipalvelinympäristön olevan hyvä vaihtoehto fyysiselle palvelinympäristölle. Työssä käytiin läpi tietoturvan keskeisiä asioita, palvelimia yleisesti, palvelinympäristöratkaisuja ja pilvipalveluntarjoajia sekä heidän tuotteitaan, jotka sopivat palvelinympäristön toteutukseen.

Lopuksi työssä luotiin virtuaalipalvelin käyttäen Microsoft Azurea ja tehtiin vertailu pilvipalvelinympäristön sekä fyysisen palvelinympäristön välillä. Työn tuloksena päädyttiin siihen, että pilvipalvelinympäristö on hyvä vaihtoehto fyysiselle palvelinympäristölle tai ainakin osaksi sellaista.



**Asiasanat**
Palvelin, Palvelinympäristö, Microsoft Azure, Amazon Web Services

**ABSTRACT**

| | | |
|---|---|---|
| **Centria University of Applied Sciences** | **Date**<br>December 2021 | **Author**<br>Janita Tokola |
| **Degree programme**<br>Information Technology | | |
| **Name of thesis**<br>SERVER ENVIRONMENT SELECTION | | |
| **Centria supervisor**<br>Sakari Männistö | | **Pages**<br>50 |
| **Instructor representing commissioning institution or company** | | |


The aim of this thesis was to guide in the selection of server environment. Purpose was to justify that a cloud server environment is a good alternative to a physical server environment. The key issues of security, servers in general, server environment solutions, cloud service providers and their products that are suitable for the impletion of a server environment, were covered in this thesis.

At the end of the thesis a virtual server was created using Microsoft Azure and a comparison between cloud server environment and physical server environment was made. As a result of the work, it was concluded that the cloud server environment is a good alternative to a physical server environment or at least as a part of a physical server environment.



**Key words**
Server, Server environment, Microsoft Azure, Amazon Web Services

## KÄSITTEIDEN MÄÄRITTELY

**Biometrinen todentaminen**

Käyttäjän identiteetin todennus biometrisen tunnisteen kuten sormenjäljen avulla

**DHCP**

Dynamic Host Configuration Protocol

**DNS**

Domain Name Server

**Etäyhteys**

Verkossa olevalle laitteelle kuten tietokoneelle muodostettava yhteys

**IP-osoite**

Tunniste, jonka avulla laite pystyy kommunikoimaan verkossa.

**IT-infrastruktuuri**

IT-laitteiden ja palveluiden muodostama kokonaisuus

**Kaksivaiheinen tunnistautuminen**

Kaksi tunnistautumistapaa yhdistävä käyttäjän todentaminen

**Pilvipalvelu**

Verkon yli käyttöresursseja, esimerkiksi virtuaalikoneita tai tallennustilaa, tarjoava palvelu.

**RAM**

Lyhenne sanoista Random Access Memory. Tietokoneen käytönaikainen muisti.

**RDP**

Lyhenne sanoista Remote Desktop Protocol. Tarkoittaa etäkäyttöprotokollaa, jonka avulla voidaan muodostaa yhteys tietokoneelta toiselle.

**Salaus**

Tiedon muuttaminen tunnistamattomaan muotoon tiedon salaamiseksi, jotta tiedosta ei olisi hyötyä sen ajautuessa vääriin käsiin

**Web-palvelin**

Välittää verkkosivun sisällön käyttäjälle käyttäen HTTP-protokollaa

# 1 JOHDANTO

Aiemmin ainoa vaihtoehto palvelinympäristölle oli toteuttaa se fyysisesti. Viimeisen vuosikymmenen aikana varteenotettavaksi vaihtoehdoksi on muodostunut myös palvelinympäristön toteuttaminen virtuaalisesti pilvipalvelun avulla. Jotta näistä kahdesta vaihtoehdosta voitaisiin valita sopivin, on hyvä perehtyä palvelinympäristön valintaan tarkemmin.

Tämä opinnäytetyö kertoo palvelinympäristön valinnasta. Työn tavoitteena on opastaa palvelinympäristöä toteuttamassa olevaa tahoa sopivan ympäristön valinnassa ja vastata kysymykseen, miksi pilvipalvelinympäristö on hyvä vaihtoehto fyysiselle palvelinympäristölle. Tässä opinnäytetyössä painopiste fyysisten palvelinympäristöjen sijaan on pilvipalvelinympäristöissä. Aluksi käydään läpi keskeisimpiä asioita tietoturvasta ja tietoturvauhista, koska ymmärrys tietoturvasta on olennaista palvelinympäristöä valitessa. Opinnäytetyössä esitellään erilaisia palvelimia ja käydään läpi palvelimien hallintaa ja tietoturvaa. Palvelimien yleisesittelyn jälkeen tutkitaan palvelinympäristöratkaisuja, kerrotaan pilvipalveluista ja käydään läpi palvelinympäristön toteuttaminen Microsoft Azure -palvelussa. Lopuksi vertaillaan pilvipalvelinympäristöä ja fyysistä palvelinympäristöä toisiinsa.

Opinnäytetyössä on käytetty lähdemateriaalina IT-alan kirjallisuutta ja useita verkkojulkaisuja. Pääpaino lähteiden käytössä on verkkojulkaisuissa, koska työhön sopivaa alan kirjallisuutta on vähäisesti saatavilla.

# 2 TIETOTURVA

Tietoturva on datan suojaamista; tavoitteena on turvata palvelun vakaa toiminta ja ehkäistä tietojen ajautumista vääriin käsiin. Tietoturva on erittäin tärkeä asia, koska tietotekniikan kautta tarjotaan suurin osa saatavilla olevista yhteiskunnan tarjoamista ja tuottamista palveluista. Hyvin toteutettu tietoturva onkin toimivan IT-infrastruktuurin kulmakiviä. (Andreasson & Koivisto 2013, 32.)

Jotta palvelinympäristöä voitaisiin hallita parhaalla mahdollisella tavalla, on hyvä perehtyä tietoturvan peruskäsitteisiin. Tietoturvan tulee ottaa huomioon kolmen osa-alueen toteutuminen: luottamuksellisuus, eheys ja käytettävyys. Näiden kolmen osa-alueen suojaamiseksi voidaan hyödyntää muun muassa palomuureja, VPN-yhteyttä, autentikointia ja fyysistä suojausta. Vaikka suojaus olisikin toteutettu hyvin, ei tietoturva kuitenkaan koskaan voi olla täysin aukoton, ja siitä syystä täytyisikin olla myös riskienhallintasuunnitelma.

## 2.1 Luottamuksellisuus

Luottamuksellisuuden tarkoituksena on suojata tiedot väärinkäytöksiltä. Tiedoilla voidaan tarkoittaa esimerkiksi arkaluontoisia tietoja, kuten henkilötietoja tai yrityksen luottamuksellisia tietoja. Jos arkaluontoiset tiedot pääsevät vääriin käsiin, lopputulema voi olla katastrofaalinen. Tästä syystä luottamuksellisuutta tulee pyrkiä suojaamaan monella eri tapaa. (Chapple 2021.) Luottamuksellisuuden säilyttämiseksi tärkeää on hyvä salasanapolitiikka, salaus sekä vahva tunnistautuminen, esimerkiksi kaksivaiheinen tunnistautuminen ja biometrinen autentikointi (Smart Eye Technology 2021).

## 2.2 Eheys

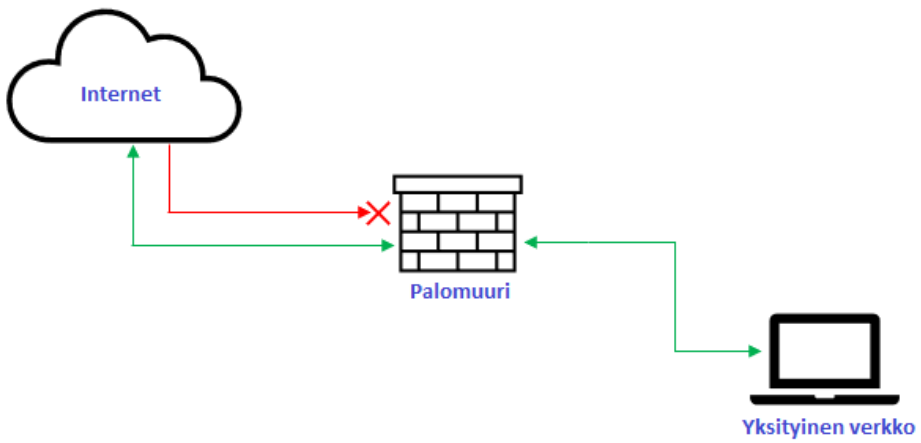
Eheydellä tarkoitetaan, että tiedot ovat sellaisia kuin niiden kuuluisikin olla ja ne eivät muutu hallitsemattomasti. Toisin sanoen suojataan tiedot niin, ettei niitä päästä tahallisesti tai tahottomasti muuttamaan luvattomasti. Vain oikeutetulla taholla tulisi olla pääsy muuttamaan tietoja. (Chapple 2021.) Hyviä esimerkkejä tavoista, joilla eheyden säilyvyys varmistetaan, ovat salaus, käyttäjävalvonta, varmuuskopiointi ja virheentunnistus (Smart Eye Technology 2021).

### 2.3 Käytettävyys

Käytettävyys takaa, että tiedot ovat luvallisten käyttäjien saatavilla keskeytyksettä. Tietojen hallinnoijan pitää huolehtia siitä, että laitteistot, kuten palvelimet, pysyvät ylhäällä. Käytettävyyden takaamiseksi tulee huolehtia muun muassa varmuuskopioinnista, vikasiedosta ja monitoroinnista. (Smart Eye Technology 2021.)

### 2.4 Palomuuri

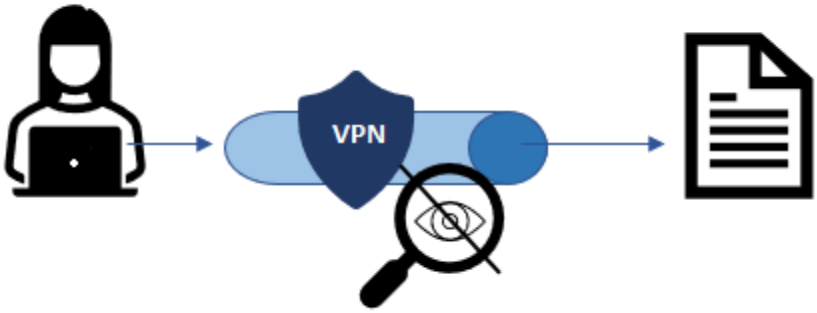
Palomuurin tehtävänä on suojata verkossa olevia laitteita tietoturvahyökkäyksiltä. Palomuurin toimintaan kuuluu monitoroida tietoliikennettä; palomuuri päästää lävitseen sallitun liikenteen ja rajoittaa tai estää liikenteen, joka ei ole toivottua (KUVA 1). Palomuuri onkin yksi tärkeimpiä osa-alueita, kun toteutetaan tietoturvaa. Palomuurin toiminta ei kuitenkaan ole välttämättä heti alusta lähtien sellaista kuin toivotaan; palomuurille täytyy asettaa sellaiset säännöt, jotka parhaiten palvelevat juuri sitä tahoa, joka palomuuria käyttää. Säännöt määrittelevät, minkälainen tietoliikenne sallitaan ja mikä ei. Palomuurin sääntöjä voidaan muuttaa tarpeen mukaan. Esimerkiksi jos yrityksessä havaitaan, että jokin työntekijöiden käyttämä tarpeeton tai korvattavissa oleva sivusto ei ole tietoturvallinen, voidaan asettaa sääntö estämään liikenne tuon sivuston kohdalla. Samaten mikäli huomataan, että jokin estetty sivusto tai verkon kautta toimiva sovellus tulisikin sallia, voidaan sääntöjä muuttaa niin, että kyseinen toiminto on jatkossa sallittu. (Andreasson & Koivisto 2013, 24.)




KUVA 1. Palomuurin toiminta (mukaillen Okta 2021.)

## 2.5 VPN

VPN on lyhenne englanninkielisestä termistä Virtual Private Network. Kun VPN on käytössä, laite pystyy yhdistymään toiseen verkkoympäristöön (KUVA 2). VPN-yhteyden muodostamiseksi tarvitaan kuitenkin toimiva paikallinen verkkoyhteys. VPN-tekniikkaa voidaan hyödyntää esimerkiksi, kun halutaan muodostaa suojattu yhteys etätöitä varten. Alkuperäinen tarkoitus VPN-yhteydelle onkin ollut yritystoiminnan piirissä. Nykyään sitä kuitenkin käytetään myös yksityishenkilöiden toimesta esimerkiksi sellaisessa tilanteessa, kun halutaan saada pääsy johonkin verkkopalveluun, joka on sallittu vain tietyssä maassa. VPN-yhteys voi myös suojata käyttäjän identiteettiä piilottaessaan käyttäjän todellisen sijainnin. (Hoffman 2021.)

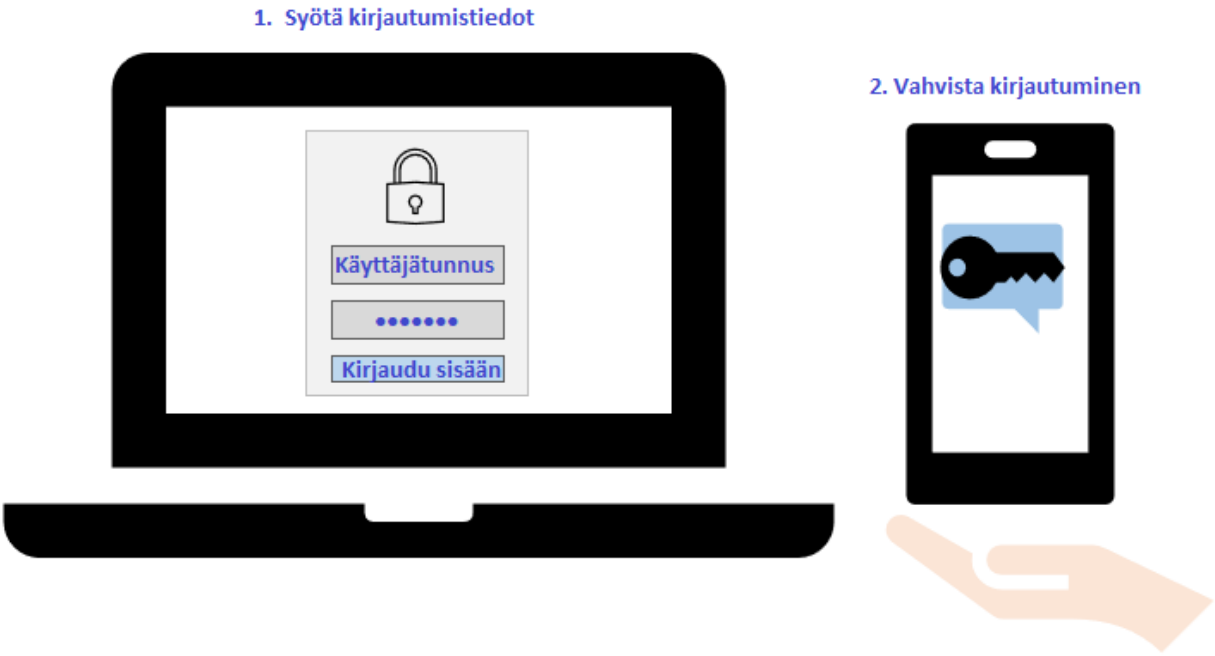



KUVA 2. VPN havainnekuva. (mukaillen F-Secure 2021.)

## 2.6 Todennus

Todennuksella varmistetaan käyttäjän identiteetti. Todennuskeinoja ovat esimerkiksi käyttäjätunnus ja salasana, kaksivaiheinen tunnistautuminen ja biometrinen todennus. Todennusta käytetään estämään luvaton pääsy järjestelmiin tai tietoihin. Kun todennustiedot täsmäävät esimerkiksi todennuspalvelimen tietoihin, käyttäjä on todennettu ja saa pääsyn järjestelmään.

Jotta todennus olisi riittävän vahvaa täytyy käyttäjätunnuskohtaisen salasanan täyttää tietyt määreet, kuten 10 merkkiä, pieniä sekä isoja kirjaimia, erikoismerkkejä ja numeroita. Salasanassa ei myöskään tulisi toistua sama merkki turhan monta kertaa. Käyttäjätunnuksen ja salasanan yhdistelmä ei kuitenkaan välttämättä yksistään riitä vahvaan todennukseen; tällöin kuvaan astuu kaksivaiheinen tunnistautuminen (KUVA 3), joka tarkoittaa kirjautumisen yhteydessä suoritettavaa kirjautumishyväksyntää esimerkiksi sovelluksen avulla. Esimerkki tällaisesta sovelluksesta on Microsoft Authenticator, joka voidaan asentaa älypuhelimeen. Kolmantena vaihtoehtona todennukseen on monivaiheinen tunnistautuminen, joka sisältää esimerkiksi käyttäjätunnuksen ja salasanan yhdistelmän, biometrisen todennuksen ja käyttäjän ennalta asettaman kysymyksen vastattavaksi. (Shacklett & Rosencrance 2021.)




KUVA 3. Kaksivaiheinen tunnistautuminen (mukaillen Mezquita 2020.)

## 2.7 Fyysinen suojaus

Virtuaalisten suojausmekanismien lisäksi on tärkeää muistaa myös fyysisen suojauksen huolellinen toteuttaminen. Palvelimet ja muut verkkoympäristöä ylläpitävät laitteet tulisi sijoittaa niin, että ne ovat

suojattuna niin luvattomalta käytöltä kuin myös esimerkiksi sääolosuhteilta ja sähkökatkoksiltakin. Luvattomalta käytöltä laitteet voidaan suojata fyysisellä tasolla kulun- ja tilojen valvonnalla. Tilaan, johon laitteet ovat sijoitettuna, olisi kannattavaa mahdollistaa pääsy ainoastaan kulkukortilla tai sähköavaimella, jotta voidaan hyödyntää kulunvalvontaa. Kulunvalvonnan merkitys korostuu esimerkiksi sellaisessa tilanteessa, kun on tarve selvittää, kuka tilassa on viimeksi käynyt. Kulun- ja tilojen valvontaa voidaan tehostaa vartioinnilla. Näiden lisäksi laitteita varten tilassa tulisi olla myös palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta. Esimerkiksi sähkövahinkojen torjuntaan voidaan käyttää UPS-järjestelmää, joka tarjoaa keskeytymättömän virransyötön. UPS-järjestelmä suojaa laitteita lyhyiltä sähkökatkoksilta. (Andreasson & Koivisto 2013, 52–53.)

### 2.8 Riskienhallintasuunnitelma

Riskienhallintasuunnitelma auttaa jäsentelemään, mitä riskejä on olemassa, miten näitä riskejä pyritään ehkäisemään ja miten toimitaan, jos riskitilanne toteutuu. Riskienhallintasuunnitelma on ehdoton yritykselle, ja sen toteuttamiseen voidaan hyödyntää esimerkiksi VAHTI-ohjetta VAHTI 22/2017. Kyseinen ohje pohjautuu ISO 31000 riskienhallinta -standardiin. (Suomidigi 2020.)

# 3 YLEISIMMÄT TIETOTURVAUHAT

Tietoturvauhat ovat yleistyneet vuosien varrella. Tietoturvauhkia esiintyy kaikissa laitteissa; etenkin niissä, jotka ovat yhdistettynä verkkoon. Teknologian kehittyessä myös tietoturvauhat ovat monimuotoistuneet. Jotta voitaisiin suojautua uhilta mahdollisimman hyvin, täytyy tietää, minkälaisia uhkia on olemassa. Eri tietoturvauhkien osuudet vaihtelevat; yleisimpiä tietoturvauhkia nykyään ovat käyttäjän manipulointi, kiristyshaittaohjelmat ja palvelunestohyökkäykset. Tietoturvauhkien tavoitteena on tuoda hyökkääjälle rahallista tai muuta hyötyä. (Gurinaviciute 2021.)

## 3.1 Käyttäjän manipulointi

Käyttäjän manipuloinnilla voidaan saada arkaluontoista tietoa hyödynnettäväksi, kuten pankkikorttitietoja tai esimerkiksi yrityksen työntekijän käyttäjätiedot. Esimerkkinä käyttäjän manipuloinnista on kalastelu; käyttäjälle lähetetään kalastelusähköpostiviesti, joka naamioidaan luotettavalta taholta tulleen näköiseksi. Kalastelusähköpostiviesti voi näyttää vaikkapa pankin lähettämältä viestiltä, jossa pyydetään avaamaan linkki pankkitietojen syöttämiseksi. Lähes kaikki raportoidut käyttäjän manipulointitapaukset olivat vuonna 2020 kalasteluyrityksiä. (Gurinaviciute 2021.)

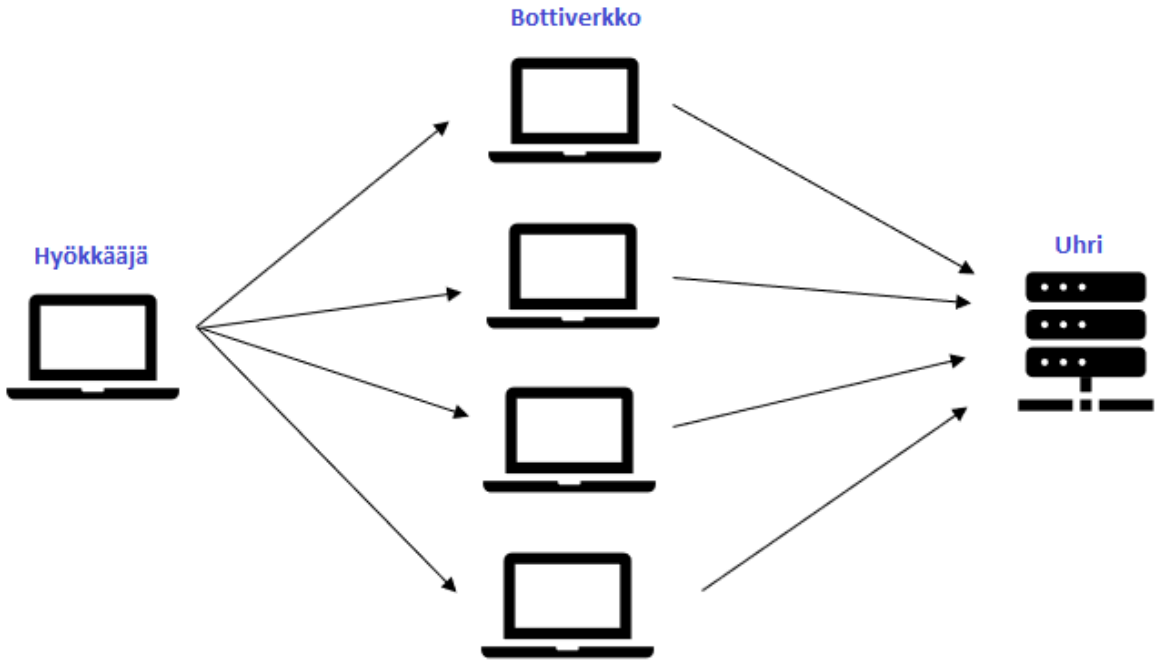
## 3.2 Kiristyshaittaohjelma

Kiristyshaittaohjelmat ovat ohjelmia, jotka saattavat asentua esimerkiksi ladatun tiedoston mukana. Kiristyshaittaohjelma voi esimerkiksi lukita osan käyttäjän tiedostoista ja pyytää suorittamaan maksun lukituksen avaamiseksi. Ideana kiristyshaittaohjelmalla on siis kiristää käyttäjältä rahaa tai muita hyödykkeitä. (Gurinaviciute 2021.)

## 3.3 Palvelunestohyökkäykset

Palvelunestohyökkäyksien päämääränä on estää jotakin palvelua toimimasta kuormittamalla palvelua tarjoavaa laitetta, kuten palvelinta. Kuormitus tapahtuu lähettämällä pyyntöjä ~~niin kauan~~ kunnes pyyn-

töjä on kertynyt niin suuri määrä, että laitteen käsittelykapasiteetti ylittyy. Hyökkääjällä on yleensä käytössään useampi laite pyyntöjen lähettämiseksi. Osa laitteista voi olla hyökkääjän omia, mutta osa taas voi olla hyökkääjän haittaohjelman avulla kaappaamia toisten henkilöiden laitteita (KUVA 4). Tätä hyökkäykseen käytettävää laitekokonaisuutta kutsutaan bottiverkoksi. (Cloudflare 2021.)




KUVA 4. Palvelunestohyökkäys (mukaillen KeyCDN 2018.)

# 4 PALVELIN

Palvelin on laite, jonka avulla ylläpidetään eri palveluita muiden tietokoneiden eli käyttäjien käytettäväksi. Palvelin voi toimia monessa eri roolissa tai sille voidaan yksilöidä oma roolinsa. Roolina voi olla esimerkiksi ylläpitää DHCP-palvelua tai DNS-palvelimena toimiminen. Palvelin on tärkeä osa IT-infrastruktuuria, johon kuuluu useita tietokoneita ja käyttäjiä. Ilman palvelinta esimerkiksi verkkosivuille pääseminen olisi mahdotonta, koska pääsy verkkosivustoille tapahtuu palvelimen välityksellä.

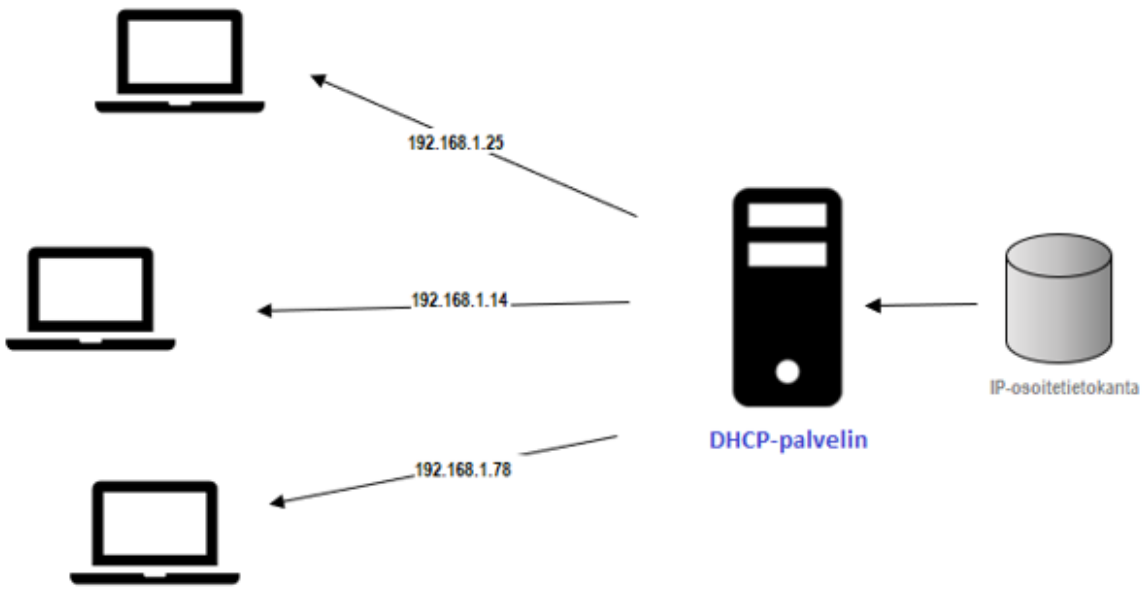
Palvelimena voidaan käyttää tavallista kuluttajatietokonetta tai palvelinkäyttöön kehitettyä laitetta. Varsinaiseen palvelinkäyttöön kehitettyjä laitteita on erilaisia kuten tornipalvelin, rack-palvelin tai bladepalvelin. Yritysmaailmassa käytetään useimmiten virtuaalipalvelimia, palvelinlaitteita tai molempia. (Posey 2021.)

## 4.1 Esimerkkejä eri palvelintyypeistä

Palvelinympäristön infrastruktuurissa tarvittavia palvelimia ovat muun muassa DHCP-palvelin, DNS-palvelin, web-palvelin ja Active Directory -domain-palvelin. Näillä palvelintyypeillä on jokaisella oma käyttötarkoituksensa tietyn toiminnallisuuden ylläpitämiseksi. (Posey 2021.)

### 4.1.1 DHCP-palvelin

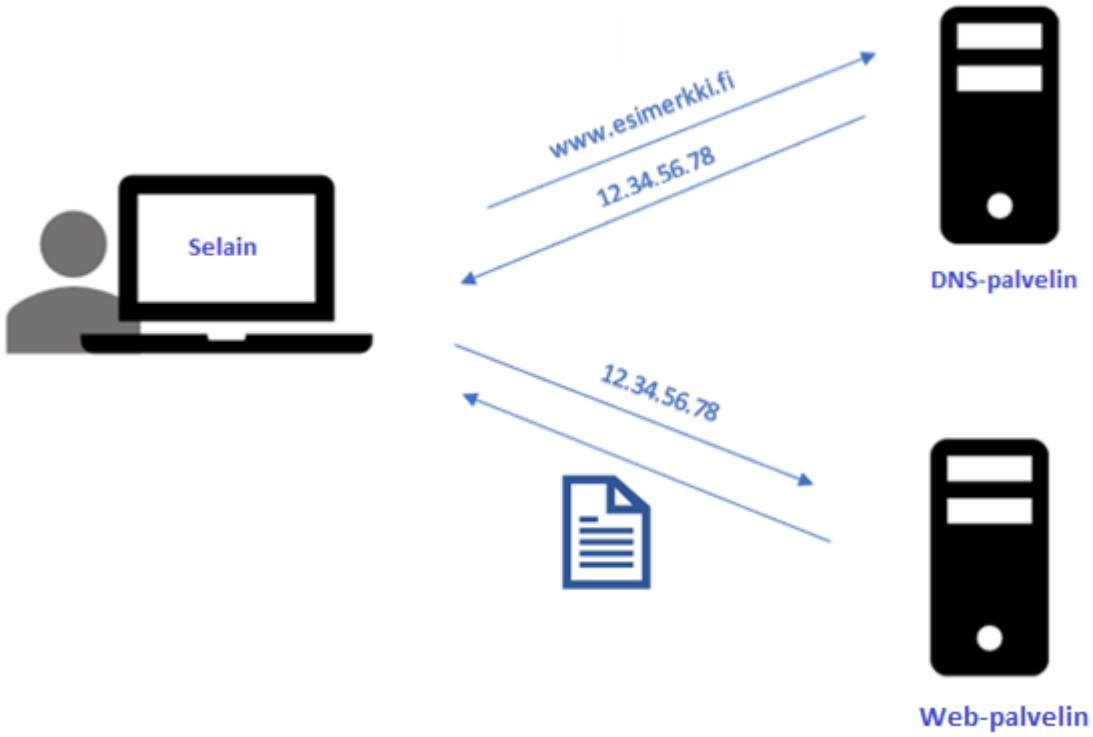
Jos laitteelle, kuten tietokoneelle, ei ole määritetty kiinteää IP-osoitetta, se hakee itselleen automaattisesti IP-osoitteen lähettämällä pyynnön DHCP-palvelimelle. DHCP-palvelimen tehtävänä on siis luovuttaa laitteelle käyttöön vapaana oleva IP-osoite ennalta määritellystä IP-avaruudesta (KUVA 6). Kun laite lopettaa saamansa IP-osoitteen käytön esimerkiksi laitteen sammuessa, laitteen käyttämä IP-osoite vapautuu ja DHCP-palvelin voi luovuttaa vapautuneen IP-osoitteen toisen laitteen käyttöön.




KUVA 6. DHCP-palvelimen toiminta (mukaillen Hazell 2015.)

### 4.1.2 DNS-palvelin

DNS-palvelin muuttaa verkkosivun osoitteen helpommin käytettävissä olevaan muotoon. Ilman DNS-palvelinta esimerkiksi web.centria.fi -sivustolle päästäisiin ainoastaan kirjoittamalla osoiteriville verkkosivuston IP-osoite eli 192.130.183.146. DNS-palvelin helpottaa siis huomattavasti Internetin selausta, koska sen avulla voidaan tarjota numeerisen osoitteen sijasta tekstimuotoinen osoite käyttäjien käytettäväksi. Palvelin hakee eri vaiheiden avulla numeerisen vastaavuuden verkko-osoitteelle ja lähettää sen vastauksena osoitetta hakeneelle selaimelle (KUVA 7). Verkkosivustojen IP-osoitteita voidaan tutkia nslookup-komennon avulla tietokoneen komentokehoteikkunassa. Komento antaa verkkosivuston IP-osoitteen lisäksi mm. tiedon tietokoneen käyttämästä DNS-palvelimesta (KUVA 8). (Fisher 2021.)




KUVA 7. DNS- ja web-palvelimen toiminta (mukaillen Khillar 2021)

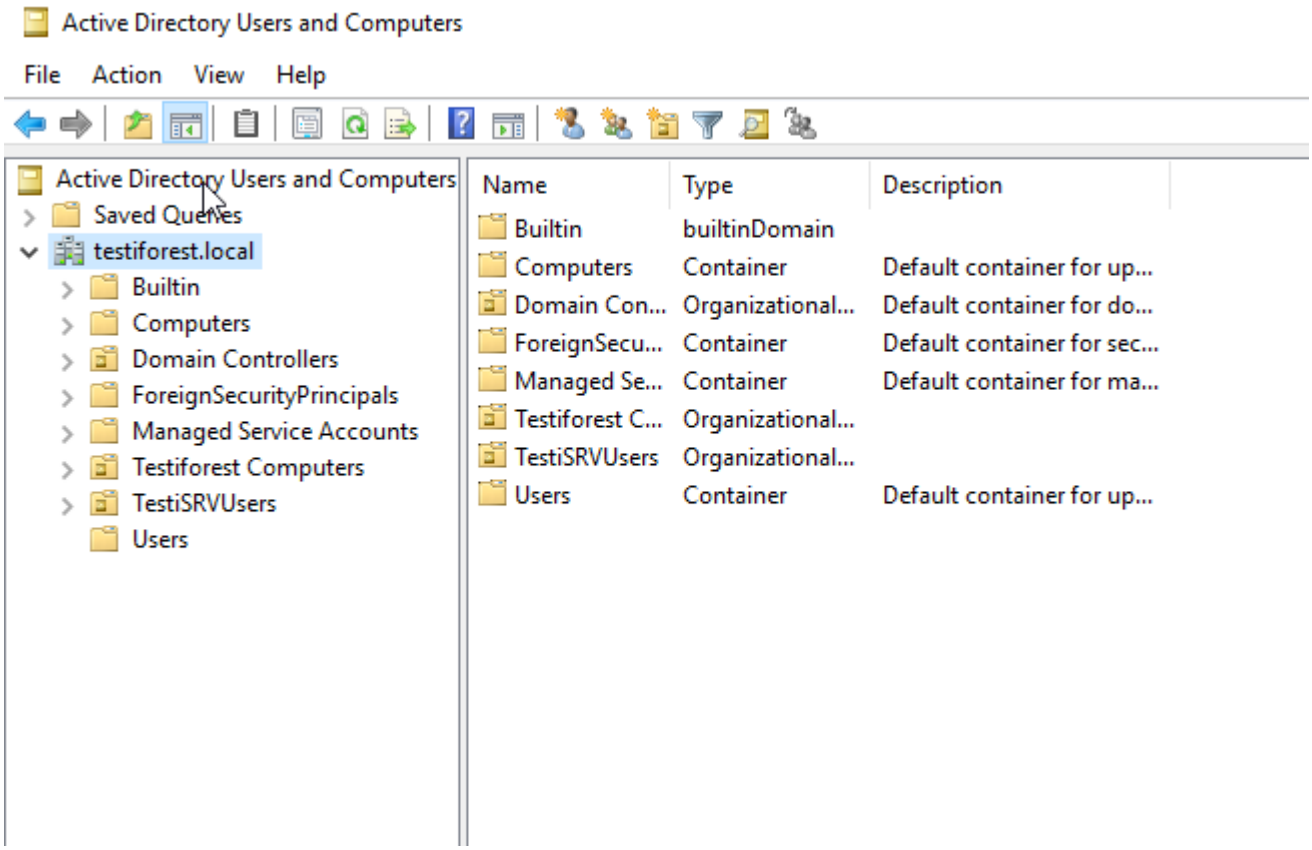
```
C:\Users\[redacted]>nslookup web.centria.fi
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    web-centria-fi.kosila.fi
Address:  192.130.183.146
Aliases:  web.centria.fi
```

KUVA 8. Nslookup-komento

### 4.1.3 Active Directory -domainpalvelin

Active Directory on Microsoftin palvelimille kehittämä palvelu, joka voidaan asentaa Windows Server -käyttöjärjestelmää käyttävälle palvelimelle rooliksi. Active Directorylla voidaan koota IT-infrastruk-

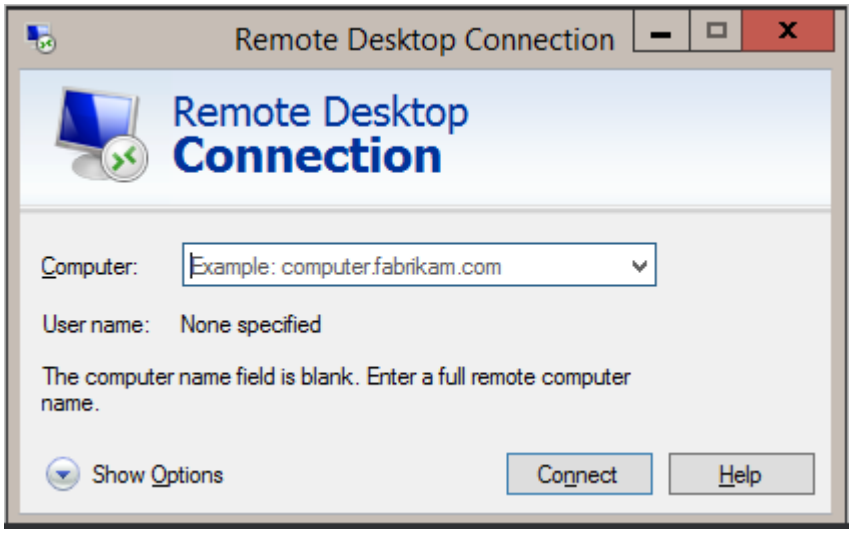
tuurin käyttäjä- ja ryhmätiedot yhteen paikkaan. Active Directoryn avulla voidaan lisätä domainille esimerkiksi käyttäjiä, työasemia ja käyttöoikeusryhmiä. Näitä voidaan hallita ja tarkastella Active Directory Users and Computers -työkalun avulla (KUVA 9). Käyttäjiä ja työasemia voidaan lisätä jäseniksi eri käyttöoikeusryhmiin, jotka antavat ryhmän mukaiset käyttöoikeudet ryhmän jäsenille. Ryhmistä voidaan myös tarvittaessa poistaa jäseniä.




KUVA 9. Active Directory Users and Computer -näkymä

### 4.2 Palvelimen hallinta

Pääsy palvelimelle tapahtuu useimmiten toiselta tietokoneelta etäyhteyden avulla. Pääsyn tulisi olla evätty kaikilta muilta paitsi määritellyiltä järjestelmänvalvojatunnuksilta. Etäyhteyden muodostamiseen voidaan käyttää esimerkiksi Microsoftin omaa Remote Desktop -sovellusta (KUVA 10) tai muun palveluntarjoajan etäyhteystyökalua, kuten BeyondTrustia. Remote Desktop -sovellusta käytettäessä syötetään palvelimen IP-osoite, jonka jälkeen syötetään kirjautumistiedot. Mikäli syötetyt kirjautumistiedot vastaavat tunnusta, jolla on käyttöoikeus palvelimeen, avautuu yhteys palvelimelle. Pääsyä palvelimelle tarvitaan esimerkiksi silloin, kun palvelimen ylläpitämään palveluun tarvitsee tehdä muutoksia.




KUVA 10. Remote Desktop (Microsoft 2021a)

### 4.3 Palvelimen hallinnan tietoturva

Yksi tärkeimmistä asioista tietoturvallisessa palvelimen hallinnassa on se, että palvelimeen on asetettu pääsy vain järjestelmänvalvojatunnuksilla. Palvelimeen ei tule mahdollistaa pääsyä sellaisille käyttäjätunnuksille, joiden käyttäjillä ei ole tarvetta tehdä muutoksia palvelimelle. On kuitenkin mahdollista, että palvelimen hallintaan käytetyt käyttäjätunnukset joutuvat vääriin käsiin. Tätä voidaan ehkäistä muun muassa vahvalla salasanapolitiikalla, joka sisältää vähimmäisvaatimukset salasanan pituudelle ja monimuotoisuudelle sekä salasanan pakollisen vaihtamisen tietyin aikavälein. Palvelinta on mahdollista suojata luvattomalta pääsyltä myös palomuurin, virustentorjuntaohjelman ja tietojen salauksen avulla. (SolarWinds 2021.)

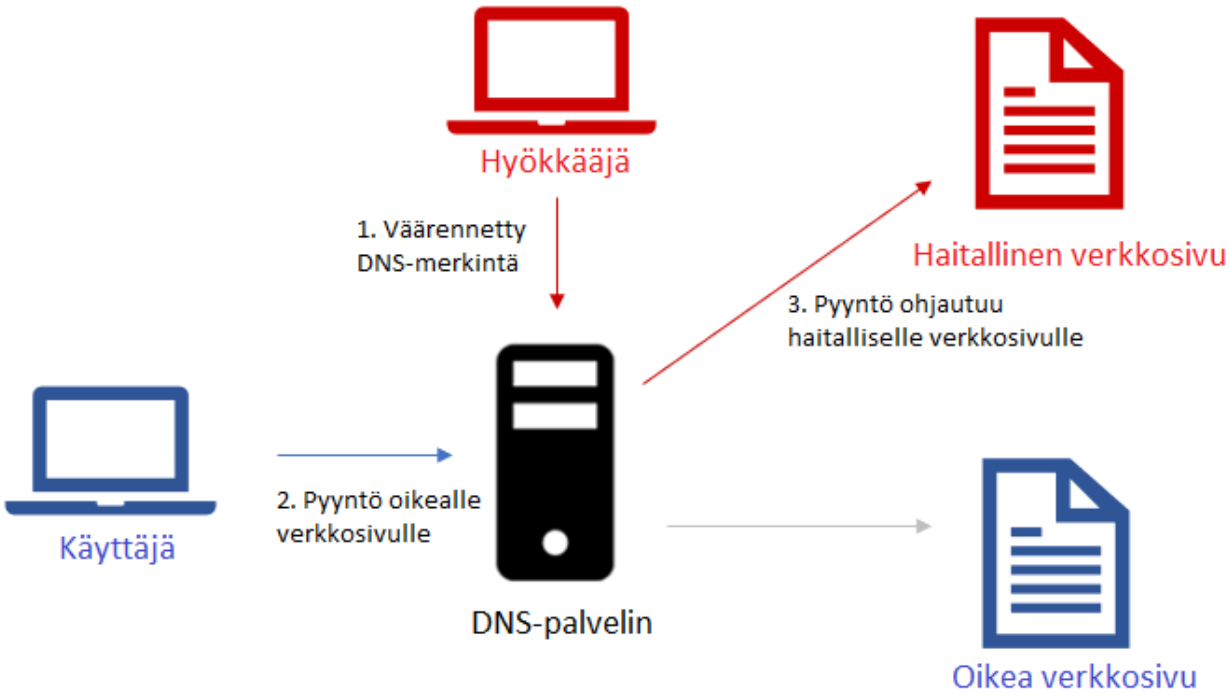
### 4.4 Palvelimiin kohdistuvat tietoturvauhat

Palvelimet ovat yhtä lailla alttiita tietoturvauhille kuin muutkin verkossa olevat laitteet. Palvelimelle pääsyä voidaan havitella esimerkiksi käyttäjän manipuloinnilla, kuten kalasteluyrityksillä, tavoitteena saada haltuun käyttäjätunnukset, jotka tarjoavat väylän palvelimelle tunkeutumiseen. Varsinaisiin palvelimeen kohdistuviin tietoturvauhkiin kuuluvat kuitenkin olennaisesti palvelunestohyökkäykset, joiden tavoitteena on hidastaa tai pysäyttää palvelimen tuottama palvelu hyökkääjän tavoitteen saavuttamiseksi. Muita palvelimiin kohdistuvia tietoturvauhkia ovat muun muassa DNS- ja DHCP-väärentäminen eli niin

kutsutut DNS- ja DHCP-spoofing. Nämä molemmat ovat man-in-the-middle-hyökkäyksiä eli hyökkäyksiä, joissa hyökkääjä asettuu käyttäjän ja palvelimen väliselle reitille.

### 4.4.1 DNS-väärentäminen

DNS-väärentämisessä hyökkääjä voi esimerkiksi uudelleen konfiguroida DNS-palvelimen ohjaamaan käyttäjät pyytämiensä verkkosivustojen sijaan haitallisille verkkosivustoille (KUVA 11). DNS-väärentämisessä hyökkääjä käyttää hyväkseen heikkouksia DNS-palvelimen tietoturvassa. Tavoitteena DNS-väärentämisessä voi olla esimerkiksi arkaluontoisten tietojen varastaminen. Tietojen päästä päähän salaus sekä DNS-väärentämisen havaitsemistyökalut ovat hyviä keinoja suojautua väärentämisyrityksiltä. (Kaspersky 2021.)




KUVA 11. DNS-väärentäminen

### 4.4.2 DHCP-väärentäminen

DHCP-väärentäminen alkaa hyökkääjän suorittamalla DHCP-palvelimen kuormittamisella. Hyökkääjä lähettää DHCP-palvelimelle pyyntöjä väärennetyllä MAC-osoitteella, kunnes DHCP-palvelimen tarjoamien IP-osoitteiden määrä on täyttynyt eikä palvelin enää kykene vastaamaan tuleviin DHCP-kyselyihin. Tämän jälkeen hyökkääjä asettaa verkkoon oman rogue DHCP-palvelimen eli nk. vihamielisen DHCP-palvelimen, jonka jälkeen alkaa varsinainen DHCP-väärentäminen. Hyökkääjä muuttaa DHCP-pyynnön lähettävän käyttäjän oletusyhdyskäytävän ja DNS-palvelinosoitteen suuntaamaan omaan verkkoonsa keräten arkaluontoista käyttäjätietoa. (Omnisecu.com 2021.)

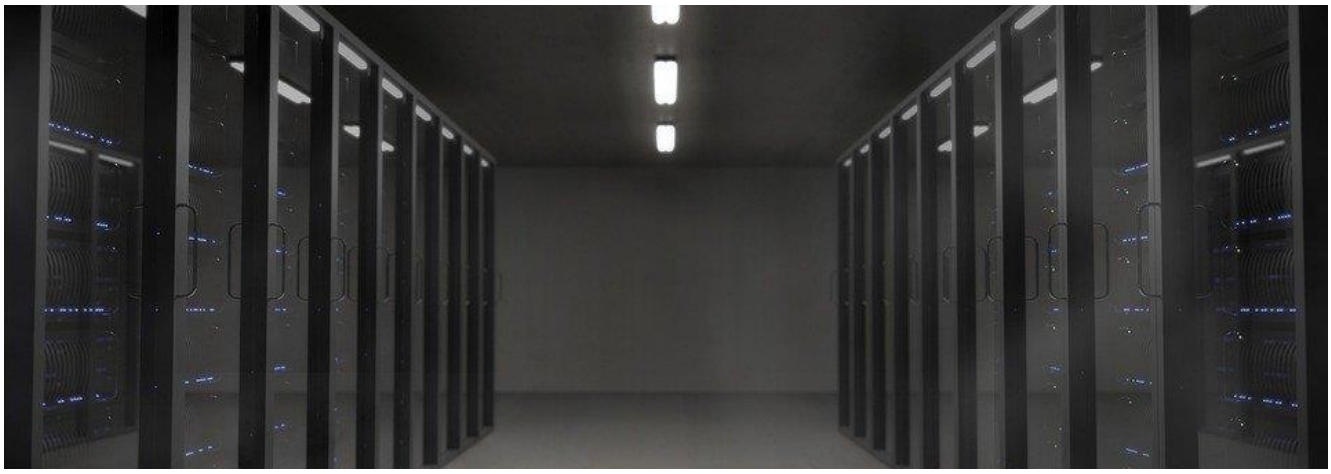
# 5 PALVELINYMPÄRISTÖRATKAISUT

Palvelinympäristö on mahdollista toteuttaa esimerkiksi fyysisten palvelinten tai pilvipalvelun avulla. Kullakin ratkaisulla on omat hyvät ja huonot puolensa. Valintaa tehdessä tulisi miettiä, mitkä ominaisuudet ovat juuri omiin tarpeisiin olennaisia. Useimmiten valintaan vaikuttavat suuressa määrin kustannukset, ylläpito- ja muutosmahdollisuudet sekä tietoturva.

## 5.1 Fyysinen palvelinympäristö

Fyysisessä palvelinympäristössä palvelimet sijaitsevat useimmiten joko omassa tai palveluntarjoajan konesalissa (KUVA 12). Fyysinen palvelinympäristö on mahdollista siis toteuttaa joko itse tai ostopalveluna palveluntarjoajalta. Itse toteutettavan palvelinympäristön palvelimet hankitaan kertahankintana, ja palvelimen tarvittavasta määrästä riippuen summa voi olla hyvinkin korkea. Esimerkiksi yhden tornipalvelimen hinta voi olla ominaisuuksista riippuen noin 400–4 600 euroa (Atea 2021).

Fyysisiä palvelinratkaisuja pohdittaessa edullisemmaksi voi tulla palveluntarjoajan konesalipalvelun ostaminen, jotka ovat yleensä kuukausimaksullisia. Konesalipalvelun valinta voi laskea vuosikohtaisia kustannuksia esimerkiksi henkilöstökustannuksissa, koska tällöin ei välttämättä tarvita yhtä monipuolista osaamista omaavaa IT-henkilöstöä. Palveluntarjoaja huolehtii muun muassa palvelinympäristön tietoturvasta ja hallinnasta. Konesalipalvelun ostamista harkitessa palveluntarjoajat on syytä kilpailuttaa sopivimman palvelun ja hintatason saamiseksi. Esimerkkejä suomalaisista yrityksistä, jotka tarjoavat konesalipalvelua, ovat Tietokeskus, Decens ja Marskidata (Tietokeskus 2021; Decens 2021; Marskidata 2021).



KUVA 12. Konesali (Schäfer 2017)

### 5.2 Palvelinympäristö pilvipalveluna

Vaihtoehtona perinteiselle fyysiselle palvelinympäristölle on valita toteutus pilvipalvelun avulla. Pilvipalvelun valinta tarjoaa joustavuutta ja parhaimmillaan paremman tietoturvan. Pilvipalvelua käytettäessä palvelimet ovat virtualisoituja. Pilvipalvelimeksi voidaan valita juuri sellaiset ominaisuudet kuin tarve vaatii. Pilvipalvelin tarjoaa samat toiminnallisuudet, kuten käyttöjärjestelmän ja palvelut, joita fyysinenkin palvelin voisi tarjota. Pilvipalvelun edut tulevat hyvin esiin joustavuuden, helppokäyttöisyyden ja kustannuksien kautta. Pilvipalvelun haitaksi voi kuitenkin muodostua se, että fyysistä pääsyä palvelimille ei ole. Tämä korostuu etenkin silloin, jos pilvipalvelu on pois käytöstä pilvipalveluntarjoajaan kohdistuvan ongelman, kuten tietoturvahyökkäyksen takia. Tällöin asiakas ei voi tehdä muuta kuin odottaa, että palveluntarjoaja ratkaisee ongelman. (Chai & Bigelow 2021.)

Kun palvelinympäristö on toteutettu pilvipalvelun avulla, käytettäviä palvelinresursseja voidaan helposti kasvattaa tai pienentää tarpeen mukaan. Pilvipalvelutilaus voidaan myös tarpeen vaatiessa lopettaa halutessa. Pilvipalvelun käytöstä aiheutuvat kustannukset skaalautuvat sen mukaan, mitä palveluita on käytössä. (Chai & Bigelow 2021.)

### 5.3 Palvelinympäristöjen tietoturva

Tietoturvan toteutuminen eri palvelinympäristövaihtoehtojen kohdalla riippuu hyvin pitkälti siitä, kuinka osaavia palvelinympäristöä kehittämässä olevat henkilöt ovat. Mikäli fyysistä palvelinympäristöä ollaan toteuttamassa itse ilman hyvää tietämystä tietoturvasta, lopputuloksena voi olla hyvinkin heikon tietoturvan omaava palvelinympäristö. Palvelinympäristön tietoturvaan vaikuttavat erityisesti myös käytössä olevat verkkoratkaisut ja niiden tietoturva. Tietoturvan toteutuminen ei siis yksistään nivoudu vain palvelimen päässä toteutettaviin tietoturvaratkaisuihin, vaan tietoturva on kokonaisuus, jossa täytyy ottaa huomioon kaikki eri aspektit, kuten verkon tietoturva. Näin ollen tapauksessa, jossa ei ole saatavilla omasta takaa tietoturva-asiantuntijoita, olisi hyvä harkita palvelinympäristön toteutusta ostopalveluna joko fyysisten konesalipalvelujentarjoajalta tai pilvipalveluntarjoajalta.

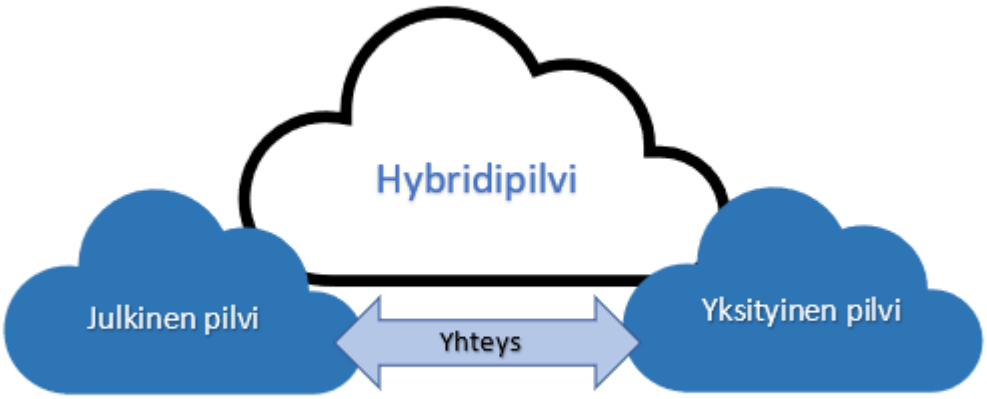
# 6 PILVIPALVELUT

Pilvipalvelut helpottavat tietotekniikkaresurssien käyttöönottoa; pilvipalveluiden avulla voidaan ottaa esimerkiksi palvelin käyttöön ilman, että täytyisi hankkia fyysinen laite. Pilvipalvelutoimintamalliin kuuluvat skaalautuvuus, nopea ja helppo käyttöön ja käytöstä poisotto. Pilvipalvelua voidaan käyttää millä vain käyttötarkoitukseen soveltuvalla verkossa olevalla päätelaitteella, kuten tietokoneella tai mobiililaitteella. Yksi pilvipalveluiden piirteistä on itsepalvelullisuus, joka tarkoittaa, että palvelu voidaan ottaa itse käyttöön tai poistaa käytöstä ilman kolmannen osapuolen, kuten asiakaspalvelijan toimia. Itsepalvelullisuus myös mahdollistaa, että tarvittavat resurssit voidaan valita itse.

Pilvimuotoja ovat julkinen pilvi, yksityinen pilvi, yhteisöllinen pilvi ja hybridipilvi. Tämän lisäksi pilvipalvelut jaetaan useimmiten kolmeen eri toimintamalliluokkaan ominaisuuksien mukaan: Infrastructure-as-a-Service, Platform-as-a-Service ja Software-as-a-Service. Edellä mainituista käytetään lyhenteitä IaaS, PaaS ja SaaS. (Salo 2012, 17–20.)

## 6.1 Pilvivaihtoehdot

Julkisen pilven, yksityisen pilven, yhteisöllisen pilven ja hybridipilven määritelmät ovat erilaisia. Kun pilvipalvelut tarjoaa kokonaan palveluntarjoaja, on kyseessä julkinen pilvi. Julkinen pilvi tarjoaa tietotekniikkaresursseja käytettäväksi maksua vastaan. Käyttäjällä, kuten yrityksellä, voi olla käytössään julkisen pilven sijasta oma yksityinen pilvi, jossa laitteet ovat yrityksen omistamia ja pilvi on vain nimenomaisen yrityksen käytössä. Laitteet eivät kuitenkaan välttämättä sijaitse samassa paikassa kuin itse yritys. Tilanteessa, jossa useampi yritys on jakanut käyttöönsä saman pilven, on kyseessä yhteisöllinen pilvi. Yhteisöllistä pilveä voi hallinnoida kolmas osapuoli. Julkista, yksityistä ja yhteisöllistä pilveä voidaan käyttää myös yhdessä, ja siitä käytetään nimitystä hybridipilvi (KUVA 13). (Salo 2012, 18.)



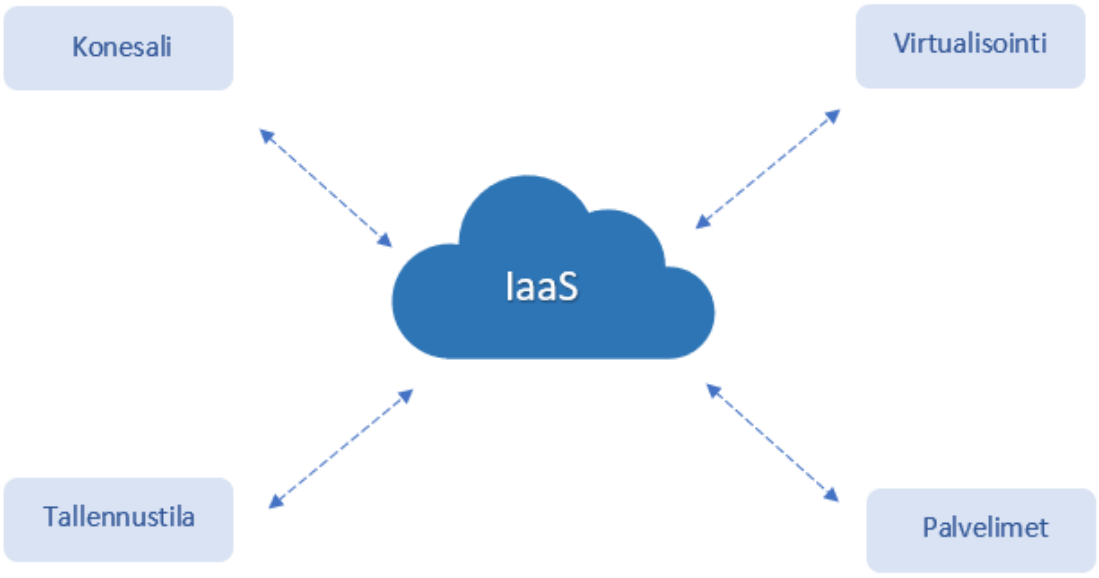

KUVA 13. Hybridipilvi

### 6.2 Pilvipalvelujen toimintamalliluokat

Pilvipalvelut jaetaan tyypillisesti kolmeen eri luokkaan toimintamalliensa mukaan: IaaS, PaaS ja SaaS. IaaS tarkoittaa infrastruktuuria palveluna, PaaS sovellusalustaa palveluna ja SaaS sovelluksia palveluna. Näistä kolmesta IaaS-mallia käytetään, kun halutaan toteuttaa palvelinympäristö pilviratkaisuna. (Salo 2012, 20.)

#### 6.2.1 IaaS

IaaS-mallissa (KUVA 14) asiakas voi valita tarpeensa mukaan maksullisia laitteistoresursseja palvelun-tarjoajalta. IaaS on hyvin skaalautuva ja laskutus tapahtuu resurssien käytön perusteella. Esimerkiksi Amazon EC2 on IaaS-mallin piiriin lukeutuva palvelu, jonka kautta voidaan ottaa käyttöön tarvittava määrä palvelimia. Amazon on yksi johtavia IaaS-palveluntarjoajia. (Salo 2012, 22–23.)




KUVA 14. IaaS-malli

### 6.2.2 PaaS

PaaS-malli tarjoaa sovellusalustoja. Sovellusalustat ovat tarkoitettu ohjelmistokehitykseen eli sovelluksien kehittämiseen, ylläpitämiseen ja testaamiseen. PaaS-tarjontaa löytyy muun muassa Amazonilta ja Microsoftilta. (Salo 2012, 23.)

### 6.2.3 SaaS

SaaS-malli tarjoaa sovelluksen käyttöön niin, että laskutus tapahtuu käytön mukaisesti (Salo 2012, 25). SaaS-mallin mukainen palvelu on esimerkiksi hyvin laajasti käytössä oleva ja tunnettu Microsoft Office 365, joka sisältää Microsoftin sovelluksia muun muassa Word-tekstinkäsittelyohjelman, Excel-taulukkolaskentaohjelman ja Outlook-sähköpostiohjelman.

# 7 PILVIPALVELUNTARJOAJAT

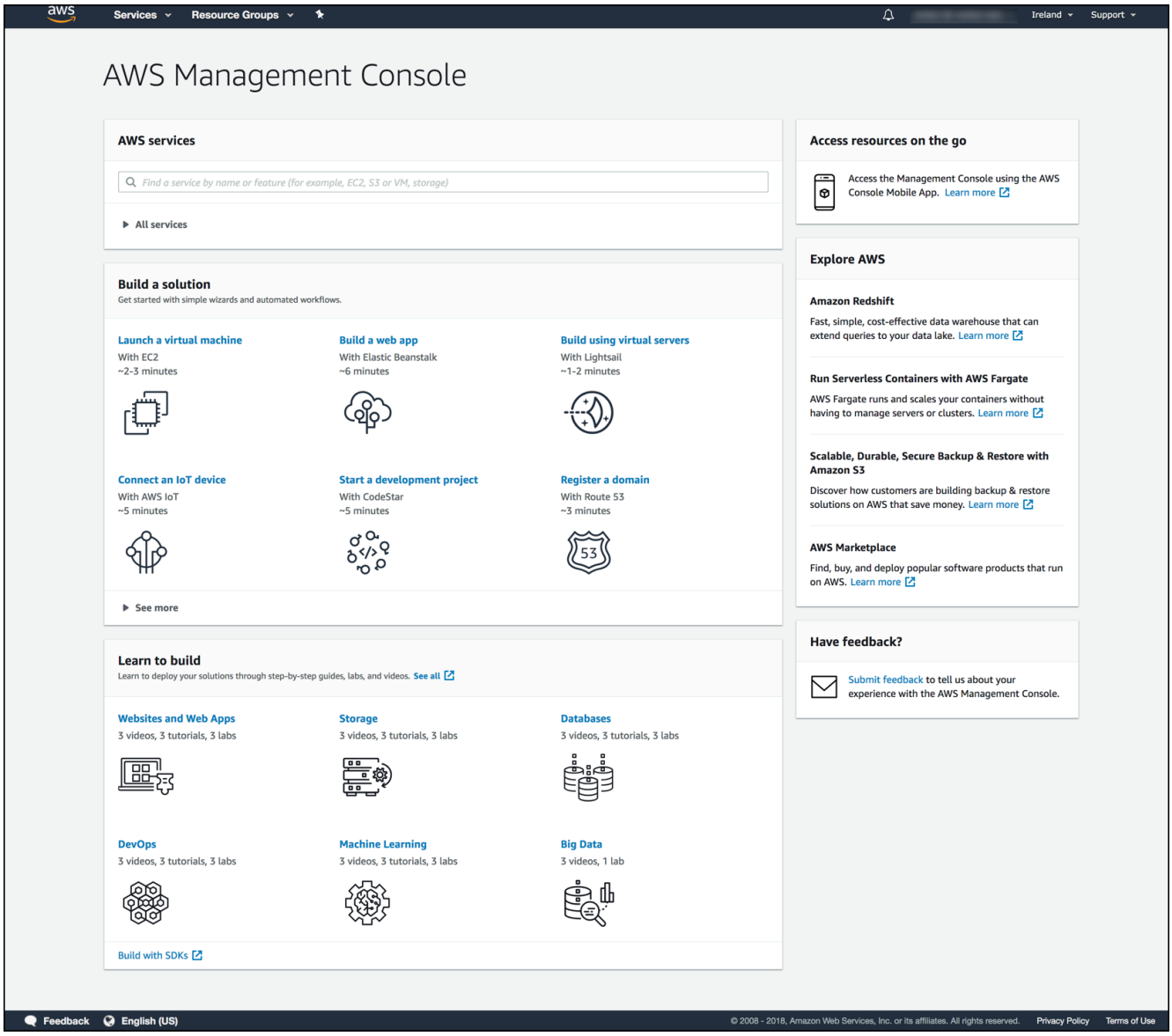
Pilvipalveluntarjoajia on useita, ja tästä syystä tulisikin perehtyä tarkemmin palveluntarjoajien tarjontaan ja eroavaisuuksiin. Vertailemalla palveluntarjoajien tuotteita toisiinsa voidaan löytää paras mahdollinen vaihtoehto pilvipohjaisen palvelinratkaisun toteutukseen. Erityisen tärkeää on perehtyä palveluntarjoajiin tietoturvan näkökulmasta. Kun tietoturva on paras mahdollinen, voidaan minimoida tietoturvaloukkausriskit. Tunnetuimpia pilvipalveluntarjoajia palvelinympäristöjen kohdalla ovat Amazon Web Services, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, IBM Cloud ja Oracle. Tästä joukosta kaksi markkinoita johtavaa ovat Amazon Web Services ja Microsoft Azure. (Dignan 2021.)

## 7.1 Amazon Web Services

Amazon Web Services on tällä hetkellä maailman johtava pilvipalveluntarjoaja. Menestystarina alkoi vuonna 2006, kun Amazon Web Services alkoi tarjoamaan verkkopohjaisia IT-infrastruktuuripalveluja. Palveluntarjoaja kertoo tarjoavansa 230 erilaista toimintoa takaamaan tietoturvaa ja on saavuttanut sertifikaatit 90 tietoturvastandardin osalta. Saatavuus on laaja; AWS on saatavilla 25 maantieteellisellä alueella (KUVA 16) ympäri maailman. (Amazon Web Services 2021a; Amazon Web Services 2021b; Amazon Web Services 2021c.)

AWS:n valikoimaan kuuluu kaksi tuotetta, jotka sopivat palvelinympäristöjen toteuttamiseen. Nämä kaksi tuotetta ovat Amazon Lightsail ja Amazon EC2. Lightsail on näistä tuotteista yksinkertaistetumpi ja sopiva pienempään toimintaan, kun taas EC2 on suunnattu laajempaan käyttöön. Tuotteita voidaan käyttää AWS-hallintakonsolin avulla (KUVA 17). Amazon mainostaa Lightsailin sopivan esimerkiksi tilanteeseen, jossa halutaan ensimmäistä kertaa kokeilla, miten AWS-ympäristö toimii. Ligthsailista voidaan sujuvasti siirtyä EC2-tuotteeseen, kun toimintaa halutaan laajentaa. AWS tarjoaa opastetun vaiheittaisen siirtymän Lightsailista EC2-tuotteeseen. (Amazon Web Services 2021d; Amazon Web Services 2021e.)


KUVA 16. Amazon Web Services kartta fyysisistä sijainneista (Amazon Web Services 2021c)




KUVA 17. AWS-hallintakonsoli (Amazon Web Services 2021g)

### 7.1.1 Amazon Lightsail

Amazon Lightsail -tuotteen käyttöönotto tapahtuu nopeasti AWS-konsolin opastuksen avulla. Tuote mahdollistaa Linux/Unix tai Windows -virtuaalipalvelimien käyttöönoton. Virtuaalipalvelimissa on sisäänrakennettu palomuuri, jonka sallimissäännöt ovat muokattavissa. Käyttökokemuksen parantamiseksi Amazon Lightsail tarjoaa tietoliikenteen yksinkertaistetun kuormantasauksen. Tuote tarjoaa myös mahdollisuuden ottaa käyttöön säiliöitä, valmiiksi konfiguroituja tietokantoja ja lisää tallennustilaa. (Amazon Web Services 2021e.)

Edullisin Amazon Lightsailiin saatava Windows-virtuaalipalvelinpaketti maksaa tällä hetkellä 8 dollaria kuukaudessa, ja se sisältää 512 megatavua muistia, yksiytimisen prosessorin, 30 gigatavun SSD-levyn tallennustilaksi ja yhden teratavun verran kuukausittaista tiedonsiirtoa. Kalleimpaan 240 dollaria kuukaudessa maksavaan Windows-virtuaalipalvelinpakettiin kuuluu 32 gigatavua muistia, 8-ytiminen prosessori, 640 gigatavun SSD-levy ja 7 teratavua kuukausittaista tiedonsiirtoa. Edullisimman ja kalleimman paketin väliltä löytyy myös muita pakettivaihtoehtoja. (Amazon Web Services 2021f.)

Amazon Web Services määrittelee Amazon Lightsail -tuotteen kohdalla tietoturvan olevan jaettuna vastuuna AWS:n ja asiakkaan välillä. Vastuu jaetaan niin, että AWS-palveluja AWS-pilvessä pyörittävän infrastruktuurin tietoturva on AWS:n vastuulla, kun taas asiakkaan vastuulla on huolehtia palvelussa käytettävien tietojen suojaamisesta, niin lakien kuin määräyksien mukaan toimiminen ja asiakasyrityksen määrittelemien tietoturvavaatimuksien toteutuminen. AWS myös huolehtii omalta osaltaan siitä, että kolmannen osapuolen auditoija testaa ja varmistaa tietoturvaa säännöllisesti. (Amazon Web Services 2021h.)

### 7.1.2 Amazon EC2

Amazon EC2 -tuotteen käyttöönotto on monipuolisuutensa johdosta hieman monimutkaisempaa verrattuna Lightsailin käyttöönottoon. Amazon EC2 -tuotetta käytettäessä voi valita itse palvelimen tekniset ominaisuudet, kuten prosessorin ja käyttöjärjestelmän. EC2 on hyvin skaalautuva ja muunnettavissa juuri omaan käyttöön sopivaksi. Tuote sopii todella suurellekin yritykselle. Se tarjoaa yli 400 virtuaalipalvelimen kapasiteetin. Virtuaalipalvelimia varten on tarjolla lukuisia eri instanssityyppejä käyttötarkoituksen mukaan. Esimerkiksi M5n-instanssit ovat sopivia web-palvelimia varten. M5n-instanssivaihtoehdot tarjoavat prosessorivaihtoehtoja 2-ytimisistä 96-ytimisiin asti ja muistia 8 gigatavusta 384 gigatavuun saakka. (Amazon Web Services 2021i; Amazon Web Services 2021j.)

Amazon EC2 -tuotteelle on valittavissa eri hinnoittelumalleja kuten On-Demand ja Savings Plans. Molemmat edellä mainituista hinnoittelumalleista laskutetaan käytön mukaan. On-Demand -mallissa laskutus tapahtuu valinnan mukaan tunti- tai sekuntiperusteisesti. Savings Plans -malli on valittavissa tuntiveloitteisesti yhden tai kolmen vuoden pituiselle aikajaksolle. Kustannuksia on mahdollista arvioida verkossa AWS Pricing Calculator -palvelun avulla. Esimerkiksi virtuaalipalvelin Windows Server -käyttöjärjestelmällä m5n.large-instanssilla maksaisi 173,66 dollaria kuukaudessa. Hinta-arvio vaihtelee sekä

instanssin että sen mukaan, mitä teknisiä ominaisuuksia määrittelee käyttöön. (Amazon Web Services 2021k; Amazon Web Services 2021l.)

Vastuu tietoturvasta jakautuu EC2-tuotteen kohdalla muutoin samoin kuin Lightsail-tuotteessakin, mutta Lightsail-tuotteelle lueteltujen vastuiden lisäksi asiakkaalla on vastuu myös muun muassa instanssien, kuten palvelimien verkkopääsyn hallinnoinnissa ja kirjautumistiedoista (Amazon Web Services 2021m).

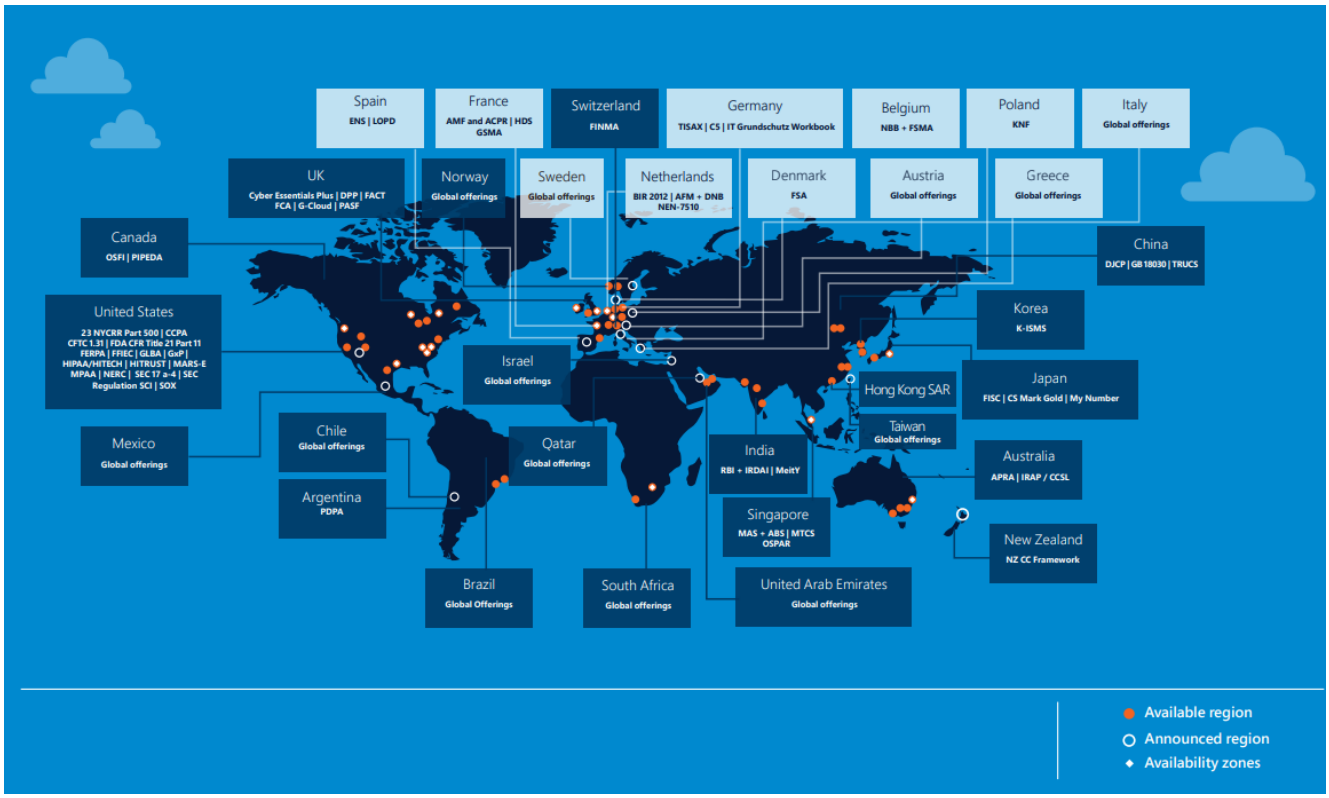
### 7.1.3 Tietoturvahyökkäykset

Amazon Web Services on kohdannut vuosien varrella muun muassa palvelunestohyökkäyksiä. Esimerkiksi vuoden 2020 helmikuussa AWS kohtasi todella voimakkaan palvelunestohyökkäyksen. Hyökkäys oli siihen mennessä maailman voimakkaimpia 2,3 terabitin sekuntinopeudellaan ja hyökkäyksen kesto oli kolme päivää. Myös vuoden 2019 lokakuussa tapahtui useita tunteja kestänyt palvelunestohyökkäys. AWS tarjoaa asiakkailleen palvelunestohyökkäyksiltä suojautumiseksi AWS Shield -palvelua, joka keskeytymättömästi havainnoi mahdollisia hyökkäyksiä ja auttaa minimoimaan hyökkäyksestä johtuvaa resurssien häiriöaikaa. AWS Shield -palvelusta on saatavilla maksuton Standard-versio ja maksullinen Advanced-versio. AWS Shield Advanced on mahdollista ottaa käyttöön esimerkiksi Amazon EC2 -tuotteen kanssa. (Kailio 2020; Karkimo 2019; Amazon Web Services 2021n.)

## 7.2 Microsoft Azure

Microsoft Azure on Amazon Web Services:n jälkeen toiseksi suosituin pilvipalveluntarjoaja. Microsoft julkaisi palvelun vuonna 2008 nimellä Windows Azure. Myöhemmin nimi vaihdettiin Microsoft Azureksi, jotta se kuvaisi paremmin palvelua, joka tarjoaa myös Linux-tuotteita. Azuren valikoima tarjoaa tällä hetkellä yli 200 tuotetta ja pilvipohjaista palvelua saataville 140:een maahan. 140 maata sijoittuvat useille kymmenille maantieteellisille alueille ja maantieteellisiä saatavuusalueita on pian yli 60 (KUVA 18). Microsoft käyttää Azuren tietoturvan edistämiseksi 1 miljardia dollaria vuodessa ja työllistää yli 3 500 maailmanlaajuisesti toimivaa asiantuntijaa. Azure tarjoaa myös yli 90 vaatimuksenmukaisuussertifikaattia. (MSV 2020; Microsoft 2021b; Microsoft 2021c; Microsoft 2021d.)

Microsoft mainostaa Azuren Windows Server -virtuaalikoneiden olevan viisinkertaisesti edullisempi käyttää kuin kilpailijansa Amazon Web Servicesin Windows Server -virtuaalikoneet. Microsoft on tehnyt vertailun 4. heinäkuuta 2021 hinnastojen mukaisesti. Vertailussa vertailtiin tietoteknisiltä ominaisuuksiltaan vastaavia Windows Server -virtuaalikoneita kunkin palveluntarjoajan US West -saatavuusalueilta hankittuna. Sopimusmuotona vertailussa oli 3 vuoden sopimus ja käyttöaika 730 tuntia kuukaudessa 12 kuukauden ajan. (Microsoft 2021e.)




KUVA 18. Microsoft Azure -kartta fyysisistä sijainneista (Microsoft 2021f)

### 7.2.1 Microsoft Azuren tarjoamat virtuaalipalvelimet

Microsoft Azure tarjoaa valikoiman Windows- ja Linux-virtuaalipalvelimia. Windows-valikoimasta voi valita joko tavanomaisen Windows Server -käyttöjärjestelmän tai Windows Server -käyttöjärjestelmän SQL-palvelin toiminnallisuudella, kun taas Linux-valikoimasta löytyy useita eri Linux-käyttöjärjestelmiä, kuten Ubuntu, SUSE Linux Enterprise ja Red Hat Enterprise Linux. Kaikkiin edellä mainittuihin on mahdollista valita myös SQL-palvelin toiminnallisuus. Sekä Windows- että Linux-palvelimiin voi valita tarvitsemansa tekniset ominaisuudet esimerkiksi luokista A, B tai D. Luokista A ja B tarjoavat pienempiin tarpeisiin sopivia vaihtoehtoja suppeammilla teknisillä ominaisuuksilla, D-luokka tarjoaa

parhaimmat tekniset ominaisuudet raskaampaan käyttöön. Esimerkiksi luokan A instanssi A2 tarjoaa kaksiytimisen prosessorin, 3.5 gigatavua RAM-muistia ja 135 gigatavun väliaikaisen tallennustilan. D-luokan instanssi D96 v5 tarjoaa 96-ytimisen prosessorin, 384 gigatavua RAM-muistia ja 3600 gigatavua väliaikaista tallennustilaa. (Microsoft 2021g; Microsoft 2021h.)

Azuren virtuaalipalvelinten hinnoittelu vaihtelee muun muassa valitun käyttöjärjestelmän, teknisten ominaisuuksien ja kuukausittaisen käyttöajan perusteella. Esimerkiksi Windows-palvelin A2-instanssin teknisillä ominaisuuksilla maksaisi tällä hetkellä keskimäärin 131 dollaria kuukaudessa ja Linux-palvelin SUSE Linux Enterprise -käyttöjärjestelmällä A2-instanssilla keskimäärin 87 dollaria kuukaudessa. A-luokan instansseille on valittavissa vain ”pay-as-you-go” -laskutus, joka tarkoittaa sitä, että sopimusta laskutetaan käytön mukaan jälkikäteen. B- ja D-luokille on saatavilla ”pay-as-you-go”-laskutuksen lisäksi 1 tai 3 vuoden laskutussopimus, jossa suoritetaan etukäteen yhdelle tai kolmelle vuodelle arvioidun käytön mukainen maksu. Microsoft on arvioinut 1 ja 3 vuoden laskutussopimuksien olevan jopa 80 % edullisempia kuin ”pay-as-you-go” -sopimus. Hinta-arvioita voi myös vertailla itse Azuren Prizing Calculator -verkkosivuston avulla. (Microsoft 2021g; Microsoft 2021i.)

Azurea käytettäessä vastuu on jaettu asiakkaan ja palveluntarjoajan välille niin, että asiakas vastaa itse ostamiensa palvelujen sisäisestä tietoturvallisuudesta ja Microsoft palvelua pyörittävien fyysisten resurssien tietoturvasta (Lanfear 2021).

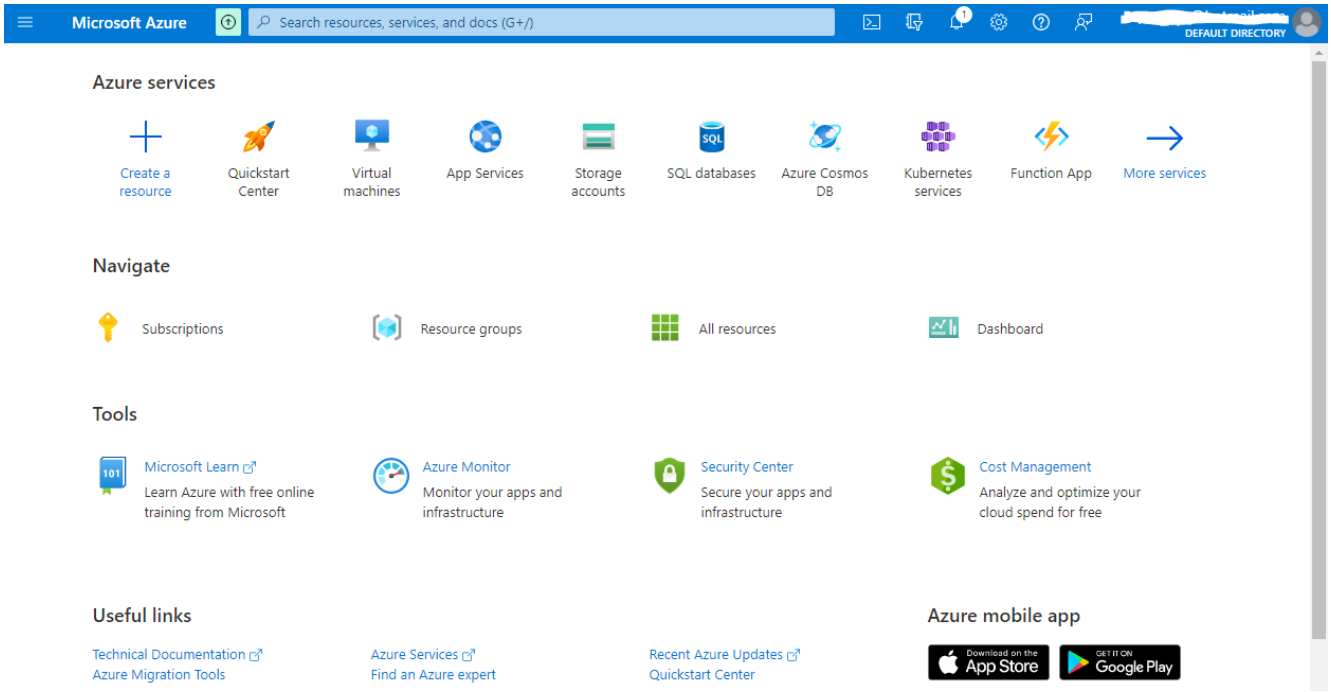
### 7.2.2 Tietoturvahyökkäykset

Kuten kilpailijansa Amazon Web Services, on myös Microsoft Azure kohdannut massiivisia palvelunestohyökkäyksiä. Viimeisin suuri palvelunestohyökkäys tapahtui lokakuun 12. päivä vuonna 2021. Hyökkäys oli voimakkuudeltaan 2,3 terabittiä sekunnissa. Hyökkäys kesti 10 minuuttia ja se kosketti eurooppalaisia Azure-asiakkaita. Tuota palvelunestohyökkäystä edeltävä suuri hyökkäys tapahtui viimeksi keväällä 2020 ja hyökkäys tapahtui yhden terabitin sekuntinopeudella. Microsoft tarjoaa palvelunestohyökkäyksiltä suojautumiseksi maksullista Azure DDoS Protection -palvelua. Palvelun suorittama monitorointi on jatkuvaa ja palvelu lieventää automaattisesti mahdollisia verkkohyökkäyksiä. Palvelu osaa mukautua älykkäästi asiakkaan resurssien mukaan ja tarjoaa näin ollen mahdollisimman sopivan suojauksen juuri käytössä oleville resursseille. Azure DDoS Protection -palvelu toimii yhdessä Azure Monitor -palvelun kanssa, joka tarjoaa reaaliaikaisia statistiikkatietoja. Apua palvelunestohyökkäystilanteessa on tarvittaessa saatavilla, DDoS Protection -palvelun ostaneille, Microsoftin nopean vasteen

DDoS Protection -tiimiltä, joka auttaa esimerkiksi analysoinnissa ja hyökkäyksen tutkimisessa. (Vaughan-Nichols 2021; Microsoft 2021j.)

# 8 PALVELINYMPÄRISTÖN TOTEUTTAMINEN KÄYTTÄEN MICROSOFT AZUREA

Palvelinympäristön toteuttamista voi kokeilla Microsoft Azurella ilmaiseksi 30 päivän kokeilujakson avulla. Kokeilujakson hyödyntäminen on hyvä tapa kartoittaa, onko juuri Azure sopiva ratkaisu palvelinympäristön toteutukseen. Kokeilujakson lunastamisen jälkeen Azure-portaali tarjoaa mahdollisuuden opastuskierrokselle, joka opastaa käyttäjää Azure-portaalin (KUVA 19) toiminnoista. Opastuskierros esittelee lyhyesti portaalin keskeisimmät toiminnot. Portaaliin tutustumisen jälkeen voi aloittaa palvelinympäristön rakentamisen valitsemalla portaalista ”Virtual machines” tai ”Create a resource”. Virtuaalikoneen luomistoiminnossa pääsee valitsemaan virtuaalipalvelimelle tarvittavat ominaisuudet.

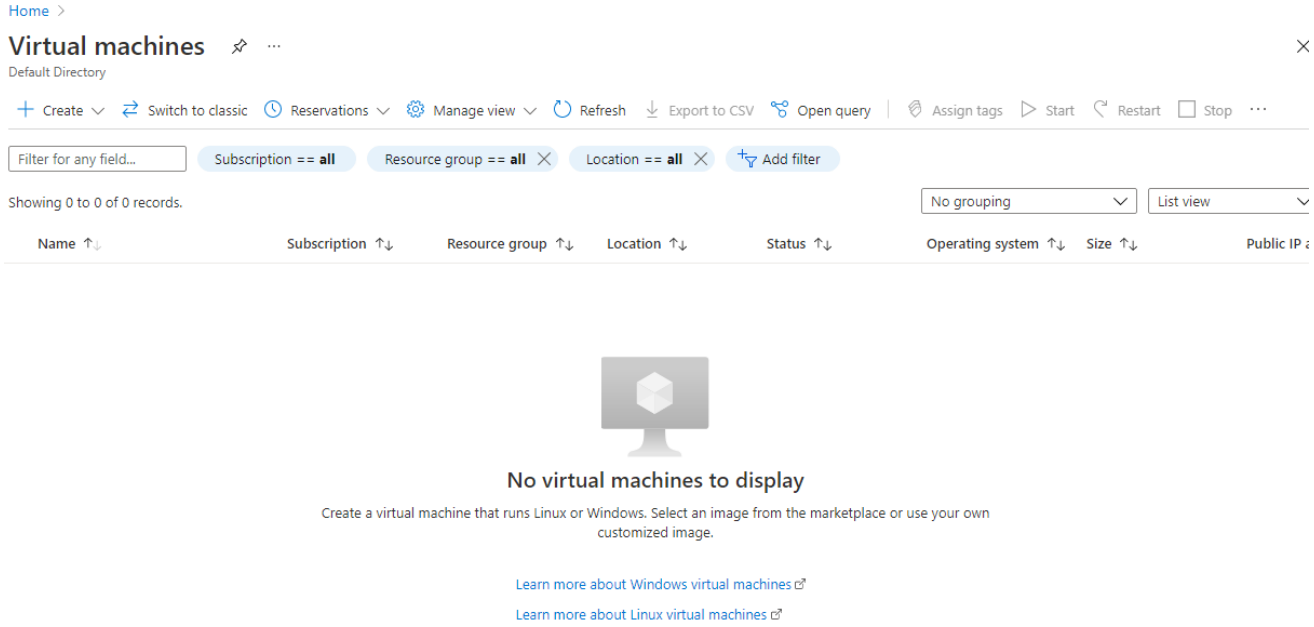



KUVA 19. Azure-portaali

## 8.1 Virtuaalipalvelimen luominen

Virtuaalipalvelimen luominen tapahtuu Azure-portaalissa ”Virtual machines” tai ”Create a resource” -toiminnon kautta. Tässä esimerkissä luodaan virtuaalipalvelin ”Virtual machines” -toiminnon kautta. ”Virtual machines” -näkymässä (KUVA 20) Create-painikkeen kautta pääsee luomaan virtuaalipalveli-

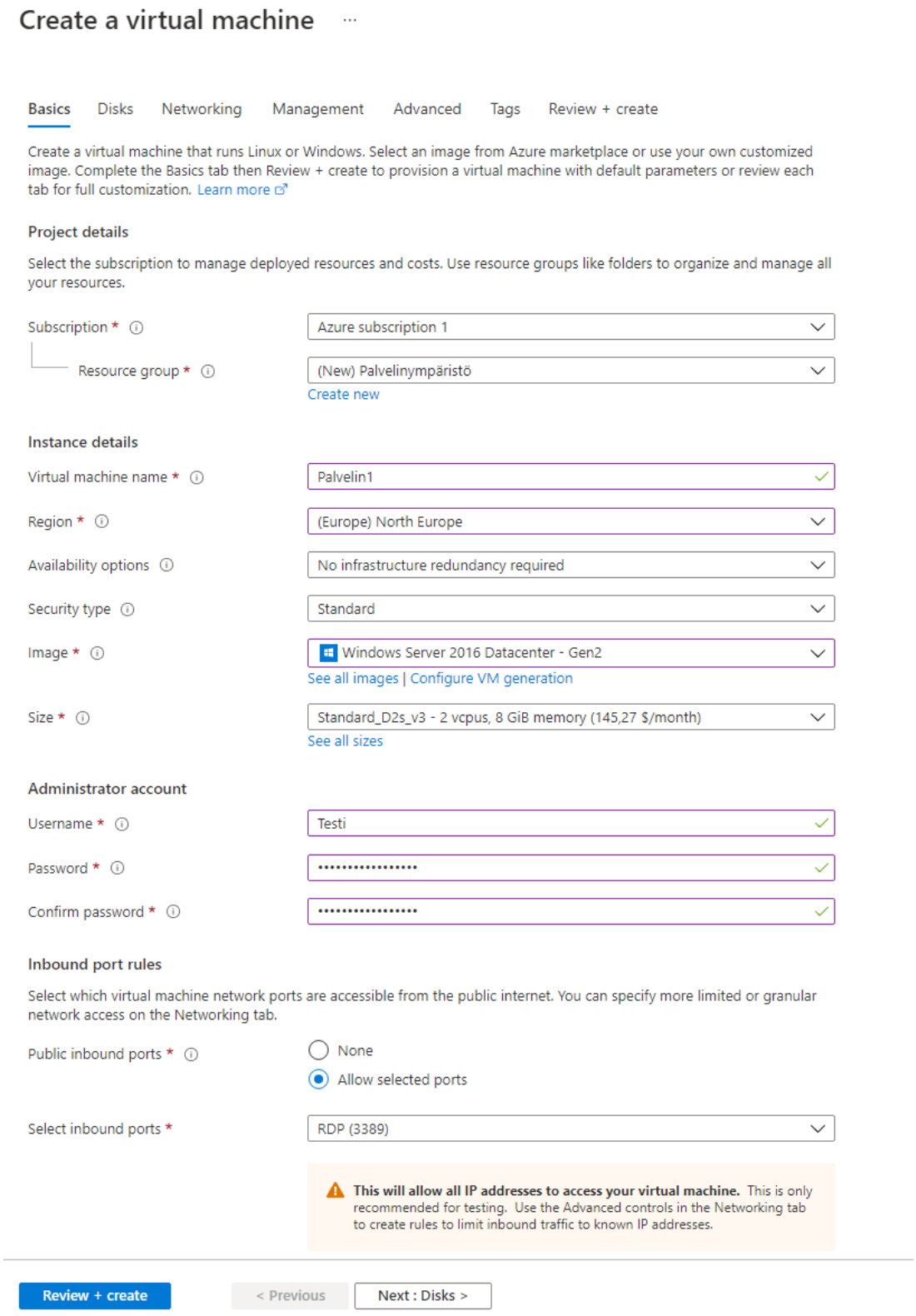
men. Virtuaalikoneen luomistoiminnossa määritellään halutut ominaisuudet virtuaalipalvelimelle. Luomistoiminnossa on 7 vaihetta: Basics, Disks, Networking, Management, Advanced, Tags ja Review + create. Näistä vaiheista esimerkissä esitellään kaikki muut paitsi Advanced- ja Tags -vaiheet.




KUVA 20. ”Virtual machines” -näkymä

### 8.1.1 Basics

Virtuaalikoneen luomistoiminnon ensimmäinen vaihe on Basics (KUVA 21), jossa määritellään perusominaisuudet virtuaalipalvelimelle kuten nimi, saatavuusalue, tietoturvatyyppi, käyttöjärjestelmä ja järjestelmänvalvojatunnus. Tässä esimerkissä valittiin saatavuusalueeksi Pohjois-Eurooppa, käyttöjärjestelmäksi Windows Server 2016 Datacenter – Gen2 ja käyttäjätunnus sekä salasana järjestelmänvalvojatunnukselle. Muut valinnat jätettiin niiden oletusmuotoon.



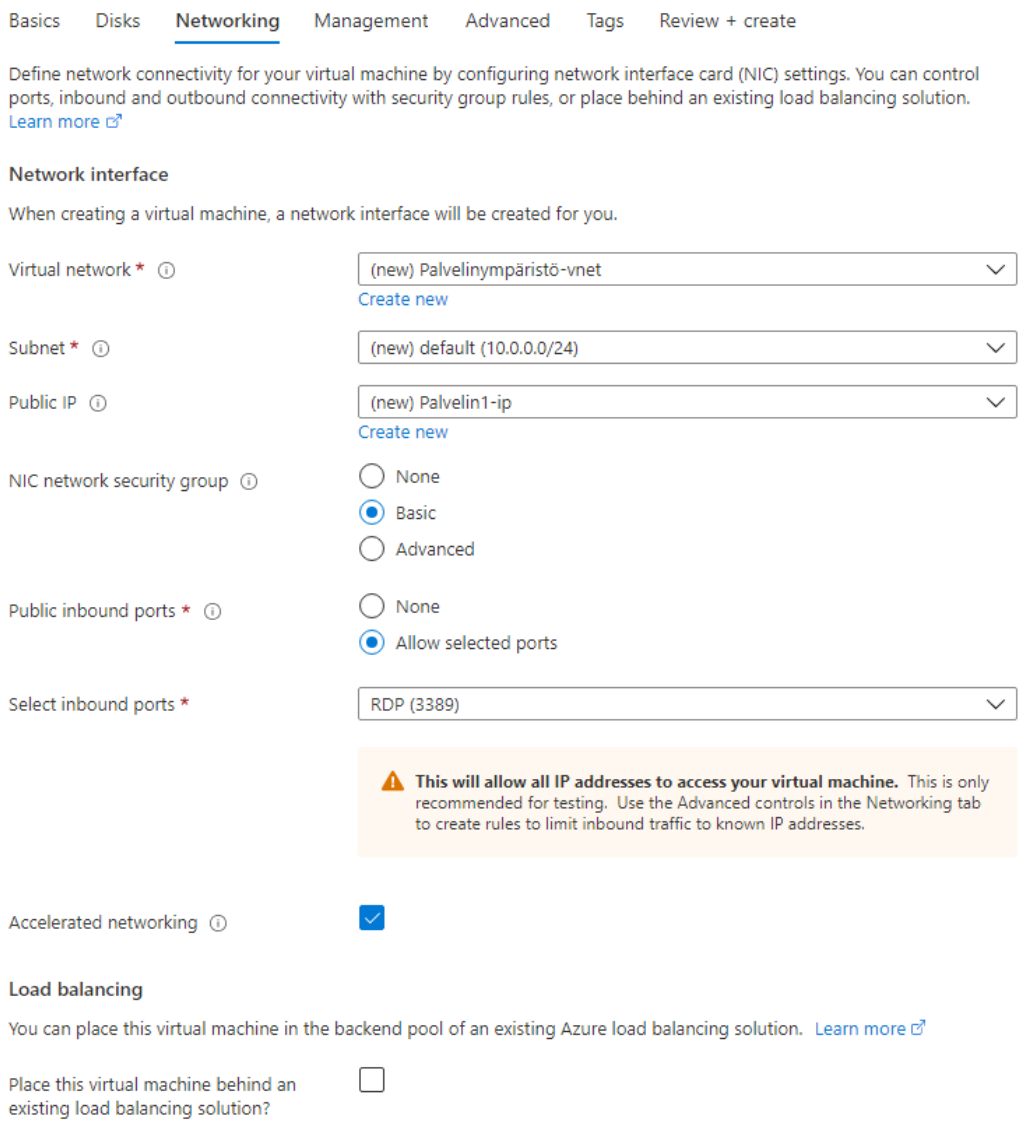

KUVA 21. Basics-vaihe

### 8.1.2 Disks

Luomistoiminnot toisessa vaiheessa, Disks, voidaan valita tallennustilan tyyppi SSD- ja HDD-vaihtoehtojen väliltä ja salauksen tyyppi tai jättää nämä valinnat oletusvalinnoiksi.

### 8.1.3 Networking

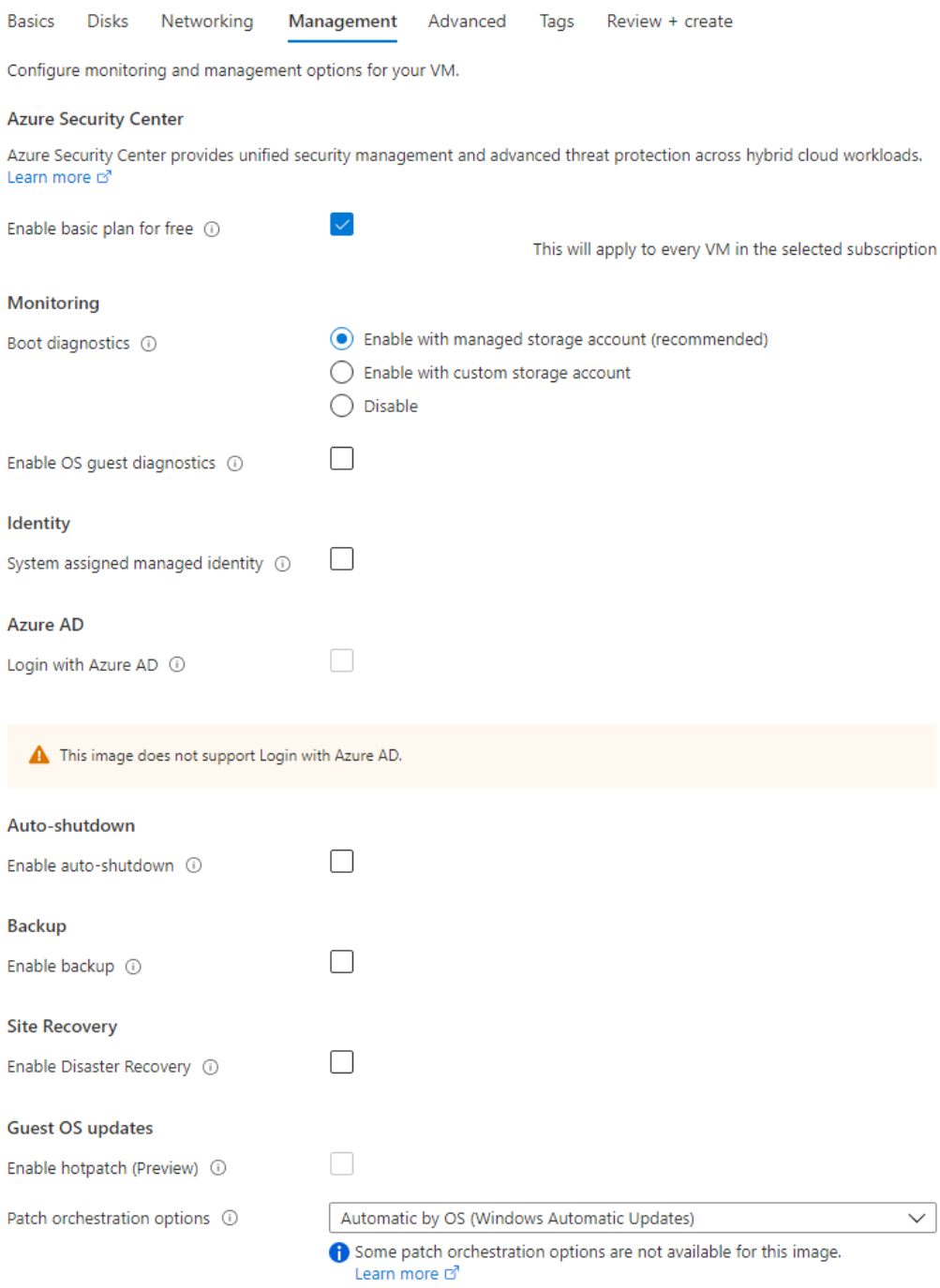
Networking-välivaiheessa on mahdollista luoda oma verkkoliitäntä haluamillaan määrityksillä virtuaalipalvelimelle tai käyttää portaalin automaattisesti luomia määrityksiä (KUVA 22).




KUVA 22. Networking-vaihe

### 8.1.4 Management

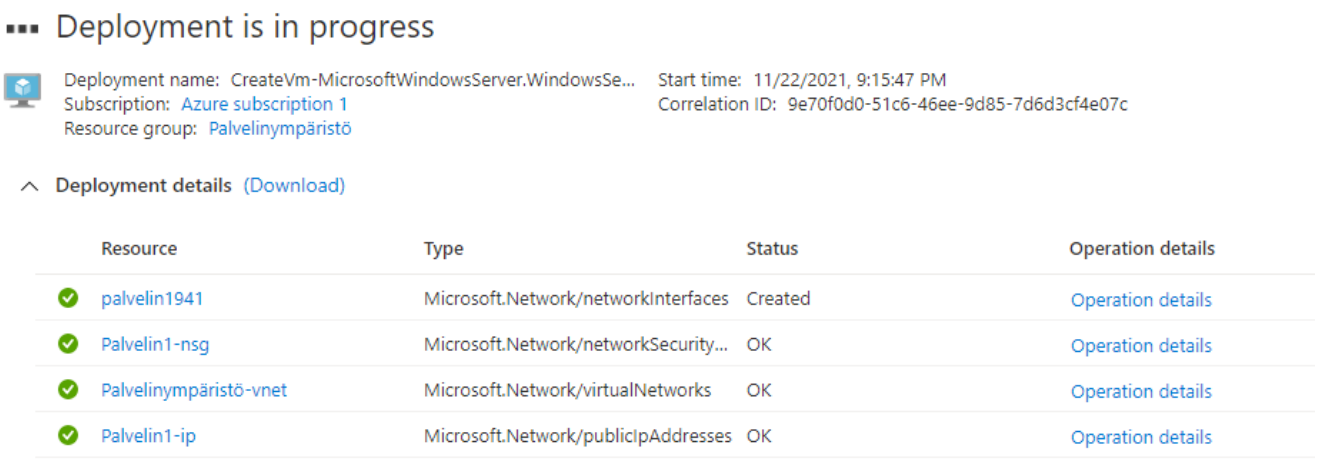
Management-vaiheessa (KUVA 23) voidaan määritellä halutut ylläpitotoiminnot esimerkiksi käynnistysdiagnostiikan monitorointiin ja ottaa käyttöön automaattinen sammutus tai varmuuskopiointi.



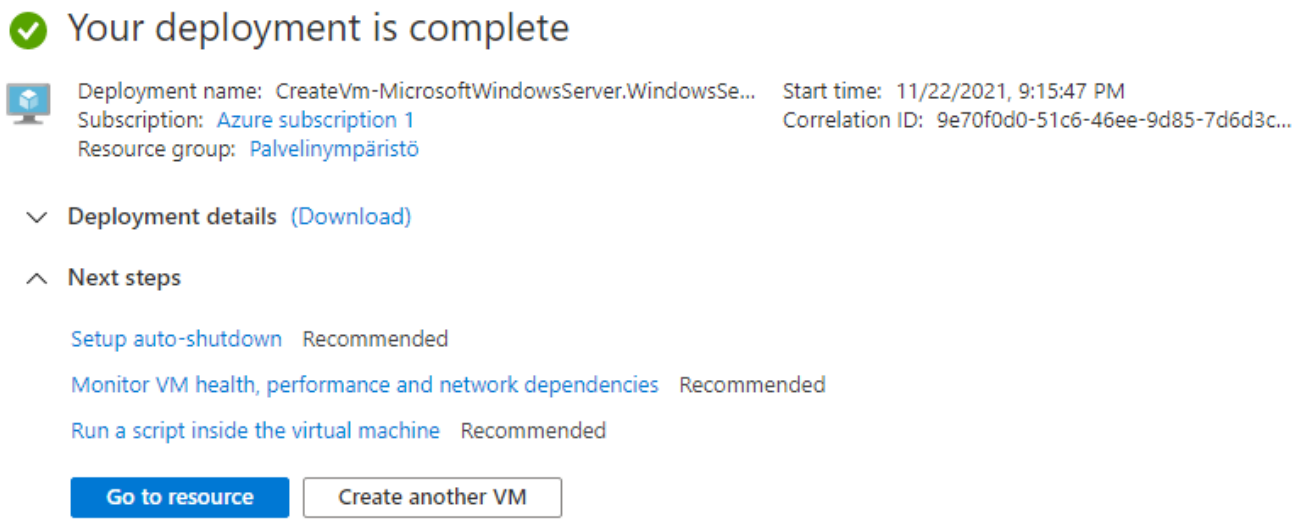

KUVA 23. Management-vaihe

### 8.1.5 Review + create

Luomistoiminnon viimeinen vaihe on Review + create, jossa näkee yhteenvedon luotavasta virtuaalipalvelimesta. Tämän jälkeen valitaan ”Create” -toiminto, jonka jälkeen portaali alkaa luomaan virtuaalipalvelinta (KUVA 24). Kun virtuaalipalvelimen luonti on valmis, portaalin sivulle tulee ilmoitus ”Your deployment is complete” (KUVA 25) ja sivun ”Go to resource” -painikkeesta päästään virtuaalipalvelimen omalle sivulle.



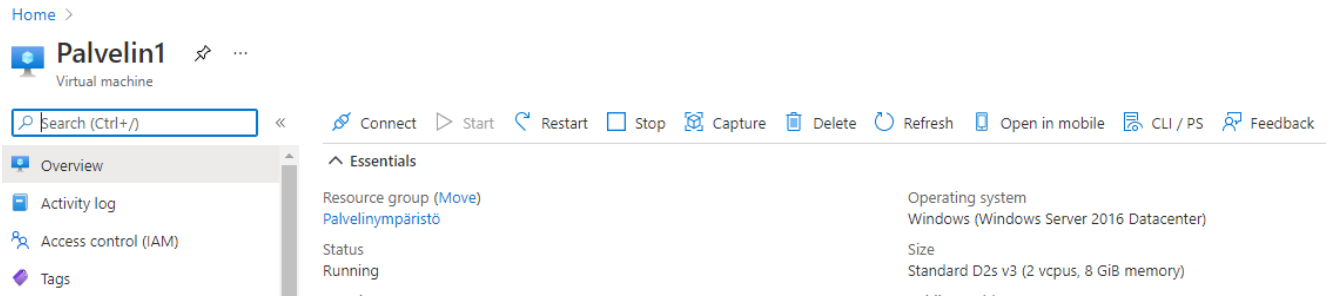

KUVA 24. Virtuaalipalvelimen luomisprosessi




KUVA 25. Virtuaalipalvelimen luomisprosessin valmistuminen

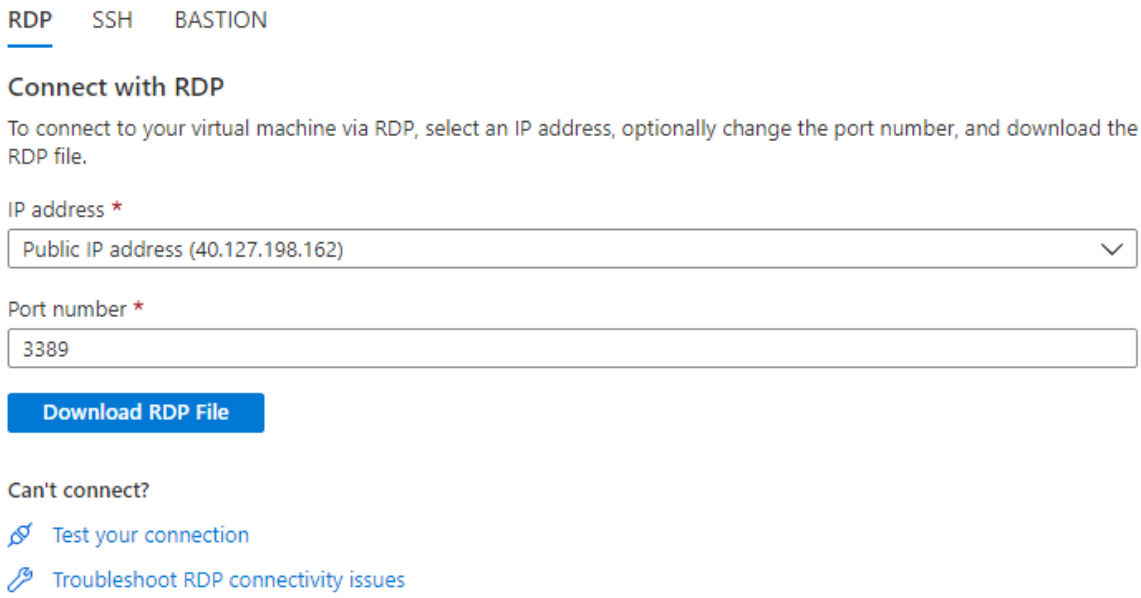
## 8.2 Virtuaalipalvelimen hallinta

Virtuaalipalvelinta pääsee hallitsemaan Azure-portaalissa esimerkiksi ”Virtual Machines” -näkymän kautta tai syöttämällä portaalin hakukenttään palvelimen nimen ja avaamalla palvelimen oman sivun (KUVA 26). Palvelimen omalta hallintasivulta saadaan avattua yhteys palvelimeen Connect-painikkeesta. Palvelimeen voi muodostaa yhteyden joko RDP:n, SSH:n tai Bastionin kautta. Tässä esimerkissä muodostamme yhteyden RDP:n kautta.

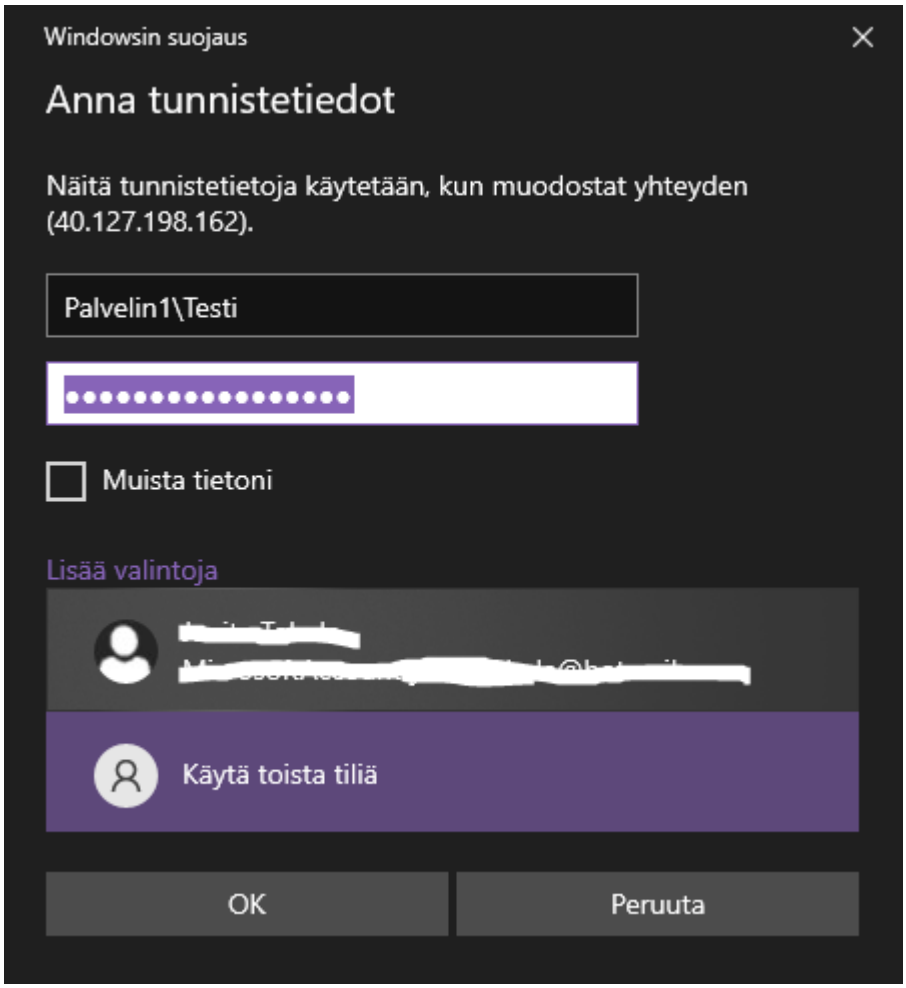



KUVA 26. Palvelimen hallintasivu

RDP-yhteyden muodostamiseksi portaalista ladataan RDP-tiedosto (KUVA 27). Kun RDP-tiedoston avaa, täytyy syöttää järjestelmänvalvojatunnuksen tunnistetiedot, jotka määriteltiin virtuaalipalvelimen luomisvaiheessa (KUVA 28). Käyttäjätunnus syötetään muodossa virtuaalipalvelinnimi\käyttäjätunnus.

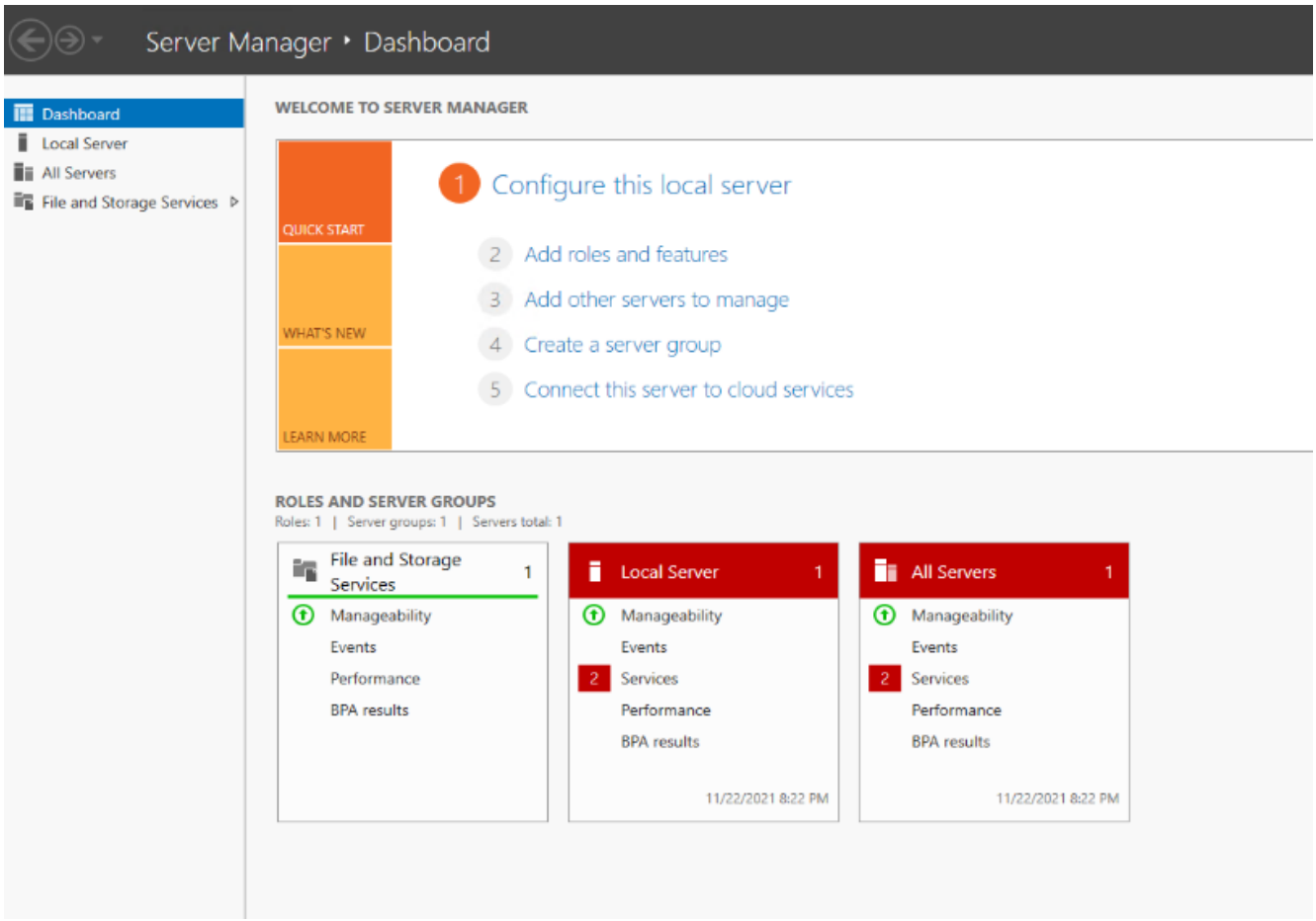



KUVA 27. RDP-tiedoston lataaminen




KUVA 28. Tunnistetietojen syöttäminen

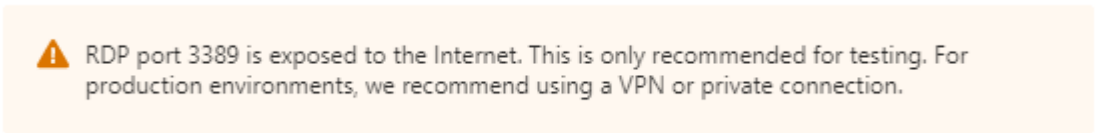
Tunnistetietojen syöttämisen jälkeen RDP-yhteys virtuaalipalvelimeen muodostuu ja palvelimen työpöytänäkymä avautuu. Palvelin käynnistää automaattisesti Server Manager -työkalun (KUVA 29), jonka avulla voidaan määrittää palvelimelle haluamansa roolin tai roolit kuten DNS- tai DHCP-roolin ”Add roles and features” -toiminnon kautta.




KUVA 29. Server Manager

## 8.3 Tietoturva

Azuressa toimivan virtuaalipalvelimen sisäisestä tietoturvasta huolehtiminen on asiakkaan vastuulla. Asiakkaan tulee huolehtia muun muassa virtuaalipalvelimen palomuuriasetuksista, virustentorjuntaohjelmistosta ja käyttöjärjestelmän ajantasaisuudesta. Azure-portaali suosittelee RDP-yhteyden muodostamista VPN-yhteyden kautta tietoturvallisemman yhteyden varmistamiseksi (KUVA 30).

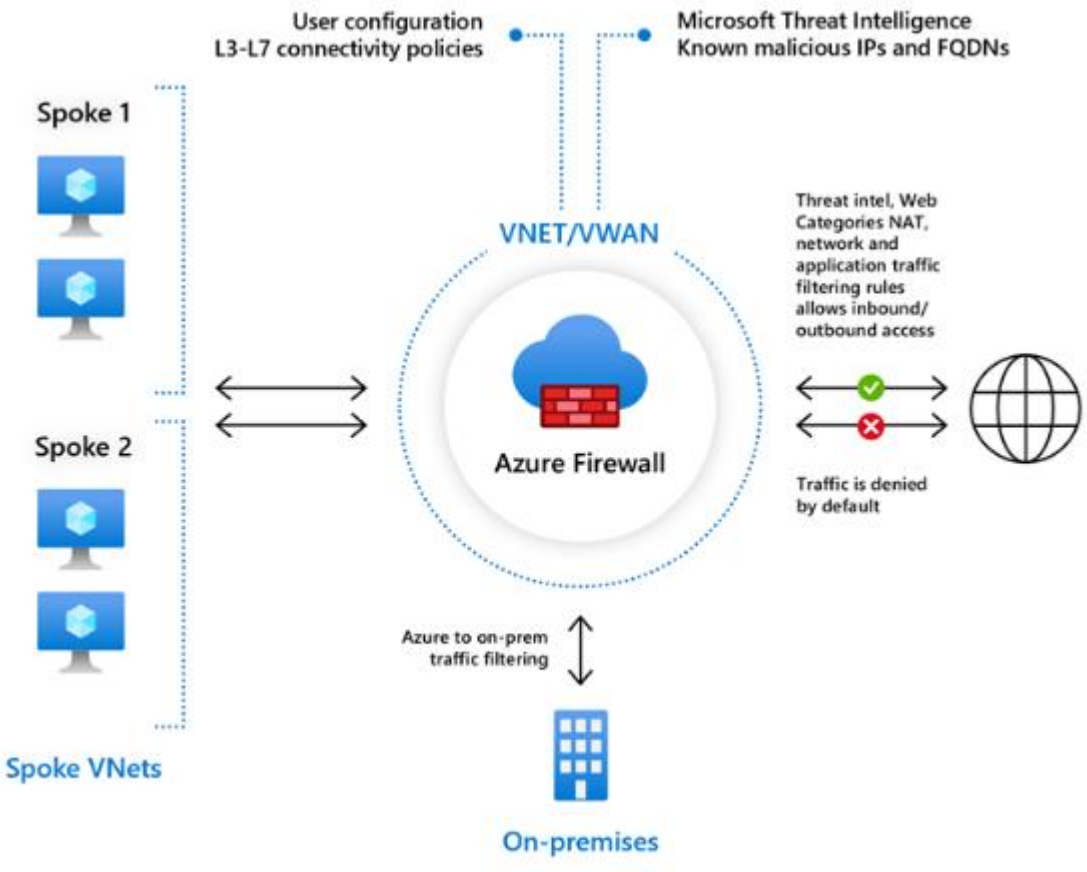



KUVA 30. Azure-portaalin varoitus RDP-yhteydestä

Virtuaalisen palvelinympäristön tietoturvaa voidaan parantaa esimerkiksi käyttämällä vahvoja salasanoja, monivaiheista tunnistautumista, asentamalla käyttöjärjestelmäpäivitykset ajallaan, uhkien monitoroinnilla ja varmuuskopioinneilla. Azuren tuotevalikoimasta löytyy tietoturvaa parantavia ja tukevia maksullisia palveluita kuten Azure Firewall, Azure Backup Service ja Microsoft Defender for Cloud. (Microsoft 2020.)

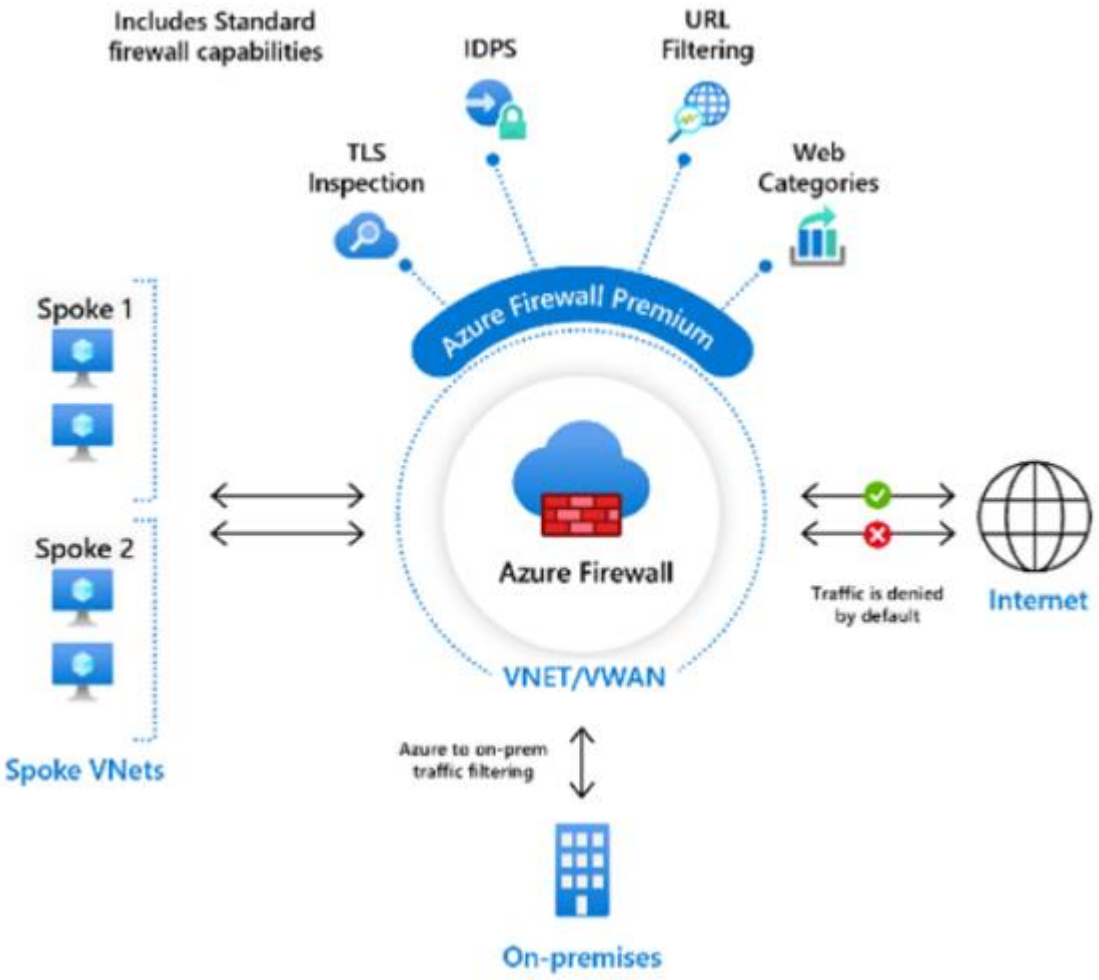
### 8.3.1 Azure Firewall

Azure Firewall jakautuu kahteen eri versioon Azure Firewall Standard ja Azure Firewall Premium. Standard-versio käyttää apunaan Microsoft Cyber Securityn uhkatietoja toimiessaan kerroksilla L3-L7 (KUVA 31). Standard-versio voi uhkatietojen avulla tunnistaa haitalliset IP-osoitteet, kun vaarallinen IP-osoite tunnistetaan antaa palomuuri hälytyksen ja estää IP-osoitteen. (Microsoft 2021k.)




KUVA 31. Azure Firewall Standard -version toiminta (Microsoft 2021k)

Azure Firewall Premium -versio (KUVA 32) tarjoaa vieläkin tehokkaampaa suojaa. Se sisältää esimerkiksi IDPS:n, joka tunnistaa haitallisia toimintakuvioita. Apunaan haitallisen toiminnan tunnistamisessa IDPS käyttää yli 58 000 tunnistetta. (Microsoft 2021k.)

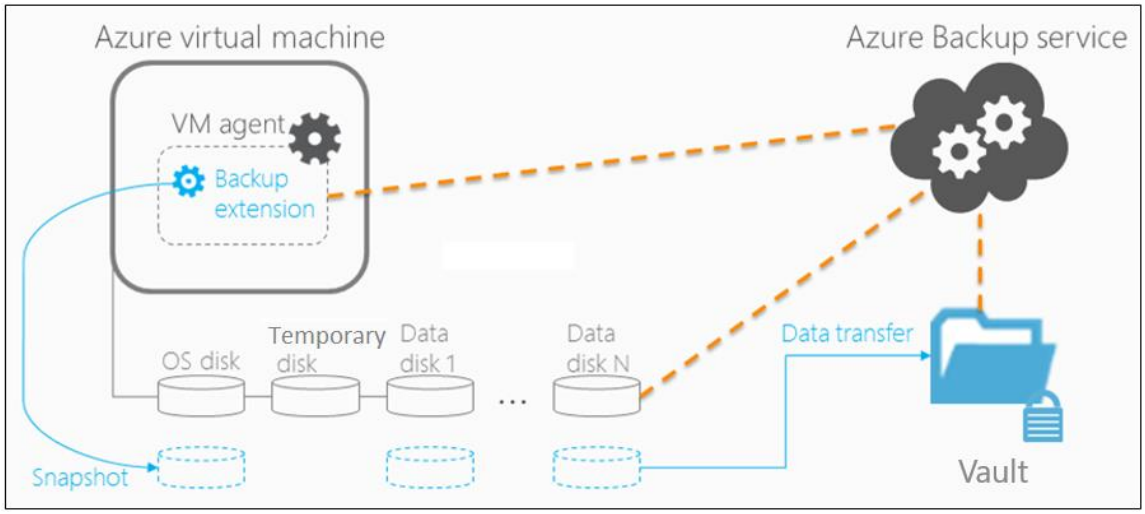



KUVA 32. Azure Firewall Premium -version toiminta (Microsoft 2021k)

### 8.3.2 Azure Backup

Azure Backup -palvelua voidaan käyttää virtuaalipalvelinten varmuuskopioimiseen (KUVA 33). Varmuuskopiointi voidaan tehdä koko virtuaalikoneelle tai osalle siitä. Varmuuskopioinnit voi aikatauluttaa tapahtumaan tiettyinä ajankohtina. Azure Backup aloittaa varmuuskopioinnin asentamalla virtuaalikoneelle varmuuskopiointiin käytettävän laajennuksen. Tämän jälkeen Backup-palvelu tallentaa laajennuksen avulla virtuaalikoneen sen hetkisen tilan ”tilannekuvaksi”. Tilannekuva on väliaikainen ja sitä käytetään virtuaalikoneen sen hetkisen tilan siirtämiseksi Backup-palveluun palautuspisteen luomista

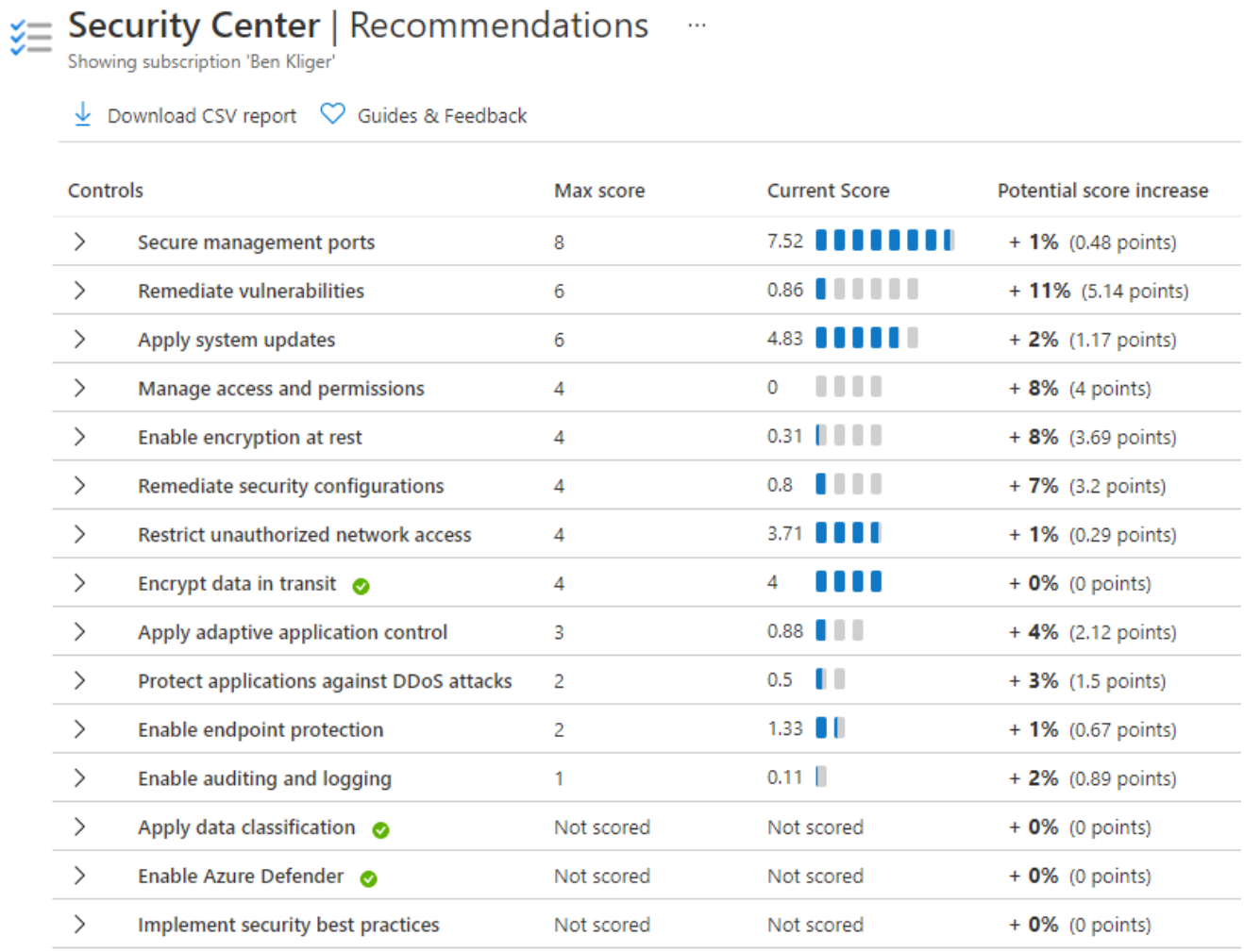
varten. Tilannekuva siirretään Vault-tallennustilaan; siirrossa voi kestää useita tunteja, mutta kuitenkin alle vuorokauden. Tilannekuvan siirron valmistuttua luodaan tilannekuvaa vastaava palautuspiste. Palautuspisteen luomisen jälkeen tilannekuva poistetaan. Varmuuskopioille käytetään SSE- eli Storage Service Encyption -salausta. Käyttöjärjestelmän ja datalevyjen salaukseen voidaan käyttää Azure Disk Encryption -salausta. (Microsoft 2021l.)




KUVA 33. Varmuuskopiointi Azure Backup -palvelulla (Microsoft 2021l)

### 8.3.3 Microsoft Defender for Cloud

Microsoft Defender for Cloud on palvelu, joka tarjoaa uhkien torjumisen lisäksi myös tietoa tietoturvan kattavuudesta ja ehdotuksia automatisoiduista toiminnoista tietoturvan parantamiseksi. Microsoft Defender for Cloud sisältää Secure Score -palvelun, joka edesauttaa virtuaaliympäristön tietoturvaa tarjoamalla reaaliaikaisen tiedon tietoturvan kattavuudesta prosentteina sekä kokonaisuutena että osa-alueittain (KUVA 34). (Microsoft 2021m; Microsoft 2021n.)




| Controls | Max score | Current Score | Potential score increase |
|---|---|---|---|
| Secure management ports | 8 | 7.52 | + 1% (0.48 points) |
| Remediate vulnerabilities | 6 | 0.86 | + 11% (5.14 points) |
| Apply system updates | 6 | 4.83 | + 2% (1.17 points) |
| Manage access and permissions | 4 | 0 | + 8% (4 points) |
| Enable encryption at rest | 4 | 0.31 | + 8% (3.69 points) |
| Remediate security configurations | 4 | 0.8 | + 7% (3.2 points) |
| Restrict unauthorized network access | 4 | 3.71 | + 1% (0.29 points) |
| Encrypt data in transit | 4 | 4 | + 0% (0 points) |
| Apply adaptive application control | 3 | 0.88 | + 4% (2.12 points) |
| Protect applications against DDoS attacks | 2 | 0.5 | + 3% (1.5 points) |
| Enable endpoint protection | 2 | 1.33 | + 1% (0.67 points) |
| Enable auditing and logging | 1 | 0.11 | + 2% (0.89 points) |
| Apply data classification | Not scored | Not scored | + 0% (0 points) |
| Enable Azure Defender | Not scored | Not scored | + 0% (0 points) |
| Implement security best practices | Not scored | Not scored | + 0% (0 points) |

KUVA 34. Security Score -palvelun arvio tietoturvasta osa-alueittain (Microsoft 2021n)

# 9 PILVIPALVELINYMPÄRISTÖ VERRATTUNA FYYSISEEN PALVELINYMPÄRISTÖÖN

Pilvipalvelinympäristö ja palvelinympäristö fyysisesti toteutettuna tarjoavat kumpikin omanlaisia hyötyjä ja haittoja. Jotta voitaisiin saada hyvä kokonaiskuva kummankin toteutustavan hyödyistä ja haitoista, vertaillaan näitä toteutustapoja osa-alueittain. Toteutustavat vertaillaan ylläpidon, mukautuvuuden, tietoturvan ja kustannuksien suhteen.

## 9.1 Ylläpito

Pilvipalvelinympäristön ylläpito on yleisesti ottaen yksinkertaisempaa ja helpompaa kuin fyysisen palvelinympäristön, koska pilvipalveluntarjoajat tarjoavat erilaisia automatisoituja ratkaisuja ylläpitoon, kuten Microsoft Azuren Backup-palvelu varmuuskopiointiin. Fyysisessä palvelinympäristössä ylläpito on manuaalisempaa ja mekaanisempaa; esimerkiksi varmuuskopiointi toteutetaan itse erilliselle varmuuskopiointipalvelimelle tai ostetun varmuuskopiointipalvelun kautta. Pilvipalvelinympäristö on kuitenkin riippuvainen pilvipalveluntarjoajasta, mikäli pilvipalvelu tai osia siitä olisi jostakin syystä alhaalla resurssit tai tietyt toimenpiteet eivät olisi tällöin saatavilla.

## 9.2 Mukautuvuus

Mukautuvuus on yksi pilvipalvelinympäristön eduista; palvelinten määrän lisääminen tai vähentäminen tapahtuu nopeasti ja vaivattomasti. Fyysisessä palvelinympäristössä palvelinten määrän lisääminen vie aikaa niin tilausaikojen kuin käyttöönoton suhteen.

## 9.3 Tietoturva

Pilvipalvelinympäristön tietoturvaa on mahdollista parantaa ja seurata pilvipalveluntarjoajan automatisoiduilla palveluilla kuten Microsoft Azure -ympäristössä Microsoft Defender for Cloud -palvelulla. Fyysisissä palvelinympäristöissä tietoturvan parannus ja seuranta täytyy toteuttaa itse esimerkiksi erillisillä laitteilla kuten palomuurilla ja haavoittuvuusskannausohjelmiston sisältävällä laitteella. Fyysistä

palvelinympäristöä toteutettaessa joudutaan vastaamaan enemmän itse tietoturvan teknisestä toteuttamisesta kuin pilvipalvelinympäristön tietoturvaa toteutettaessa.

### 9.4 Kustannukset

Fyysisen palvelinympäristön toteuttaminen ja toteuttamisen jälkeinen palvelinympäristön ylläpito ja laitteiston uusiminen aiheuttaa suuriakin kertakustannuksia kun taas pilvipalvelinympäristöä laskutetaan käytön mukaan. Kustannuksiin vaikuttaa myös tarvittava asiantuntijoiden määrä ja näin ollen henkilöstökustannukset voivat olla suurempia fyysisessä palvelinympäristössä, koska tarvittava tietämys on yleensä suurempaa kuin pilvipalvelinympäristöä käyttäessä. Pilvipalvelinympäristön käyttäminen voi tuoda tilakustannussäästöjä, koska omia tiloja palvelimille ei tarvita. (Collins 2020; Reed 2018.)

# 10 POHDINTA

Tutkiessani palvelinympäristövaihtoehtoja sain itseni vakuutettua siitä, että pilvipalvelinympäristö on erittäin hyvä vaihtoehto fyysiselle palvelinympäristölle tai ainakin osaksi sellaista. Sain opinnäytetyötä tehdessä paljon uutta tietämystä palvelinympäristöistä ja vahvistettua aiempaa tietämystäni aiheesta. Ennen opinnäytetyön kirjoitusta ajattelin Microsoftin olevan kaikista paras pilvipalveluntarjoaja palvelinympäristöjä ajatellen, mutta tutkiessani Amazonin tarjontaa huomasin myös sen olevan todella hyvä pilvipalveluntarjoaja.

Työn tekoa hankaloittavaksi ongelmaksi osoittautui lähdemateriaalien englanninkielisyys; joitakin termejä ja asioita oli haastavaa muotoilla suomenkieliseksi. Laajoja lähteitä ei juurikaan löytynyt vaan tietoperustaa piti koota hyvin monien lyhyempien lähdemateriaalien perusteella. Alun perin työssä oli tarkoitus esitellä useampiakin pilvipalveluntarjoajia tarkemmin, mutta lopulta päätin rajata esiteltävät pilvipalveluntarjoajat kahteen suosituimpaan, jotta esittelyt voisivat olla pidempiä ja monipuolisempia.

Sisältö opinnäytetyölle olisi voinut olla teknisempää, mutta halusin pitää opinnäytetyön osa-alueet teknisyytensä osalta yhteneväisinä ja helposti ymmärrettävinä. Tavoitteena opinnäytetyölle oli opastaa palvelinympäristön valinnassa ja antaa vastaus kysymykseen, miksi pilvipalvelinympäristö on hyvä vaihtoehto fyysiselle palvelinympäristölle. Tavoite toteutui melko hyvin ja oma tiivistetty vastaukseni edellä olevaan kysymykseen olisi: ”Pilvipalvelinympäristö on hyvä vaihtoehto fyysiselle palvelinympäristölle, koska pilvipalvelinympäristö on mukautuvampi ja kustannustehokkaampi”.

**LÄHTEET**

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma. Viitattu: 6.10.2021.

Amazon Web Services. 2021a. Cloud computing with AWS. Saatavissa: https://aws.amazon.com/what-is-aws/. Viitattu: 23.9.2021.

Amazon Web Services. 2021b. About AWS. Saatavissa: https://aws.amazon.com/about-aws/. Viitattu: 23.9.2021.

Amazon Web Services. 2021c. Global Infrastructure. Saatavissa: https://aws.amazon.com/about-aws/global-infrastructure/?hp=tile&tile=map. Viitattu: 23.9.2021.

Amazon Web Services. 2021d. Amazon Lightsail or Amazon EC2. Saatavissa: https://aws.amazon.com/free/compute/lightsail-vs-ec2/?sc_icampaign=Adoption_Campaign_FY21-ec2-lightsail-ribbon&sc_ichannel=ha&sc_icontent=awssm-8071_aquire&sc_ioutcome=Enterprise_Digital_Marketing&sc_iplace=ribbon&trk=ha_a134p000006wAZdAAM~ha_awssm-8071_aquire&trkCampaign=pac-edm-2020-lightsail-ec2. Viitattu: 14.11.2021.

Amazon Web Services. 2021e. Amazon Lightsail features. Saatavissa: https://aws.amazon.com/lightsail/features/. Viitattu: 14.11.2021.

Amazon Web Services. 2021f. Amazon Lightsail pricing. Saatavissa: https://aws.amazon.com/lightsail/pricing/. Viitattu: 14.11.2021.

Amazon Web Services. 2021g. Usability Improvements for AWS Management Console Now Available. Saatavissa: https://aws.amazon.com/about-aws/whats-new/2018/11/aws-management-console-usability-improvements/. Viitattu 14.11.2021.

Amazon Web Services. 2021h. Security in Amazon Lightsail. Saatavissa: https://lightsail.aws.amazon.com/ls/docs/en_us/articles/security. Viitattu: 17.11.2021.

Amazon Web Services. 2021i. Amazon EC2. Saatavissa: https://aws.amazon.com/ec2/. Viitattu: 14.11.2021.

Amazon Web Services. 2021j. Amazon EC2 Instance Types. Saatavissa: https://aws.amazon.com/ec2/instance-types/. Viitattu: 14.11.2021.

Amazon Web Services. 2021k. Amazon EC2 pricing. Saatavissa: https://aws.amazon.com/ec2/pricing/. Viitattu: 14.11.2021.

Amazon Web Services. 2021l. Configure Amazon EC2. Saatavissa: https://calculator.aws/#/createCalculator/EC2. Viitattu: 14.11.2021.

Amazon Web Services. 2021m. Security in Amazon EC2. Saatavissa: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security.html. Viitattu: 14.11.2021.

Amazon Web Services. 2021n. AWS Shield. Saatavissa: https://aws.amazon.com/shield/. Viitattu: 17.11.2021.

Atea. 2021. Tornipalvelimet. Saatavissa: https://www.atea.fi/eshop/products/tietokoneet-ja-laitteisto/palvelimet/tornipalvelimet/. Viitattu: 1.11.2021.

Chai, W. & Bigelow, S. 2021. Cloud server. TechTarget. Saatavissa: https://searchcloudcomputing.techtarget.com/definition/cloud-server. Viitattu: 3.11.2021.

Chapple, M. 2021. Confidentiality, Integrity And Availability – The CIA Triad. Saatavissa: https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/. Viitattu: 7.10.2021.

Cloudflare. 2021. What is a DDoS attack? Saatavissa: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. Viitattu: 14.10.2021.

Collins, T. 2020. Cloud vs. Dedicated Server Cost: Which Is The Better Deal? Atlantech Online. Saatavissa: https://www.atlantech.net/blog/cloud-vs.-dedicated-server-cost-which-is-the-better-deal. Viitattu: 28.11.2021.

Decens. 2021. Konesali- ja kapasiteettipalvelut. Saatavissa: https://decens.fi/palvelut/konesalipalvelut/. Viitattu: 3.11.2021.

Dignan, L. 2021. Top cloud providers in 2021: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players. Saatavissa: https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/. Viitattu: 23.9.2021.

F-Secure. 2021. Paras VPN 2021. Saatavissa: https://www.f-secure.com/fi/home/articles/best-vpn. Viitattu: 7.10.2021.

Fisher, T. 2021. DNS Servers: What Are They and Why Are They Used? Lifewire. Saatavissa: https://www.lifewire.com/what-is-a-dns-server-2625854. Viitattu: 26.10.2021.

Gurinaviciute, J. 2021. 5 biggest cybersecurity threats. Security Magazine. Saatavissa: https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats. Viitattu: 14.10.2021.

Hazell, L. 2015. How does DHCP work? Cybersecurity News. Saatavissa: https://cybersecuritynews.co.uk/how-does-dhcp-work/. Viitattu: 23.10.2021.

Hoffman, C. 2021. What Is a VPN, and Why Would I Need One? How-To Geek. Saatavissa: https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/. Viitattu 7.10.2021.

Kailio, A. 2020. AWS joutui kaikkien aikojen voimakkaimman palvelunestohyökkäyksen kohteeksi. Tivi. Saatavilla: https://www-tivi-fi.ezproxy.centria.fi/uutiset/aws-joutui-kaikkien-aikojen-voimakkaimman-palvelunestohyokkayksen-kohteeksi/19b5f4f0-698a-4991-8efe-e714f7e66f79. Viitattu: 17.11.2021.

Karkimo, A. 2019. Pilvijätin kimppuun käytiin raisulla palvelunestohyökkäyksellä: Amazonia pommitettiin tunteja, myös Google kompasteli. Tivi. Saatavilla: https://www-tivi-fi.ezproxy.centria.fi/uutiset/pilvijatin-kimppuun-kaytiin-raisulla-palvelunestohyokkayksella-amazonia-pommitettiin-tunteja-myos-google-kompasteli/5f0b60e8-6418-4203-90fb-fed33883da16. Viitattu: 17.11.2021.

Kaspersky. 2021. What is DNS Cache Poisoning and DNS Spoofing? Saatavissa: https://www.kaspersky.com/resource-center/definitions/dns. Viitattu: 3.11.2021.

KeyCDN. 2018. DDoS Attack. Saatavissa: https://www.keycdn.com/support/ddos-attack. Viitattu: 14.10.2021.

Khillar, S. 2021. Difference Between Name Server and DNS. Saatavissa: http://www.differencebetween.net/technology/difference-between-name-server-and-dns/. Viitattu: 26.10.2021.

Lanfear, T. 2021. Shared responsibility in the cloud. Microsoft. Saatavissa: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. Viitattu: 21.11.2021.

Marskidata. 2021. Konesalipalvelut. Saatavissa: https://www.marskidata.fi/konesalipalvelut/. Viitattu: 3.11.2021.

Mezquita, T. 2020. Two-Factor Authentication. CyberHoot. Saatavissa: https://cyberhoot.com/cybrary/two-factor-authentication/. Viitattu 7.10.2021.

Microsoft. 2020. Best practices for defending Azure Virtual Machines. Saatavissa: https://www.microsoft.com/security/blog/2020/10/07/best-practices-for-defending-azure-virtual-machines/. Viitattu: 22.11.2021.

Microsoft. 2021a. Connect to remote Azure Active Directory-joined PC. Saatavissa: https://docs.microsoft.com/en-us/windows/client-management/connect-to-remote-aadj-pc. Viitattu: 1.11.2021.

Microsoft. 2021b. What is Azure? Saatavissa: https://azure.microsoft.com/en-us/overview/what-is-azure/. Viitattu: 21.11.2021.

Microsoft. 2021c. Azure compliance. Saatavissa: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/. Viitattu 21.11.2021.

Microsoft. 2021d. Strengthen your security posture with Azure. Saatavissa: https://azure.microsoft.com/en-us/overview/security/. Viitattu 21.11.2021.

Microsoft. 2021e. Pay less with Azure. Saatavissa: https://azure.microsoft.com/en-us/overview/azure-vs-aws/cost-savings/. Viitattu: 21.11.2021.

Microsoft. 2021f. Azure global compliance. Saatavissa: https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-global-compliance-map/AzureComplianceInfographic.pdf. Viitattu: 21.11.2021.

Microsoft. 2021g. Pricing calculator. Saatavissa: https://azure.microsoft.com/en-gb/pricing/calculator/#virtual-machines. Viitattu: 21.11.2021.

Microsoft. 2021h. Virtual Machine series. Saatavissa: https://azure.microsoft.com/en-us/pricing/details/virtual-machines/series/. Viitattu: 21.11.2021.

Microsoft. 2021i. Azure Reserved Virtual Machine Instances. Saatavissa: https://azure.microsoft.com/en-gb/pricing/reserved-vm-instances/. Viitattu: 21.11.2021.

Microsoft. 2021j. Azure DDoS Protection. Saatavissa: https://azure.microsoft.com/en-us/services/ddos-protection/#overview. Viitattu: 21.11.2021.

Microsoft. 2021k. What is Azure Firewall? Saatavissa: https://docs.microsoft.com/en-us/azure/firewall/overview. Viitattu: 22.11.2021.

Microsoft. 2021l. An overview of Azure VM backup. Saatavissa: https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction. Viitattu: 23.11.2021.

Microsoft. 2021m. What is Microsoft Defender for Cloud? Saatavissa: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction. Viitattu: 23.11.2021

Microsoft. 2021n. Secure score in Microsoft Defender for Cloud. Saatavissa: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls. Viitattu: 23.11.2021.

MSV, J. 2020. A Look Back At Ten Years Of Microsoft Azure. Forbes. Saatavilla: https://www.forbes.com/sites/janakirammsv/2020/02/03/a-look-back-at-ten-years-of-microsoft-azure/. Viitattu: 21.11.2021.

Okta. 2021. Firewall: Definition, How They Work and Why You Need One. Saatavissa: https://www.okta.com/sg/identity-101/firewall/. Viitattu: 7.10.2021.

Omnisecu.com. 2021. DHCP Starvation attacks and DHCP spoofing attacks. Saatavissa: https://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php. Viitattu: 3.11.2021.

Posey, B. 2021. What is a Server? TechTarget. Saatavissa: https://whatis.techtarget.com/definition/server. Viitattu: 23.10.2021.

Reed, J. 2018. Physical Servers vs. Virtual Machines: Key Differences and Similarities. Nakivo. Saatavissa: https://www.nakivo.com/blog/physical-servers-vs-virtual-machines-key-differences-similarities/. Viitattu: 28.11.2021.

Salo, I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo. Viitattu: 14.11.2021.

Shacklett, M. & Rosencrance, L. 2021. Authentication. TechTarget. Saatavissa: https://searchsecurity.techtarget.com/definition/authentication. Viitattu 7.10.2021.

Schäfer, E. 2017. Saatavilla: https://pixabay.com/fi/photos/palvelin-tilaa-palvelimen-huone-2160321/. Viitattu: 1.11.2021.

Smart Eye Technology. 2021. Confidentiality, Integrity, & Availability: Basics of Information Security. Saatavissa: https://getsmarteye.com/confidentiality-integrity-availability-basics-of-information-security/. Viitattu: 7.10.2021.

SolarWinds. 2019. What Is Server Management? Definition, Best Practices, and Best Software. Saatavissa: https://www.dnsstuff.com/server-management. Viitattu: 1.11.2021.

Suomidigi. 2020. VAHTI 22/2017 Ohje riskienhallintaan. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-222017-ohje-riskienhallintaan. Viitattu: 14.10.2021.

Tietokeskus. 2021. Konesalipalvelut. Saatavissa: https://www.tietokeskus.fi/kayttopalvelut/konesalipalvelut/. Viitattu: 3.11.2021.

Vaughan-Nichols, S. 2021. Microsoft Azure fends off huge DDoS Attack. ZDNet. Saatavilla: https://www.zdnet.com/article/microsoft-azure-fends-off-huge-ddos-attack/. Viitattu: 21.11.2021.