Toni Pehkonen

Mikroyrityksen identiteetti- ja laitehallinta pilvipalvelujen avulla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

27.12.2017

Metropolia

Tekijä Otsikko Sivumäärä Aika	Toni Pehkonen Mikroyrityksen identiteetti- ja laitehallinta pilvipalvelujen avulla 126 sivua 27.12.2017
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	tieto- ja viestintätekniikka
Ammatillinen pääaine	Communication Networks and Applications
Ohjaaja	Lehtori Tapio Wikström

Insinöörityössä selvitettiin, mihin hintaan ja miten yrityksen perusinfrastruktuuritarpeet voitaisiin toteuttaa pilvipalveluilla fyysisten palvelinten ja perinteisen konesalikapasiteetin ostamisen sijaan. Työssä luotiin kolme erilaista ratkaisua, joissa viiden henkilön esimerkkiyritykselle toteutettiin identiteetti- ja laitehallinta ja tiedostonjakoratkaisu, otettiin käyttöön sähköpostipalvelu ja asennettiin toimistosovellukset.

Insinöörityön ratkaisuissa tutkittiin uudenlaista tapaa hallita käyttäjien identiteettiä ja työasemia ja toteutettiin myös infrastruktuuri pilveen perinteisellä tapaa. Ensimmäisessä ratkaisussa työaseman ja pilven välille ei tarvinnut luoda erillistä yhteyttä, mutta muissa ratkaisuissa luotiin Point-to-Site-VPN-yhteys työaseman ja pilvessä sijaitsevan infrastruktuurin välille.

Insinöörityön lähtökohtana oli luoda yrityksen perusinfrastruktuuri ilman fyysisiä palvelimia ja toteuttaa ratkaisut mahdollisimman edullisesti. Kustannussyiden takia ratkaisuja toteutettiin palvelinten vikasietoisuuden suhteen vastoin parhaita käytäntöjä, ja kaikille ratkaisuille ei saavutettu pilvipalvelutarjoajan palvelutasosopimusta. Ratkaisut toteutettiin kuitenkin tietoturva huomioon ottaen. Palveluiden saatavuudessa luotettiin pilvipalveluiden korkeaan käytettävyyteen, mutta palvelimet turvattiin virhetilanteiden varalta erillisellä varmuuskopiointiratkaisulla.

Lopputuloksena syntyi kolme kustannustehokasta ja nopeasti käyttöönotettavaa ratkaisua toteuttamaan mikroyrityksen perusinfrastruktuuritarpeet. Uudenlainen tapa osoittautui insinöörityössä käyttöönotetulla laitehallinnan laajuudella helppokäyttöiseksi ja toimivaksi ratkaisuksi ja muut ratkaisut pystyttiin luomaan lopulta luonnistuneesti. Tavoitteena oli tuottaa myös mahdollisimman helppokäyttöinen ja itsepalveluperiaatteella toimiva kokonaisuus, mutta tietoliikenneyhteyksien manuaalisella konfiguroimisella ja kolmannen ratkaisun työasemien käyttöönotossa ei pystytty täyttämään näitä työlle asetettuja tavoitteita. Pilvipalvelut osoittautuivat joustavaksi ja kustannustehokkaaksi vaihtoehdoksi perinteisille ratkaisuille.

Avainsanat	Active Directory, Azure AD, EMS, pilvipalvelut, Intune, Office 365

Author	Toni Pehkonen
Title	Micro-enterprise identity and device management with cloud services
Number of Pages	126 pages
Date	27 December 2017
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Professional Major	Communication Networks and Applications
Instructor	Tapio Wikström, Senior Lecturer

This Thesis examined how much it will cost and how to create micro-enterprises basic infrastructure services with cloud services, without buying any on-premises´ hardware or paying for traditional datacenter capacity. The study implemented three different solutions that provided identity and device management, file sharing solution, deployed email service and installed office apps to five people in a company.

Thesis solutions examined a modern way to control users´ identities and devices and one of the solutions deployed infrastructure to cloud in a traditional way. There was no need to create extra connectivity between workstation and cloud in the first solution, but other solutions did require Point-to-Site VPN connection between workstation and infrastructure that located in cloud.

The idea of this thesis was to create a company basic infrastructure services without physical hardware and to provide different solution costs as cost-effectively as possible. Solutions were implemented against the fault tolerance best practices and they did not reach cloud service provider service-level agreement, because of the costs. Cloud services general availability for the services were trusted on these solutions, but servers were backed up for user errors with a cloud-based backup service.

As a result of this study three cost-effective and fast-paced solutions were created to provide basic infrastructure services to micro-enterprise. On the thesis device management scope, the modern way turned out to be easy to manage and in the end other working solutions could also be created successfully. The goal of solutions was to be easy to use and managed by self-service. With the manual configuration of data connections and workstation deployment in solution three, the goal was not met. Cloud services prove to be flexible and cost-effective alternative to traditional solutions.

Keywords	Active Directory, Azure AD, cloud services, EMS, Intune, Office 365

Sisällys

Lyhenteet

AD	Active Directory. Windows-toimialueessa käytettävä käyttäjätietokanta ja hakemistopalvelu.
Azure AD	Microsoftin pilvipohjainen käyttäjätietokanta ja hakemistopalvelu.
Azure AD DS	Azure Active Directory Domain Services. Azure AD:n laajennus ylläpidetyksi toimialuepalveluksi.
DC	Domain Controller. Windows-toimialueen palvelin, joka vastaa kaikkiin toimialueen tunnistuspyyntöihin.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
GPO	Group Policy Object. Toimialueessa käytettävä erilaisien käytäntöjen kokoelma.
IaaS	Infrastructure as a Service. Infrastruktuuri palveluna.
IP-osoite	Internet Protocol Address. Verkkoliikenteessä laitteiden yksilöimiseen käytettävä osoite.
MFA	Multi-Factor Authentication. Henkilön identiteetin tunnistaminen käyttämällä kahta tai useampaa tunnistusmenetelmää.
OU	Organization Unit. Microsoft Active Directoryssa objektien ryhmittämiseen käytettävä säilö.
PaaS	Platform as a Service. Alusta palveluna.
PING	Packet Internet Groper. Pingiä tai ”pingaamista” käytetään verkkolaitteen yhteyden testaamiseen IP-verkoissa.

RAID	Redundant Array of Independent Disks. Tekniikka, jolla useampi kiintolevy voidaan yhdistää yhdeksi loogiseksi kiintolevyksi.
SaaS	Software as a Service. Sovellus palveluna.
SSO	Single sign-on. Kertakirjautuminen yhdellä tunnistautumisella useampaan palveluun.
VNET	Virtual Network. Azuren loogisesti eristetty virtuaalinen verkko.
VPN	Virtual Private Network. Tapa liittää verkkoja toisiinsa suojatulla yhteydellä julkisen verkon kautta.

1 Johdanto

Insinöörityön tavoitteena on selvittää, miten mikroyrityksen laite- ja identiteetinhallinta toteutetaan Microsoftin pilvipalveluilla ja kuinka paljon sen toteuttaminen maksaa. Pieni aloittava yritys voi pilvipalveluilla toteuttaa nopeasti infrastruktuurin kuukausilaskutuksella ilman suurta kertasijoitusta fyysisiin palvelimiin ja ilman palveluntarjoajan toimitus- ja muutosaikatauluja tai määräaikaisia sopimuskausia. Kolmessa erilaisessa ratkaisussa toteutetaan keskitetysti hallittavat käyttäjätunnukset, laitehallinta ja tiedostonjakoratkaisu ja otetaan käyttöön Office 365 -palvelut. Office 365:n osuudessa määritellään myös mikroyritykselle sopivat Office 365 -versiot, jotka sisältävät sähköpostin ja asennettavat työpöytäsovellukset. Lopuksi vertaillaan eri vaihtoehtoja käytettävyyden, ominaisuuksien ja kuukausittaisten kustannusten osalta. Painotus pidetään ratkaisujen edullisuudessa, jolloin joudutaan toteuttamaan asioita vastoin parhaita käytäntöjä ja tinkimään suorituskyvystä.

Ensimmäisessä ratkaisussa toteutetaan käyttäjien identiteettihallinta Azure Active Directorylla ja laitehallinta Intunella. Toisessa ratkaisussa laajennetaan Azure AD pilvessä toimivaksi toimialueeksi Azure Active Directory Domain Services -palvelulla. Kolmannessa ratkaisussa toteutetaan toimialue pilveen perinteisesti, asentamalla toimialue virtuaalikoneeseen ja laitehallintana tässä ratkaisussa käytetään Group Policya.

Vaatimuksena ratkaisulle on internetyhteys ja työasemien täytyy olla varustettuna vähintään Windows 10 Pro -versiolla, jossa on mahdollista liittyä perinteiseen toimialueeseen ja suorittaa Azure AD Join. Esimerkkinä tässä insinöörityössä käytetään viiden henkilön yritystä, joille luodaan keskitetysti hallittavat käyttäjätunnukset:

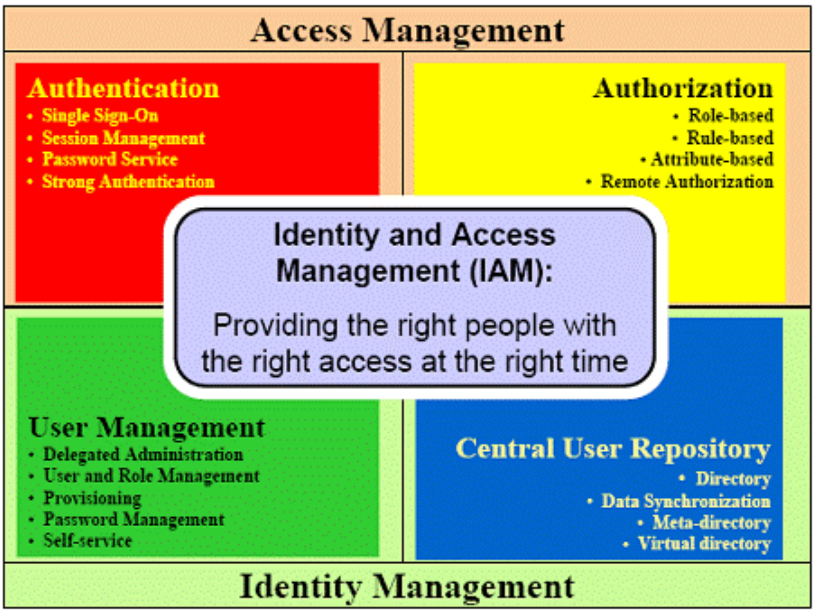
- Anssi Asentaja
- Esa Esimies
- Mikko Myyjä
- Tanja Talous
- Tomi Toimari.

Jokainen käyttäjä edustaa sukunimestään pääteltävää roolia yrityksessä. Tiedostonjakoratkaisussa tehdään tiedostojaot näiden roolien mukaan, jolloin pääsy on rajattu vain

tämän roolin käyttäjälle ja toimitusjohtajalle. Myöhemmin yrityksen palkatessa esimerkiksi uuden myyjän hänelle annetaan saman oikeudet kuin Mikko Myyjälle. Yritykselle tehdään myös tiedostojako yhteistä tiedonvaihtoa varten, johon kaikilla työntekijöillä on pääsy.

2 Identieetin- ja pääsynhallinta

Identiteetin- ja pääsynhallinta (Identity and access management, IAM) käsittää prosesseja ja teknistä ratkaisua toteuttaa käyttäjille digitaalinen identiteetti, jolla on pääsy käyttäjälle myönnettyihin järjestelmiin ja palveluihin (1). Niemen (2) mukaan identiteetinhallinnan tavoitteena on toteuttaa oikealle ihmiselle oikeat pääsyoikeudet ja oikeaan paikkaan. Identiteetin- ja pääsynhallinta voidaan jakaa kuvan 1 osoittamiin osa-alueisiin. Identiteetinhallintajärjestelmiä on lukuisia, mutta tämä työ keskittyy perinteiseen yritysympäristössä käytössä olevaan Microsoftin Active Directoryyn (AD) ja uudehkoon pilvipohjaiseen Azure Active Directoryyn (Azure AD).



Kuva 1. Identiteetin- ja pääsynhallinnan osa-alueet (1).

2.1 Todennus

Identiteetin todennus, käytetään myös nimeä autentikointi (authentication), suoritetaan kun käyttäjä, järjestelmä tai laite pyytää pääsyä johonkin sovellukseen tai järjestelmään. Identiteetin haltija välittää vaadittavat tiedot identiteetistään, usein käyttäjätunnuksen ja salasanan, minkä jälkeen annettu identiteetti todennetaan keskitetystä käyttäjähakemistosta. Onnistuneen todennuksen jälkeen identiteetti on vahvistettu ja sessio luodaan identiteetin haltijan ja kohdejärjestelmän välille. Session päättyessä, joko kirjauduttaessa ulos sessiosta tai automaattisesti esimerkiksi aikakatkaisun vuoksi, ei identiteetin haltijalla ole enää pääsyä järjestelmään ilman uutta todennusta. (1; 2.)

2.2 Valtuutus

Identiteetin todentamisen jälkeen katsotaan, onko identiteetillä valtuudet päästä pyydettyyn järjestelmään. Identiteetit voidaan valtuuttaa yksittäin, tai valtuutus voidaan toteuttaa esimerkiksi rooliin perustuvalla pääsynvalvonnalla (Role-Based Access Control, RBAC), jolloin rooleihin liitetään käyttäjiä ja valtuudet annetaan rooleille. Attribuuttiin perustuvassa pääsynvalvonnassa (Attribute-Based Access Control, ABAC) pääsy sallitaan, jos identiteetin attribuuttien arvot vastaavat määriteltyjä. (1; 3, s. 32, 35.)

Active Directoryssä oikeudet annetaan yleensä ryhmille, joihin lisätään käyttäjiä. Azure Active Directoryssa on mahdollista luoda dynaamisia ryhmiä, joille määritetään attribuutteihin perustuvia sääntöjä, ja kaikki käyttäjät, joille sääntö on tosi, tulevat ryhmän jäseniksi. Käyttäjä poistuu ryhmästä, jos attribuutti ei vastaa enää sääntöä. Esimerkiksi jos dynaamisen ryhmän sääntönä on, että osasto-attribuutti on myynti, poistuu käyttäjä ryhmästä, kun hänen tietoihinsa päivitetään uusi osasto. (4.)

2.3 Käyttäjän hallinta

Hallinta käsittää kaikenlaisen käyttäjätileihin liittyvän hallinnoinnin: luomisen ja poistamisen, ryhmät, roolit ja salasanat. Osa näistä voidaan ulkoistaa käyttäjälle itselleen. Azure AD:n maksullisen tilauksen ominaisuuksia ovat itsepalveluportaali salasanan nollaamiselle ja käyttäjille voidaan antaa oikeudet tehdä ryhmiä tai hallita ryhmien jäsenyyksiä itsepalveluryhmillä (4; 5; 6).

2.4 Keskitetty käyttäjähakemisto

Käyttäjähakemistossa sijaitsevat kaikki identiteetit, ja hakemistossa suoritetaan identiteetin todennus (1). Identiteetit sijaitsevat keskitetysti yhdessä hakemistossa, jolloin esimerkiksi käyttäjän salasana tarvitsee vaihtaa vain yhdessä paikassa ja kaikilla todennusta vaativilla palveluilla on käytettävissä muuttuneet tiedot uutta todennusta tehtäessä.

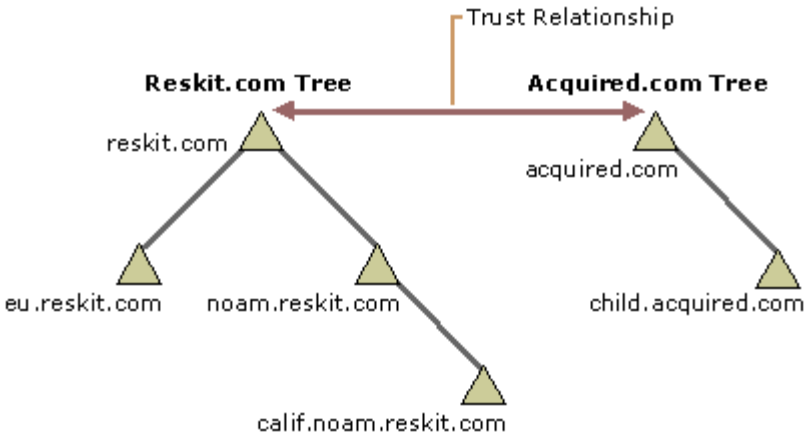
Active Directory

Active Directory Domain Services on Windows-palvelimeen asennettava rooli, joka luo toimialueen, jonka keskitettynä käyttäjähakemistona Active Directory toimii. Roolin asennuksen jälkeen palvelimesta tulee toimialueen ohjauskone (Domain Controller, DC), joka vastaa toimialueen autentikointipyyntöihin. Rooli sisältää erilaisia työkaluja joilla toimialuetta voidaan hallita, mutta resursseja hallitaan pääasiassa Active Directory Users and Computers -työkalulla.

Active Directoryn hierarkkinen rakenne perustuu X.500-stantardiin. AD:n juurena toimii metsän juuritoimialue (forest root domain), joka on AD DS -roolin asennuksen yhteydessä luotavan metsän ensimmäinen toimialue (7; 8). Metsässä voi olla useita puita (Trees), jotka voivat koostua toimialueista ja alitoimialueista (child-domain). Pienelle yritykselle, jolla ei ole tarvetta eriyttää resursseja toisistaan, luodaan yhden toimialueen metsä.

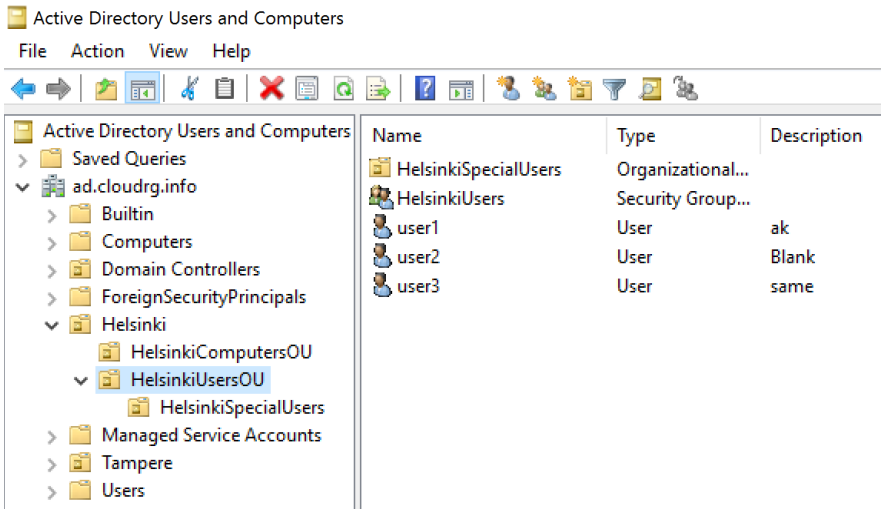
Yleensä organisaatiolla on metsässä vain yksi puu, ja yritysostojen tai sulautumisten yhteydessä organisaatioiden Active Directory -puut yhdistetään luottosuhteilla yhdeksi metsäksi. Juuritoimialue ja sen alitoimialueet samassa puussa muodostavat yhtenäisen DNS-nimiavaruuden (Domain name system -namespace). Juuritoimialueen nimi voi olla esimerkiksi yritys.fi, ja sen kahden eri alitoimialueen DNS-nimet voivat olla helsinki.yritys.fi ja tampere.yritys.fi. (9.)

Metsien, puiden ja toimialueiden hierarkkinen rakenne on havainnollistettu kuvassa 2.



Kuva 2. Kahden puun metsä useilla alitoimialueilla. Kolmion kuvaa toimialuetta. (8.)

Resurssien hallinnan kannalta tärkein työkalu on Active Directory Users and Computers, jossa hierarkkisena juurena on toimialue. Jokaisella toimialueella on oma Active Directory. Resurssit tallennetaan hakemistoon objekteina. Hakemisto sisältää oletussäilöt konetileille, käyttäjätunnuksille, oletusryhmille ja muiden toimialueiden luottosuhteille (Computers, Users, Builtin ja ForeignSecurityPrincipals). Näitä säilöjä ei voi poistaa, eikä niihin voi kohdistaa ryhmäkäyttöjä (Group Policy). Domain Controllers -niminen organisaatioyksikkö (Organizationa Unit, OU) luodaan automaattisesti, johon kaikkien Domain Controllereiden konetilit menevät toimialueeseen liityttäessä. Järjestelmänvalvoja voi luoda uusia OU:ita, ryhmiä, käyttäjiä ja konetilejä. Käyttäjä- ja konetili voi olla osa useaa ryhmää, ryhmä voi olla osa toista ryhmää ja OU:n sisällä voi olla useita OU:ita (kuva 3), jotka sisältävät ryhmiä ja/tai käyttäjiä. Järjestelmänvalvoja voi myös delegoida toiselle järjestelmänvalvojalle hallinnan OU-kohtaisesti. (10.)



Kuva 3. Esimerkki Active Directoryn rakenteesta.

Ryhmäkäytännöt (Group Policy, GP) sisältävät valtavan määrän asetuksia, joilla voidaan hallita käyttäjiä ja koneita. Automaattisesti luotu Default Domain Controllers Policy -niminen ryhmäkäytäntöobjekti (Group Policy Object, GPO), kohdistuu Domain Controllers OU:hun ja näin ollen kaikkiin palvelimiin, jotka toimivat DC:inä. Järjestelmänvalvoja voi luoda GPO:ita ja kohdistaa OU kohtaisesti tai koko toimialueeseen. OU:hun kohdistetun GPO:n asetukset kohdistuvat myös sisäkkäisiin OU:ihin.

Active Directory käyttää hakemistopalvelun protokollana LDAP:a (Lightweight Directory Access Protocol), jota myös UNIX-käyttöjärjestelmät tukevat ja jota myös monet muut hakemistopalvelut käyttävät. LDAP on myös oma autentikointi- ja valtuutusprotokolla, jolla Active Directoryn tietoja voidaan hakea, muokata, päivittää ja poistaa TCP/IP-protokollan avulla. AD käyttää autentikointi protokollanaan pääasiallisesti joko NTLM:ää (NT Lan Manager) tai useimmiten turvallisempaa kerberosta, ja kerberos toimii yhdessä lDAP:n kanssa haettaessa tietoa AD:sta. (7; 11; 12; 13.)

Azure Active Directory

Koska työntekijät käyttävät yhä enemmän organisaation ulkopuolisia työkaluja eri päätelaitteilla, on eri tunnusten hallinnoiminen muuttunut hankalammaksi ja IT-osasto on osittain menettänyt hallinnan. Azure Active Directory mahdollistaa tuhansien SaaS-sovellusten integroimisen osaksi keskitettyä identiteetti- ja pääsynhallintaratkaisua ja antaa samalla IT-osastolle mahdollisuuden sallia tai evätä pääsy sovellus- ja käyttäjäkohtaisesti. Se sisältää myös versiosta riippuen kattavan määrän työkaluja ja raportteja mm.

sovellusten käyttöasteesta. Se mahdollistaa samalla myös MFA:n (Multi Factor Authentication), jossa käyttäjän pitää tunnistautua salasanan lisäksi jollakin toisella tekijällä, esimerkiksi puhelimella, ja kertakirjautumisen (Single sign-on, SSO), jolloin käyttäjä kirjautuu automaattisesti ilman tunnusten syöttämistä uuteen sovellukseen, kun autentikointi on jo kerran tehty (7; 14.)

Azure AD:n hierarkia on litteä, eikä se tue Organization Uniteja. Kaikki käyttäjät ja ryhmät löytyvät hakemiston juuresta. Perinteisen AD:n käyttäjät voidaan synkronoida paikallisesta ympäristöstä Azure AD:hen Azure AD Connect -työkalun avulla. Tämä mahdollistaa esimerkiksi itsepalveluportaalin käyttäjille salasanan nollaamisen MFA:ta käyttäen, jolloin salasana vaihdetaan Azure AD:hen ja synkronoidaan sitten paikalliseen AD:hen. (7; 14.)

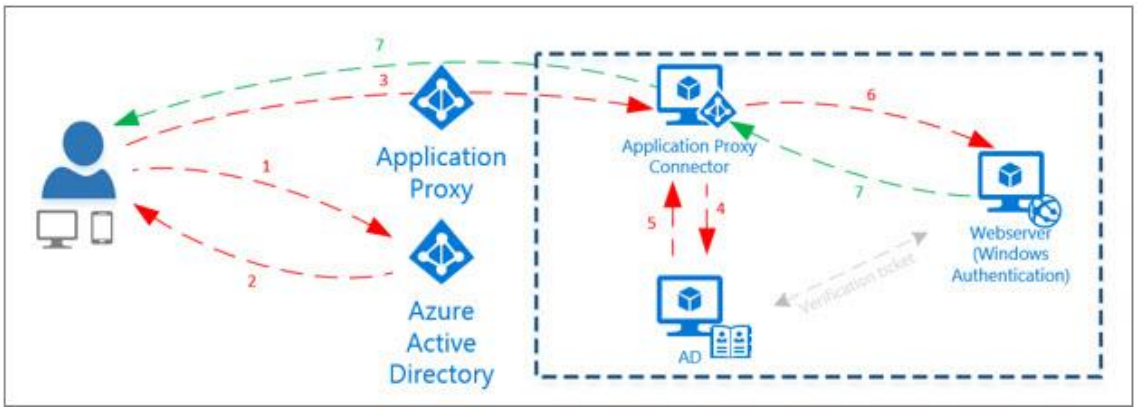
Azure AD:sta on neljä eri versiota free, basic, premium P1 ja premium P2, jotka tarjoavat erilaisia ominaisuuksia (taulukko 1). Nimensä mukaisesti free on ilmainen 500 000 käyttäjään asti, ja muissa versioissa maksetaan jokaisesta käyttäjästä version mukainen kuukausihinta. (15.)

Taulukko 1. Azuren eri versioiden erot (15).

	FREE	**BASIC**	**PREMIUM P1**	**PREMIUM P2**
Price user / month		**0.844€**	**5.06€**	**7.59€**
Common Features				
Directory Objects 1	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit
User/Group Management (add/update/delete)/ User-based provisioning, Device registration	✓	✓	✓	✓
Single Sign-On (SSO)	10 apps per user (pre-integrated SaaS and developer-integrated apps)	10 apps per user (free tier + Application proxy apps)	No Limit (free, Basic tiers + Self-Service App Integration templates)	No Limit (free, Basic tiers + Self-Service App Integration templates)
B2B Collaboration 7	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓
Connect (Sync engine that extends on-premises directories to Azure Active Directory)	✓	✓	✓	✓
Security/Usage Reports	3 Basic Reports	3 Basic Reports	Advanced Reports	Advanced Reports
Premium + Basic Features				

Group-based access management/provisioning		✓	✓	✓
Self-Service Password Reset for cloud users		✓	✓	✓
Company Branding (Logon Pages/Access Panel customization)		✓	✓	✓
Application Proxy		✓	✓	✓
SLA		✓	✓	✓
Premium Features				
Self-Service Group and app Management/Self-Service application additions/Dynamic Groups			✓	✓
Self-Service Password Reset/Change/Unlock with on-premises writeback			✓	✓
Device objects two-way synchronization between on-premises directories and Azure AD (Device write-back)			✓	✓
Multi-Factor Authentication (Cloud and On-premises (MFA Server))	Available on extra payment	Available on extra payment	✓	✓
Microsoft Identity Manager user CAL4			✓	✓
Cloud App Discovery			✓	✓
Connect Health6			✓	✓
Automatic password rollover for group accounts			✓	✓
Conditional Access based on group and location			✓	✓
Conditional Access based on device state (Allow access from managed devices)			✓	✓
Identity Protection				✓
Privileged Identity Management				✓
Azure Active Directory Join – Windows 10 only features				
Join a device to Azure AD, Desktop SSO, Windows Hello for Azure AD, Administrator Bitlocker recovery	✓	✓	✓	✓
MDM auto-enrollment, Self-Service Bitlocker recovery, Additional local administrators to Windows 10 devices via Azure AD Join, Enterprise State Roaming			✓	✓

Azure AD tarjoaa myös valmiiksi julkiseen internetiin rakennetun identiteettipalvelun, kun organisaation omaan Active Directoryyn ei haluta pääsyä internetistä. Omaan Active Directoryyn voidaan muodostaa suojattu yhteys Azure Active Directorystä ja näin julkaista omia sovelluksia käytettäväksi julkisen internetin kautta autentikoimalla ensin Azure AD:ssa, jolloin pääsy sallitaan suojatulla yhteydellä organisaation sisäverkkoon, kuten kuvassa 4. (16.)



Kuva 4. Kirjautuminen On-Premises-sovellukseen Azure AD:n todennuksen kautta (16).

Azure AD:n autentikointi tapahtuu julkisen internetin välityksellä HTTPS-yhteydellä. Azure AD käyttää autentikointiprotokollinaan SAML-, OAuth 2.0- ja WS-federaatiota. (7.)

3 Pilvipalvelut

Esittelen pilvipalvelut Azuren ominaisuuksien näkökulmasta. Suurilla pilvipalveluluiden tarjoajilla on jokaisella oma selaimen kautta käytettävä portaali, jossa hallitaan valtavaa määrää erilaisia palveluita. Neljä suurinta toimijaa ovat Amazon, Microsoft, Google ja IBM. Amazonin markkinaosuus on IaaS- (Infrastructure as a service) ja PaaS-palveluissa (Platform as a service) suurempi kuin kolmen seuraavaksi suurimman toimijan markkinaosuus yhteensä. (17.)

Pilvipalvelut ovat joukko palveluita, joiden fyysistä sijaintia ei välttämättä tiedetä ja joita käytetään internetin kautta erilaisilla päätelaitteilla. Jokainen selaimella käytettävä websovellus ei ole pilvipalvelu, vaan NIST (Nation Institute of Technology) on määritellyt pilvipalveluille viisi ominaispiirrettä (Essential Characterics). (17; 18.) Ominaispiirteet esiteet luvussa 3.1.

Pilvipalveluiden kulmakivinä ovat datakeskukset, joista resursseja jaetaan, ja virtualisointi, jolla resursseja jaetaan. Kuten jokainen web-sovellus ei ole pilvipalvelu, eivät myöskään kaikki datakeskukset, joissa virtualisoidaan asiakkaiden käyttöjärjestelmiä, ole pilvipalveluita. Pilvipalveluiden erottavin tekijä verrattuna perinteisiin datakeskuspalveluihin ja samalla merkittävin ominaispiirre on itsepalvelu tarpeen vaatiessa (on-demand self-service). Se mahdollistaa käyttäjän ottaa milloin vain ja minkä verran vain resursseja käyttöönsä. (18.)

Virtuaalikoneiden suorituskykyä ei valita syöttämällä haluttua määrä suoritintehoa, keskusmuistia tai mahdollisesti tehokkaampaa grafiikkakorttia, vaan ne valitaan valmiista malleista. Mallisarjojen sisällä mallien ominaisuudet eroavat esimerkiksi keskusmuistin ja suorittimien määrässä ja eri mallisarjat painottavat eri ominaisuuksia, esimerkiksi suorittimien tai kiintolevyjen suorituskykyä.

Joissakin palveluissa resurssin määrä saattaa näyttää asiakkaalle rajattomalta, mutta Azuressa on melkeinpä kaikissa resursseista enimmäismäärät, joita voi sitten nostaa tiettyyn pisteeseen asti asiakaspalvelun kautta. Erilaiset rajoitukset, joita voi nostaa asiakaspalvelun kautta, ovat esimerkiksi virtuaalikoneissa käytettävien virtuaalisten suorittimien (vCPU) määrä 20:sta 10 000:een, verkkokortit (Network interface card, NIC) 300:sta 10 000:een, virtuaaliverkot 50:stä 500:aan ja staattiset julkiset IP-osoitteet 20:stä johonkin rajaan asti, joka ei ole saatavilla julkisesti. (19.)

3.1 Pilvipalveluiden ominaispiirteet

NIST:n pilvipalveluiden määritelmässä oli ennen mukana vielä kahdeksan yleistä piirrettä, mutta ne jätettiin pois viimeisestä virallisesta versiosta. Vaikka ne eivät virallisessa määrityksessä olekaan, ne on hyvä mainita, koska nämä ominaisuudet kuvaavat hyvin ainakin johtavia pilvipalveluiden tarjoajia:

- massiivinen skaalautuvuus (massive scaling)
- yhtenäisyys (homogenity)
- virtualisointi (virtualization)
- halvat ohjelmistot (low cost software)
- joustava tietojenkäsittely (resilient comouting)

- maantieteellisesti hajautettu (geographic distribution)
- palvelusuutautuneisuus (service orientation)
- kehittynyt tietoturva (advanced security). (20.)

Usein myös pilvipalvelun tarjoajat antavat palveluille palvelutasosopimuksen (Service Level Agreement, SLA). Palvelutasosopimuksessa luvataan prosentuaalisena lukuarvona palvelun olevan käytettävissä kuukauden tarkastelujaksolla. Azuren tapauksessa eri palveluille on eritasoisia saatavuuslupauksia 99 %:in ja 99,99 %:n välillä kuukausittaisella tasolla. Jos palvelu epäonnistuu täyttää SLA, Microsoft tarjoaa hyvityksiä kuukausimaksuun kyseiselle palvelukategorialle. Yleensä ilmaiset palvelut eivät ole SLA:n piirissä ja esimerkiksi virtuaalikoneita pitää luoda vähintään kaksi toteutettavan sovelluksen toiminnan turvaamiseksi, jolloin vähintään yhdelle virtuaalikoneelle luvataan 99,95 %:n SLA. Yhdelle virtuaalikoneelle luvataan 99,9 %:n SLA, jos se käyttää SSD-levyjä. (21.)

Itsepalvelu (On-demand self-service)

Pilvipalveluiden käyttäjä voi ottaa käyttöön erilaisia tietoteknisiä resursseja itsepalveluna, ilman palveluntarjoajan fyysisiä toimenpiteitä, kuten laitteiston asennusta tai kaapelointia (18). Palveluntarjoajasta riippuen on mahdollista eri tekniikoilla ottaa käyttöön esimerkiksi useita virtuaalikoneita, moniin virtuaaliverkkoihin, joissa on erilaisia palomuureja. Tämä voi tapahtua yksinkertaisimmillaan Azuren tapauksessa valmiista template-galleriasta, josta valitaan template ja täytetään vaadittavat parametrit. Templaten voi myös muokata mieleiseksi ja sen jälkeen käynnistää templaten rakennus. Pilvipalveluiden ominaispiirteisiin kuuluu, että kaikki tämä tapahtuu hyvin nopeasti, koska datakeskuksen toiminnot ovat automatisoituja eivätkä ne tarvitse fyysisiä toimenpiteitä. Virtuaalikoneen voi saada luotua muutamassa minuutista ja VPN-yhdyskäytävän käyttöönotossa voi mennä puolikin tuntia tai enemmän.

Laaja käytettävyys (Broad network access)

Pilvipalvelut ovat käytettävissä internet-yhteyden kautta useilla päätelaitteilla, kuten puhelimilla, tableteilla ja tietokoneilla (18). Idea pilvipalvelun käytettävyydessä on juuri siinä, että poistuttaessa työpaikalta samat palvelut ovat käytettävissä kotikoneella, työkoneella ilman vpn-yhteyttä tai vaikka julkisessa kulkuvälineessä mobiilisti. Pilvipalvelui-

den hienous on myös alustariippumattomuus: koska useimmat SaaS-sovellukset (Software as a Service) ja myös portaalit toimivat selaimella, ne ovat näin ollen alustariippumattomia.

Resurssien yhdistäminen (Resource pooling)

Resurssien, kuten tietokoneitten, verkkojen ja tallennusjärjestelmien toiminta, on virtualisoitu, jolloin useista fyysisistä isoista rinnakkaisista järjestelmistä luovutetaan käyttäjälle hänen valitsemansa määrä virtuaalista resurssia. Eri resurssityypit muodostavat valtavan isoja yhdistettyjä resursseja (Resource pools), jolloin yhdessä fyysisessä laitteistossa on useiden käyttäjien, tietoturvallisesti toisistaan eristettyjä virtuaalisia osuuksia resursseista.

Fyysisen resurssin jakaminen virtuaalisiksi, tarpeen mukaan käyttöönotettaviksi resursseiksi mahdollistaa resurssin korkeamman käyttöasteen, mikä tuo palveluntarjoajille kustannussäästöjä. Asiakkaan vapauttama resurssi voidaan ottaa seuraavalle asiakkaalle käyttöön automaattisesti. Kun poolissa on tarvetta lisäkapasiteetille, voidaan fyysisen laitteiston kapasiteetti lisätä pooliin käytettäväksi resurssiksi ja jakaa siitä eteenpäin asiakkaille tarpeen mukaan. (18.)

Nopea joustavuus (Rapid elasticity)

Toinen pilvipalveluiden erottavin tekijä itsepalvelun lisäksi verrattuna perinteiseen datakeskukseen, on nopea joustavuus ja skaalautuvuus (rapid elasticity and scalability). NIST kuvailee nopean joustavuuden yksinkertaisesti resurssien skaalautumiseksi kysynnän mukaan, joissakin tapauksissa automaattisesti. Resurssien määrän saattaa näyttää käyttäjälle rajoittamattomalta ja se mahdollistaa käyttäjälle resurssien käyttöönoton, milloin vain ja minkä verran vain. (22.)

Nykyisin ainakin isoimpien pilvipalvelutoimijoiden ratkaisut ovat erittäin joustavia ja skaalautuvia, mikä on varmasti yksi syy pilvipalveluiden suureen suosioon. Joustavuus on automatisoitu ja orkestroitu (orchestrated) älykkyys, jolla skaalautuvuus mahdollistetaan. Palveluissa voi määrittää vaikkapa web-palvelimille ala- ja yläarvot prosessorin käyttöasteelle, jolloin palvelu luo lisää virtuaalikoneita jakamaan kysynnän nostamaa kuormaa. Kuormantasaaja (load balancer) jakaa uusia käyttäjiä määriteltyjen sääntöjen mukaisesti virtuaalikoneiden kesken. Kysynnän laskiessa virtuaalikoneita sammutetaan pois käytöstä, jolloin ne eivät enää aiheuta kustannuksia. Palveluissa voi vapaasti määritellä raja-

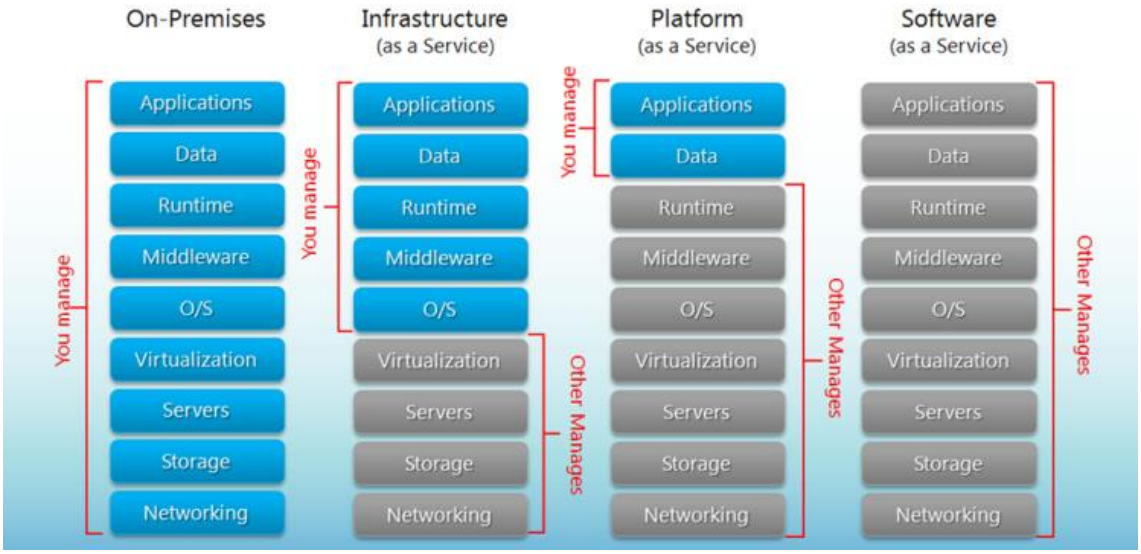
arvoja ja kohdistaa ne erilaisiin mittareihin, vaikkapa keskusmuistin määrään tai levyn lukunopeuksiin. Skaalausta voi myös tehdä manuaalisesti, esimerkiksi ennen sesonkia tai tiettyä tapahtumaa, jolloin tiedetään käyttöasteen nousevan. (18.)

Mitattava palvelu (Measured service)

Palveluiden laskutus tehdään yleensä minuutti-, tai tuntikohtaisesti, ja palvelut ovat useimmiten irtisanottavissa saman tien, jolloin ei jää maksettavaksi pitkää sopimuskautta. Pilvipalveluissa käyttöä voidaan mitata esimerkiksi aikamääreellä, käyttäjien määrällä, siirtonopeudella ja tallennuskapasiteetilla. Resurssien käytöstä on mahdollista saada yksityiskohtaista tietoa ja luoda raportteja. Näin myös pilvipalveluiden ylläpitäjille on helppo hoitaa laskutus hallittaessa useita asiakkuuksia tai kohdistaa laskuja osastokohtaisesti. Azuressa on eri palveluiden monitorointi hyvin vahvassa roolissa, mutta usein syvällisemmästä monitoroinnista ja edistyksellisistä raporteista joutuu maksamaan lisähintaa. Monitoroinnin runsaus ja älykkyys mahdollistavat myös erilaisten älykkäiden tietoturvaratkaisujen toteutuksen, kuten käyttäjän epätavallisen toiminnan tai epätavallisesta paikasta tai epätavalliseen aikaan kirjautumisen tunnistaminen.

3.2 Palvelumallit

Pilvipalveluissa on yleistynyt, että kaikkea tarjotaan palveluna, on erilaisia as a service -yhdistelmiä, joista yleisimmät ovat SaaS (Software as a Service), PaaS (Platform as a Service) ja IaaS (Infrastructure as a Service). Näitä kolmea palvelumallia erottaa palveluntarjoajan ja käyttäjän hallitsema osuus palvelusta. (23; 24.) Hyvä tapa erottaa nämä palvelut toisistaan, on vertailla niiden hallintamallia, joka on kuvattu englanniksi kuvassa 5 ja suomeksi kuvassa 6.



Kuva 5. Pilvipalvelumallit englanniksi (23).

Infrastructure as a Service (IaaS)

IaaS-palvelussa käyttäjällä on virtuaalikone, johon hän itse asentaa tarvitsemansa ohjelmistot ja käyttää konetta tarvitsemallaan tavallaan. Palveluntarjoaja vastaa virtuaalikoneen infrastruktuurista: sähköstä, jäähdytyksestä, verkosta, tallennusjärjestelmistä ja virtuaalipalvelimen isäntäkoneesta (host), ja kaikki tämä yleensä vikasietoisena. Käyttäjällä voi olla mahdollisuus valita palveluntarjoajalta haluamansa käyttöjärjestelmä, jonka lisenssin hinta on sisällytetty virtuaalikoneen hinnoitteluun. Käyttöjärjestelmään voi valita myös valmiiksi asennettuja ja lisensoituja ohjelmistoja, jolloin hinta nousee, mutta käyttäjä ei joudu huolehtimaan ohjelmistojen lisensseistä.

Palveluntarjoaja vastaa isäntäkoneesta, joka tarjoaa virtuaalikoneelle resursseja, ja sitä tukevasta infrastruktuurista. Käyttöjärjestelmän ja siihen asennettujen ohjelmien toiminta jää käyttäjän vastuulla. (23.)

Platform as a Service (PaaS)

PaaS-palvelut tarjoavat kehittäjille kehitysympäristön valmiina. Se mahdollistaa kehittäjille nopean pääsyn itse tekemiseen, eli ohjelmoimiseen, ilman tarvetta konfiguroida käyttöjärjestelmää, apukirjastoja tai järjestemäriippuvuksia. PaaS-palveluina voidaan tarjota esimerkiksi myös ylläpidetty tietokanta tai web-julkaisujärjestelmä. Alustaa pystyy muokkaamaan rajoitetusti vastaamaan omia tarpeita, esimerkiksi alustan tietyn ohjelmointikielen version voi vaihtaa asetuksista. Alustapalvelujen hienouksiin kuuluu muun muassa

tuki jatkuvalle integraatiolle (Continuous Integration, CI), jatkuvalle toimittamiselle (Continuous Delivery, CD) ja käyttöönotto paikoille (Deployment slots), jossa testauksessa olevan verkkosivu voidaan vaihtaa tuotantokäyttöön nopeasti. (23; 24.)

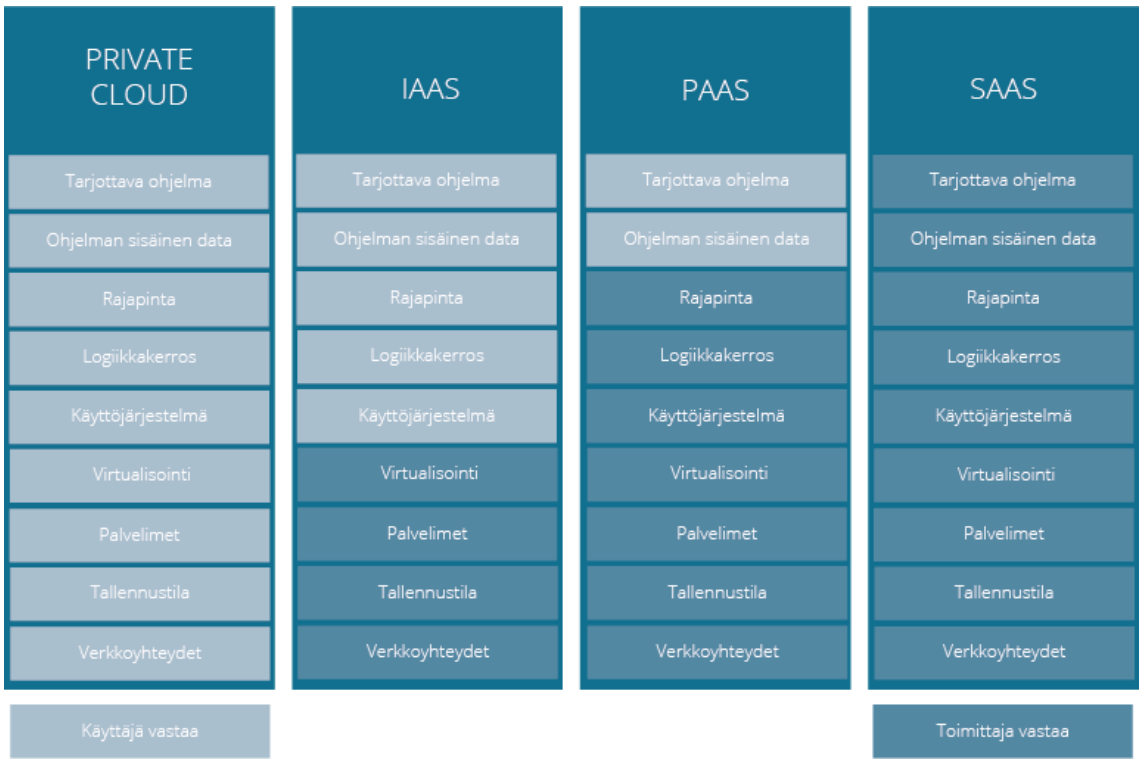
PaaS-palvelut siis säästävät kehittäjien aikaa ja tuovat samalla lisäkerroksen tietoturvallisuutta, koska käyttöjärjestelmään ei ole pääsyä. Samalla ne tarjoavat myös valmiin ympäristön asiasta tietämättömille päästä kirjoittamaan koodinsa ja julkaista oman sovelluksensa internetiin.

Software as a Service (SaaS)

SaaS-sovellukset toimivat internetyhteydellä selaimen kautta. Huonona puolena voi pitää vaatimusta internetyhteydelle, mutta hyvinä puolina ohjelmia ei tarvitse asentaa käyttäjien työasemille ja ne ovat käytössä myös missä vain eri päätelaitteilla. Ohjelmistopäivityksiä ei tarvitse tehdä, vaan kun ohjelmistotoimittaja päivittää ohjelman, päivittyy se kaikille asiakkaille automaattisesti. Ohjelmistot tukevat myös korkea käytettävyyttä (high availibility), ja varmuuskopiointi voi myös olla toteutettuna toimittajan puolelta. (23; 24.)

SaaS-sovellukset mahdollistavat yrityksille paremman kustannuksien ennakoimisen kuukausimaksullisuuden takia ja ne vapauttavat henkilökunnan resurssien tarvetta ohjelmistojen päivityksistä. Myös sovelluksen siirto omasta hallinnasta pilvipohjaiseksi poistaa sovelluksen palvelinten ostamiseen, ylläpitämiseen, huoltamiseen ja konfiguroimiseen tarvittavaa työvoimaa ja rahaa. Toisaalta SaaS-sovelluksiin siirtymisestä saattaa aiheutua erilaisia kustannuksia, esimerkiksi identiteettien integroimisesta tai migraatiosta. Myös suurilla käyttäjämäärillä, SaaS:n käyttäjäpohjainen hinnoittelu saattaa kasvattaa kustannukset hyvinkin suuriksi, jolloin voi olla edullisempaa pitää palvelu omassa hallinnassa.

Azuressa SaaS-sovelluksiin voidaan integroida kertakirjautuminen (Single sign-on, SSO) Azure AD:n tunnuksille. Azuressa AD:hen on esi-integroituja sovelluksia, jotka voidaan ottaa käyttöön nopeasti ja toiset sovellukset taas vaativat monimutkaisempaa integrointia. Azure AD tukee erilaisia kirjautumistapoja SaaS-sovelluksiin, muun muassa yrityksen jaettua tunnusta esimerkiksi sosiaalista mediaa varten. Omia sovelluksia voi myös integroida osaksi Azure AD:tä, jolloin niihin voi kirjautua Azure AD:n tunnuksilla. Palvelumallit on esitelty suomeksi kuvassa 6, jossa private cloud edustaa omaa yksityistä pilveä tai datakeskusta.

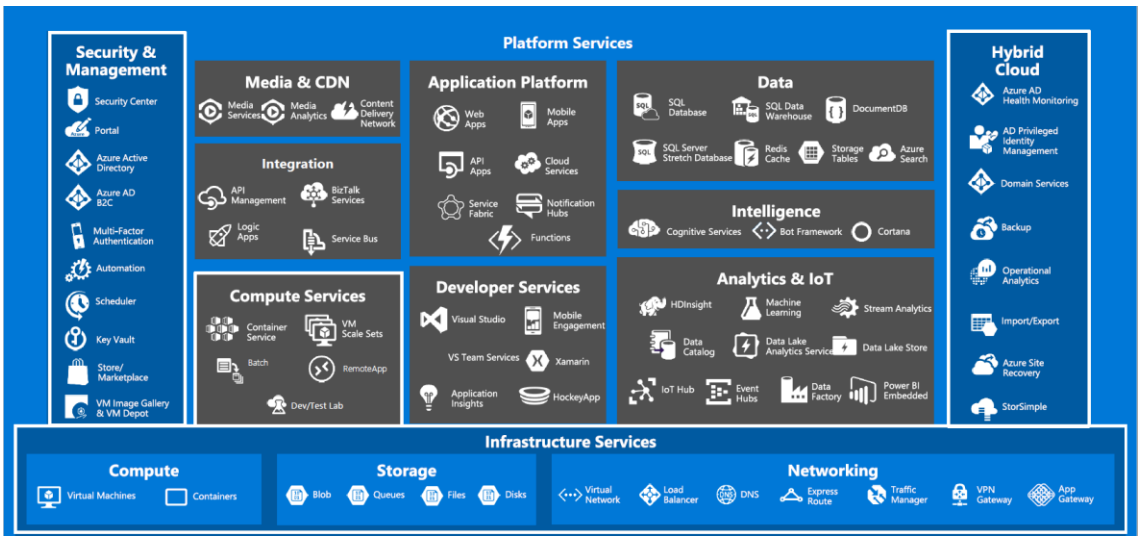


Kuva 6. Pilvipalvelumallit suomeksi (24).

4 Microsoftin pilvipalvelut

4.1 Microsoft Azure -pilvipalvelualusta

Microsoft Azure on Microsoftin julkinen pilvipalvelualusta, alun perin julkaistu vuonna 2010 nimellä Windows Azure ja uudelleen nimetty nykyiseen muotoonsa vuonna 2014 (25). Kuvassa 7 näkyy Microsoftin Azuren palveluiden lajittelu 11 kategoriaan.



Kuva 7. Osa Azuren paleluvalikoimasta (26).

Azuren uudistuttua vuonna 2012, tuli saataville uusi portaali, jossa resurssien hallita keskittyi ryhmiin. Vanhassa portaalissa (Azure Services Manager, ASM), tunnetaan myös nimellä klassinen, kaikki resurssit olivat omissa kategorioissaan, jolloin yhden palvelun tai ratkaisun riippuvuuksien hahmottaminen ja hallinta oli hankalampaa. Uudessa portaalissa (Azure Resource Manager, ARM) Microsoft esitteli resurssiryhmät (Resource Groups), jotka ovat loogisia resurssien ryhmittelijöitä. Resurssiryhmä voi sisältää resursseja useista kategorioista, esimerkiksi virtuaalikoneita, kuormanjakajia, julkisia IP-osoitteita ja virtuaaliverkkoja. Näin ollen käytettäessä yhtä resurssiryhmää jollekin sovellukselle nähdään kaikki sen käyttämät resurssit yhdessä näkymästä. (25; 27.)

Laskutustiedot saa Azuresta myös resurssiryhmäkohtaisesti. Vaihtoehtoisesti resurssien laskutustietoja voi kerätä eri resurssiryhmistä antamalla resursseille uudessa portaalissa tägejä (tags). Tällä hetkellä pientä osaa palveluista voi hallita vain vanhan portaalin kautta, joitakin molempien kautta, ja useimmat palvelut ovat siirtyneet hallittaviksi ainoastaan uuden portaalin kautta. (27.)

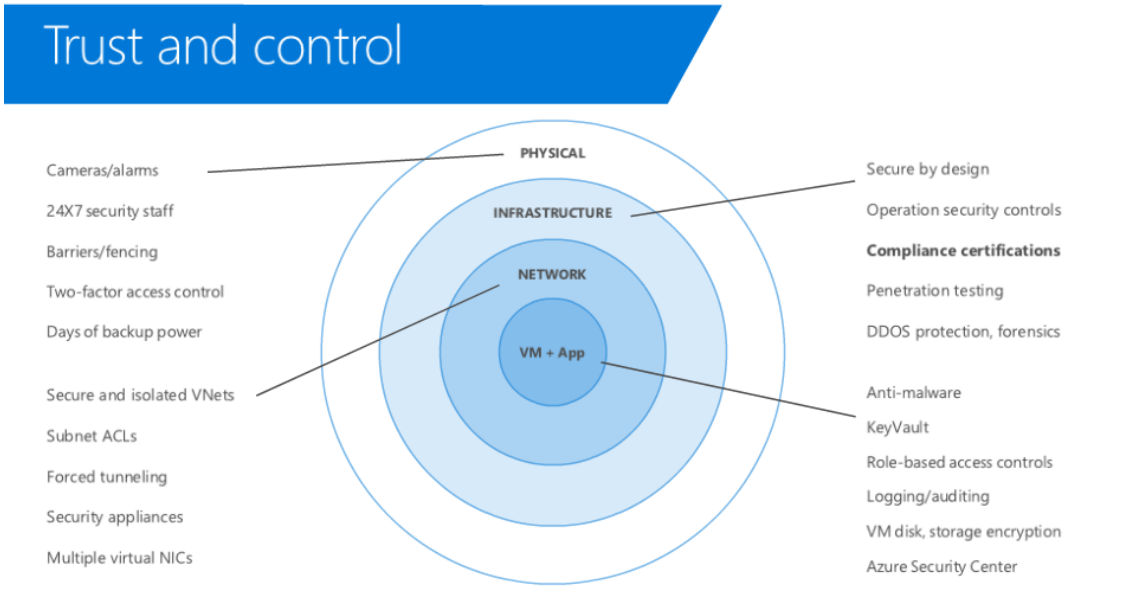
Azuren datakeskukset

Azuren datakeskuksien määrä on runsaslukuisin muihin pilvipalveluiden tarjoajiin verrattuna. Azure toimii tällä hetkellä 34 alueella. Suomea lähimmät ovat Pohjois-Euroopassa Irlannissa ja Länsi-Euroopassa Alankomaissa. Valittaessa Azuren storage accountin replikoinniksi Geo reduntant storage, data replikoituu ensisijaisen datakeskuksen ja sen

vastaparin välillä, joka sijaitsee samassa maassa tai maanosassa, mutta kuitenkin yleensä vähintään 400 kilometrin päässä. (28; 29.)

Jos esimerkiksi katastrofi tuhoaa toisen datakeskuksen, datakeskuksien välisellä replikoinnilla asiakkaiden data on suojassa toisessa datakeskuksessa. Datakeskukset toimivat kahdensuuntaisina pareina samalla alueella, jolloin Euroopasta ei tehdä kopioita Amerikkaan ja niin edespäin, poikkeuksena Brasilia, jonka data replikoituu yksisuuntaisesti Amerikkaan. (28.)

Yksittäisten virtuaalikoneiden turvallisuus koostuu Azuressa monesta kerroksesta. Fyysinen turvallisuus alkaa datakeskuksen monivaiheisesta fyysisestä turvallisuudesta ja päättyy kiintolevyille, jossa asiakkaan data on mahdollista säilyttää salattuna. Asiakkaan käyttöjärjestelmään ja sovelluksiin on mahdollista suojata pääsyä internetistä useilla suojaus- ja valvontamekanismeilla. Koko turvallisuuden kerroksia on kuvattu kuvassa 8.



Kuva 8. Azuren turvallisuuden eri kerrokset virtuaalikoneelle (26).

Kaikki palvelut tai kaikki virtuaalikonemallit eivät ole käytettävissä kaikissa datakeskuksissa. Microsoftin sivuilla on erittely jokaisen datakeskuksen käytettävissä olevista palveluista. Kaikki Azuren datakeskukset eivät myöskään ole julkisesti kaikkien käytettävissä, vaan jotkut datakeskukset ovat pelkästään hallituksille tai ne ovat kolmansien osapuolien hallinnassa. (29.)

Hallinta

Azuren hallitsemiseen tarvitaan tilaus (subscription). Yhdellä tunnuksella voi olla käytettävissä useita tilauksia. Tunnuksella näkyvät kaikki resurssit, joiden tilauksiin tunnuksella on käyttöoikeus ja uusia resursseja luotaessa valitaan, mille tilaukselle se luodaan. Tilauksissa on määritelty enimmäismäärät resursseille, joista on mainittu luvussa 3 ja tilaukset muodostavat erilliset laskutukset.

Azuren tilausta voi hallita Microsoft-käyttäjätunnuksella tai työpaikan tai oppilaitoksen käyttäjätunnuksella. Uutta tilausta luotaessa Azure luo automaattisesti Azure AD:n, jonka verkkotunnuksen alku muodostuu käyttäjän nimestä ja päättyy .onmicrosoft.com-verkkotunnukseen. Yrityksille on EA-portaali (Enteprise Agreement), jossa voidaan hallita eri tilauksia, laskutuksia ja lisenssien alennuksia. (31; 32.)

Azuren resursseihin pääsyä voidaan rajoittaa rooleihin perustuvilla käyttöoikeuksilla. Roolille voi antaa pääsyn tilaus-, resurssiryhmä- tai resurssikohtaisesti. Azuressa on paljon valmiita rooleja, ja niitä voi luoda myös itse ja antaa roolille tarvittavat käyttöoikeudet. Rooli täytyy antaa käyttäjälle tai ryhmälle Azure Active Directorystä tai joissakin tapauksissa sovellukselle. Azuressa voi käyttää myös toimintansa mukaan kuvailevasti nimettyjä CanNotDelete- tai ReadOnly-lukkoja samoin laajuuksin kuin rooleja.

Näiden lisäksi voidaan tilaus- tai resurssiryhmäkohtaisesti käyttää joko valmiita tai itse määriteltyjä resurssikäytäntöjä (Resource Policy). Niillä voidaan esimerkiksi sallia resurssien luominen vain tietylle alueelle, käyttää vain tietynlaisia virtuaalikonemalleja tai vaatia SQL-version olevan tietty versio. (33; 34; 35.)

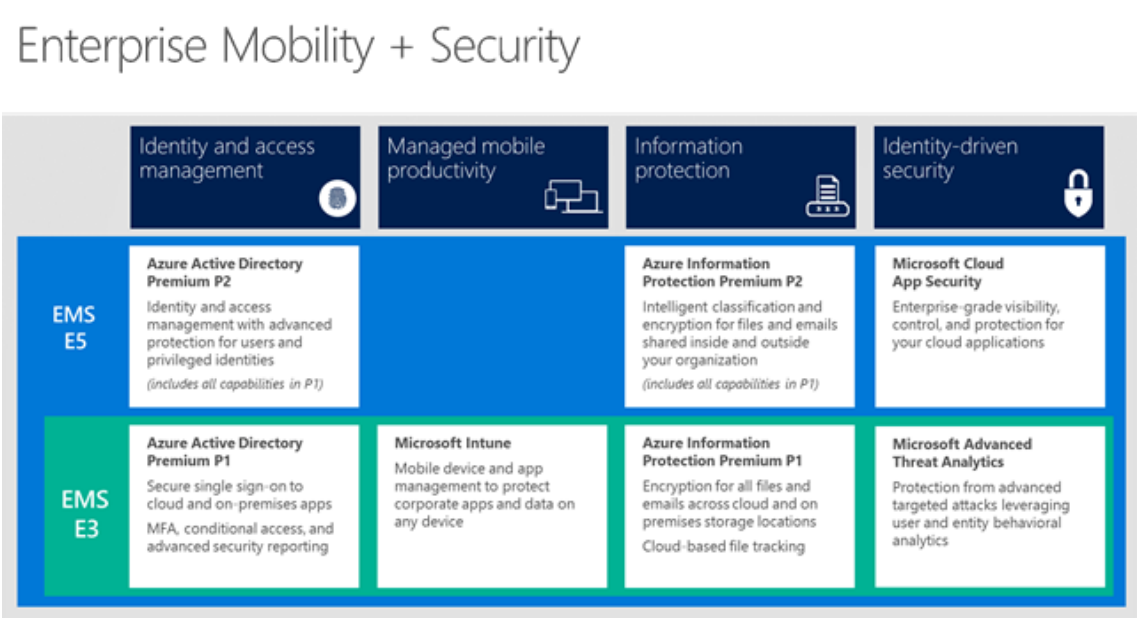
Käyttäjällä on yksi Azure AD, joka autentikoi käyttäjän, mutta käyttäjä voidaan lisätä myös muihin hakemistoihin vieraaksi. Azure AD:n järjestelmänvalvojat roolin käyttäjät eivät ole Azuren tilauksen järjestelmänvalvojia, vaan ne ovat kaksi erillistä roolia. (36.)

Azurea voi hallita portaalista, PowerShellilla, API:en kautta ja muita käyttöjärjestelmiä tukevalla Azure CLI:llä (Command Line Interface). Tässä insinöörityössä käytetään pääosin portaalia, hieman PowerShellia ja Azuren palveluista pääosin infrastruktuuripalveluita ja Azure Active Directoryä. Azuren hinnoittelua käsitellään loppuyhteenvedossa käytettyjen palvelujen mukaan.

Enteprise Mobility + Security (EMS) -palvelupaketti

Enteprise Mobility + Security (EMS) on palvelupaketti, joka sisältää Azure Active Directory Premiumin ja Intunen. EMS-pakettia käytetään tässä insinöörityössä, koska sen kuukausihinta on edullisempi kuin palvelut erikseen ostettuna. EMS sisältää myös muita, yhdessä toimimaan tarkoitettuja tietoturvaohjelmistoja. MDM (Mobile Device Management) -ratkaisu Intune on tässä insinöörityössä paketin pääasiallinen tuote, jolla toteutetaan laitehallinta kahdessa ensimmäisessä ratkaisussa. Azure Active Directory Premiumia tarvitaan sen laitteen automaattisen rekisteröinnin MDM-ratkaisuun ominaisuuden takia.

EMS-akronyymi tarkoitti ennen Enteprise Mobility Suitea, kunnes vuonna 2016 Microsoft vaihtoi akronyymin tarkoitusta kuvaamaan lisääntyneitä tietoturvaominaisuuksia. EMS-pakettia myydään E3- ja E5-versiona. Jälkimmäinen sisältää joukon edistyksellisimpiä ominaisuuksia, joita ei käytetä tässä insinöörityössä. Azure Active Directory P2 kuuluu myös E5-pakettiin, joka sisältää identiteettien ja tiedostojen suojaamista ja valvomista ja järjestelmänvalvojien oikeuksien valvontaa ja rajaamista lisääviä ominaisuuksia. E5-paketti sisältää kaikki E3-paketin ominaisuudet. Eri versioiden eroavaisuuksia voi tarkastella kuvasta 9. Tässä insinöörityössä E3-paketti on riittävä ja edullisempi ratkaisu 7,40 euron käyttäjäkohtaisella kuukausihinnallaan verrattuna E5:n 12,65 euron hintaan. Vertailun vuoksi, erikseen ostettuna Azure AD P1 maksaa 5,06 euroa, P2 7,59 euroa ja Intune 5,10 euroa jokaiselta käyttäjältä kuukaudessa. (37; 38; 39.)



Kuva 9. EMS-versioiden eroavaisuudet (37).

Yrityksen työntekijöiden mobiililaitteiden, omien laitteiden ja etänä tapahtuvan työn lisääntyminen on kasvattanut työntekijöiden päätelaitevalikoimaa ja vienyt laitteet ja tiedostot pois yrityksen lähiverkosta, mikä vaikeuttaa tiedostojen ja laitteiden hallintaa. EMS-paketti on Microsoftin identiteettipohjainen, digitaalisen transformaation tietoturvaratkaisu, joka on luotu hallitsemaan juuri näiden muutoksien tuomia tietoturvahaasteita.

MDM-ratkaisulla voidaan hallita laitteiden sovelluksia, tietoturvaa, asetuksia ja pääsyä internetin kautta yrityksen tiedostoihin tietoturvallisella laitteella, ilman lähiverkko tai VPN-yhteyttä. MDM-ratkaisulla voidaan tietoturvallisesti tukea myös BYOL (Bring Your On Device) -tilanteita, jossa työntekijät käsittelevät työtiedostoja omilla laitteilla.

Pilvipohjaisessa Intunessa voi hallita Android-, Apple- ja Windows-laitteita. Intunella voidaan toimittaa laitteisiin sertifikaatteja, Wifi- ja VPN-profiileja, konfiguroida Bitlocker-salaus tehdä omia konfigurointeja käyttäen OMA-URI-arvoja. Yrityksen tiedostojen avaus voidaan rajoittaa vain sallittuihin sovelluksiin, ettei esimerkiksi tiedostoja voi synkronoida muihin pilvitallennuspaikkoihin, ja suojata yrityksen tiedostot käyttäjän omista tiedostoista Intunella konfiguroitavalla WIP:llä (Windows Information Protection). Intunella on mahdollista toteuttaa myös MAM (Mobile Application Management) -ratkaisu, jossa asennetaan yrityksen hallinnoimia sovelluksia mobiililaitteille ja mahdollisesti rajoitetaan niiden toimintaa yrityksen tiedostojen suojaamiseksi. (40; 41; 42; 43.)

4.2 Office 365 -tuotteet

Office 365 on kuukausimaksullinen, Microsoftin pilvestä hallittava ohjelmistokokonaisuus, joka sisältää perinteiset Office-sovellukset tai versiosta riippuen ainoastaan selaimen kautta käytettävät SaaS Office Online -sovellukset. Nämä ohjelmat on toteutettu rajatuilla toiminnallisuuksilla ja ne ovat ilmaisia käyttää ilman Office-tilausta.

Office 365 käyttää Intunen lailla käyttäjähakemistonaan Azure Active Directoryä. Luotaessa Office 365 -tilausta tunnuksella, jolla ei ole Azure AD:ta, Office luo ilmaisen Azure AD:n. Officen portaalista onnistuu tunnuksien hallitseminen, mutta todellisuudessa muutokset tapahtuvat Azuren puolella. (36; 44; 45; 46; 47; 48; 48.)

Versiosta riippuen Office 365 sisältää perinteiseen kerralla maksettavaan Officeen verrattuna ilmaisia Skype-minuutteja, OneDrive-tallennustilaa, monipuolisemmat mobiiliso-

vellukset, lisenssin useaan laitteeseen ja jatkuvasti päivittyvät uusimmat Office-sovellukset. Halvimmissa Office 2016 -paketeissa ei ole Outlook-, Publisher- ja Access-sovelluksia, jotka on sisällytetty kaikkiin Office 365 -paketteihin. (47; 48; 49.)

Office 365:ssä on SaaS-sovellusten kustannushyödyt, joista on kerrottu luvussa 3.2 Palvelumallit. Näiden lisäksi Microsoft jatkuvasti kehittää ja päivittää Office-ohjelmia ja tuo käyttäjille uudet versiot käytettäväksi nopealla aikataululla, ilman lisäkustannuksia. Periteisiin ohjelmistopäivityksiin tarvitaan yrityksen IT-osaston työtunteja, ja kustannuksia saattaa tulla vielä käyttäjien ongelmatilanteista. Office 365:ssä panostetaan myös tuottavuuden lisäämiseen, joten tätä kautta nopeasti käytettävissä olevat uudet ominaisuudet voivat tuoda myös välillisiä taloudellisia hyötyjä.

Office 365:stä myydään eri versioita yksityis- ja yrityskäyttöön. Yritysversioissa on lisäksi erilaisia yrityskäyttöön suunnattuja Saas-sovelluksia, kuten Microsoftin ylläpitämä Microsoft Extchange, Yammer ja Sharepoint Online. Ominaisuudet ovat jatkuvan kehityksen alla, ja tilauksiin saattaa tulla lisää ominaisuuksia tai ominaisuudet voivat muuttua. (48; 49.)

Office 365:ssä on useita yritysversioita erilaisilla kuukausihinnoilla. Tilauksia voi myös päivittää tosiin tilauksiin, ja käyttäjillä voi olla erilaisia tilauksia. Joitakin palveluita voi myös ostaa erillisellä kuukausihinnalla heikommin varustellun Office 365 -tilauksen rinnalle. Halvimmat vaihtoehdot eivät sisällä ollenkaan asennettavia Office-sovelluksia, vaan ainoastaan selaimen kautta käytettävät versiot. Officen yritysversiota on business- ja enteprise-kategoriassa, joiden merkittävin eroavaisuus on business-tilauksen 300 käyttäjän enimmäisrajoitus. (50; 51.)

Erilaisia Office 365- ja Office 2016 -versioita on runsaasti, ja versioiden eroa ja sisältöä alkaa olla vaikeata hahmottaa, vaikka tutkisi asiaa Microsoftin omilta sivuilta. Monesti Microsoft esittää Office 365- ja 2016-pakettien eroavaisuuksiksi kuukausimaksullisuuden lisäksi vain 365-tilaukseen sisältyvät Outlook-, Publisher- ja Access-sovellukset, mutta ne sisältyvät kuitenkin kalliimpiin 2016-paketteihin. Microsoft näyttää myös haluavan siirtää käyttäjät kohti Office 365 -tilauksia, koska se on ilmoittanut Office 2016:n tuen loputtua 13.10.2020 eväävänsä Office 2016 -käyttäjiltä pääsyn OneDrive- ja Skype for Busines -sovelluksiin. (52.)

Kun katsotaan halvinta ratkaisua, rajautuvat Office 365 Business 8,80 €/kk ja Office 365 ProPlus 12,90 €/kk pois puuttuvan sähköpostin vuoksi ja Office 365 Business Essentials

4,20 €/kk ja Office 365 Enterprise E1 6,70 €/kk puuttuvien työpöytäsovelluksien takia. Halvimmat vaihtoehdot, jotka sisältävät sähköpostin ja työpöytäversiot Office-sovelluksista, ovat Office 365 Business Premium 10,50 €/kk ja Office 365 Enterprise E3 19,70 €/kk. Sopiva on myös Office 365 Enterprise E5, joka on monipuolisin ja kallein paketti, jossa on enemmän puhe-, tietoturva- ja analytiikkatyökaluja 34,40 €:n kuukausihinnalla. Hinnat ovat yhdelle käyttäjälle kuukaudessa, ilman arvonlisäveroa ja tilattaessa tuote vuodeksi. (46; 47.)

Erot Business Premium- ja Enterprise E3 -versioiden välillä ovat pienet, ja ne ovat enemmän business- ja enterprise-tuotteiden välillä kuin vain näiden kahden tuotteen. Versiot sisältävät erilaiset sähköpostiratkaisut. Business sisältää Exchange online -palvelupaketti 1:n, erikseen ostettuna 3,40 €/kk, ja enterprise sisältää palvelupaketti 2:n, joka maksaa erikseen ostettuna 6,70 €/kk. Enterprise-versioissa postilaatikon enimmäiskoko on 100 gigatavua ja arkistopostilaatikon tallennustila on rajoittamaton. Business-versioissa pääasiallisen ja arkistopostilaatikon enimmäiskoko on kummassakin 50 gigatavua. Lisäksi on joitain pieniä eroja arkistopostilaatikon poistettujen viestien tallennustilassa, poistettujen ja muokattujen viestien säilytyksessä ja muita pieniä ominaisuuseroja. (50; 51.)

Myös OneDriveen tarjotaan tallennustilaa business-versioissa 1 teratavu, ja vähintään viiden käyttäjän enterprise-tilauksissa on oletuksena 5 teratavun tallennustilaraja, jota voi nostaa asiakaspalvelun kautta rajattomasti. Lisäksi business-versioista puuttuu monia pieniä ominaisuuksia, jotka löytyvät enteprise-versioista, kuten Skype online palvelupaketti 2:nen. (45; 52.)

5 Ratkaisu 1: Azure Active Directory + Intune

Verkkotunnus tai toimialue on osa käyttäjänimeä Azure Active Directoryssä ja sähköpostiosoitteessa. Käyttäjänimen ja sähköpostiosoitteen yksinkertaistamisen takia kannattaa yritykselle rekisteröidä verkkotunnus verkkotunnusvälittäjältä. Yritykselle ostetun verkkotunnuksen ja Azuren verkkotunnuksen liittämisprosessin jälkeen on myös yksinkertaista ja edullista toteuttaa yritykselle oma verkkosivu Azurella, käyttäen esimerkiksi Azuren App Servicea.

Tässä insinöörityössä käytettiin info- ja tech-ylätason (Top-Level-Domain, TLD) verkkotunnuksia niiden edullisuuden vuoksi. Ostin tätä ratkaisua varten tpaaddemo.info-verkkotunnuksen. Verkkotunnus liitetään Azure AD:hen, ja tämän jälkeen tehdään yrityksen käyttäjille Azure AD -tunnukset muodossa käyttäjätunnus@tpaaddemo.info, jossa käyttäjätunnuksesta tehdään etunimi.sukunimi-muotoinen.

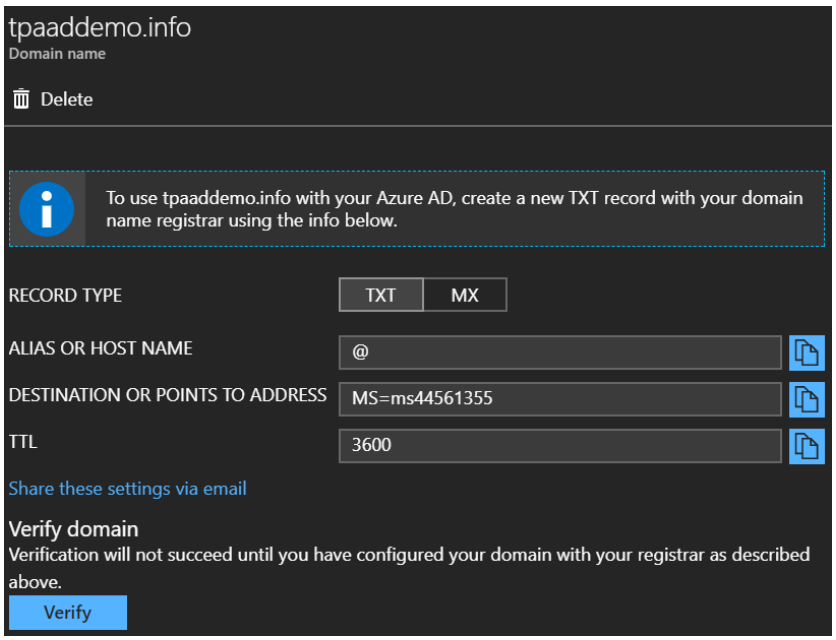
Azure AD ja Intune konfiguroidaan niin, että käyttäjän suorittaessa Azure AD join hän pääsee kirjautumaan laitteelle Azure AD -tunnuksella ja laite rekisteröidään automaattisesti Intunen hallintaan.

Lisäksi otetaan Office 365 -palvelut käyttöön ja toteutetaan pakettiin kuuluvalla Sharepoint Onlinella tiedostonjakoratkaisu. Intunen toiminnallisuuksia demonstroidaan asentamalla 7-Zip-sovellus ja Office 365:n -työpöytäsovellukset Intunen kautta. Intunella ei toteuteta työasemia koskevia määrityksiä.

5.1 Verkkotunnuksen liittäminen Azure Active Directoryyn

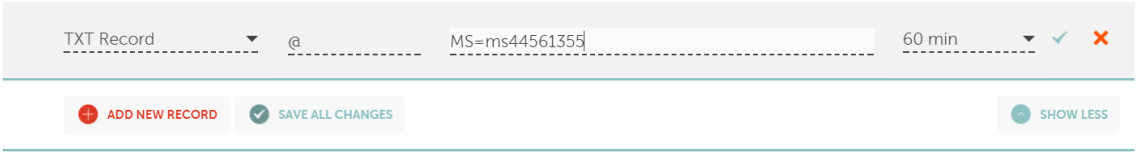
Käytän tässä insinöörityössä termiä verkkotunnus (domain), kun puhun ostetun verkkotunnuksen käsittelemisestä internetin kautta käytettävissä palveluissa, ja termiä toimialue (domain), kun sitä käytetään (Azure) Active Directoryn kanssa, vaikka ne tarkoittavat oikeastaan samaa asiaa.

Verkkotunnus liitetään Azure Active Directoryn Domain names -kohdasta. Halutun verkkotunnuksen syöttämisen jälkeen Azure pyytää lisäämään verkkotunnuksen DNS-tietueisiin sen määrittelemän txt-tietueen varmistaakseen, että käyttäjä omistaa sivun. Kuvassa 10 näkyy, minkälaisen tietueen Azure haluaa tässä tapauksessa sivuilta löytyvän, jotta verkkotunnuksen omistajuus voidaan vahvistaa



Kuva 10. Oman verkkotunnuksen lisääminen Azureen.

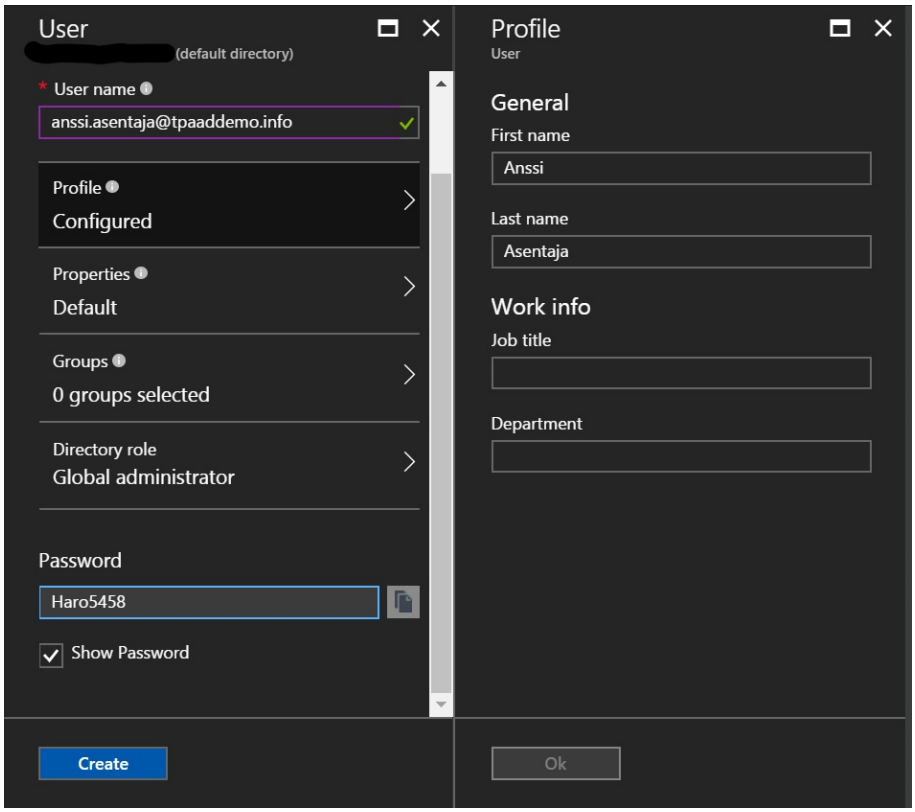
Rekisteröijästä riippuen ovat hallintatyökalut erilaisia. Kuvassa 11 lisätään vaaditun mukainen tietue namecheap.com-rekisteröijälle. Arvot voi kätevästi kopioida Azuresta tekstikentän viereisellä kopiointi-painikkeella. DNS-tietueen lisäämisen jälkeen pitää odottaa muutamista minuuteista tunteihin sen leviämistä internetin DNS-palvelimiin, jotta Azure voi vahvistaa verkkotunnuksen ja sitä voidaan käyttää Azuressa. (54.)



Kuva 11. Namecheapin hallintapaneelin tietueiden lisäys.

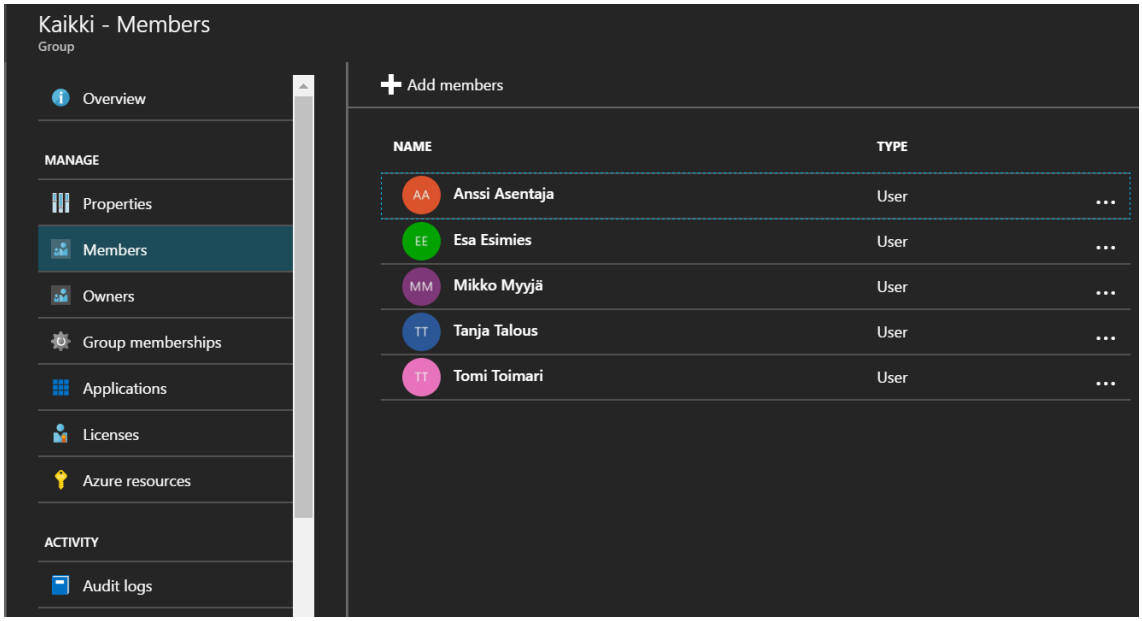
5.2 Käyttäjien ja ryhmien luominen

Käyttäjät luodaan Azure AD:n Users and Groups -kohdasta. Kuvassa 12 näkyy Anssi Asentajan käyttäjätilin luominen. Azure generoi käyttäjälle kertakäyttöisen salasanan, joka täytyy vaihtaa ensimmäisellä kirjautumiskerralla. Anssille on annettu myös Global administrator -rooli, jolla hän saa täydet oikeudet Azure AD:hen ja pystyy hallitsemaan sen käyttäjiä järjestelmänvalvojan roolissa. Global administrator -rooli antaa Azure Active Directoryn lisäksi täydet oikeudet palveluihin, jotka federoivat Azure AD:stä identiteetin, kuten Skype for Business Online, Exchange Online ja Sharepoint Online. (54.)



Kuva 12. Käyttäjän luominen Azure AD:hen.

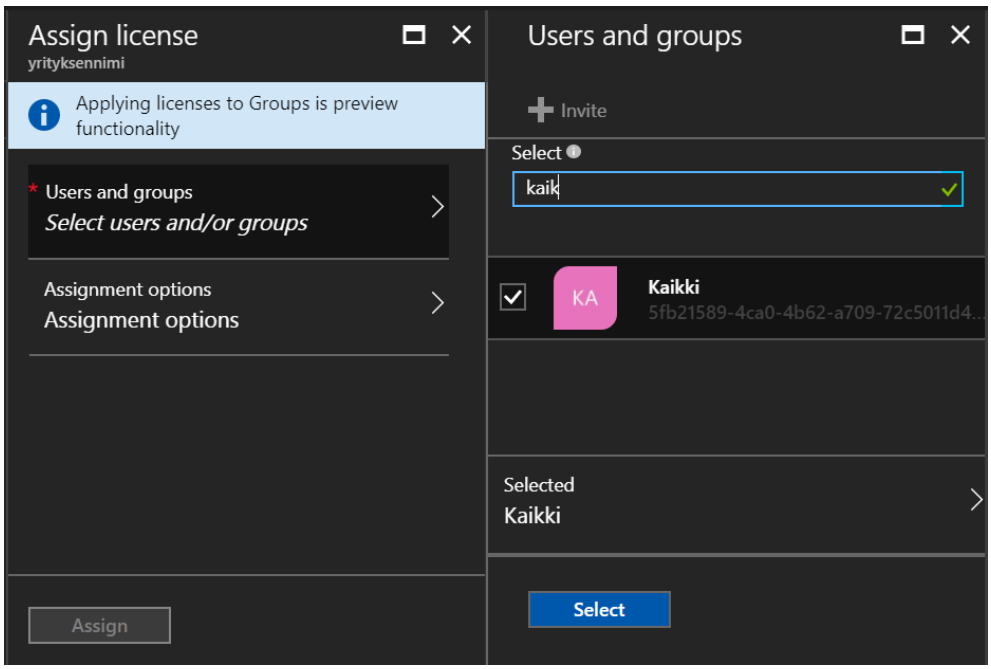
Ryhmät tehdään myös Azure AD:n Users and Groups -kohdasta. Kuvassa 13 olen tehnyt Kaikki-nimisen ryhmän, johon on lisätty jäseniksi kaikki käyttäjät. Ryhmään voi liittää käyttäjän luontivaiheessa tai lisätä käyttäjät ryhmän jäseneksi, kun kaikki käyttäjät on luotu. Tälle ryhmälle jaetaan EMS-lisenssi ja sallitaan rekisteröityminen Intunen laitehallintaan.



Kuva 13. Azure AD:n Kaikki-ryhmä, johon on liitetty kaikki käyttäjät.

5.3 Lisenssien jakaminen ja Azure AD:n nimeäminen

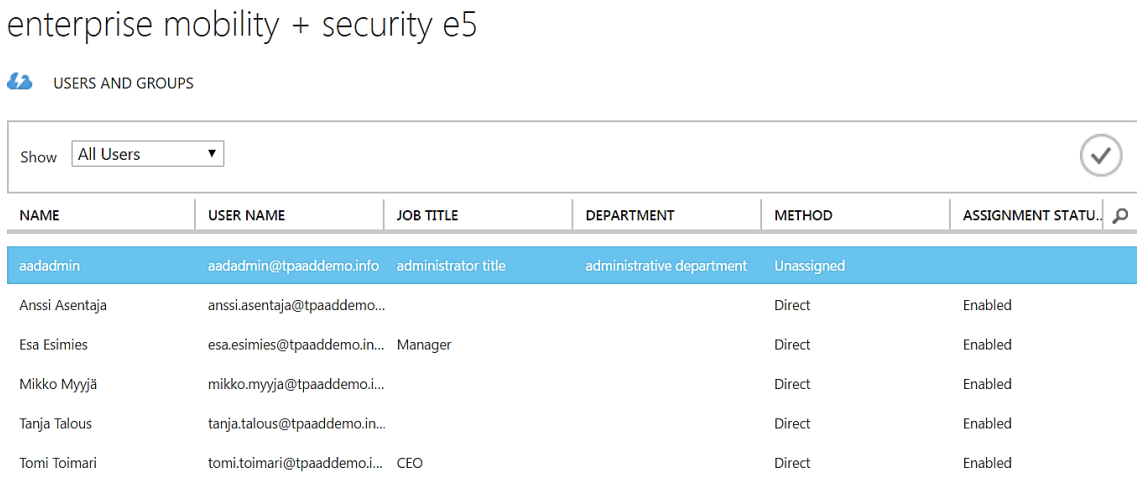
Insinöörityötä varten otin ilmaiseen koekäyttöön Enteprise Mobility + Security E5:n Azure AD:n Licenses-kohdasta. Lisenssin käyttöönoton jälkeen sen voi jakaa yksittäisille käyttäjille tai ryhmälle. EMS-lisenssi lisätään Kaikki-ryhmälle (kuva 14): Azure AD > Licences > All Products > Enteprise Mobility + Security *E3/E5* > Licensed Groups > Assign. Assigment options -kohdasta voi valita, mitä lisenssin toiminnallisuuksia jaetaan ryhmälle. Oletuksena on kaikki toiminnallisuudet.



Kuva 14. Lisenssin antaminen Kaikki-ryhmälle.

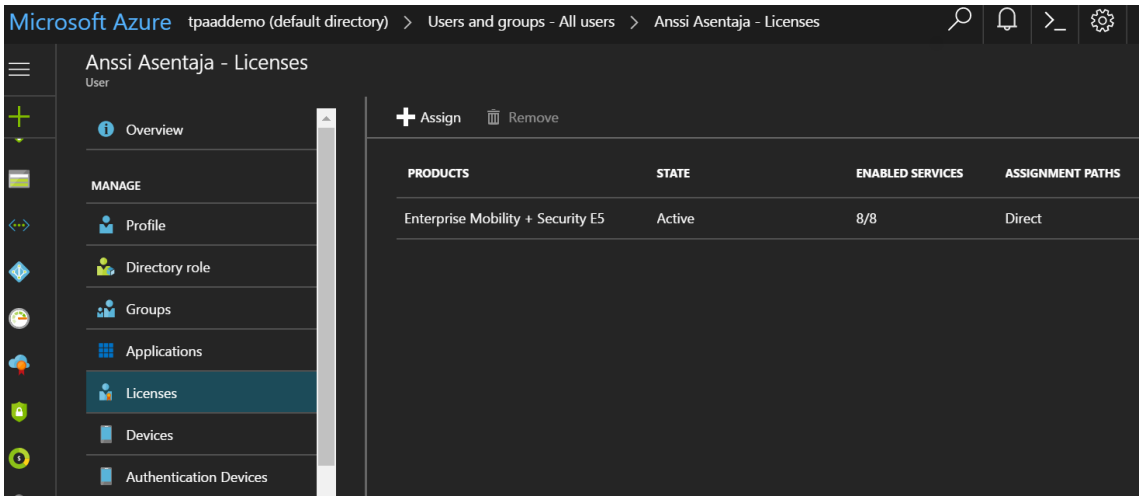
En saanut lisenssejä menemään perille asti, vaan prosessointi oli aina kesken, eikä Reprocess-painikkeen klikkaaminen portaalista auttanut. Lisenssien jakamisesta ryhmälle toiminnallisuuden preview-tilan takia kokeilin jakaa lisenssiä yksittäisille käyttäjille ja eri lisenssin toiminnallisuuksilla, mutta lopputulos oli aina sama. Sain jaettua lisenssit vanhan portaalin kautta yksitellen käyttäjille valitsemalla control-nappulalla useamman käyttäjän kerralla ja vahvistamalla valinnat assign-painikkeella (kuva 15).

Lisenssien jakamisen epäonnistuminen johtui todennäköisesti siitä, että olin kirjautunut Microsoft-tilillä enkä tpaaddemo.info-toimialueeseeni kuuluvana järjestelmänvalvojana. Myöhemmin tehtävä Office 365 -lisenssin jakaminen ryhmälle onnistui uudesta portaalista Anssi Asentajan -tunnuksella.



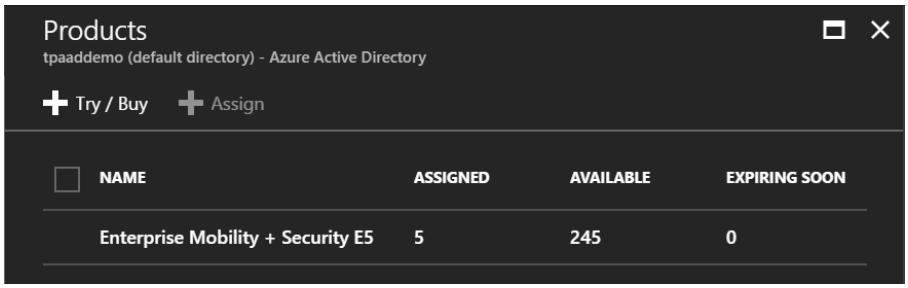
Kuva 15. Vanhan portaalin Azure Active Directoryn lisenssin näkymä.

Lisenssin jakamisen jälkeen katsottaessa uudesta portaalista Anssi Asentajan lisenssejä näkyi lisenssin jakaminen onnistuneen myös uudesta portaalista (kuva 16). Lisenssin jakamisen tyyppi näkyy suoraan käyttäjälle jaettuna Method- tai Assigment path -sarakkeessa merkinnällä ”Direct” ja ryhmälle jaettuna merkinnälllä ”Inherited”.



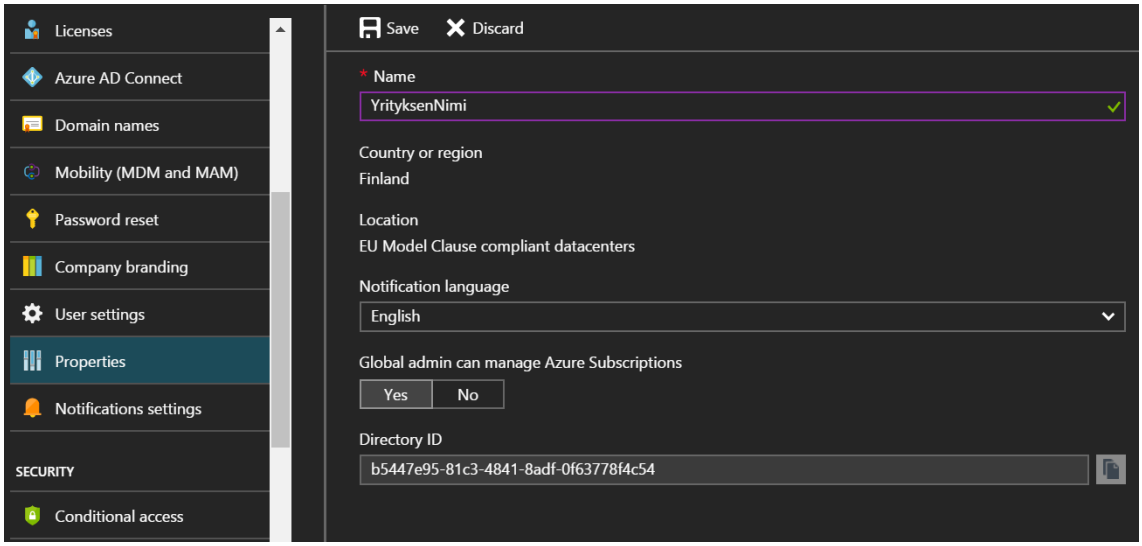
Kuva 16. Azure AD:n käyttäjän lisenssinäkymä.

Käyttöönotettujen lisenssien määrä tunnistautui oikeaksi myös uudessa portaalissa (kuva 17). Kuvassa 17 on Azure AD:n Licenses-kohta, josta näkyy myös lisenssien kokonaismäärä ja pian umpeutuvat lisenssit.



Kuva 17. EMS-tuotteen lisenssit.

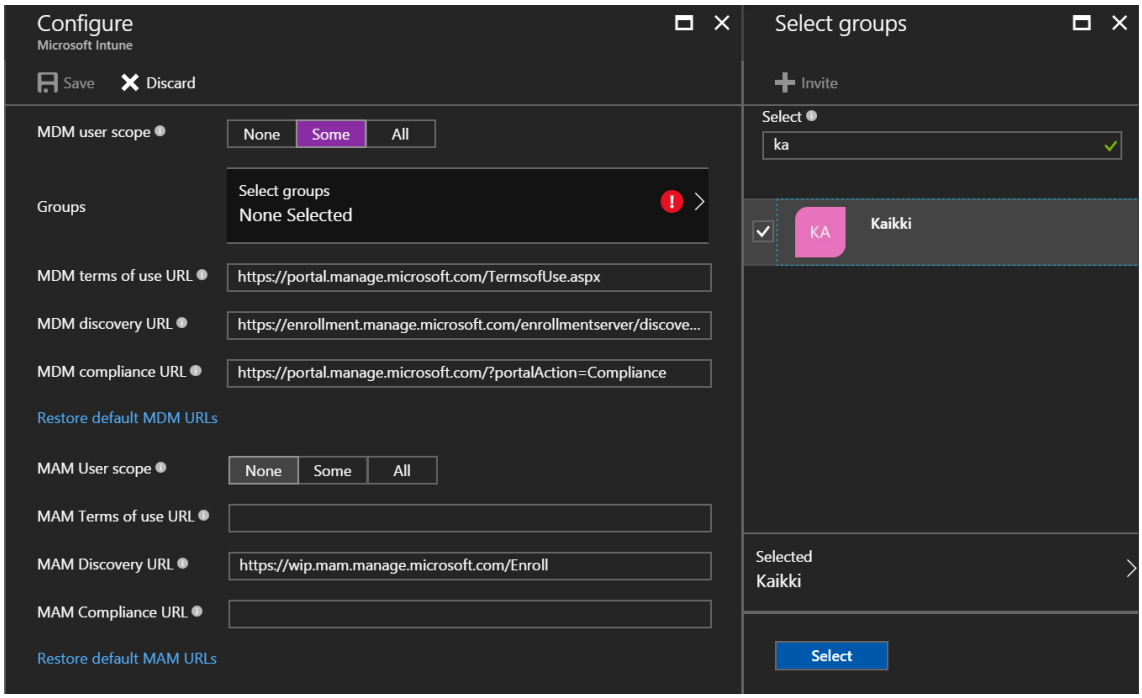
Azure AD:ssa näkyvän hakemiston nimen voi muuttaa Azure AD:n Properties-kohdassa (kuva 18), mikä näkyy käyttäjille muun muassa Azure AD:hen liittymisessä.



Kuva 18. Azure AD:n nimeäminen.

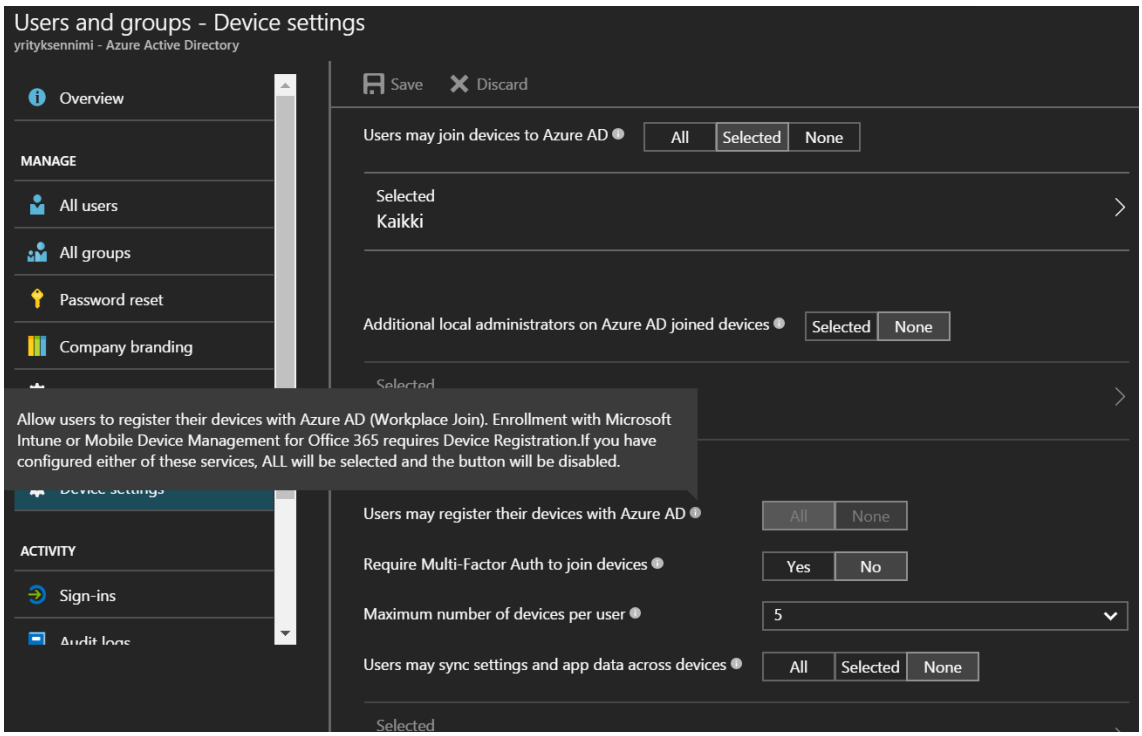
5.4 Intunen konfigurointi

Azuresta voi valita MDM- ja MAM-ratkaisuksi myös toisen tuotteen, esimerkkisi VMwaren AirWatchin, mutta tässä insinöörityössä käytetään Intunea. Kaikki-ryhmälle määritellään laitteiden automaattinen rekisteröinti Intuneen Azure AD:n asetuksista: Azure AD > Mobility (MDM and MAM) > Microsoft Intune > MDM user scope:Some ja Groups:*Kaikki* (kuva 19). Tästä valikosta voi määrittää Intunen myös MAM-ratkaisuksi. (54.)



Kuva 19. Kaikki-ryhmälle annetaan oikeus rekisteröidä Intunen laitehallintaan.

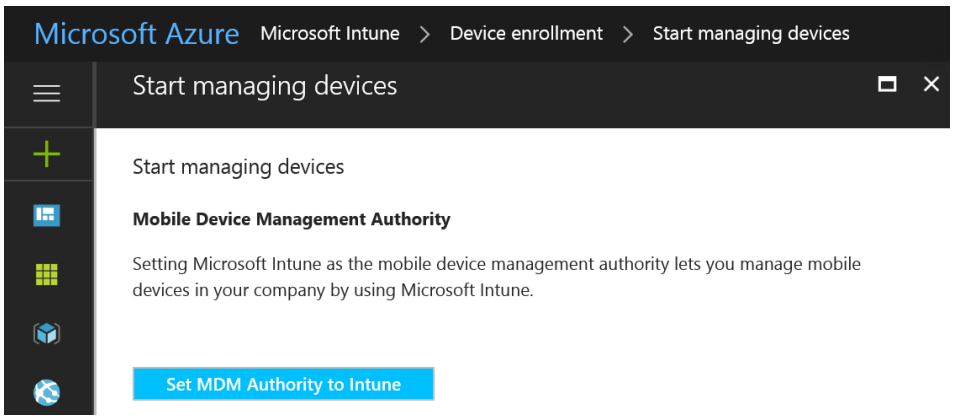
Azure AD:sta löytyy vielä Users and groups -kohdasta Device settings, jossa voi muun muassa lisätä rekisteröityihin laitteisiin määritellyn paikallisen järjestelmänvalvojan ja valita käyttäjät, jotka voivat rekisteröidä laitteen (kuva 20). Täältä täytyy olla valittuna Kaikki-ryhmä tai kaikki käyttäjät kohdassa Users may join devices to Azure AD.



Kuva 20. Azure AD:n laiteasetukset.

Näiden lisäksi täytyy Intunen asetuksista valtuutta Intune mobiililaitteiden hallintasovellukseksi. Minulla oli hieman vaikeuksia löytää Intunen hallintakonsolia Azuresta. Koetin lisätä Intunen Azuren plus-painikkeella, jolla lisätään uusia palveluita, mutta se päättyi Intunen ostamisesta kertovaan verkkosivuun. En päässyt kirjautumaan Intunen vanhaan portaaliin, vaan sekin päättyi virheilmoituksiin. Huomasin, ettei vanha portaali toimi Chromella, koska portaali käyttää Silverlight-tekniikkaa, joka ei ole enää tuettuna kaikissa selaimissa, mutta Internet Explorerin kautta pystyin kirjautumaan. Vanhasta portaalista onnistui myös konfiguroida Intune vaadituksi MDM authorityksi, muita toimintoja en kokeillut. (56.)

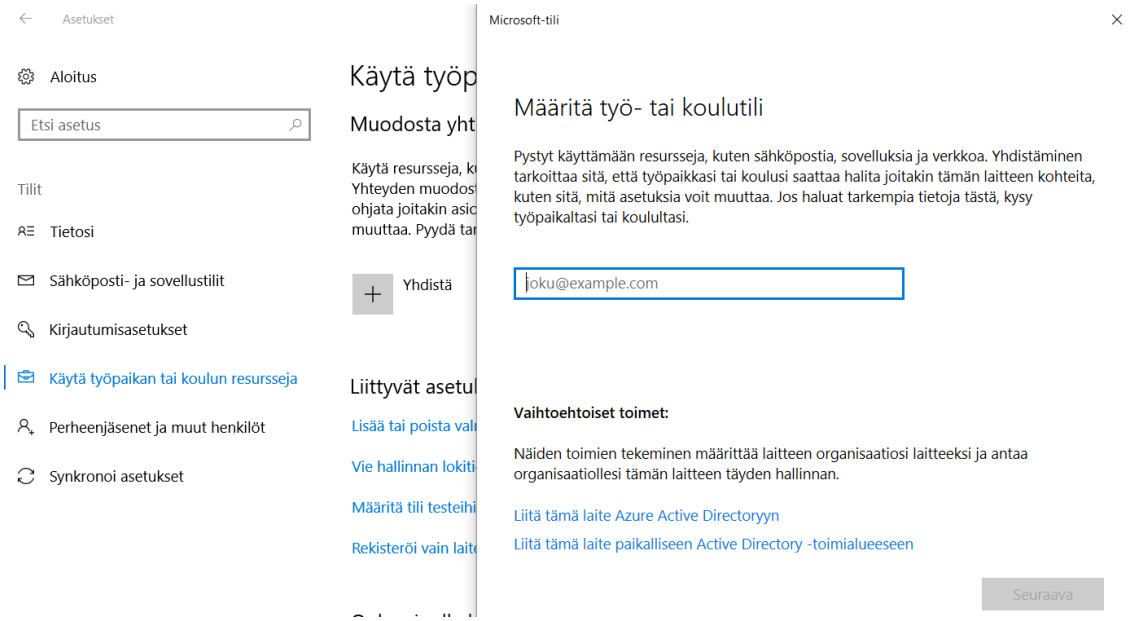
Vanhassa portaalissa oli uuteen portaaliin linkki, jota klikkaamalla sain Intunen hallinnan näkyviin Azuressa. Huomasin sen jälkeen Intunen hallinnan onnistuvan samalla tavalla kuin muidenkin Azuren palveluiden, joita ei näy vasemman laidan valikossa. Lisää palveluita voi lisätä suosikkeihin tai käyttää vasemmassa alareunassa olevasta More services -painikkeesta. Sen jälkeen valitaan Intunesta Device enrollment > Start managing devices ja painetaan ”Set MDM Authority to Intune” (kuva 21).



Kuva 21. Intunen valtuuttaminen mobiililaitteiden hallintasovellukseksi.

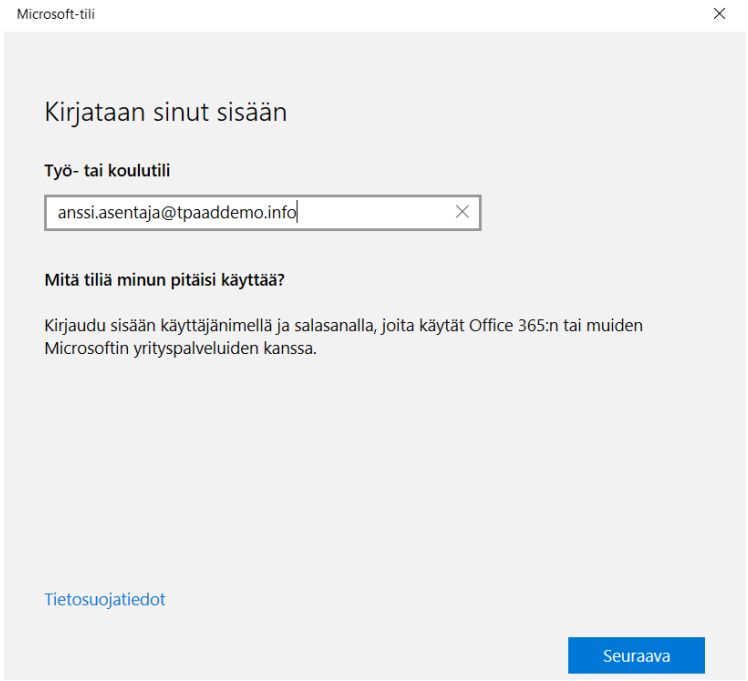
5.5 Laitteen yhdistäminen Azure Active Directoryyn

Kun Azure Active Directorystä on sallittu käyttäjille laitteiden rekisteröiminen ja MDM-ratkaisu on konfiguroitu, voidaan laitteelle suorittaa Azure AD Join laitteen automaattisella rekisteröinnillä Intuneen. Tämän voi suorittaa myös suoraan otettaessa uutta tietokonetta käyttöön, ilman että tarvitsee mennä Windowsin työpöydälle asti. Jo käyttöönotetussa laitteessa liittyminen Azure Active Directoryyn tapahtuu Windows 10:n asetusvalikosta > Tilit > Käytä työpaikan tai koulun resursseja > Yhdistä (kuva 22). Tähän ei vielä kirjoiteta käyttäjänimiä, vaan valitaan Liitä tämä laite Azure Active Directoryyn. Tässä kohdassa voi lisätä organisaatiotunnuksen, jota käytetään erilaisissa BYOD (Bring Your Own Devices) -tilanteissa. Näin voidaan toteuttaa esimerkiksi SSO, muttei Azure AD -tunnuksilla työasemalle kirjautumista käyttäen.



Kuva 22. Windows 10:n erilaiset vaihtoehdot käyttää laitetta työympäristössä.

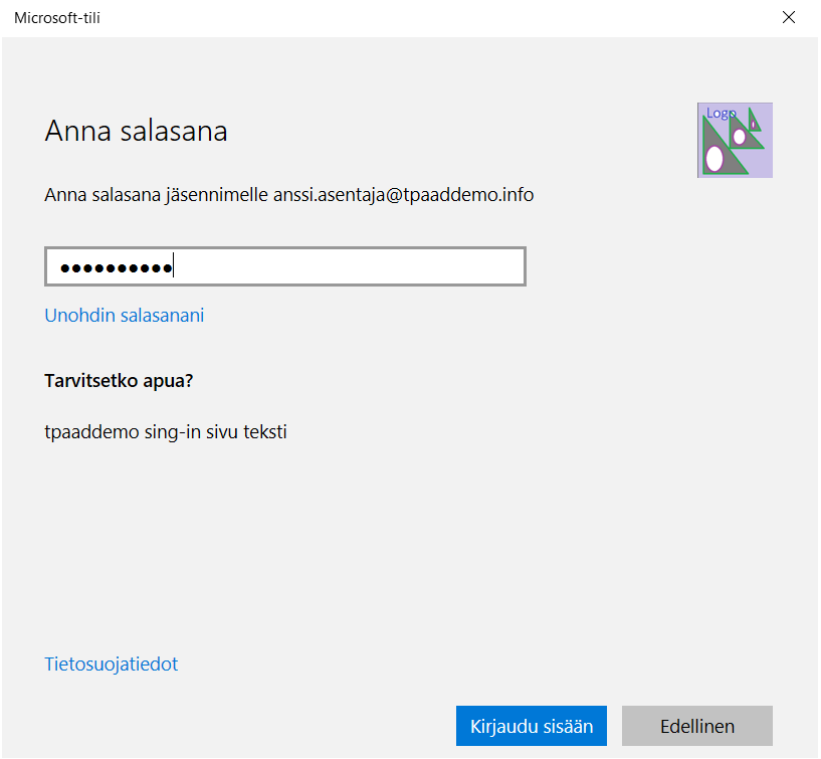
Seuraavaksi määritellään käyttäjätunnus, jolla Azure AD:hen liitytään (kuva 23). Tästä käyttäjätunnuksesta tulee koneen paikallinen järjestelmänvalvoja.



Kuva 23. Azure AD Join -kirjautuminen.

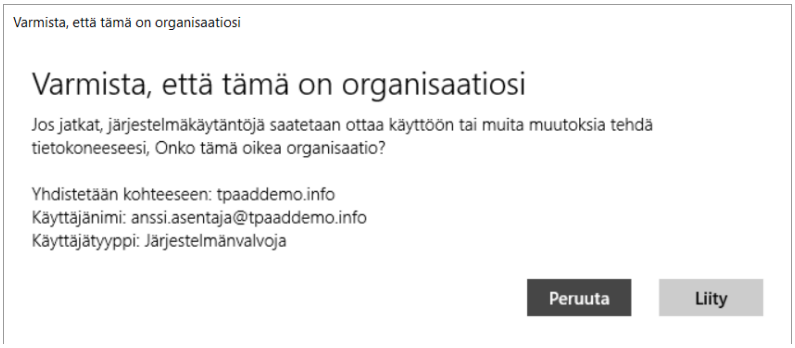
Seuraavaksi annetaan käyttäjätunnuksen salasana. Kuvassa 24 näkyy räätälöity kirjautumisikkuna, jossa on määritelty oma logo ja kirjautumissivun teksti. Räätälöintiä pääsee tekemään Azure AD:n Company branding -kohdassa. Tein Paintilla nopeasti muutaman

kuvan testauksen vuoksi ja syötin tekstiruutuihin esimerkkitekstejä. Räätälöinti näkyy myös kirjauduttaessa Microsoftin pilvipalveluihin selaimen kautta.



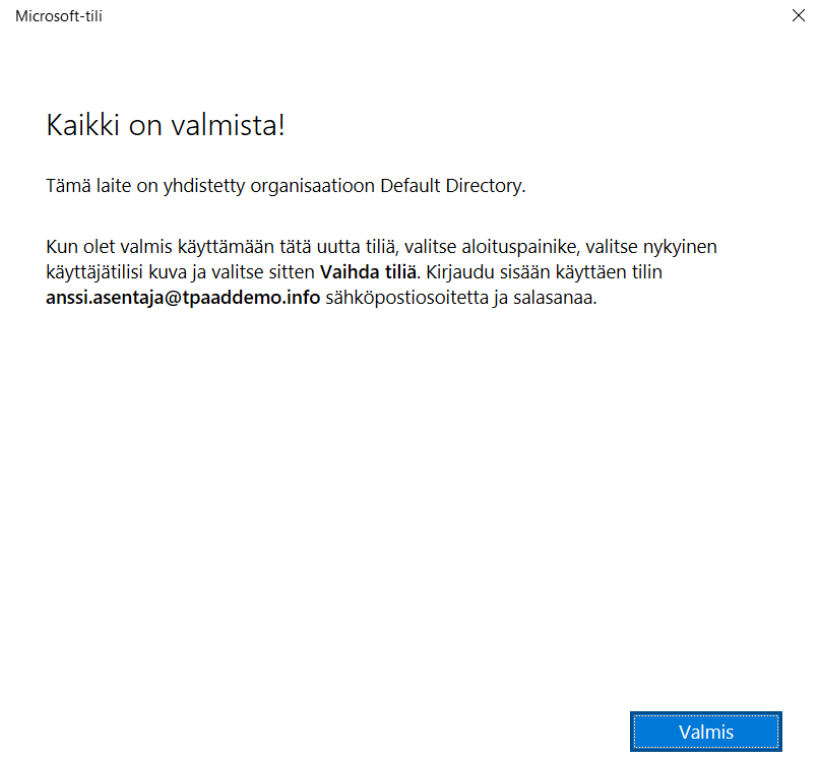
Kuva 24. Salasanan antaminen Azure AD Joinissa.

Autentikoinnin onnistuttua ja lisensoinnin ollessa kohdallaan, tulee kuvan 25 mukainen ikkuna, josta valitaan Liity.



Kuva 25. Azure AD Joinin autentikoinnin onnistuminen.

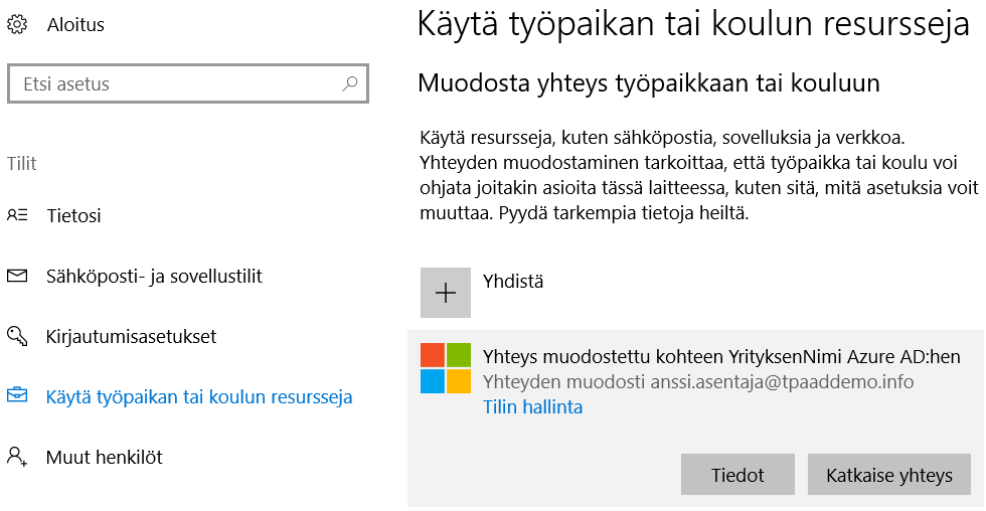
Tämän jälkeen liittyminen on onnistunut ja laitteeseen voi kirjautua Azure AD:n tunnuksella. Liittymisen onnistumisesta kertovassa ikkunassa näkyy Azure AD:n nimi, ja jos sitä ei vaihda, näkyy Default Directory -teksti liittymisen tekevälle käyttäjälle (kuva 26).



Kuva 26. Onnistunut Azure AD Join.

Kävin vaihtamassa Azure AD:n nimeksi ”YrityksenNimi” (kuva 18) ja kirjauduin laitteeseen Anssi Asentajana. Kirjautumisessa täytyi vahvistaa henkilöllisyys puhelulla, tekstiviestillä tai mobiilisovelluksella, vaikka en ollut valinnut Azure AD:n laiteasetuksista MFA (Multi Factor Authentication) -autentikointia eikä sinne ole syötetty käyttäjille puhelinnumeroa. Olin konfiguroinnit aikaisemmin vanhassa portaalissa muihin tarkoituksiin MFA:n käyttöön, minkä takia se mahdollisesti tuli nyt käyttöön.

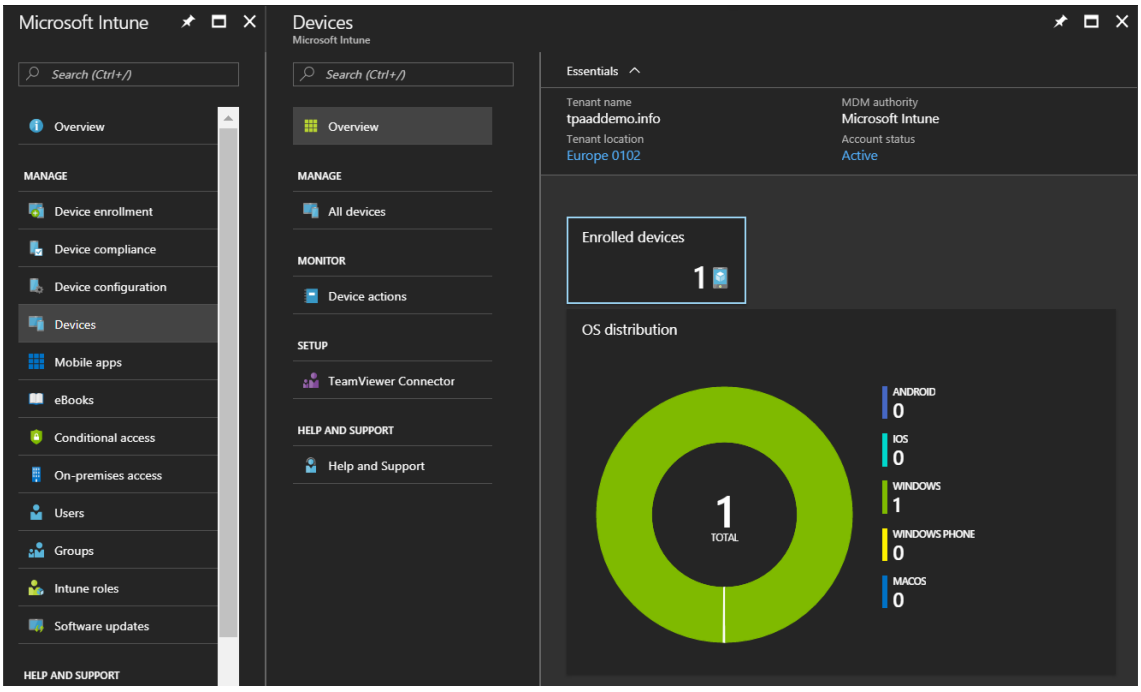
Annoin tässä vaiheessa puhelinnumeron ja valitsin tekstiviesti autentikoinnin ja syötin tekstiviestillä saamani numerosarjan sille varattuun kohtaan. Sen jälkeen täytyi laitteelle antaa PIN-koodi. Ikkunan ohjeiden mukaan sen täytyy olla vähintään 6 merkkiä eikä se saa olla yleinen numerosarja kuten 123456 tai 111111. Laitteesta voi vahvistaa liittymisen onnistumisen Windows 10:n asetukset-valikon tili-valikosta (kuva 27).



Kuva 27. Azure AD Joinin suorittanut työasema.

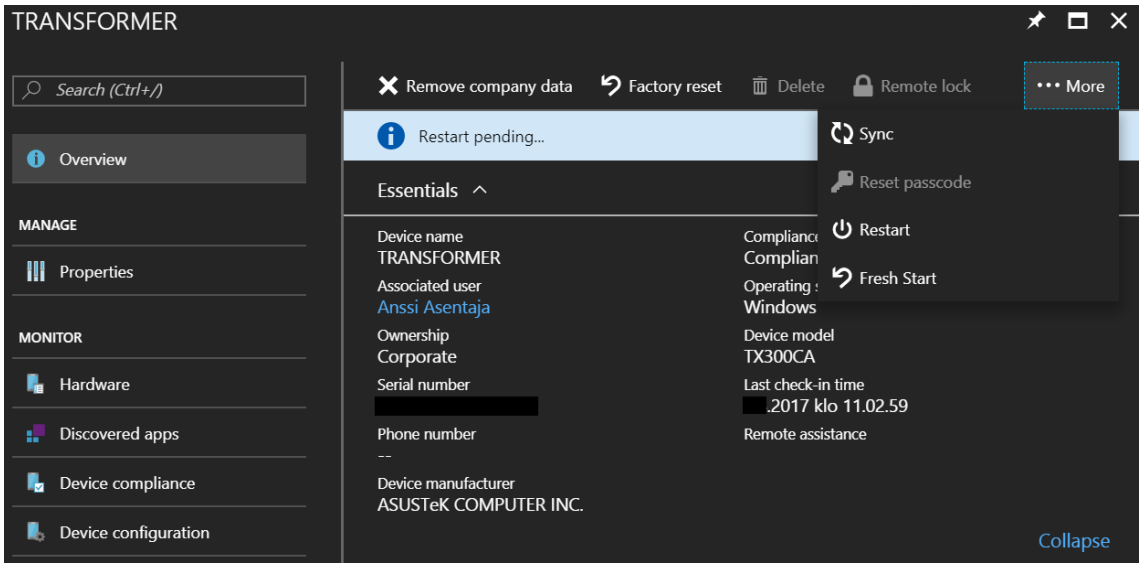
5.6 Intunen laitehallinta

Onnistuneesti suoritetun Azure AD Joinin jälkeen Intunessa näkyy yksi rekisteröitynyt laite (kuva 28).



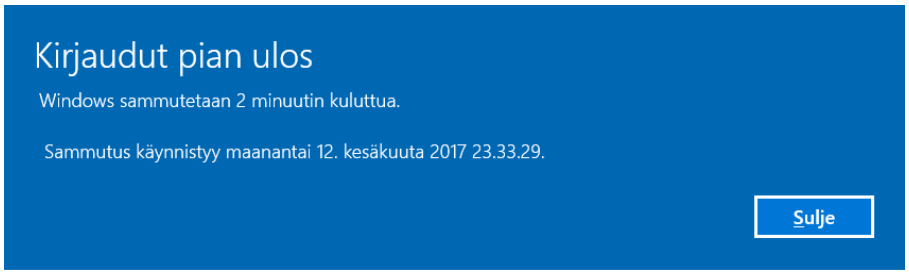
Kuva 28. Intunen laitenäkymä.

Laitteita pääsee hallitsemaan Azuren kohdasta Intune > Devices > All devices > *HallittavaLaite*. Testasin yhteyden toimivuutta Intunen ja laitteen välillä suorittamalla more-valikosta laitteen uudelleenkäynnistyksen (kuva 29).



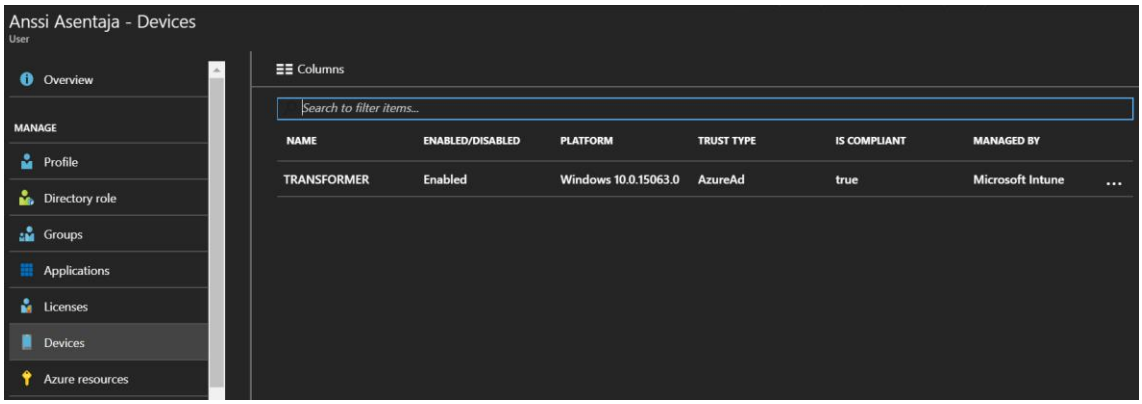
Kuva 29. Laitteen uudelleenkäynnistys Intunesta.

Hyvin pian komento tavoitti laitteen ja ilmoitti laitteen uudelleenkäynnistymisestä kahden minuutin kuluttua (kuva 30).



Kuva 30. Intunesta suoritettu uudelleenkäynnistys laitteessa.

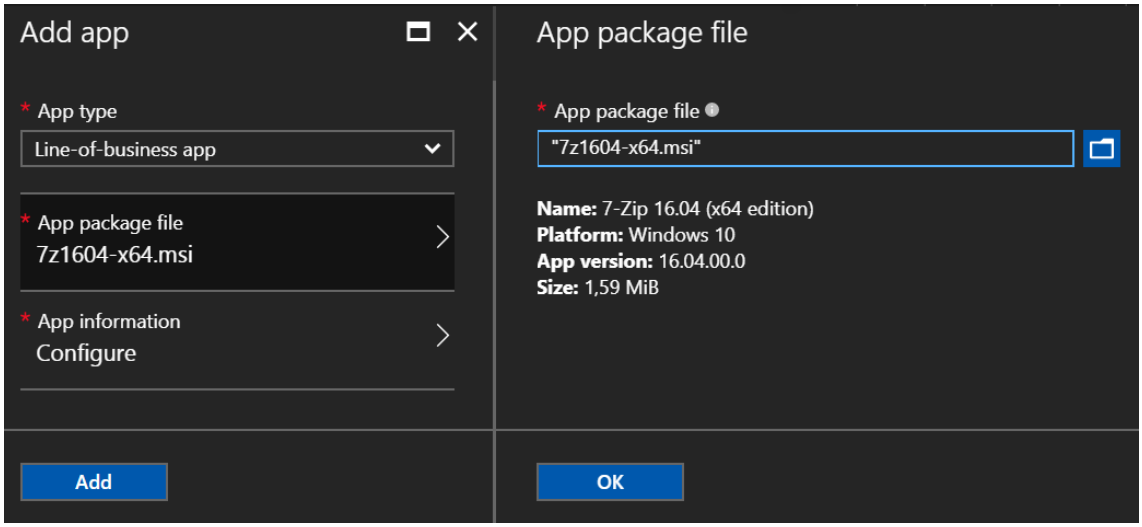
Käyttäjän laitteet näkyvät myös Azure AD:n käyttäjän Devices-kohdassa (kuva 31).



Kuva 31. Azure AD:n käyttäjän laitteet.

Ohjelman lisääminen Intuneen

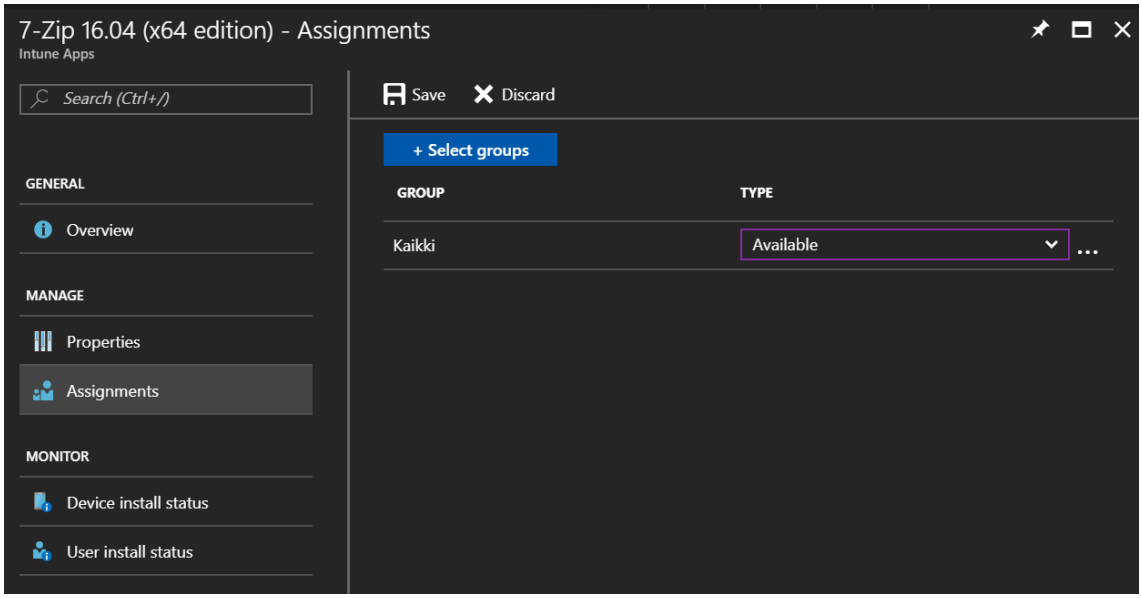
Intunesta pystyy asentamaan ohjelmia Windows 10 -koneille kohdasta Microsoft Intune > Mobile apps > Apps > Add > App type: Line-of-business app. Kuvassa 32 olen lisäämässä 7-Zip-ohjelman MSI-pakettia. Intuneen voi lisätä Windowsille .msi-, .appx- ja .appxbundle-päätteisiä ohjelmia.



Kuva 32. Ohjelman lisääminen Intuneen.

Asennustiedon lisäämisen lisäksi ohjelmalle täytyy antaa kuvaus ja julkaisija, jotka näkyvät käyttäjille Intunen yritysportaalissa. Ohjelmalle voi valita myös ohjelmakategorian ja lisätä asennuksessa käytettäviä komentoriviargumentteja (command line arguments), joilla voi muokata asennusta.

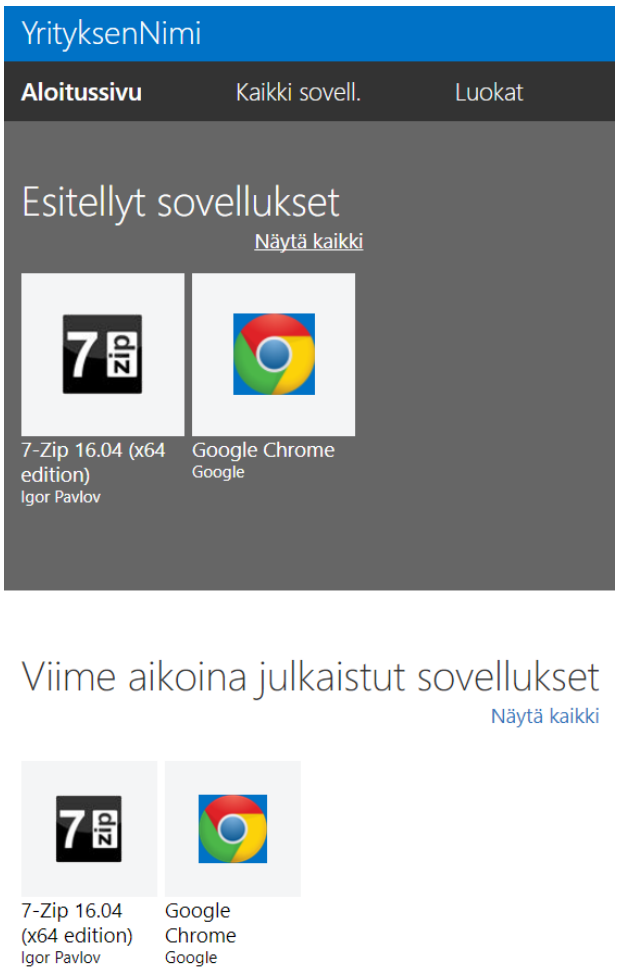
Ohjelman lisäämisen jälkeen täytyy ohjelmalle määrittää käyttäjät, jotka voivat asentaa ohjelman. Kuvassa 33, käytetään taas luotua Kaikki-ryhmää. Ohjelman asennuksen tyypiksi on valittu ”Available”, jolloin käyttäjä voi halutessaan asentaa ohjelman Intunen yritysportaalista, mutta se ei ole pakollista. Tyypiksi voi valita myös not applicable, required, uninstall ja available with or without enrollment.



Kuva 33. Intunen ohjelman jakaminen ryhmälle.

Ohjelman asentaminen Intunen yritysportaalista

Käyttäjät kirjautuvat Intunen yritysportaaliin osoitteessa https://portal.manage.microsoft.com (kuva 34). Myös tätä portaalia pääsee muokkaamaan yrityskohtaisemmmaksi Intunen Mobile apps -valikon Company Portal branding -kohdasta. Portaalissa voi selata ohjelmia kategorioitten mukaan, mutta kategorioiden määrittäminen ohjelmalle ei ole pakollista. Ohjelmia voi etsiä myös portaalin hakutoiminnolla.

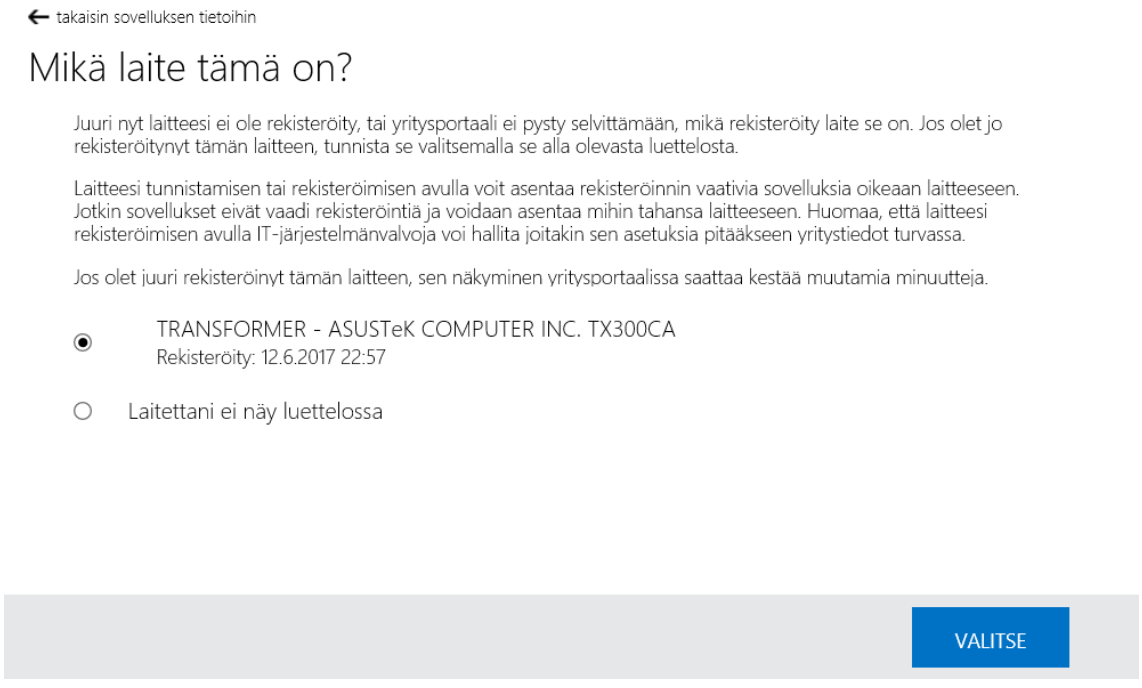


Kuva 34. Muokkaamaton Intunen yritysportaali.

Yrittäessäni asentaa 7-Zip-ohjelmaa Intuneen rekisteröidyllä laitteelta Anssi Asentajana ohjelman asenna-painike ei ollut käytettävissä (kuva 35). Ikkunan ohjeiden mukaan siirryin vahvistamaan laitetta rekisteröidyksi.

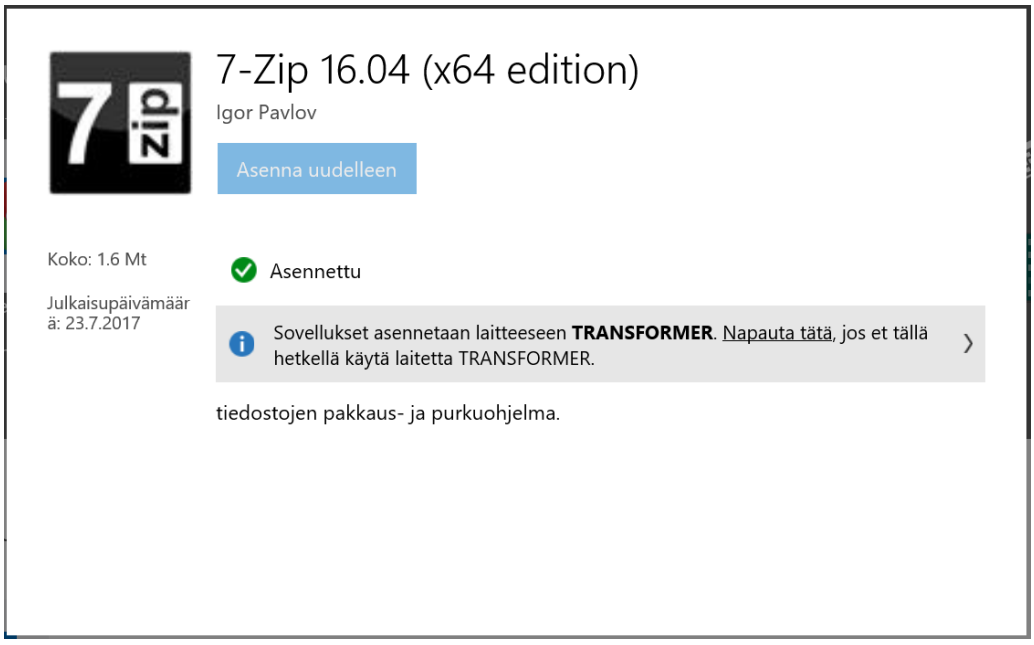
Kuva 35. Ensimmäisen ohjelman asennus Intunen yritysportaalista.

Valitsin laitteen kuvan 36 mukaisessa listassa ja painoin Valitse-painiketta. Kuvan selitteksteistä ilmenee, ettei yritysportaali pystynyt selvittämään laitetta, ja sen takia se piti erikseen valita rekisteröityjen laitteiden listasta.



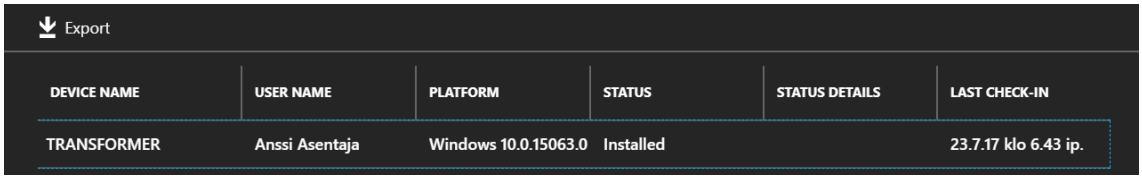
Kuva 36. Rekisteröidyn laitteen valitseminen Intunen yritysportaalissa.

Laitteen vahvistamisen jälkeen muuttui ohjelman asenna-painike aktiiviseksi. Valitsin asenna, ja koska 7-zipin asennustiedosto oli alle kaksi megatavua, oli ohjelman asennus hyvin nopeasti valmis. Kuvassa 37 on ohjelman asennusikkuna asennuksen jälkeen.



Kuva 37. Asennettu ohjelma Intunen yritysportaalista.

Intunesta näkee ohjelman overview-valikosta ohjelman asennustilanteen graafisena näkymänä laitteille ja käyttäjille. Asennustilanteita ovat: Installed, not installed ja failed. Kuvassa 38 näkyy ohjelman Device install status -näkymä. Export-painikkeesta saa luotua CSV-muotoisen raportin ohjelman asennustilanteesta myös User install status -näkymästä.



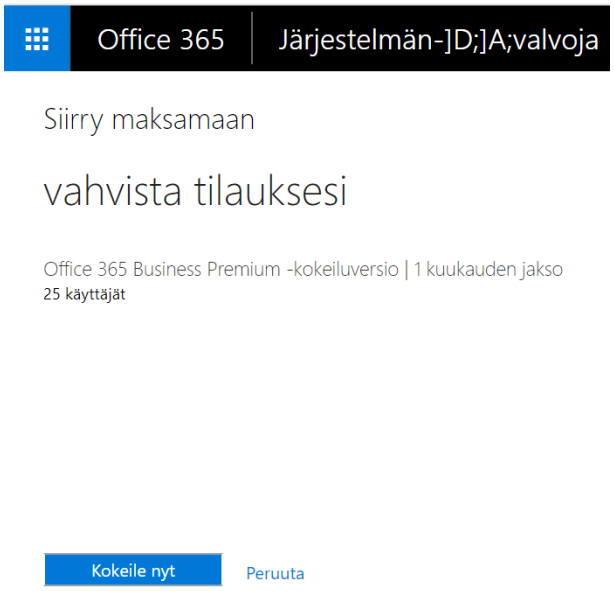
Kuva 38. Ohjelman asennustilanteen näkymä Intunessa.

5.7 Office 365 -palveluiden määritys

Office 365 -tilaus kannattaa tehdä Azure AD -tunnuksella, jolloin Azure AD:n käyttäjät ovat heti käytettävissä Officen puolella. Tunnuksella täytyy olla Global Admin- tai Billing Admin -oikeudet, jotta sillä voidaan luoda Office 365 -tilaus. Office 365 -tilaus otetaan käyttöön Anssi Asentajana, jolle määriteltiin käyttäjän luomisvaiheessa Global Admin -oikeudet. Officen versioksi valittiin kuukauden ilmaisella kokeiluajalla Office 365 Business Premium, joka sisältää toimistosovellukset ja sähköpostin. Tämän Office-version normaalihinta on 10,50 € kk/käyttäjä (45). Tällä hetkellä kokeiluversio on saatavilla myös Office Enterprise E3 -versiosta.

Office 365 tilauksen tekeminen ja DNS-tietueiden lisääminen

Kokeiluversion saa ilmaiskäyttöön Office-version tuotesivulta. Kokeiluversion tietolomakkeen kohdassa valitaan ” Haluatko lisätä tämän olemassa olevaan tilaukseen? Kirjaudu sisään”. Kirjaudutaan sisään riittävät oikeudet omaavana käyttäjänä, Anssi Asentajana. Tunnistautumisen jälkeen sivu pyytää vahvistamaan kokeiluversion tilauksen (kuva 39). Vahvistuksen jälkeen sivu kehottaa ottamaan uudet käyttöoikeudet käyttäjille käyttöön ja kertoo tilauksen olevan käytössä 25 käyttäjälle. Nyt Anssi Asentaja on kirjautunut Office 365 admin center -portaaliin, josta hallitaan sen palveluita. Admin centeriin pääsee osoitteesta portal.office.com.



Kuva 39. Office 365 -tilauksen vahvistaminen.

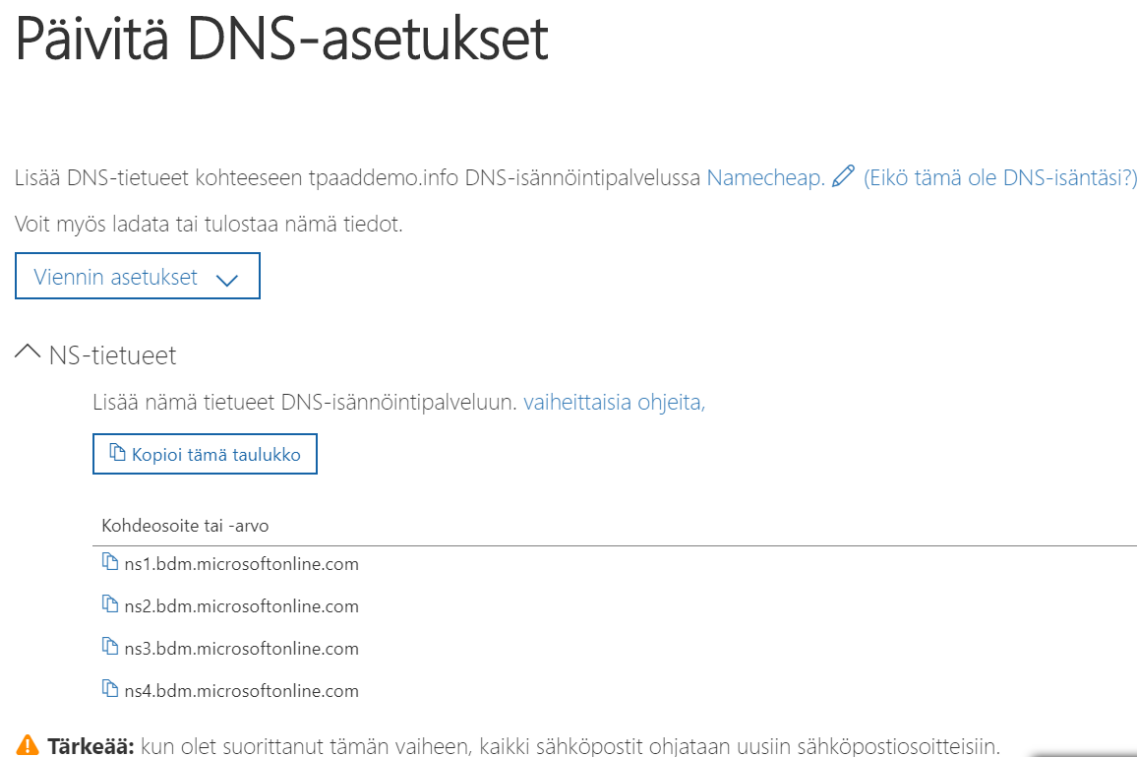
Office 365 lisenssit voidaan jakaa käyttäjille Office 365 admin center -portaalissa aktiiviset käyttäjät -kohdassa tai Azure AD:n lisenssien kautta ryhmälle. Admin centerissä ei lisenssin jakaminen suoraan ryhmälle onnistunut, koska Anssi Asentajalla ei ollut Exchange Online -käyttöoikeutta. Azuressa lisenssin jakamista ryhmälle on käsitelty luvussa 5.3 Lisenssien jakaminen. Tässä tapauksessa Kaikki-ryhmälle jaetaan Azure AD:n lisensseihin ilmaantunut Office 365 Business Premium -lisenssi.

Verkkotunnus on lisätty luvussa 5.1 Verkkotunnuksen liittäminen Azure Active Directoryyn, eikä sitä tarvitse lisätä enää uudestaan Officen puolelle. Officen palvelut tarvitsevat kuitenkin toimiakseen erilaisien DNS-tietueiden lisäämistä verkkotunnuksen rekisteröijälle. Office 365:ssä on tätä varten ohjattu toiminto kohdassa Aloitus > Toimialueet > Muokkaa toimialuetta > *YrityksenToimialue*.

Kohdassa ”Määritä online-palvelut” voi valita ”Määritä online-palvelut puolestani (suositus)” tai ”Hallitsen itse DNS-tietueita”. Valitsemalla jälkimmäisen vaihtoehdon sivu kertoo mitä, tietueita pitää lisätä Exchangea, Skypeä, Office 365 MDM:ää ja muita palveluita varten, jotta ne toimivat. Sivu vähän hämäävästi näytti ensimmäisenä ruutuna lisättävien DNS-tietueiden tiedot, josta piti painaa ohjattua toimintoa eteenpäin, jotta pääsee online-palveluiden määrityskohtaan.

Valitsemalla ensimmäisen vaihtoehdon, Office luo vaaditut tietueet automaattisesti, kun sille siirretään verkkotunnuksen nimipalvelut. Tässä ratkaisussa valitaan ensimmäisen vaihtoehto, minkä jälkeen on mahdollista syöttää esimerkiksi jo olemassa olevan verkkosivun DNS-nimi ja IP-osoite Office 365:n nimipalvelimille. Jos olemassa olevan verkkosivun osoitetta ei luo Officen nimipalvelimille, ei internetistä enää pääse verkkosivun osoitteeseen, koska Officen nimipalvelimet eivät osaa reitittää liikennettä siihen IP-osoitteeseen.

Uuden DNS-tietueiden lisäämisen tai tämän kohdan ohituksen jälkeen sivu on tunnistanut verkkotunnuksen rekisteröijän ja kertoo verkkotunnuksen rekisteröijälle lisättävien nimipalvelimien nimet (kuva 40). Jokaisella rekisteröijällä on vähän erilaiset hallintatyökalut, mutta Office tarjoaa hyvin ohjeita eri rekisteröijille.



Kuva 40. Office 365:n nimipalvelimet.

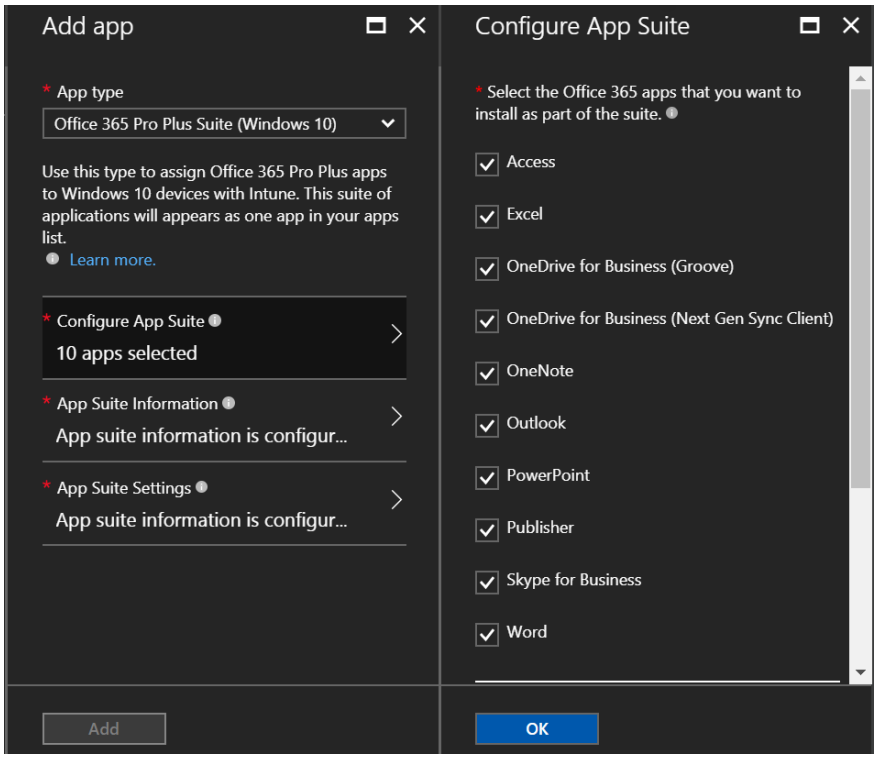
Seuraavaksi muokataan verkkotunnuksen nimipalvelimet osoittamaan Office 365:n nimipalvelimiin (kuva 41), jotka hoitavat tästä lähtien kaiken nimenselvennyksen verkkotunnukselle. Uusien DNS-tietueiden lisääminen onnistuu jatkossa Office 365:stä: Aloitus > Toimialueet > *ToimialueesiNimi* > Mukautetut tietueet > + Uusi mukautettu tietue.

Kuva 41. Namecheap-rekisteröijän nimipalvelimien hallinta.

Nimipalvelimien siirtämisen jälkeen Officelta vei 35 minuuttia saada nimenselvennys valmiiksi. Tämän jälkeen Outlookin web-versiosta lähetetyt sähköpostit toimivat eri käyttäjiltä ulkoisiin sähköpostiosoitteisiin ilman viivettä.

Intunessa on valmiina Mobile apps > Apps > Add -kohdasta Office 365 Pro Plus Suiten asennus Windows 10:lle (kuva 42). Tämä paketti pitää sisällään Office 365:n asennettavat toimistosovellukset. Intunesta on mahdollista valita paketista asennettavat sovellukset ja lisäksi asentaa pakettiin kuulumattomat Project Online Desktop Client- ja Visio Pro for Office -sovellukset. Windows 10 -laitteille täytyy olla asennettuna Creators Update -päivitys, ja Office-paketti voidaan asentaa vain laitteeseen, jossa ennestään ole Officea asennettuna. (57.)

Asetuksista pystyy määrittämään, julkaistaanko 32- vai 64-bittinen versio, automaattisen käyttöehtojen hyväksyminen, päivitysasetukset, jaetun tietokoneen aktivoinnin ja lisäkieliversioiden asennuksen officelle, joita ei ole jo asennettuna käyttäjän Windowsiin. Officen asetuksien lisäksi täytyy Intunen yritysportaalissa konfiguroida käyttäjälle näkyvät tiedot ohjelmasta.

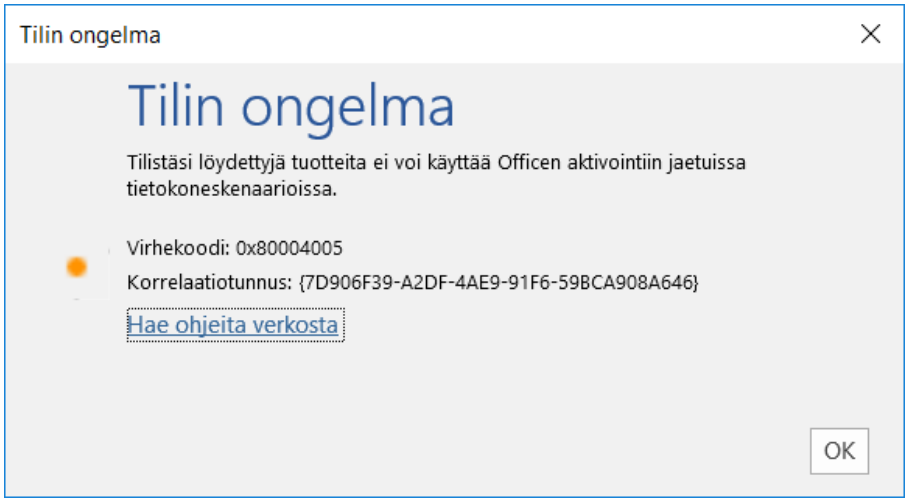


Kuva 42. Office 365 -sovellusten julkaiseminen Intunessa.

Kuten muissakin Intunessa julkaistussa sovelluksissa, täytyy Officellekin määrittää käyttäjät, jotka voivat sovelluksen asentaa. Määritin tähän Kaikki-ryhmän ja asennuksen tyypiksi ”Required”, jolloin paketin pitäisi asentua kaikkiin koneisiin ilman käyttäjän toimia.

Available-vaihtoehtoa ei ollut valittavissa Office 365 -tuotteiden asennuksessa, jolloin sen olisi voinut halutessaan asentaa yritysportaalista. Ryhmiä ja Intunen yritysportaalia on käsitelty edellisessä luvussa.

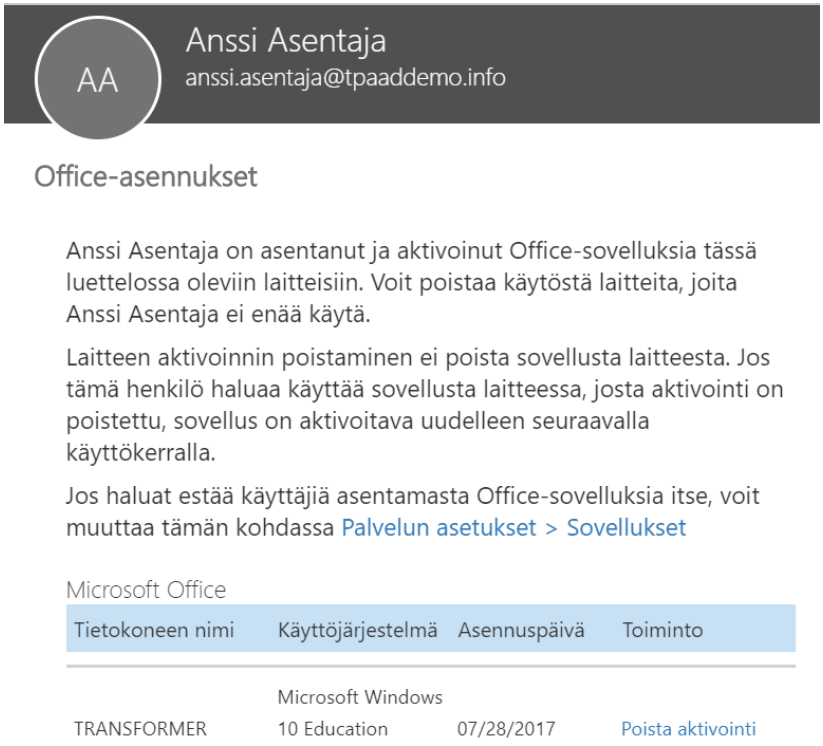
Minulla oli valittuna jaetun tietokoneen aktivointi, jolloin asennuksen jälkeen avatessani Office-ohjelman pyydettiin kirjautumistietojen antamista aktivointia varten. Tietojen antamisen jälkeen päättyi aktivoinnin vahvistaminen kuvan 43 mukaiseen virheilmoitukseen. Poistin Office-ohjelmiston koneelta ja julkaisin uuden Office-paketin, jossa ei ole valittuna jaetun tietokoneen lisenssiä.



Kuva 43. Office 365:n jaetun tietokoneen aktivointi virhe.

Office 365 -ohjelmien määritys työasemalla

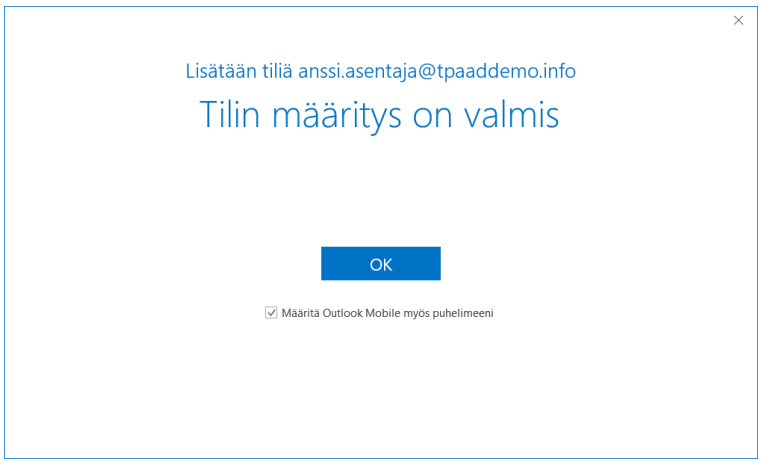
Asensin Officen uudelleen toisesta paketista, jossa ei ollut valittuna jaetun tietokoneen lisenssiä. Asennuksen valmistumisesta ei tullut mitään ilmoitusta. Huomasin ohjelmien kuvakkeiden ilmestyneen ja varmistin asennuksen valmistuneen Intunesta. Asennuksen jälkeen ei kysytty aktivoimisesta käynnistäessäni Word-ohjelman, mutta Wordin tili-kohtaa tarkasteltaessa näytti siltä, ettei tuote ollut aktivoitu. Officen portaalista katsottuna näytti tuotteen aktivointi olevan kunnossa (kuva 44).



Kuva 44. Officen aktivointi Officen-portaalista.

Käynnistin Outlookin määritelläkseni sähköpostilaatikon. Outlook pyysi antamaan sähköpostiosoitteen tilin lisäämistä varten, jolloin annoin Anssi Asentajan sähköpostiosoitteen. Sen jälkeen ponnahti Windowsin kirjautumisikkuna, johon pyydettiin AzrureAD\anssi.asentaja@tpaaddemo.info-tunnuksen salasanaa. Syötin salasanan ja valitsin "Muista tunnistetietoni". Tämän jälkeen tilin määritys oli valmis ja Outlook tarjosi vielä Outlook Mobilen määrittämistä puhelimeen (kuva 45). Valitsemalla Outlook Mobilen määrittämisen aukeaa selaimeen Microsoftin sivu, jossa pystyy sähköpostiosoitteen antamalla saamaan sähköpostiin latauslinkin Outlook Mobileen.

Kun tilin määritys oli vahvistettu, Outlook käynnistyi ja ilmoitti määrittävänsä sähköpostilaatikkoa. Koska Anssilla ei ollut montakaan sähköpostia, määrittäminen oli valmis muutamassa sekunnissa ja sähköposti oli otettu käyttöön.



Kuva 45. Outlook-tilin määritys valmiina.

5.8 SharePoint Onlinen tiedostojako

Tässä ratkaisussa tiedostojako toteutetaan Office 365:een sisältyvällä Sharepoint Onlinellä. Sharepoint on paljon muutakin, mutta tässä insinöörityössä se on työkalu toteuttamaan tiedostojenjako. Tomi Toimarille määritetään pääsy kaikkiin kansioihin ja yksittäisille käyttäjille määritetään pääsy heidän tehtäviään vastaavaan kansioon. Tomi Toimarin tulee määrittää nämä oikeudet, ja tätä varten hänestä tehdään Sharepoint-järjestelmänvalvoja Office 365:n admin center -portaalissa.

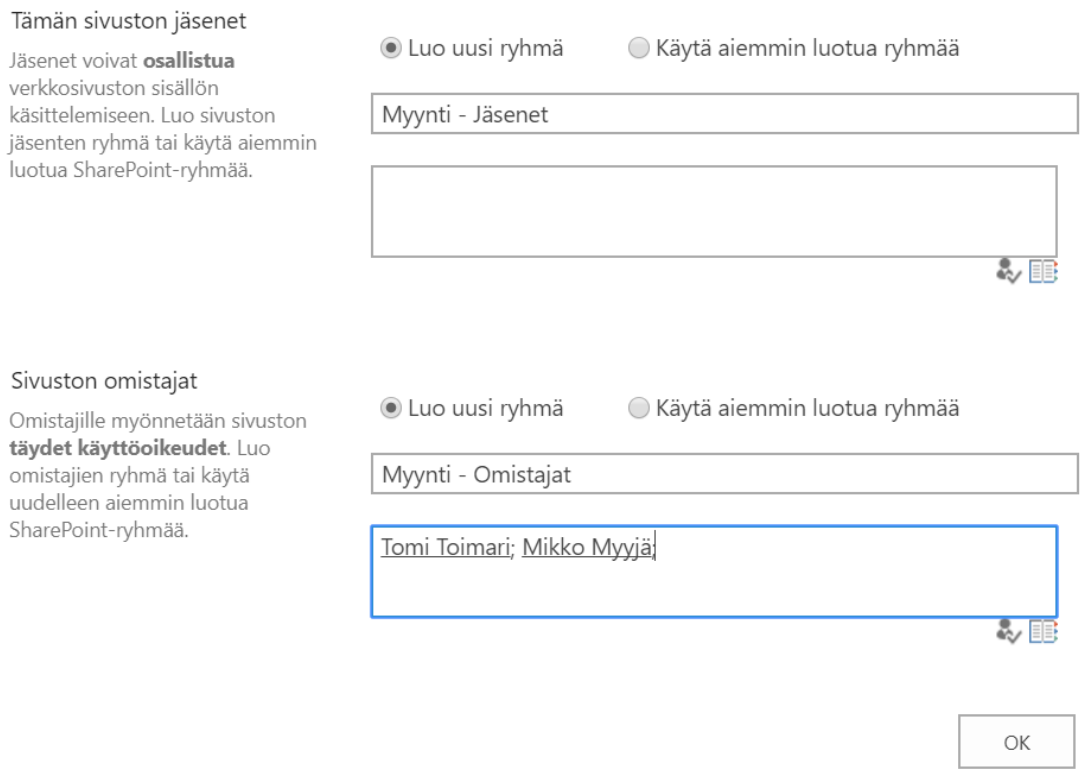
Sharepoint-ryhmäsivustojen määrittäminen

Office 365:een kirjaudutaan Sharepoint-ylläpitäjänä tai Global-admininä, esimerkiksi login.microsoftonline.com-osoitteen kautta. Tiedostojakoa varten haluttiin luoda kokonaan uusi SharePoint-ryhmäsivusto (Team site), jonka nimeksi annettiin filet. Sivuston luominen onnistuu valitsemalla Office 365 -portaalin sovelluksen käynnistimestä (app launcher) SharePointin ja painamalla Create Site -painiketta. Luodulle filet-sivustolle jätettiin Tomi Toimari ainoaksi omistajaksi ja muut käyttäjät lisättiin jäseneksi.

Ryhmäsivuston juuressa kaikilla käyttäjille on oikeudet, mutta erikseen määriteltäviä oikeuksia varten lisätään jokaiselle käyttäjäroolille oma alisivusto (team subsite). Mikko Myyjän roolille tehdyn alisivuston nimeksi annettiin Myynti, ja myynti-nimeä käytettiin myös määriteltävässä URL-osoitteessa, joka on muotoa *verkkotunnus*.share-

point.com/sites/*MääriteltäväPääsivu/MääriteltäväAlisivu.* Sivuston malliksi valittiin työryhmäsivusto ja kieleksi suomi. Käyttöoikeuksiksi valittiin ”Käytä yksilöllisiä käyttöoikeuksia” pääsivun käyttöoikeuksien sijaan, jolloin käyttöoikeudet voi määrittää haluamikseen.

Oikeuksia määriteltäessä Myynti-alisivulle lisätään Mikko Myyjä omistajaksi ja poistetaan Tomi Toimari käyttäjistä (kuva 46). Sivu muodosti myös oletuksena uuden tyhjän Myynti vierailijat-ryhmän, jolla on lukuoikeudet, mutta siihen ei kuitenkaan lisätty käyttäjiä. Näitä periaatteita noudattaen tehtiin myös muut neljä alisivustoa. (58.)

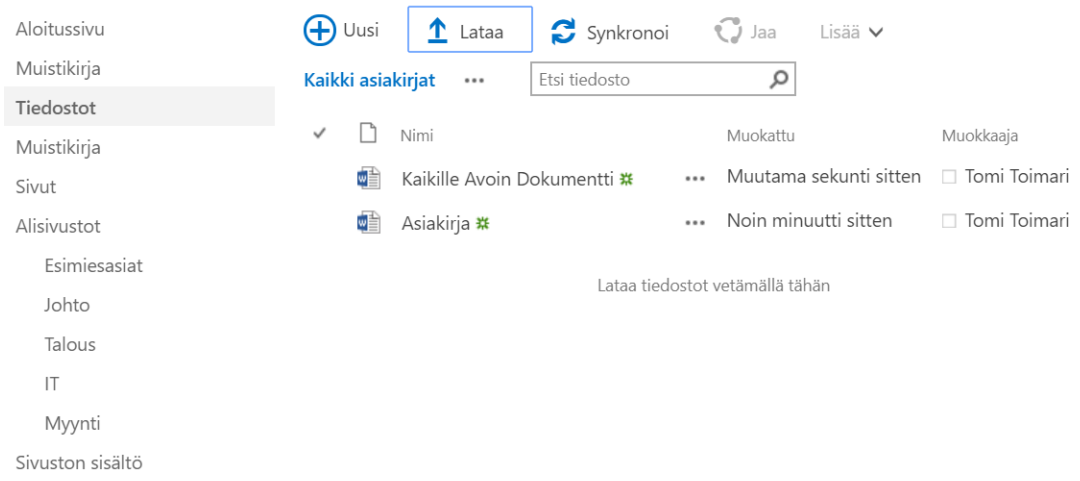


Kuva 46. SharePointin alisivuston oikeuksien antaminen.

Jokaiselle sivustolle SharePoint luo uusia ryhmiä, joilla on eritasoisia oikeuksia kyseiseen sivustoon. Uusia henkilöitä voi kätevästi lisätä ryhmään, jolloin oikeudet tulevat myös tiedostojakoon. Tomi Toimari on nyt liitettynä joka ryhmään erikseen, mutta parempi tapa olisi luoda ”Kaikki oikeudet” -ryhmä, joka liitetään kaikkiin sivustoihin omistajaksi ja jonka jäseneksi Tomi liitettäisiin.

Kun kaikki alisivustot on luotu, lisätään pääsivustoon satunainen dokumentti, joka on kaikkien käyttäjien käytettävissä. Näin saadaan jokin tiedosto ladattua pilvestä koneelle, kun synkronointia otetaan käyttöön ja voidaan havainnoida synkronoinnin onnistuminen.

Pääsivustosta tulee olla valittuna Tiedostot-kohta, jolloin sinne voi lisätä tiedostoja Lataa palvelimeen -painikkeesta luomalla dokumentin Uusi-painikkeesta tai raahaamalla koneelta tiedostoja ja pudottamalla ne kuvan 47 osoittamaan ”Lataa tiedostot vetämällä tähän” -kohtaan.

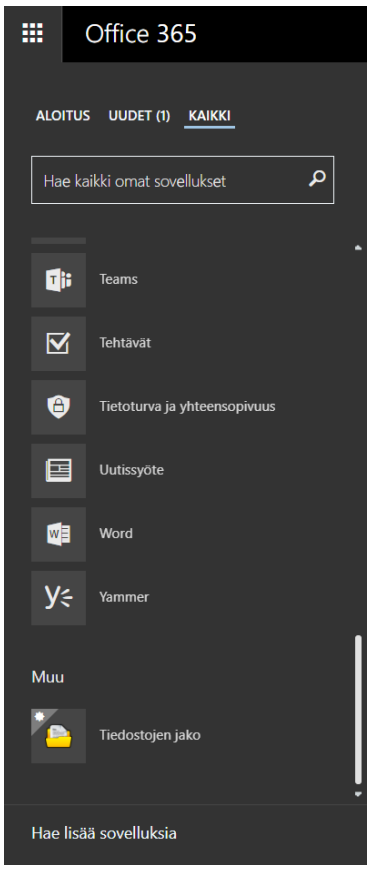


Kuva 47. SharePoint Onlinen ryhmäsivuston tiedostot.

Oikopolun luominen tiedostojakoon

Käyttäjille voi lisätä oikopolun tiedostojakoon esimerkiksi Office 365:n Sovelluksen käynnistin -valikkoon. Se lisätään Officen admin centeristä Asetukset > Organisaarprofiili > "Lisää mukautettuja näkymiä organisaatiollesi: Muokkaa" > "Lisää mukautettu näkymä" ja antamalla näkymälle nimen, osoitteen, kuvauksen ja kuvan. Osoitteeksi voi antaa suoraan ryhmäsivuston tiedostot-kohdan, jolloin käyttäjä näkee heti kaikille jaetut dokumentit ja alisivustot, joihin hänellä on käyttöoikeus.

Tämän jälkeen oikopolku on käytettävissä sovelluksen käynnistimessä valittaessa näytettäväksi kaikki sovellukset (kuva 48). Järjestelmänvalvojana voi lisätä myös omia sivuja käyttäjille SharePointin vasemman laidan linkkeihin "Featured Links" -painikkeella tai lisätä linkin Office 365 -otsikkopalkkiin, joilla voidaan toteuttaa myös oikopolku tiedostojakoon. (58.)



Kuva 48. Office 365:n App launcheriin tehty oma pikakuvake.

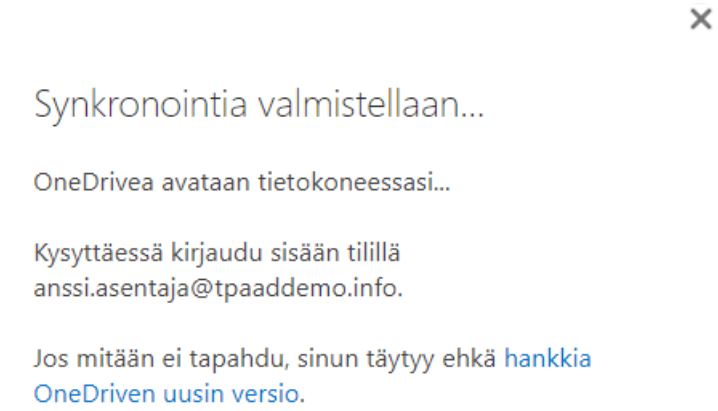
SharePoint-kirjaston synkronointi

Tässä vaiheessa otetaan SharePoint-kirjastojen synkronointi käyttöön Anssi Asentajalle. Synkronoitua kirjastoa voi käyttää Windowsissa, kuten tavallista tiedostoja sisältävää kansiota. Kaikki tiedostoihin tehdyt muutokset synkronoituvat pilveen ja sitä kautta muille käyttäjille, jotka ovat synkronoineet saman kirjaston.

En saanut synkronoitua SharePoint-kirjastoja OneDrive for Business -sovelluksella, vaikka yritin usealla eri tavalla. Havaitsin SharePoint-kirjaston synkronoinnin onnistuvan Windows 10:een esiasennetulla, uuden sukupolven OneDrive-sovelluksella. Tätä varten SharePoint täytyy konfiguroida käyttämään uutta OneDrive-synkronointisovellusta Office 365:n admin centerin kohdasta Hallintakeskukset > SharePoint > asetukset > Share-Point-synkronointiohjelma: Käynnistä uusi ohjelma.

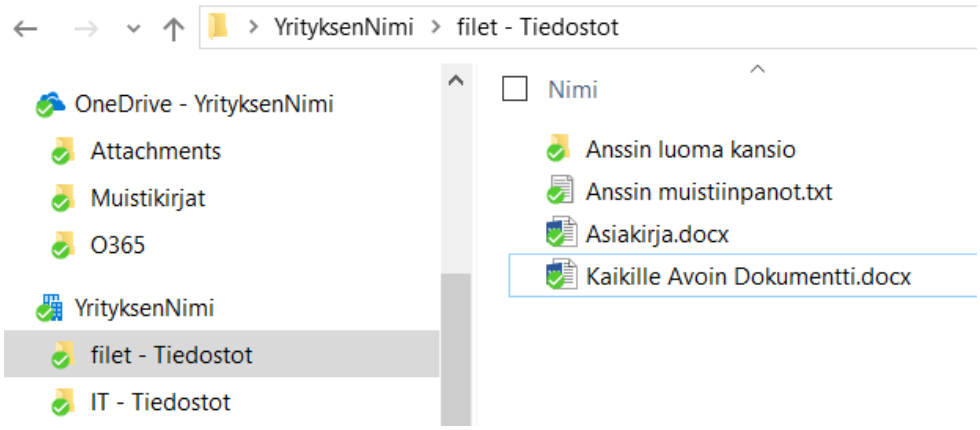
Kuvassa 49 olen käynnistämässä synkronointia Synkronoi-painikkeesta filet-pääsivustolta. Kuvan ilmoituksessa näkyvä teksti kertoo OneDriven uusimmasta versiosta, jolloin

SharePoint on oikein konfiguroitu käyttämään sitä synkronointiin. Selaimen ponnahdusikkunan haluaa myös avata Microsoft OneDriven. Filet-pääsivuston näkymä on samanlainen kuin kuvassa 47, mutta Anssi Asentajalle määritettyjen oikeuksien takia hän näkee vain IT-alisivuston.



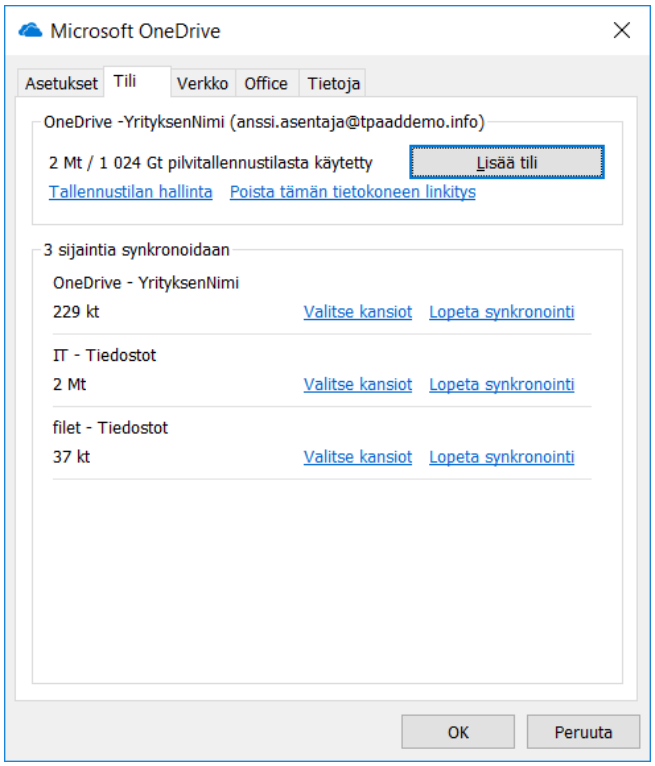
Kuva 49. SharePoint-kirjaston synkronointi uudella OneDrive-sovelluksella.

Synkronointi on sivuston ohjeita seuraamalla nopeasti käyttöönotettu. Tein saman myös IT-alisivulle, johon Anssi Asentajalle annettiin oikeudet. Kuvassa 50 näkyy, että vaikka alisivu sijaitsee filet-pääsivuston alla SharePointissa, ne ovat samalla tasolla tietokoneelle synkronoituna. Kuvassa näkyy myös yksityisten tiedostojen käyttöön tarkoitetun OneDriven olevan toiminnassa SharePoint-kirjastojen rinnalla. Kuvasta näkee myös, että luvussa 5.3 Lisenssien jakaminen ja Azure AD:n nimeäminen määritelty Azure AD:n nimi tulee näkyviin myös OneDrive ja SharePoint-kirjastojen nimissä.



Kuva 50. Synkronoidut SharePoint-kirjastot ja henkilökohtainen OneDrive.

OneDrive for Business -synkronointisovelluksen suurin puute OneDrive-synkronointisovellukseen verrattuna on valikoiva synkronointi -toiminnon puuttuminen. Kuvassa 51 näkyy OneDrive-sovelluksen synkronoidut sijainnit, joista pääsee erikseen määrittämään jokaiselle kohteelle synkronoitavat kansiot. Näin ollen kaikista pilvessä sijaitsevista tiedostostoista ei tarvitse pitää paikallista kopioita, vaan tiedostoja voidaan ottaa tarpeen mukaan käyttöön tai pois käytöstä.



Kuva 51. OneDrive-sovelluksen synkronoitavat kohteet.

6 Ratkaisu 2: Azure Active Directory Domain Services

Insinöörityön toinen ratkaisu vaatii toimiakseen käyttöönotetun Azure AD:n, joka laajennetaan Microsoftin ylläpitämäksi toimialueeksi (Azure AD DS). Käyttäjän identiteettinä käytetään Azure AD:n tunnuksia, ja erillistä laitehallinta ratkaisua ei oteta käyttöön, vaan siihen voi käyttää Intunea. Tämä ratkaisu voidaan laajentaa suoraan ensimmäisessä vaihtoehdossa esitellyn ratkaisun jatkeeksi, mikä mahdollistaa Active Directoryn autentikointia hyödyntävien sovelluspalvelimien rakentamisen pilveen käyttäen olemassa olevia tunnuksia autentikointiin.

Tässä ratkaisussa ei oteta erikseen Office 365 -palveluita käyttöön, koska toteutus olisi samanlainen kuin ratkaisussa 1. SharePoint-tiedostonjakoratkaisun sijaan tässä rakennetaan toimialueeseen liitetty virtuaalikone, jolla toteutetaan käyttäjille tiedostonjakoratkaisu VPN-yhteyden välityksellä. Azuren virtuaaliverkkoon (VNET) luodaan Point-to-Point-VPN-yhteys, jolloin yhteyden muodostamista varten käyttäjien koneille täytyy konfiguroida VPN-yhteys. Tiedostot eivät ole käytettävissä julkisessa internetissä, vaan käyttäjien täytyy muodostaa suojattu VPN-yhteys käyttääkseen tiedostopalvelimen tiedostoja.

6.1 Azure Active Directory Domain Services -palvelu

Azure Active Directory Domain Services tarjoaa Microsoftin ylläpitämän vikasietoisen toimialueen, jossa on kaksi Domain Controlleria. Tämä vapauttaa yrityksen palvelimen ylläpitotöistä, kuten tietoturvapäivityksistä, varmuuskopioinneista, ongelmien ratkomisista ja suojauksien toteuttamisesta.

Kaikki tavallisen Active Directoryn ominaisuudet eivät ole käytettävissä, mutta palvelu on Microsoftin jatkuvan kehityksen alla. Palveluun ei voi esimerkiksi lisätä uutta Domain Controlleria tai laajentaa Active Directoryn skeemaa (schema). Azure AD DS mahdollistaa toimialueen rakentamiseen virtuaaliverkkoon yksinkertaisesti, ja siihen liittyneet palvelimet voivat hyödyntää tuettuja ominaisuuksia, kuten LDAP:a, Kerberosta, NTLM:ää ja Group Policya.

Domain Controllereihin ei voi yhdistää etätyöpöytäyhteydellä, mutta niitä voi hallita toimialueeseen liittyneellä Windows-virtuaalikoneella asentamalla siihen RSAT (Remote Server Administration Tools) feature. RSAT-paketti on joukko työkaluja, jotka mahdollistavat etänä palvelinten palveluiden hallinnan, kuten Active Directoryn, DNS:n ja DHCP:n. RSAT-paketin voi asentaa myös Windows 10:lle, mutta tässä ratkaisussa ei työasemilla ja Domain Controllereilla ole suoraa yhteyttä, joten palveluiden hallinta ei onnistu työasemasta käsin. Tämän takia RSAT-paketti asennetaan luotavalle tiedostopalvelimelle. (59.)

6.2 Käyttöönotto

Verkkojen esivalmistelut

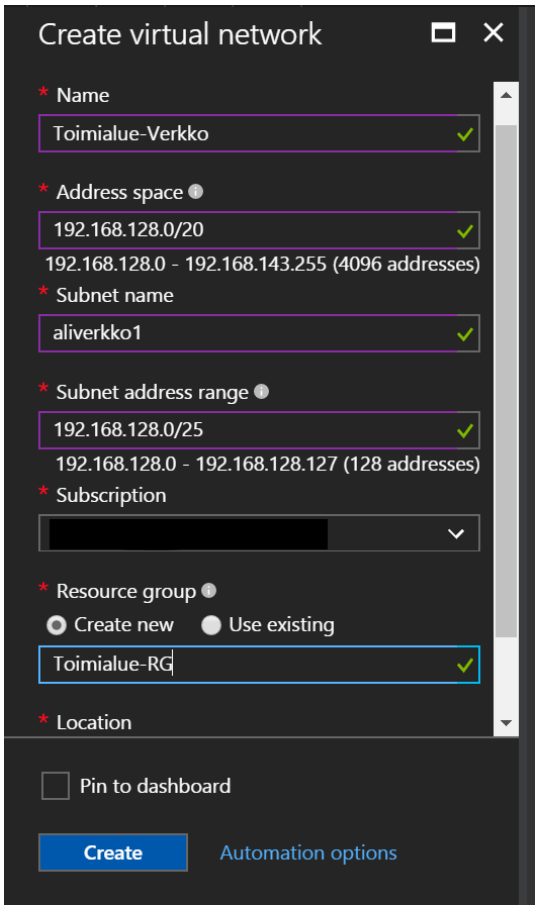
Azure AD DS:lle täytyy määrittää virtuaaliverkko, johon DC:t luodaan ja johon toimialuepalvelut tulevat käytettäväksi. Tällä hetkellä palvelu on saatavilla ainoastaan vanhan portaalin puolella, ja näin ollen se on mahdollista ottaa käyttöön vain vanhan puolen virtuaaliverkossa. Vanhan puolen ja uuden puolen verkkojen yhdistämisessä on rajoituksia, minkä takia tässä ratkaisussa käytetyllä konfiguraatiolla työasemilla ei ole yhteyttä vanhan puolen verkkoon, jossa DC:t sijaitsevat.

On suositeltavaa ottaa kaikki uudet palvelut käyttöön uudella puolella, minkä takia sovelluspalvelimet luodaan uudelle puolelle. Uuden ja vanhan puolen virtuaaliverkot ovat erilaisia, eikä uuden puolen virtuaalikonetta voi määrittää käyttämään vanhan puolen virtuaaliverkkoa. Uudelle puolelle luotavien sovelluspalvelimien ja Domain Controllereiden kommunikoinnin mahdollistamiseksi täytyy luoda yhteys vanhan ja uuden puolen virtuaaliverkkojen välille. Taulukossa 2 on havainnollistettu luotujen virtuaaliverkkojen ja aliverkkojen osoiteavaruudet. Taulukossa on myös myöhemmin määriteltävä VPN-yhdyskäytävän aliverkko. Kuten taulukosta huomaa, verkko tarvitsee aliverkosta kaksi osoitetta, minkä lisäksi Azure varaa palveluilleen vielä kolme osoitetta. (59.)

Taulukko 2. Ratkaisu 2:ssa käytettävien verkkojen osoiteavaruudet.

Portaali	**Verkon/aliverkon nimi**	**Osoiteavaruus**	**Ensimmäinen käyttävissä oleva osoite**	**Viimeinen käyttävissä oleva osoite**
Vanha	Domain-VNET-Classic	10.0.128.0/20	10.0.128.4	10.0.143.254
Vanha	aliverkko-1	10.0.128.0/25	10.0.128.4	10.0.128.126
Uusi	Toimialue-Verkko	192.168.128.0/20	192.168.128.4	192.168.143.254
Uusi	aliverkko1	192.168.128.0/25	192.168.128.4	192.168.128.126
Uusi	GatewaySubnet	192.168.143.192/26	192.168.143.196	192.168.143.254

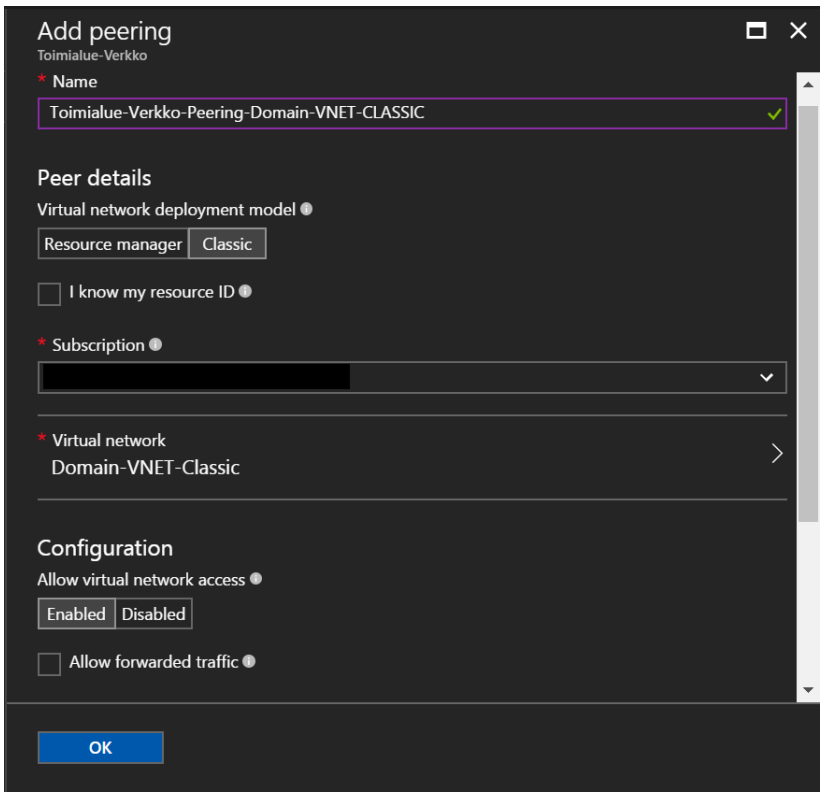
Kuvassa 52 on nähtävissä uuden portaalin Toimialue-Verkko virtuaaliverkon ja sen aliverkko: ”aliverkko1”:n luominen.



Kuva 52. Virtuaaliverkon luominen Azuressa.

Virtuaaliverkot voidaan yhdistää joko VPN-yhteydellä, tai jos ne sijaitsevat samalla alueella (Region), ne voidaan yhdistää VNET-Peering-tekniikalla. VPN:ssä täytyy maksaa yhdyskäytävän (Gateway) kustannuksista 22,59 €/kk – 784,27 €/kk. Datansiirtokustannuksia ei ole saman alueen välisessä datansiirrossa. VNET-peeringin kustannukset muodostuvat käytön mukaan, ja ne ovat tällä hetkellä 0,009 € gigatavulta sisään ja ulos verkosta. (60; 61.)

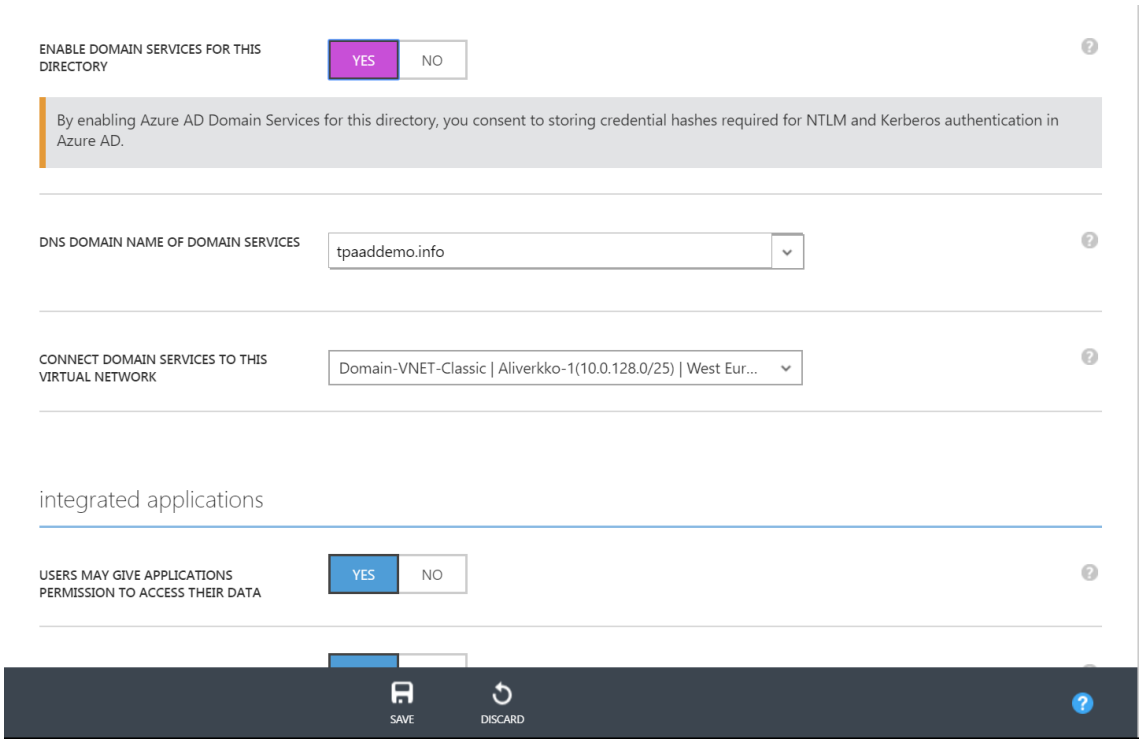
Kun Azure AD DS -palvelu saadaan toimimaan uudessa portaalissa, voidaan palvelimet ja DC:t luoda samaan verkkoon, jolloin verkkojen yhdistäminen on tarpeetonta. Nyt kuitenkin toteutin sen edullisemmalla ja yksinkertaisemmalla vaihtoehdolla eli VNET-peering-tekniikalla. Virtuaaliverkon asetuksissa on kohta peering, josta pääsee lisäämään uuden peering-yhteyden (kuva 53).



Kuva 53. Virtuaaliverkon uusi peering-yhteys.

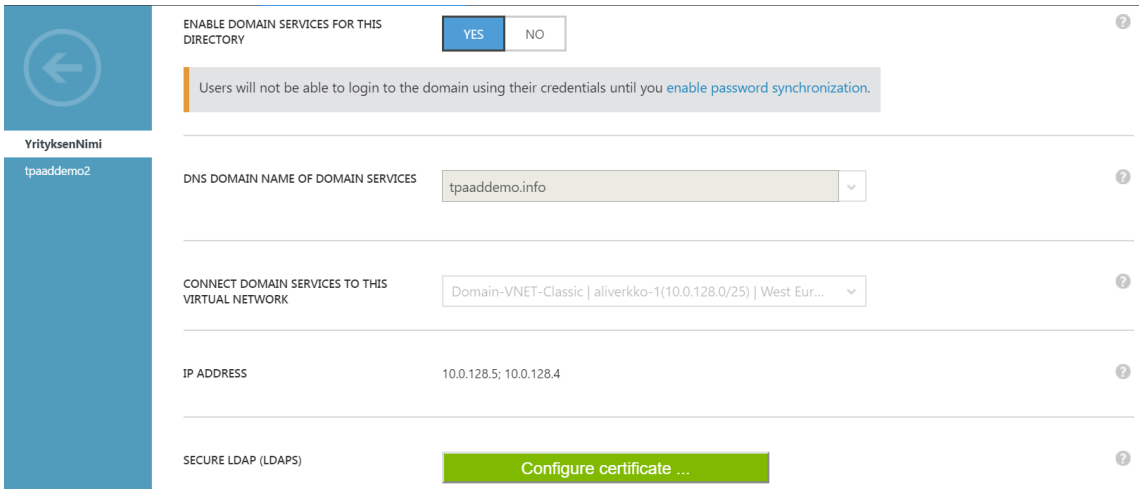
Toimialuepalveluiden käyttöönotto

Azure AD DS otetaan käyttöön vanhassa portaalissa Azure AD:n configure -valikosta valitsemalla ENABLE DOMAIN SERVICES FOR THIS DIRECOTRY -kohdassa YES, valitsemalla Azureen liitetyistä hakemistoista Domain-nimi ja määrittämällä, mihin virtuaaliverkkoon DC:t luodaan (kuva 54). Muutokset tallennetaan portaalin SAVE-painikkeella, minkä jälkeen Domain Controllereiden luonti käynnistyy. Prosessi kestää useita kymmeniä minuutteja.



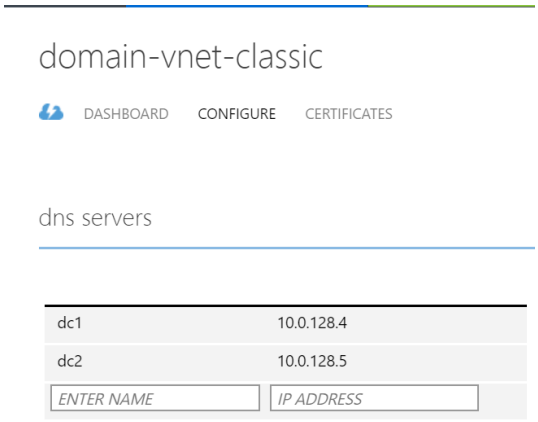
Kuva 54. Vanhan portaalin Azure AD DS -palvelun käyttöönotto.

Ensin Domain Services -kohtaan ilmestyy ensimmäisenä valmistuneen DC:n IP-osoite, ja toisen DC:n IP-osoite tulee vähän myöhemmin näkyviin (kuva 55). Molempiin virtuaaliverkkoihin konfiguroidaan nämä DC:t DNS-palvelimiksi, jotta virtuaaliverkkojen välinen nimenselvennys ja VPN-yhteyden kautta tulevat nimenselvityspyynnöt onnistuvat.



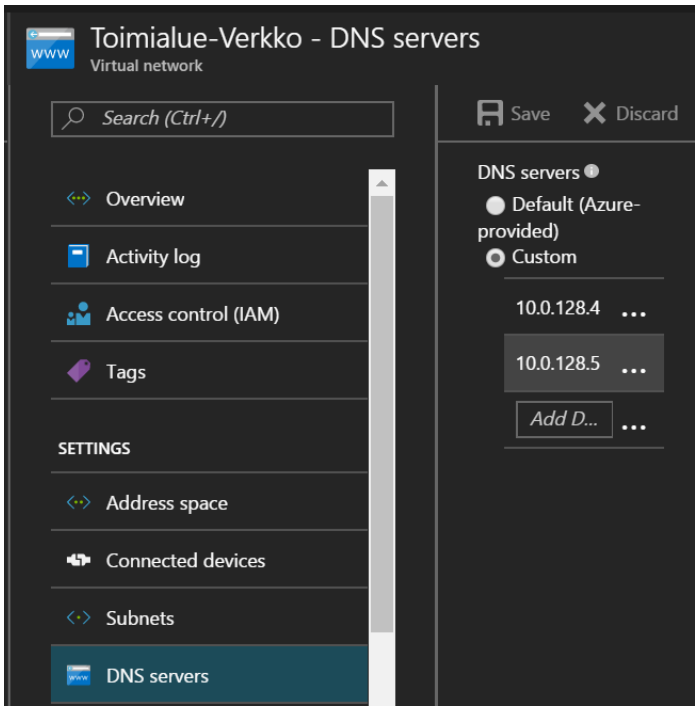
Kuva 55. Azure AD DS-palvelun valmis käyttöönotto.

Kuvassa 56 konfiguroidaan vanhan portaalin virtuaaliverkon DNS-palvelimet osoittamaan luotujen Domain Controllereiden IP-osoitteisiin. Palvelimille pitää määrittää nimet, esimerkiksi dc1 ja dc2, ja palvelimien osoitteet.



Kuva 56. Vanhan portaalin virtuaaliverkon asetukset.

Kuvassa 57 määritetään virtuaaliverkon DNS-palvelimet uudessa portaalissa, jossa ei tarvitse antaa nimeä, vaan pelkkä IP-osoite riittää (59).



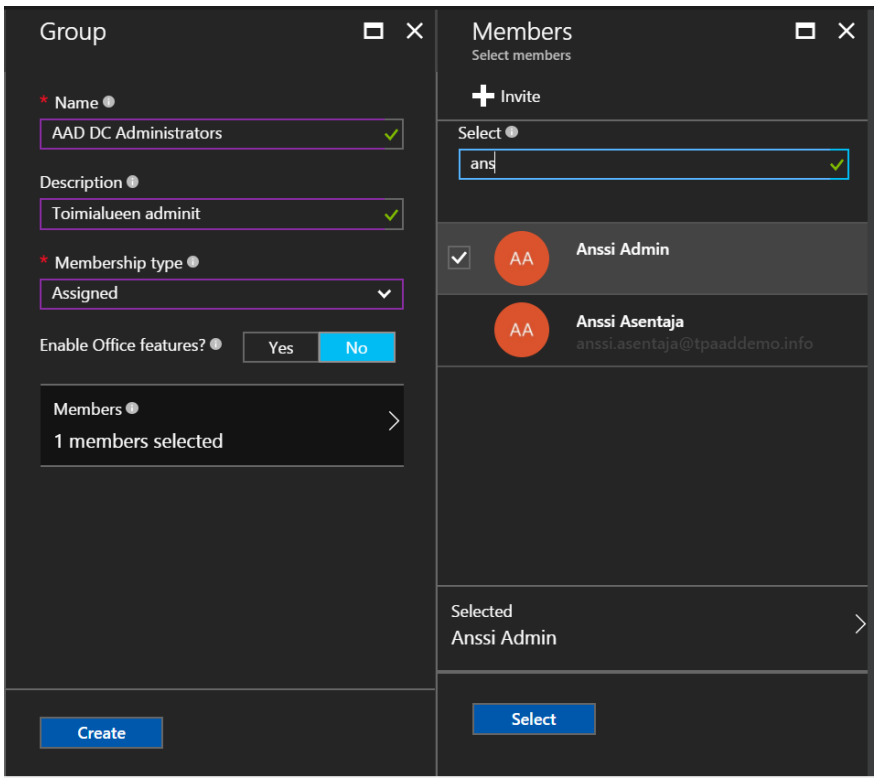
Kuva 57. Uuden portaalin virtuaaliverkon DNS-palvelimet.

Toimialueen järjestelmänvalvoja tunnuksen konfigurointi

Azure AD DS -palvelussa ei ole mahdollista saada Domain- tai Enterprise Administrator -tason tunnuksia. Jotta toimialueeseen voisi liittyä ja Domain Controllereita hallita, tarvitaan käyttäjätunnus, jolla on tavallista käyttäjää enemmän oikeuksia. Azure Active Directoryyn pitää tehdä erityinen järjestelmänvalvojaryhmä, jonka jäsenillä on oikeus liittyä toimialueeseen.

Tämän ryhmän nimeksi tulee antaa tarkalleen ”AAD DC Administrators”, jotta sen jäsenet saavat järjestelmänvalvojan oikeuksia. Ryhmän jäsenet on toimialueeseen liittyneissä koneissa lisätty paikalliseen järjestelmänvalvojat (Local Administrators) -ryhmään ja sallittu etätyöpöytäyhteyden muodostaminen näihin koneisiin. Azure AD DS -palvelun Domain Controllereihin ei voi muodostaa etätyöpöytäyhteyttä, ja rajoitus pätee myös tämän ryhmän käyttäjiin.

Palvelinten ylläpitoa ja konfiguroimista varten luodaan anssi.admin-käyttäjätunnus ja tunnus liitetään AAD DC Administrators -ryhmään sen luontivaiheessa (kuva 58). Anssi Asentajalle luotiin erillinen järjestelmänvalvoja-tunnus palvelimien hallintaa varten. Järjestelmänvalvojan tunnuksia ei kannata käyttää päivittäisessä käytössä tietoturvallisuuden takia, ja tunnus kannattaa nimetä vähemmän ilmiselväksi, mutta tämän insinöörityön luettavuuden vuoksi tunnus on liitetty Anssi Asentajan henkilöllisyyteen.



Kuva 58. Käyttäjän lisääminen AAD DC Adminstrators -ryhmään.

Salasana synkronoinnin käyttöönottaminen

Käyttäjien pitää vielä vaihtaa salasana, jotta tunnistautuminen alkaa toimimaan virtuaaliverkon toimialueessa. Azure AD DS tarvitsee tunnuksien salasanatiivisteet (credential hashes) autentikoidakseen käyttäjiä. Azure AD:ssa ei ole tähän tarkoitukseen sopivia tiivisteitä, eikä se osaa niitä automaattisesti tehdä. Kun Azure AD DS on otettu käyttöön ja käyttäjä vaihtaa salasanan, Azure AD luo tiivisteen ja replikoi sen Azure AD DS:n Domain Controllereille, jolloin autentikointi alkaa toimia salasanan vaihtaneelle käyttäjälle. Kaikkien käyttäjien täytyy siis vaihtaa salasana luodakseen salasanatiiviiste. (59.)

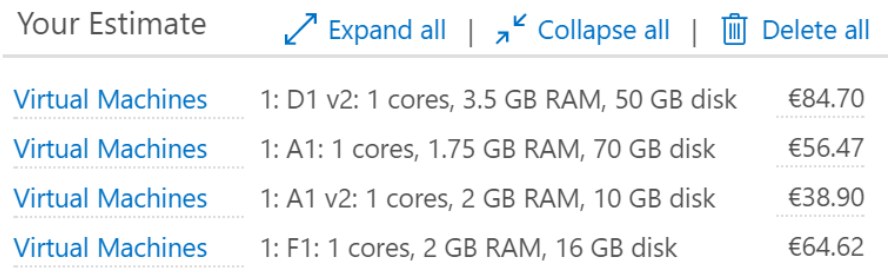
6.3 Tiedostopalvelin

Tiedostopalvelimeksi valittiin ensin 84,70 euroa kuukaudessa maksava D1_V2-virtuaalikone, jossa on yksi virtuaalinen suoritin (vCPU), 3,5 GB muistia ja tuki kahdelle virtuaaliselle kiintolevylle, kummallekin 500 IOPS:n (Input/Output Operations Per Second) suorituskyky. Tärkeimpänä valintaperusteena oli hinta ja kohtuullinen suorituskyky. Kun tiedostopalvelin oli testattu käytössä, sen malliksi vaihdettiin ensin A1 ja sen jälkeen A1_v2, ja testattiin näillä malleilla, muuttuuko tiedostojen lisäämiseen palvelimelle kuluva aika

yhden koneen tiedonsiirrossa. Havaittiin, ettei tiedostojen siirtämiseen käytetty aika muuttunut merkittävästi ottaen huomioon verkon nopeuden satunnaiset vaihtelut ja ettei tälle testille oltu luotu häiriöttömiä olosuhteita. Tarkemmat vertailut eri ratkaisujen välisistä tiedonsiirtonopeustesteistä ovat luettavissa insinöörityön yhteenvetoluvussa.

A-sarjan virtuaalikoneissa on keskenään samantehoinen prosessori, mutta uudempi versio (v2) tarjoaa enemmän muistia vähemmällä hinnalla. D_V2- ja F-sarjassa on myös saman tehoinen, A-sarjaa huomattavasti tehokkaampi prosessori. F-sarja tarjoaa samaa prosessointitehoa vähemmällä keskusmuistilla ja halvemmalla hinnalla verrattuna D-sarjaan. (62; 63.)

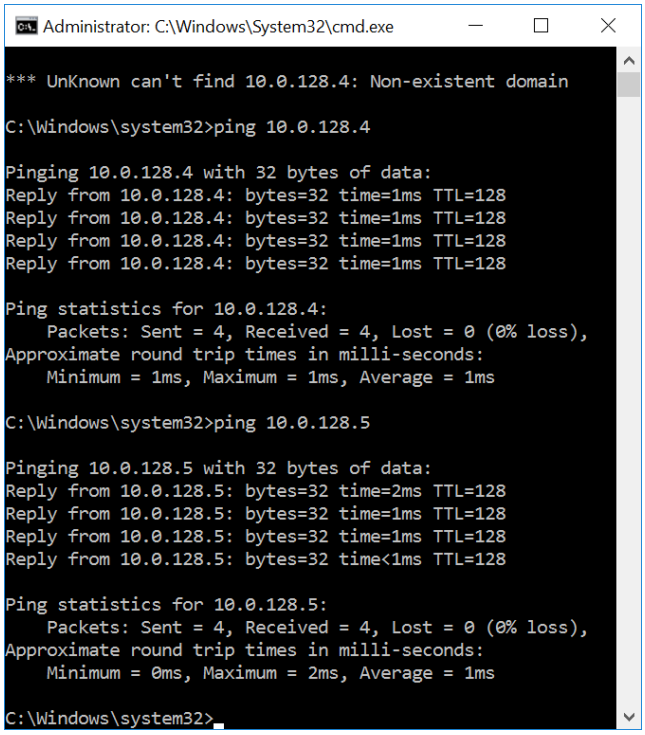
Jälkeenpäin tarkasteltuna A1:n testaaminen oli turha A1_V2:n edullisemman hinnan ja isomman keskusmuistin määrän vuoksi. F-sarjalaista ei myöskään tässä ratkaisussa testattu, mutta sitä käytetään ratkaisu 3:ssa. F1-tarjoaa edullista suorituskykyä ja samanhintaisessa F1S:ssä on tuki SSD-levyille ja yhteensä 3200 IOPS:n suorituskyky kiintolevyille. SSD-levyjä ei lähdetty testaamaan, koska verkon nopeus on rajoittavin tekijä tiedostojen siirrossa VPN-yhteyden kautta. Yhteistä kaikilla mainituilla konemalleilla on yhden virtuaalisen suorittimen (vCPU) käyttö ja tuki kahdelle kiintolevylle. Konemallien ominaisuuksien vertailu ja hinnat Länsi-Euroopan datakeskukselle ovat nähtävissä kuvassa 59. Kuvassa näkyvät myös eri konemallien väliaikaislevyjen koot, joita ei voi käyttää pysyvään tiedostojen tallennukseen. (63; 64.)



Kuva 59. Azuren virtuaalikonemallien vertailua (63).

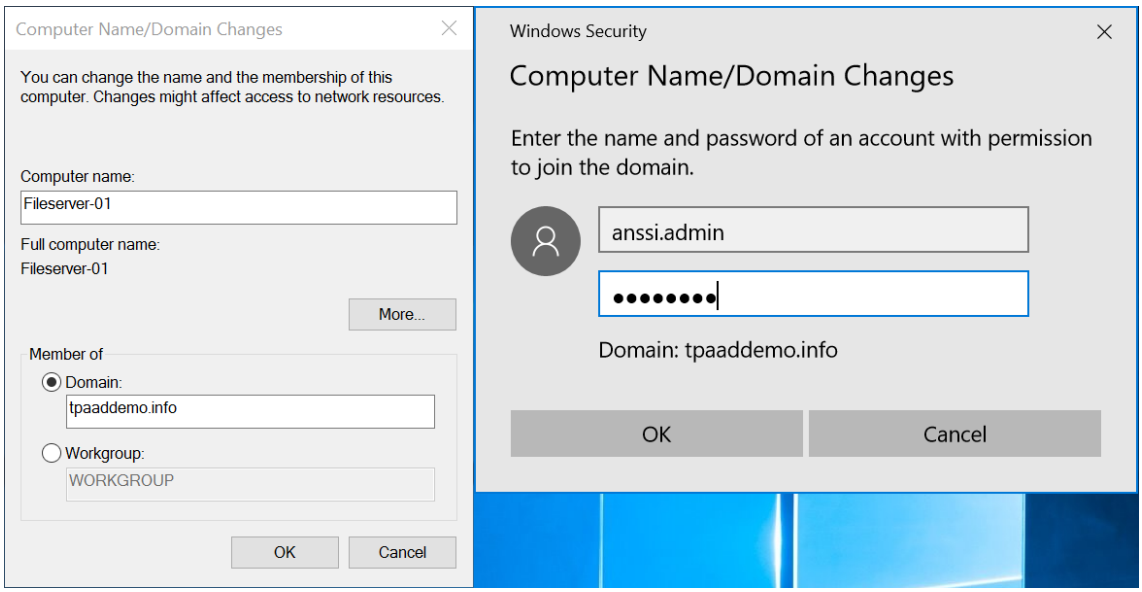
Tiedostopalvelimen valmistelu

Kun Windows Server 2016 -virtuaalikone on luotu ja saatu käyntiin, testataan verkon toimivuus pingaamalla Domain Controllereita. Ennen pingausta testasin nslookup-komentoa, josta jäi epäonnistumisen teksti kuvaan 60. Sen jälkeen onnistuin pingaamaan molempia Domain Controllereita. Nslookupilla voi testata, onko palvelin luonut reverse lookup zoneen PTR-tietueen, jolla voidaan tehdä IP-osoitteelle nimenselvennys tietokonenimeksi (hostname), ja pingillä voi testata, onko testattavalla koneella verkkoyhteys määriteltyyn IP-osoitteeseen, olettaen ettei pingausta ole estettynä verkossa.



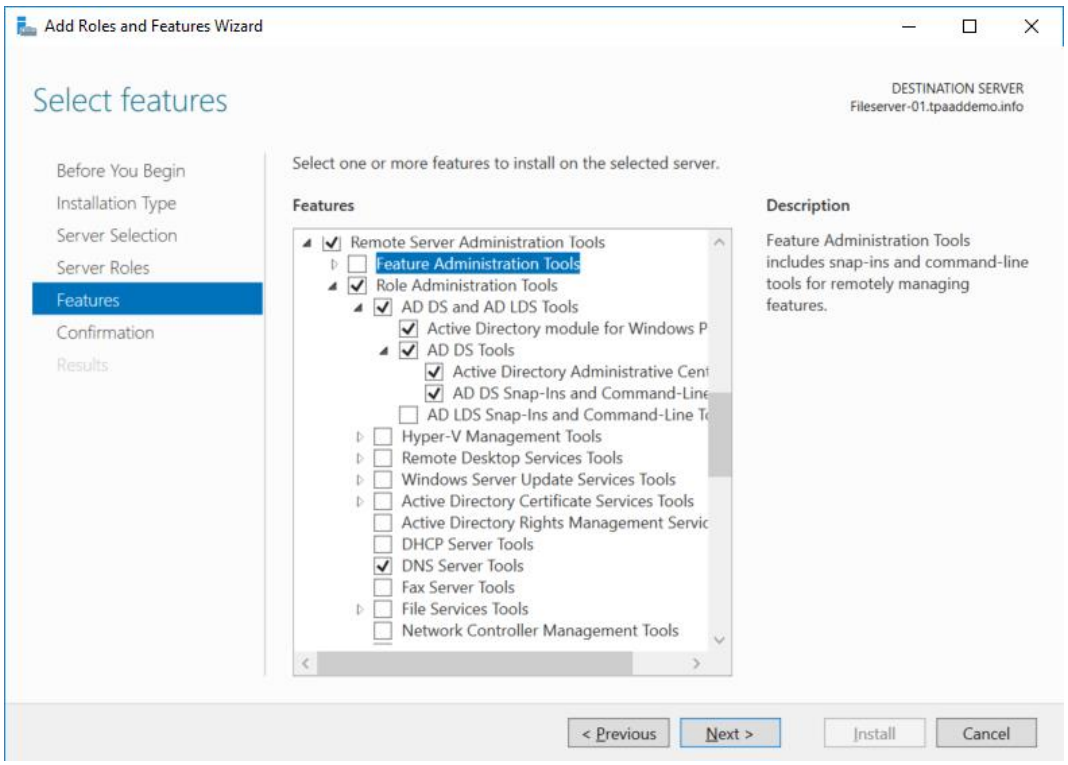
Kuva 60. Domain Controllereiden pingaus.

Kun yhteyden toimivuus varmistettu on, liitetään tiedostopalvelin osaksi toimialuetta (kuva 61). Toimialueen nimi on konfiguroitu Azure AD DS:n asetuksissa, ja liittymiseen käytetään AAD DC Administrators -ryhmän anssi.admin -jäsentä.



Kuva 61. Toimialueeseen liittyminen.

Kun palvelin on liitetty onnistuneesti toimialueeseen ja uudelleenkäynnistyksen jälkeen kirjauduttu sisään toimialueen anssi.admin-tunnuksella, käynnistetään roolien ja toimintojen asennusohjelma (Add Roles and Features). Active Directoryn hallintaan valitaan ”Remote Server Administration Tools” -toiminnon alta ”AD DS and AD LDS Tools” -toiminto ja sen lisäksi DNS:n hallintaan valitaan DNS Server Tools -toiminto ja asennetaan ne (kuva 62).

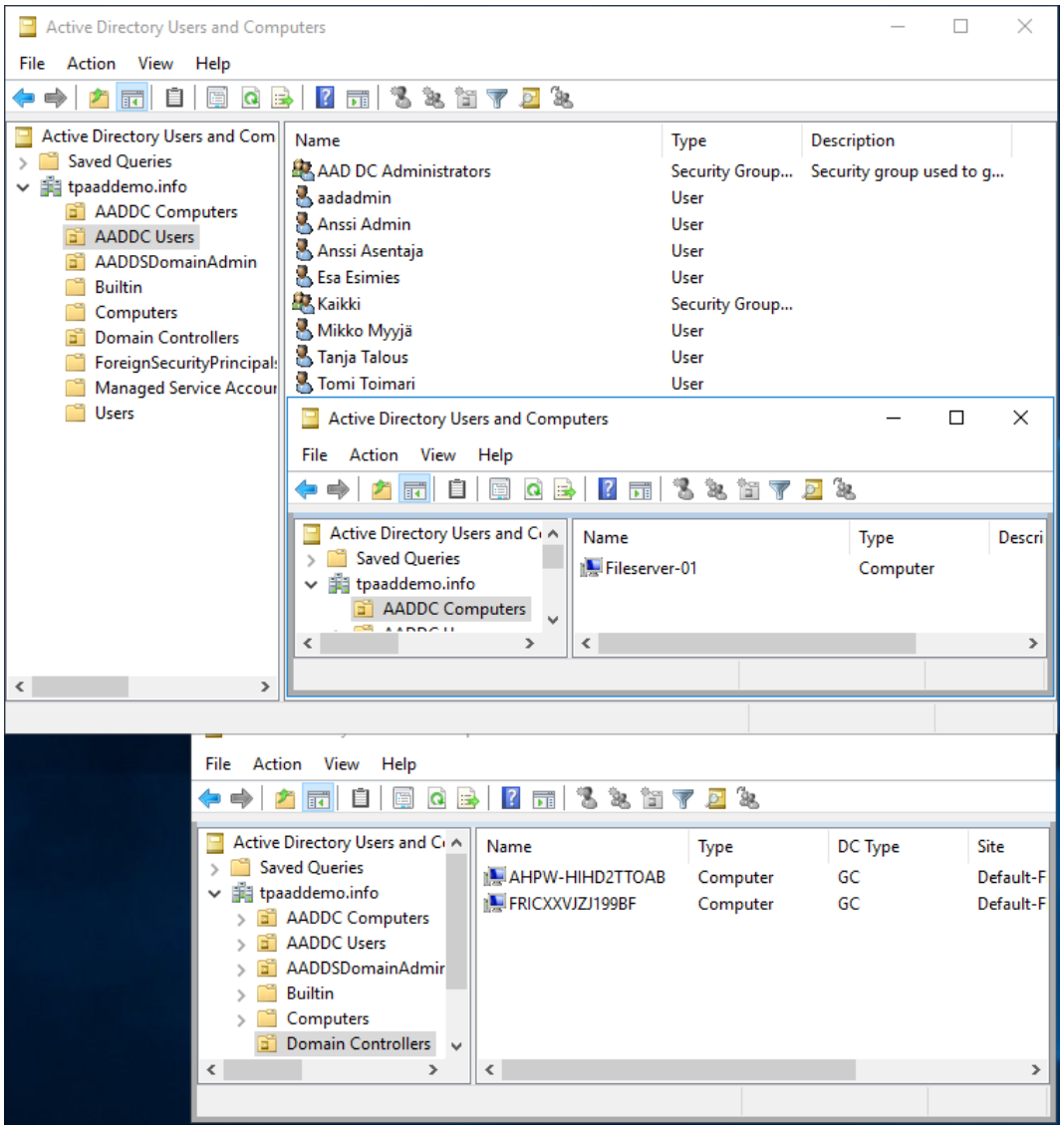


Kuva 62. RSAT-työkalujen asennus Windows Server 2016:ssa.

RSAT-työkalujen asennuksen jälkeen tiedostopalvelimella on muun muassa seuraavat työkalut toimialueen hallintaan:

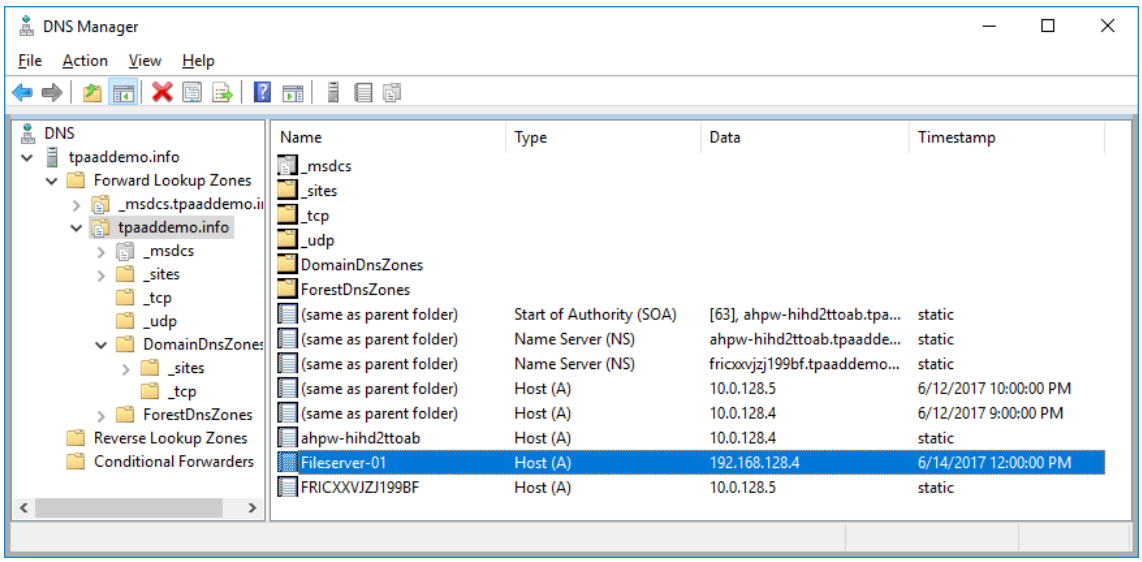
- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Module for Windows Powershell
- Active Directory Sites and Services
- Active Directory Users and Computers.

Kaikissa työkaluissa ei ole käytettävissä kaikkia toimintoja, käyttäjätunnuksen rajoitetuttujen oikeuksien vuoksi. Tarkastelemalla Active Directory Users and Computers -työkalulla AADDC Users -säilöä voidaan todeta kaikkien käyttäjien replikoituneen Azure AD:sta (kuva 63). Eri säilöjä tutkimalla voidaan varmistaa myös tiedostopalvelimen konetunnuksen olemassaolo toimialueessa ja nähdään palvelun luomien Domain Controllereiden konetunnukset.



Kuva 63. Active Directory Users and Computers -työkalun näkymä.

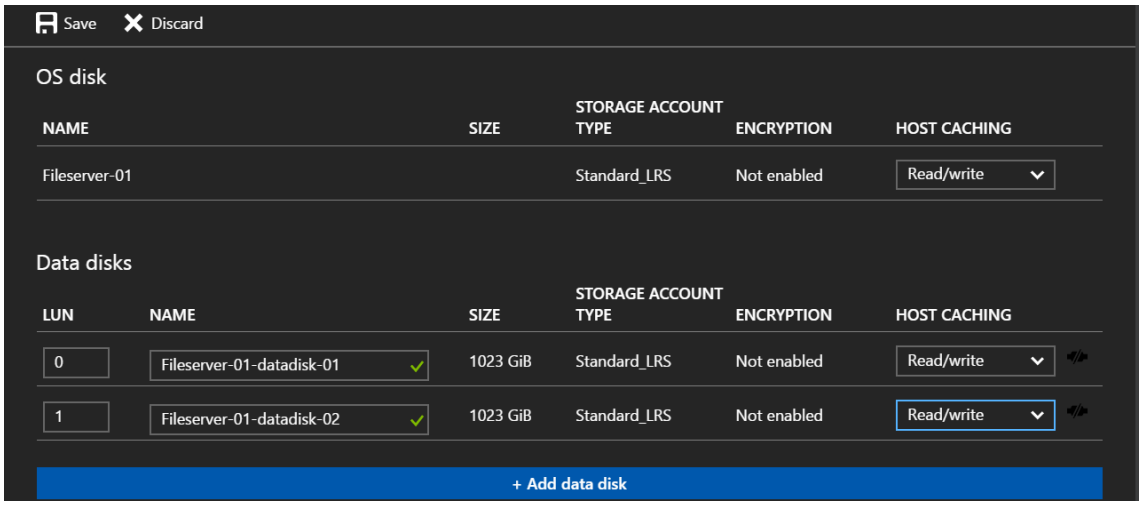
DNS managerilla päästään hallitsemaan toimialueen DNS-palveluita. Sitä tutkimalla huomaa, ettei reverse lookup zonea ole määritetty. Kuvasta 64 näkyy, että tiedostopalvelimelle on luotu oma A-tietue, ja myös Domain Controllereiden valmiiksi luodut A-tietueet ovat nähtävissä. Valmiiksi luotuja tietueita ei pidä mennä muuttamaan, tai koko palvelun toiminta saattaa häiriintyä. (59.)



Kuva 64. DNS-näkymä Azuren ylläpitämästä toimialueesta.

Tiedostopalvelimen käyttöönotto

Lisäsin Azuren portaalista tiedostopalvelimelle kaksi levyä virtuaalikoneen Disks-kohdasta (kuva 65). Levyn enimmäiskoon raja oli ennen 1 023 GB, nykyään raja on 4 095 GB. SSD-levyjä ei luotu kustannussyistä, ja niiden suorituskykyä ei myöskään tarvita tähän käyttötarkoitukseen.



Kuva 65. Azuressa levyjen lisäys virtuaalikoneeseen.

Virtuaalilevyistä luodaan Windows Server 2016:een esiasennetulla File and Storage Services -roolilla kokonaislevykapasiteetin yhdistävä, kahden teratavun storage pool, josta luodaan samankokoinen virtuaalilevy. Virtuaalilevyn storage layoutiksi valitaan ”Simple”,

joka vastaa RAID-0:aa. Tällöin data kirjoitetaan tasaisesti molemmille levyille. Virtuaalilevystä voi luoda haluamansa kokoisia osioita, mutta tiedostonjaolle käytetään yhtä, koko storage poolin ja virtuaalilevyn kapasiteetin käyttävää osiota.

Muut konfiguraatiot mahdollistavat datan säilymisen ja storage poolin toiminnan jatkumisen, jos jokin levyistä rikkoutuu. Azuressa on kuitenkin jokaisesta levystä kaksi muuta kopiota samassa datakeskuksessa, storage accountin datakeskuksen paikallisella (Locally-redundant storage) replikointikonfiguraatiolla, joten levyjen vikasietoisuutta ei tarvita enää käyttöjärjestelmästä käsin. Simple-konfiguraatiolla on koko levyjen muodostama kapasiteetti käytössä, ja se on myös vaihtoehdoista suorituskykyisin, vaikka verkkoyhteys onkin suorituskyvyn rajoittavin tekijä.

Kun storage poolista on luotu koko sen kapasiteetin käyttävä osio, voidaan sinne luoda kansioita, määrittää niille tarvittavat oikeudet ja jakaa ne verkon kautta. Jokaiselle käyttäjäroolille luodaan omat kansiot, ja käyttäjille annetaan täydet oikeudet omaan kansioonsa. Sen lisäksi Tomi Toimarille määritetään luku- ja kirjoitusoikeudet kaikkiin kansioihin ja luodaan avoin- ja yhteiset-kansiot, joihin kaikilla käyttäjillä on luku- ja kirjoitusoikeudet.

Käyttäjärooleille kannattaa tehdä ryhmä, liittää käyttäjät ryhmään ja antaa kansion oikeudet ryhmälle. Näin uusi henkilö voidaan liittää osaksi ryhmää, ja henkilö saa samat käyttöoikeudet kuin muutkin ryhmän jäsenet, ilman että henkilölle tarvitsee erikseen antaa oikeuksia useisiin paikkoihin.

Tiedostojako olisi voitu toteuttaa myös yhdellä levyllä tai luomalla RAID-0-tasoinen konfiguraatio levynhallinnasta. Storage pool on näistä vaihtoehdoista ketterin, ja sen käytössä olevien kansiojakojen kapasiteettia voi kahden levyn simple-konfiguraatiossa kasvattaa lisäämällä parillinen määrä levyjä.

Vaikka levyjen vikasietoisuutta ei tarvitsekaan enää luoda virtuaalikoneesta käsin, ei Azuren levyjen vikasietoisuus ole varmuuskopiointiratkaisu, vaan se täytyy toteuttaa erikseen. Azuren vikasietoisuus ei suojaa eikä auta palauttamaan vahingossa tai väärän konfiguroinnin vuoksi poistettuja tiedostoja. Azuressa on varmuuskopiointia varten Azure Backup -palvelu, joka otetaan käyttöön.

6.4 Point-to-Site-VPN-yhteyden määritys PowerShellilla

Yrityksen työntekijöille täytyy luoda yhteys vielä Azuren virtuaaliverkkoon, jotta he voivat käyttää tiedostopalvelinta. Suojatun VPN-yhteyden määrittäminen Azuren portaalista kuvataan tarkemmin ratkaisu 3:ssa. Tässä ratkaisussa luodaan VPN-yhteys uuden portaalin Toimialue-Verkko-virtuaaliverkkoon, jossa tiedostopalvelin on. Tiedostopalvelimella on yhteys vanhan portaalin Domain-VNET-Classic-virtuaaliverkkoon VNET-Peeringillä, mutta yhteys on vain näiden verkkojen välinen tällä konfiguraatiolla, jolloin VPN-yhteyden kautta ei ole pääsyä Domain Controllereihin.

Tein VPN-yhteyden tässä ratkaisussa PowerShellillä. Käytetty skripti näkyy esimerkkikoodissa 1. Yhdyskäytävän luonnissa komennolla New-AzureRmVirtualNetworkGateway PowerShell antoi Internal server errorin statuskoodilla 500, mikä saattoi johtua resurssien nimeämisestä isoilla kirjaimilla. Päädyin tekemään tämän vaiheen eli yhdyskäytävän luomisen portaalista käsin (kuva 66), jonka luominen kesti 36 minuuttia. Tämän jälkeen piti vielä määrittää VPN-clienttien käyttämät osoitteet (address pool) ja lisätä autentikointiin käytettävä julkinen avain Azureen, mitkä edellä mainittu komento olisi onnistuessaan suorittanut. VPN-yhdyskäytävän luonnin jälkeen samalla skriptillä ladataan Azuresta VPN-yhteyden asennusohjelma, jonka voi asentaa työntekijän koneelle. VPN-clientin voi ladata myös portaalista yhdyskäytävän asetuksista, kun yhdyskäytävä on konfiguroitu valmiiksi.

```
Login-AzureRmAccount
Get-AzureRmSubscription
Select-AzureRmSubscription -SubscriptionName "Sinun Tilauksesi"

$VNetName  = "Toimialue-Verkko"
$SubName = "aliverkko1"
$GWSubName = "GatewaySubnet"
$GWSubPrefix = "192.168.143.192/26"
$VPNClientAddressPool = "192.168.100.0/24"
$RG = "Toimialue-RG"
$Location = "West Europe"
$GWName = "Toimialue-Verkko-GW"
$GWIPName = "Toimialue-verkko-GWPIP"
$GWIPconfName = "gwipconf"


$Vnet = Get-AzureRmVirtualNetwork -Name $VNetName -ResourceGroupName $RG
add-AzureRmVirtualNetworkSubnetConfig -Name $GWSubName -AddressPrefix
$GWSubPrefix -VirtualNetwork $VNet
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet

$subnet = Get-AzureRmVirtualNetworkSubnetConfig -Name $GWSubName
-VirtualNetwork $vnet

$pip = New-AzureRmPublicIpAddress -Name $GWIPName -ResourceGroupName $RG
-Location $Location -AllocationMethod Dynamic
$ipconf = New-AzureRmVirtualNetworkGatewayIpConfig -Name $GWIPconfName -Subnet
$subnet -PublicIpAddress $pip
#Sertifikaatin luonti Powershellillä
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
```

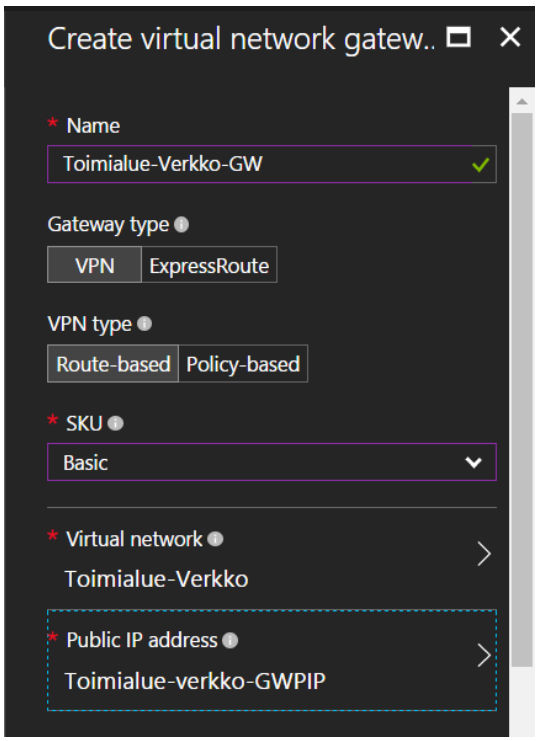
```
-Subject "CN=P2SRootCertti2017" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage
CertSign
# Exporttaa julkinen avain talteen certmg.msc työkalulla
New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SChildCertti2017" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
# Exporttaa yksityinen avain talteen certmg.msc työkalulla
$P2SRootCertName = "P2SRootCertti2017.cer"
$filePathForCert = "C:\Certit\Ratkaisu2-julkinenAvain.cer" # tähän exportattu
avain
$cert = new-object System.Security.Cryptography.X509Certificates.X509Certifi-
cate2($filePathForCert)
$CertBase64 = [system.convert]::ToBase64String($cert.RawData)
$p2srootcert = New-AzureRmVpnClientRootCertificate -Name $P2SRootCertName
-PublicCertData $CertBase64

New-AzureRmVirtualNetworkGateway -Name $GWName -ResourceGroupName $RG `
-Location $Location -IpConfigurations $ipconf -GatewayType Vpn `
-VpnType RouteBased -EnableBgp $false -GatewaySku Basic `
-VpnClientAddressPool $VPNClientAddressPool -VpnClientRootCertificates
$p2srootcert

# WARNING: The output object type of this cmdlet will be modified in a future
release.
#New-AzureRmVirtualNetworkGateway : An error occurred.
#StatusCode: 500
#ReasonPhrase: Internal Server Error
#OperationID : '477d7396-6768-45c5-9751-0438c23b4c76'
#At line:1 char:1
#+ New-AzureRmVirtualNetworkGateway -Name $GWName -ResourceGroupName $RG ...
#+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
#    + CategoryInfo          : CloseError: (:) [New-AzureRmVirtualNetworkGate-
way], NetworkCloudException
#    + FullyQualifiedErrorId : Microsoft.Azure.Commands.Network.NewAzureVirtu-
alNetworkGatewayCommand

Get-AzureRmVpnClientPackage -ResourceGroupName $RG `
-VirtualNetworkGatewayName $GWName -ProcessorArchitecture Amd64
# Komento antaa url-osoitteen, josta VPN-clientin voi ladata
"https://mdsbrketwprodsn1prod.blob.core.windows.net/cmakexe/e45733d1-ff08-
4d56-ae2a-56905f57ca96/amd64/e45733d1-ff08-4d56-ae2a-56905f57ca96.exe?sv=2015-
04-05&sr=b&sig=6NNWiyZs%2BAzbWmORHCudOKQI3etZlUV%2FDF
XDda3M4ZY%3D&st=2017-06-15T15%3A11%3A40Z&se=2017-06-
15T16%3A11%3A40Z&sp=r&fileExtension=.exe"
```

Esimerkkikoodi 1. VPN-yhdyskäytävän luominen.



Kuva 66. VPN-gatewayn luominen portaalista.

VPN-yhteyden määritys työasemalta

Sertifikaatin ja VPN-clientin asennuksen jälkeen voidaan työntekijän koneelta yhdistää VPN:llä Azuren virtuaaliverkkoon. Palvelimen jaettuihin kansioihin ei kuitenkaan saada yhteyttä, vaikka VPN-yhteys on muodostettu onnistuneesti ja pingaus ja etätyöpöytäyhteys tiedostopalvelimeen toimii. Tarkastelemalla palvelimen ja työaseman välistä verkkoliikennettä pakettianalysaattorilla huomataan kuvan 67 mukaisia virheilmoituksia, kun työasemalla yritetään päästä käsiksi verkkojakoon.

```
192.168.100.6   192.168.128.4   SMB2    232 Negotiate Protocol Request
192.168.128.4   192.168.100.6   SMB2    366 Negotiate Protocol Response
192.168.100.6   192.168.128.4   SMB2    519 Session Setup Request, INITIATOR_NEGO, INITIATOR_META_DATA
192.168.128.4   192.168.100.6   SMB2    153 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
192.168.100.6   192.168.128.4   SMB2    199 Session Setup Request, NTLMSSP_NEGOTIATE
192.168.128.4   192.168.100.6   SMB2    417 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
```

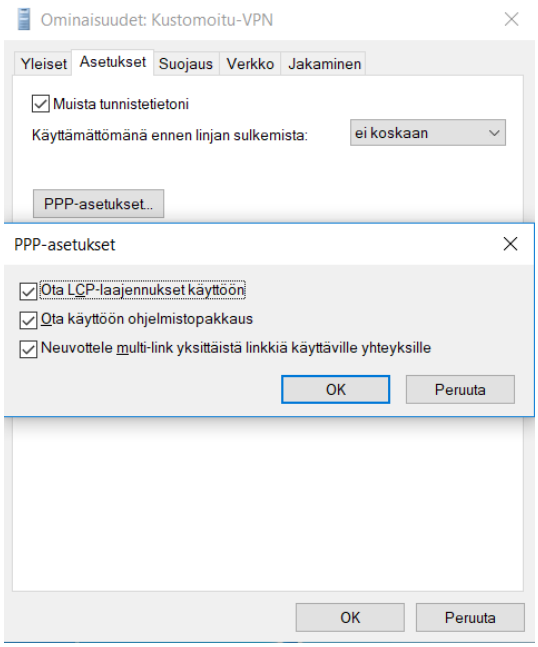
Kuva 67. Wiresharkin analyysi palvelimen ja työaseman välisestä verkkoliikenteestä.

Ongelma on yhteyden muodostuksessa verkkojakoon. Palvelimelle välittyy VPN-yhteyden tunnistetietoja, jolla ei ole oikeuksia verkkojakoon, eikä käyttäjä pääse syöttämään omia tietojaan. VPN-yhteyden konfiguraatiossa on UseRasCredentials=1-parametri, jonka arvon vaihtaminen nollaksi lopettaa virheellisten tunnistetietojen välittämisen palvelimelle. Tämän rasphone.pbk-konfiguraatiotiedoston muokkaaminen ei kuitenkaan

auta, koska yhteys ylikirjoittaa muutokset omalla konfiguraatiollaan aina yhteyden uudelleen muodostuksessa.

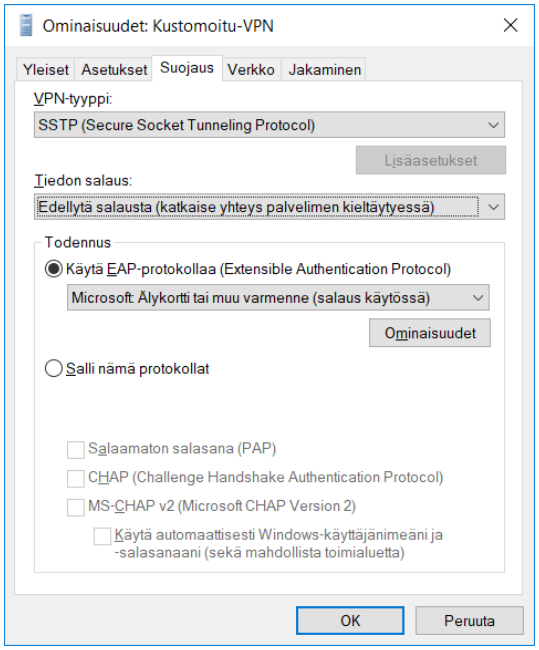
Tämän takia VPN-yhteys täytyy määrittää manuaalisesti ja määrittää se käyttämään Azuresta ladatusta VPN-clientista löytyvää tunneliosoitetta. Tunneliosoitteen saa purkamalla VPN-clientin asennustiedoston ja avaamalla .pbk-päätteisen tiedoston, tai jos VPN-clientti on asennettu, sen saa VPN-clientin Ominaisuudet > näytä loki -painikkeesta ja etsimällä lokista tunneliosoite-kohdan, joka on tässä yhteydessä seuraavanlainen: Tunneliosoite = azuregateway-e45733d1-ff08-4d56-ae2a-56905f57ca96-e899b98f56fe.cloudapp.net. Lokia tarkastelemalla voidaan myös huomata, että käyttäjänimen kohdalla lukee asennetun sertifikaatin nimi ja toimialue-kohta on tyhjä. Nämä seikat todennäköisesti aiheuttavat yhteyden epäonnistumisen verkkojakoon.

Luotaessa Windowsissa uutta VPN-yhteyttä täytyy yhteydelle määrittää nimi ja osoitteeksi äsken poimittu tunneliosoite, ja riippuen siitä mitä kautta yhteyden luo, mahdollisesti myös VPN-tyypiksi SSTP (Secure Socket Tunneling Protocol). Kun VPN-yhteys on luotu, Windows luo VPN-yhteydennimisen verkkosovittimen, jonka ominaisuuksista määritellään tarvittavat asetukset yhteyden muodostamista varten. Verkkosovittimen Yleiset-välilehdellä määritellään kohteen isäntänimeksi poimittu tunneliosoite. Asetukset-välilehdeltä määritellään PPP-asetukset kuvan 68 mukaisesti.



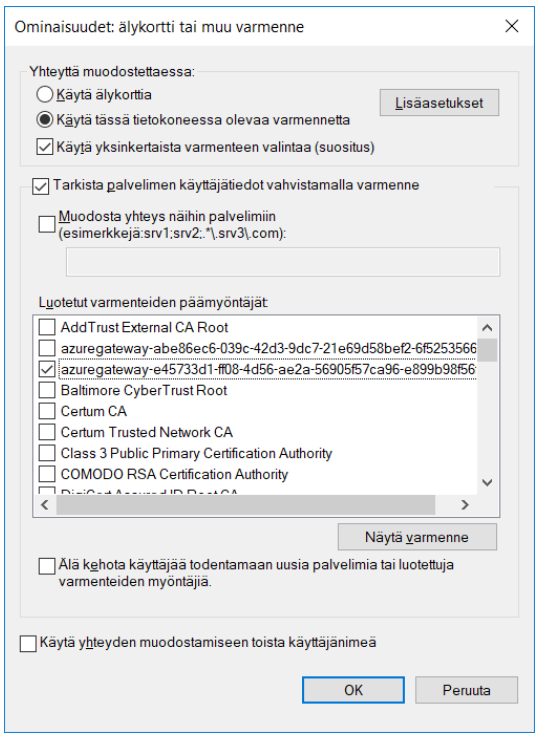
Kuva 68. VPN-yhteyden asetukset.

Suojaus-välilehdellä täytyy VPN-tyypiksi olla valittuna SSTP ja todennus konfiguroitu kuten kuvassa 69, jolloin Ominaisuudet-painikkeesta pääsee määrittämään sertifikaatin todennusta varten.



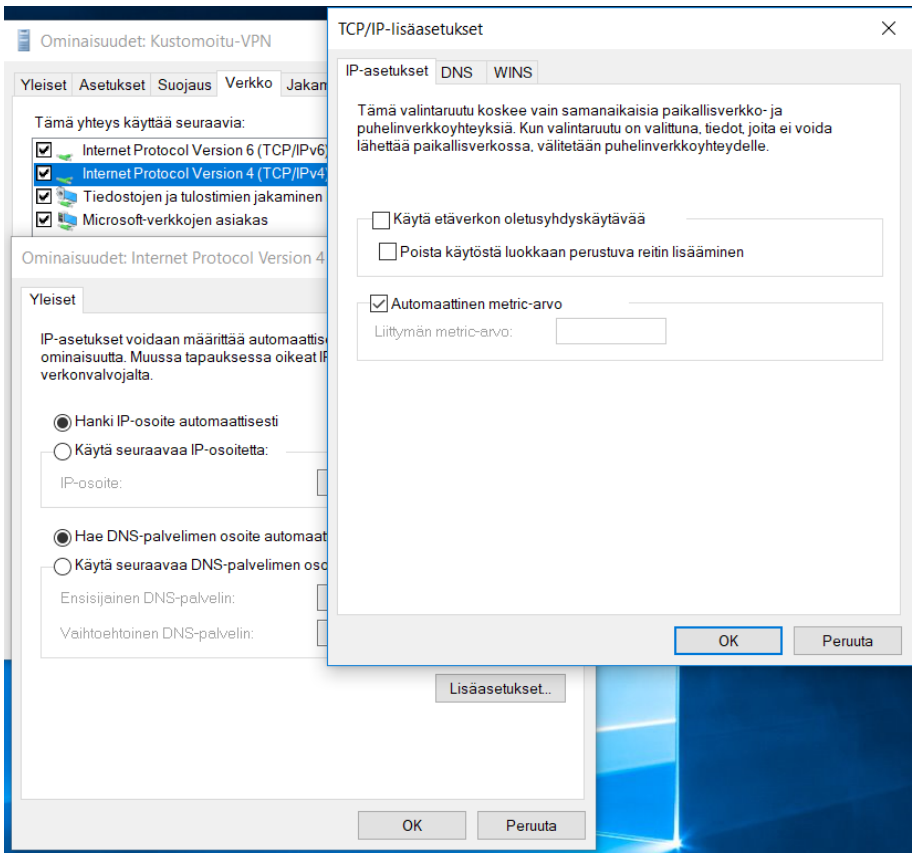
Kuva 69. VPN-yhteyden suojausasetukset.

Ominaisuudet-ikkunassa täytyy laittaa valinta kohtaan ”Käytä tässä tietokoneessa olevaa varmennetta” ja ottaa valinta pois kohdasta ”Muodosta yhteys näihin palvelimiin”. Yhteyden muodostamiseen käytettävä sertifikaatti täytyy olla asennettuna koneeseen, jolloin se valitaan käytettäväksi luettelosta ”Luotetut varmenteiden päämyöntäjät” (kuva 70).



Kuva 70. VPN-yhteyden todentamisasetukset.

Verkko-välilehdeltä konfiguroidaan ”Internet Protocol Version 4 (TCP/IPv4)” > ”Ominaisuudet” > ”Lisäasetukset” ja otetaan valinta pois kohdasta ”Käytä etäverkon oletusyhdyskäytävää” (kuva 71). Näin estetään kaiken internetiin tarkoitetun liikenteen menemistä VPN:n lävitse Azureen.

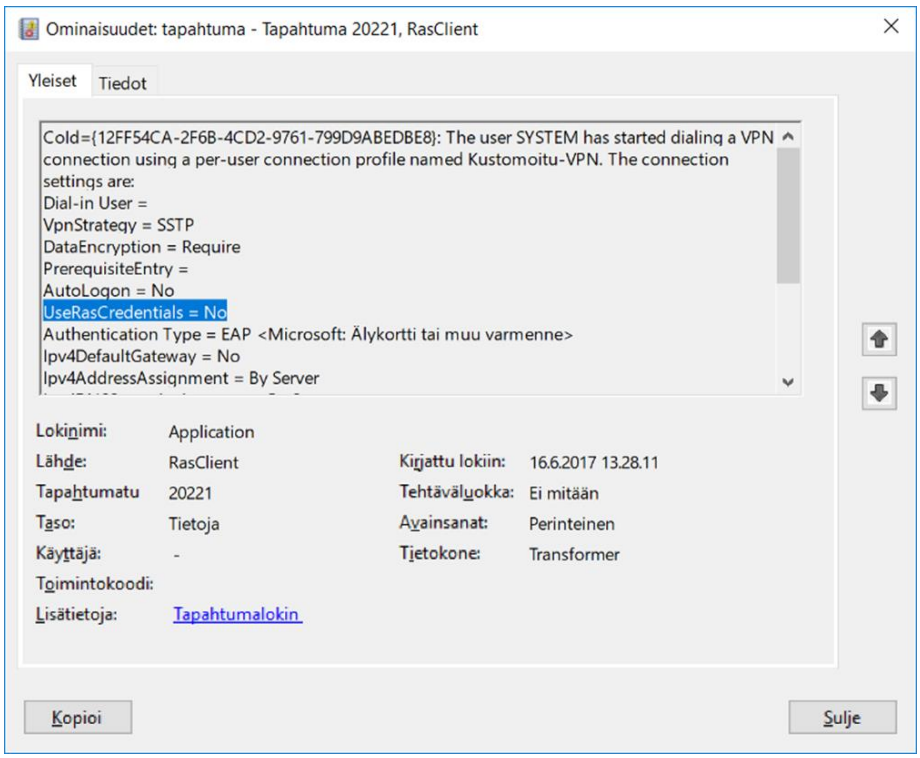


Kuva 71. VPN-yhteyden verkko-ominaisuudet.

Tämän jälkeen VPN-yhteys on konfiguroitu, mutta koneen reititystaulukossa ei ole tietoa VPN-yhteyden takana olevista verkoista, jotka Azuresta ladattava VPN-clientti lisää aina reititystaulukkoon muodostaessaan uudelleen yhteyden. Nämä aliverkot voi lisätä komentorivillä route add ”*Lisättävän aliverkon osoite”* MASK ”*aliverkon maski” ”VPN-yhteyden jakama IP-osoite”*. Tässä tapauksessa esimerkiksi VPN-yhteys on jakanut osoitteen 192.168.100.1 ja reititystaulukkoon pitäisi lisätä reitti Azuren virtuaaliverkon aliverkkoon 192.168.128.0/25, jolloin komento seuraavanlainen: route add 192.168.128.0 MASK 255.255.255.128 192.168.100.1. Koska VPN-yhteyden jakama IP-osoite vaihtuu joka kerta kun yhteys muodostetaan uudelleen, täytyy reitti tai reitit lisätä aina uudelleen, ja tämän takia täytyy reititystaulukosta poistaa myös reitit, jotka viittaavat vanhaan IP-osoitteeseen komennolla route delete *aliverkon osoite*.

Tämän kaiken reittien lisäämisen ja poistamisen voi automatisoida esimerkiksi PowerShell-skriptillä, jonka voi Windowsin tehtävien ajoitus -työkalulla määrittää käynnistymään aina, kun havaitaan VPN-yhteyden muodostuminen. Internetistä löytyy tähän ohjeita, joita pystyy muokkaamaan vastaamaan omia verkkoja.

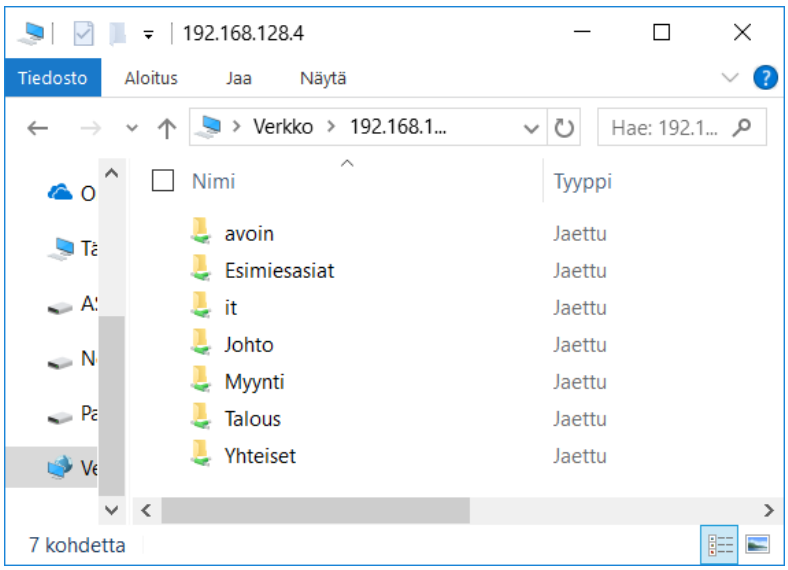
VPN-yhteyden luomisen jälkeen vieläkään ei päästä verkkojakoon käsiksi, sillä VPN-yhteydessä on edelleen määritettynä UseRasCredentials = 1 (tosi), ja se täytyy vaihtaa 0:ksi (epätosi). VPN:n konfiguraatiotiedostot löytyvät VPN-clientin asennuksen jäljiltä kansiopolusta ”C:\Users*Käyttäjänimi*\AppData\Roaming\Microsoft\Network\Connections\Cm*yksilöllinenVPN-tuniste*”. Täällä sijaitsevaa .pbk-päätteistä tiedostoa käytetään määrittämään VPN-yhteyksien asetuksia. Tässä tiedostossa sijaitsee Azuren VPN-clientin ja manuaalisesti luodun VPN-yhteyden konfiguraatiot, joten muutokset täytyy tehdä oikean yhteyden kohdalla, jotta ne kohdistuvat oikein. Kun muutokset on tehty ja tallennettu ja VPN-yhteys muodostettu, voidaan tapahtumienvalvonnasta varmistaa, ettei yhteys käytä vääriä tunnistetietoja (kuva 72).



Kuva 72. VPN-yhteyden muodostaminen tapahtumienvalvonnassa.

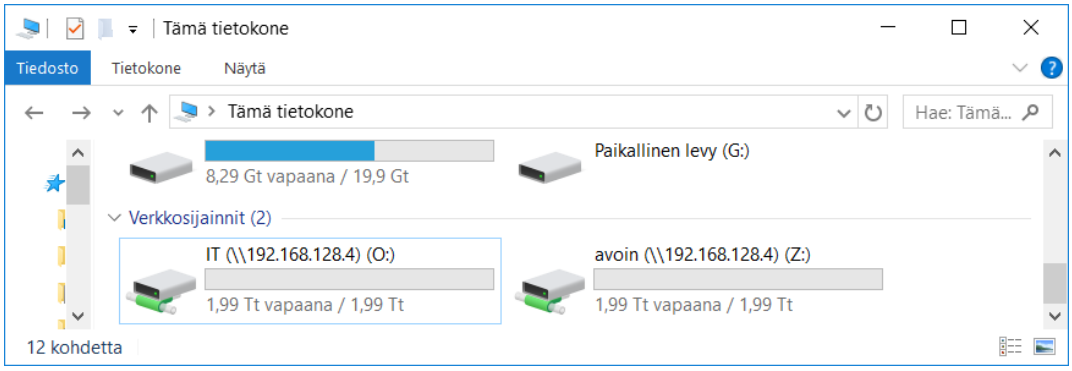
Verkkojaot

Verkkojaot toimivat kuten pitääkin Anssi Asentajalla. Palvelimen puolelta ei piilotettu jakoja käyttäjiltä, jolla ei ole niihin oikeuksia, vaan Anssi Asentaja näkee kaikkien kansioiden olemassaolon (kuva 73).



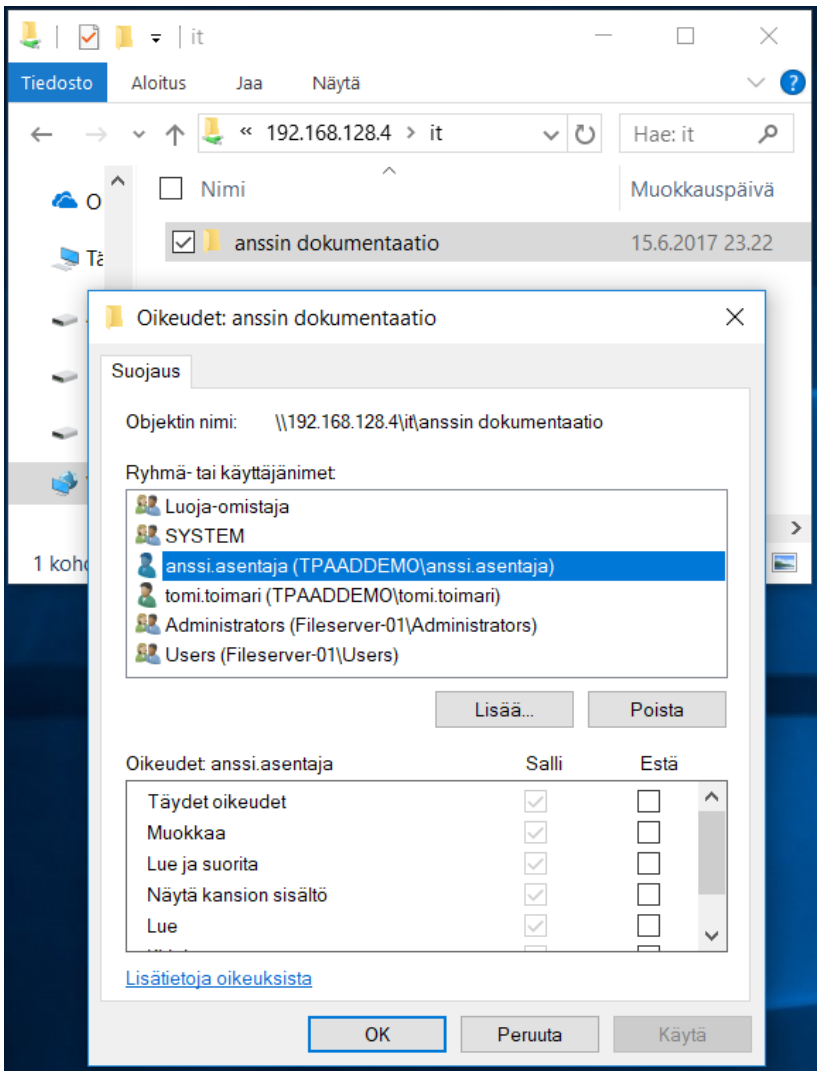
Kuva 73. Kaikki tiedostopalvelimesta jaetut kansiot.

Kun yhteys on toiminnassa, käyttäjät voivat lisätä palvelimen kansiojakoja verkkoasemiksi, jotka säilyvät resurssienhallinnassa uudelleen käynnistyksen jälkeenkin (kuva 74).



Kuva 74. Anssi Asentajan IT-kansio ja yrityksen yhteinen kansiojako lisättynä verkkoasemiksi.

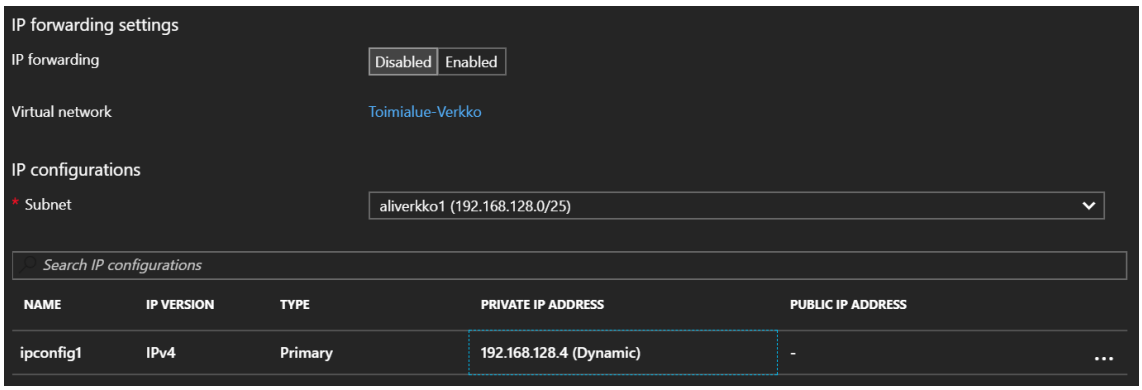
Kansioikeudet toimii, kuten on määritettykin, ja Anssi Asentajalla ei ole pääsyä muihin kuin oman roolinsa kansioihin. Oikeuksia voi tarkastella kansion tai tiedoston ominaisuuksista, mutta oikeuksia ei voi muokata tai lisätä, koska yhteyttä Domain Controllereihin ei ole (kuva 75).



Kuva 75. Verkkojaon oikeudet-näkymä.

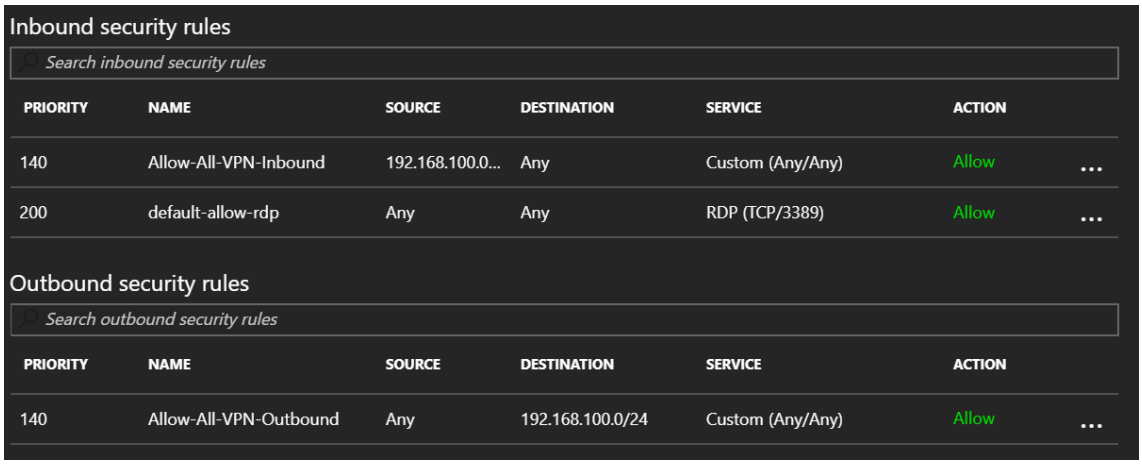
6.5 Virtuaaliverkon suojaus

Kun palvelimien hallinnasta vastaavalle henkilölle on konfiguroitu VPN-yhteys Azureen, kannattaa palvelimen julkinen IP-osoite poistaa palvelimen verkkokortin asetuksista ja muodostaa etätyöpöytäyhteys ja muut yhteydet ainoastaan suojatun VPN-yhteyden kautta (kuva 76). Mikäli VPN-yhteyteen tulee ongelmia, voidaan palvelimeen lisätä tilapäisesti julkinen IP-osoite. Virtuaaliverkossa käytettävä yksityinen IP-osoite kannattaa palvelimissa myös muuttaa staattiseksi, jolloin määritetty IP-osoite pysyy aina samana. Tämä on erityisen tärkeää, koska tässä ratkaisussa ei ole DNS-palvelua käytettävissä ja yhteys palvelimeen muodostetaan IP-osoitetta käyttäen.



Kuva 76. Fileserver-01-palvelimen verkkokortista on poistettu julkinen IP-osoite.

Network security groupin (NSG) voi liittää aliverkkoon tai virtuaalikoneen verkkokorttiin ja rajoittaa sallittavaa liikennettä. NSG:llä voidaan luoda sääntöjä, jotka sallivat tai kieltävät liikennettä lähde- ja kohde-IP-osoitteiden ja porttien perusteella. Jos NSG:n takana on Windows-palvelimia, täytyy RDP-protokolla sallia sisään päin, jotta palvelimiin voidaan muodostaa etätyöpöytäyhteys. VPN-yhteyden ja Azuren virtuaaliverkon välistä liikennettä ei tarvitse erikseen sallia, mutta sitä on käytetty kuvassa esimerkkinä kuvassa 77.



Kuva 77. Network security groupin säännöt.

6.6 Käyttäjien identiteetti

SID (security identifier) -tunniste on eri Azure Active Directoryn ja Azure Active Directory Domain Servicesin käyttäjillä. Suoritetuissa tiedostojakotesteissä identiteetti vaikutti samalta, koska käyttäjä autentikoi samalla tunnuksella ja samalla salasanalla. Yhteyttä ei VPN:n läpi ollut Domain Controllereihin, mutta näissä testeissä se ei haitannut. Kun

Azure AD DS tulee toimimaan uuden portaalin virtuaaliverkossa, tilanne voi olla erilainen, todennäköisesti kuitenkin toimivampi ratkaisu. Yrityksen kannattaa pilotoida käyttämiänsä toimintoja ja testata niiden toiminta ympäristössä, mutta insinöörityön testeissä autentikointi tiedostonjakopalvelimella toimi oletetulla tavalla.

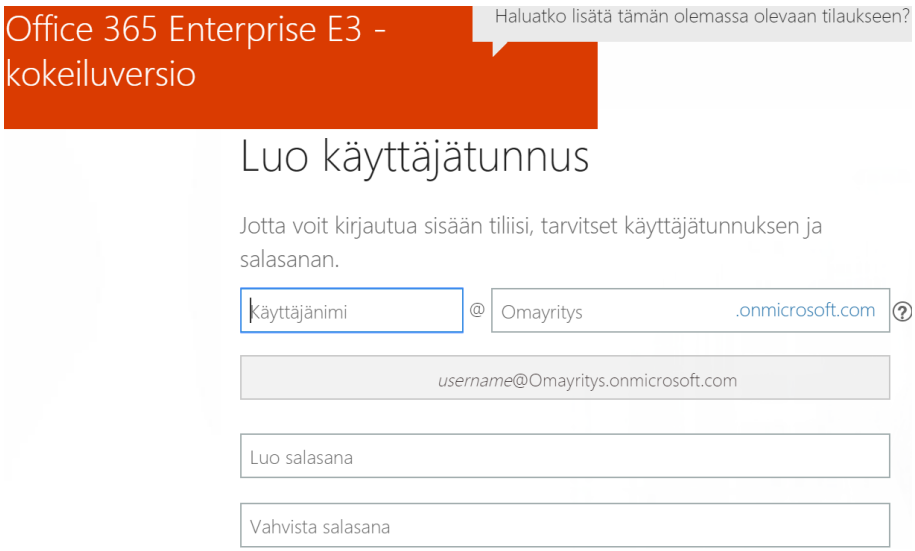
7 Ratkaisu 3: IaaS Domain Controller

Ratkaisu 3 on toteutukseltaan ja tekniikaltaan lähimpänä perinteistä Active Directorya ja työasemien hallintaa. Tässä ratkaisussa asennetaan Azuren virtuaalikoneeseen toimialue, luodaan tähän virtuaaliverkkoon Point-to-Site-VPN-yhteys, liitetään työasema perinteisellä tavalla toimialueeseen ja otetaan Office 365 -palvelut käyttöön. Active Directory toimii käyttäjien identiteetinhallintana, ja Group Policya käytetään laitehallintaratkaisuna.

Ratkaisussa luodaan myös erillinen tiedostopalvelin, jolla toteutetaan tiedostonjakoratkaisu, kuten ratkaisu 2:ssa. Lopuksi määritellään Azuren Backup-palvelulla palvelimille varmuuskopiointiratkaisu, synkronoidaan toimialue Azure AD:hen ja hyödynnetään työasemalla Azure AD:n kertakirjautumisominaisuutta (Single sing-on, SSO).

7.1 Office 365 -palveluiden käyttöönotto

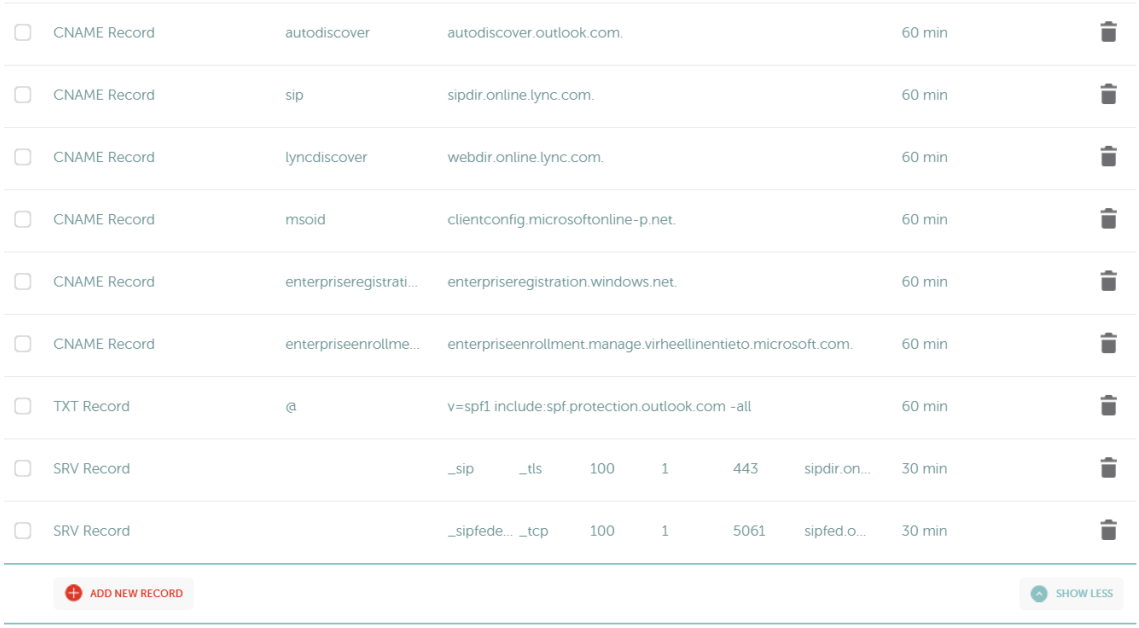
Ratkaisu 1:stä poiketen tein tässä ratkaisussa ensin Office 365 Enteprise E3 -tilauksen. Kuvassa 78 näytetään Officen kokeiluversioon luotavan käyttäjätunnuksen tekeminen. Kuvassa nähtävään Omayritys-laatikkoon kirjoitettava nimi tulee käyttöön Sharepoint- ja OneDrive-internetosoitteisiin. Esimerkiksi yrityksen ”abc123” OneDriveen voi kirjautua abc123-my.sharepoint.com-osoitteen kautta.



Kuva 78. Office 365 -tilauksen käyttöönotto.

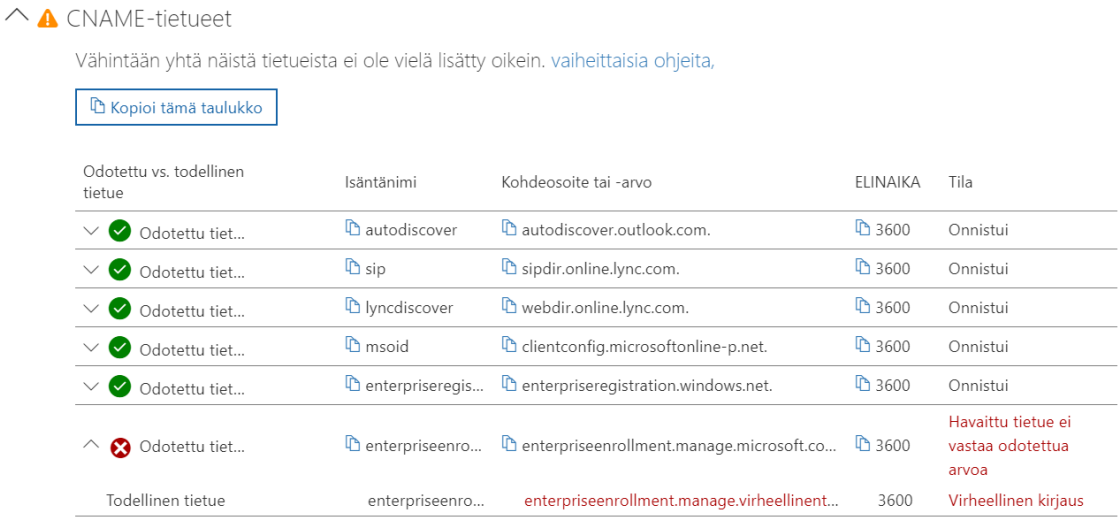
Kun Office 365 -tilaus oli käyttöönotettu, liitin verkkotunnuksen Officen hallintaportaalissa. Verkkotunnuksen pystyy vahvistamaan omistamakseen tarkistussähköpostilla, jossa ICANN WHOIS:n hakemalle verkkotunnuksen yhteyshenkilölle lähetetään sähköpostitse tarkistuskoodi, jonka syöttäminen Officeen vahvistaa verkkotunnuksen omistajan. Myös Azuressa käytössä oleva määritetyn TXT-tietueen lisääminen verkkotunnuksen rekisteröijälle on käytettävissä Office 365:ssä verkkotunnuksen omistajuuden vahvistamiseen. Tätä asiaa on käsitelty luvussa 5.1 Verkkotunnuksen liittäminen Azure Active Directoryyn ja Office-palveluiden käyttöönottoa tarkemmin luvussa 5.7 Office 365 -palveluiden määritys.

Ratkaisu 1:stä poiketen en siirtänyt verkkotunnuksen nimipalvelimia osoittamaan Office 365:n nimipalvelimiin, vaan valitsin hallitsevani DNS-tietueita itse, jolloin verkkotunnuksen alle on itse lisättävä Officen antamat yhdeksän tietuetta, jotta Office 365 -palvelut toimivat (kuva 79).



Kuva 79. Namecheap-rekisteröijälle lisätty Office 365:n vaatimat DNS-tietueet.

DNS-tietueiden määrityksen onnistumisen takaamiseksi Officesta voi valita tietueiden tarkastuksen nappulaa painamalla, jolloin kerrotaan, puuttuuko jokin tietue tai onko jokin tietue lisätty väärin (kuva 80). Kuvassa olen ominaisuuden demonstroimiseksi lisännyt väärän tietueen, jolloin käyttäjälle näytetään virheellinen ja oikea tietue.



Kuva 80. Office 365:n DNS-tietueiden tarkastus.

Verkkotunnuksen liittämisen jälkeen loin esimerkkiyrityksen loput käyttäjät käyttäen lisättyä verkkotunnusta ja annoin Anssi Asentaja -käyttäjälle käyttäjäroolin ”Yleinen järjestel-

mänvalvoja”. Azuren portaaliin siirryttäessä ovat käyttäjätunnukset käytettävissä rekisteröidyn verkkotunnuksen Azure Active Directoryssä. Azure AD on nyt käytettävissä Azuren portaalin kautta, mutta muiden resurssien luontia varten täytyy luoda Azure-tilaus. Hyödynsin tätä ratkaisua varten Azuren tarjoamaa ilmaista kuukauden kokeiluaikaa 170 euron krediteillä.

7.2 Virtuaalikoneiden luominen

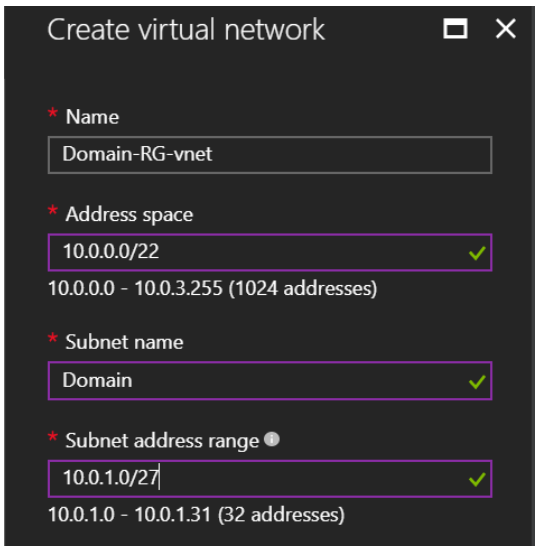
Tilauksen käyttöönoton jälkeen voidaan Azureen luoda laskutettavia resursseja. Tiedostojen jakaminen voidaan teknisesti toteuttaa yhdellä palvelimella, joka on samalla Domain Controller, mutta DC:ltä ei ole tietoturvariskien takia suositeltavaa jakaa tiedostoja. Parhaiden käytäntöjen mukaan DC-palvelimia pitäisi olla vähintään kaksi, jotta toisen ollessa pois käytöstä voivat toimialuepalvelut jatkaa toimimista yhden DC:n turvin. Jos yhtään DC:tä ei ole käytettävissä, eivät käyttäjät pysty käyttämään todentamista vaativia palveluita, kuten tiedostonjakoa. Näin ollen saadaan palvelimien vähimmäismääräksi kolme, ja jos tiedostonjaon toiminta halutaan turvata toisella tiedostopalvelimella, tarvitaan neljä palvelinta.

Tämän insinöörityön ratkaisujen tuli kuitenkin olla edullisia, minkä takia tämä ratkaisu toteutetaan kahdella palvelimella: yhdellä vähän resursseja käyttävällä Windows Server 2016 Server Core Domain Controllerilla ja yhdellä tiedostopalvelimella. Vikasietoisuutta ei tässä ratkaisussa edellä mainituista syistä toteuteta, vaan luotetaan Azuren infrastruktuurin tarjoamaan vikasietoisuuteen. Toiminnan jatkuvuuden turvaamiseksi ja käyttäjien virhetilanteiden varalta DC:lle ja tiedostopalvelimelle luodaan aikataulutettu varmuuskopiointi. Varmuuskopioista palvelin voidaan palauttaa aikaisempaan tilaan luomalla siitä uusi virtuaalikone, tai varmuuskopiota voidaan käyttää yksittäisten tiedostojen palauttamiseen. Backup-palvelussa oletuksena olevan Geo-redundant-replikoinnin ansiosta varmuuskopiot ovat tallessa datakeskuksen vastaparissa esimerkiksi Azuren datakeskuksen tuhoutumisen varalta.

Domain Controlleriksi luodaan CoreDC-01-niminen virtuaalikone Pohjois-Euroopan datakeskukseen. Server Coren vähäisen resurssien käytön vuoksi valitaan virtuaalikonemalliksi yhdellä jaetulla suorittimella ja 0,75 GB:n keskusmuistilla varustettu A0. Tämän konemallin kuukausihinta on hyvin edullinen 12,55 €. A0-konemallin jaettu suoritin tarkoittaa, että sitä käyttää myös jonkun toisen asiakkaan samanmallinen virtuaalikone.

Palvelimet on tietoturvallisesti eriytetty toisistaan, mutta toisen asiakkaan kova prosessorin käyttö heikentää toisen asiakkaan virtuaalikoneen suorituskykyä. Tässä insinöörityössä testataan, riittääkö A0-konemallin suorituskyky, ja tarvittaessa päivitetään konemalli 38,90 €/kk maksavaan A1-konemalliin, jossa on yksi virtuaalinen suoritus ja 2 GB keskusmuistia. (64.)

Virtuaalikoneen yhteydessä luodaan uusi Azuren paikallisen datakeskuksen replikoinnilla varmistettu (Locally Redundant Storage, LRS) storage accountia, sekä virtuaaliverkko osoiteavaruudella 10.0.0.0/22. DC:lle luodaan Domain-niminen aliverkko osoiteavaruudella 10.0.1.0/27 (kuva 81).



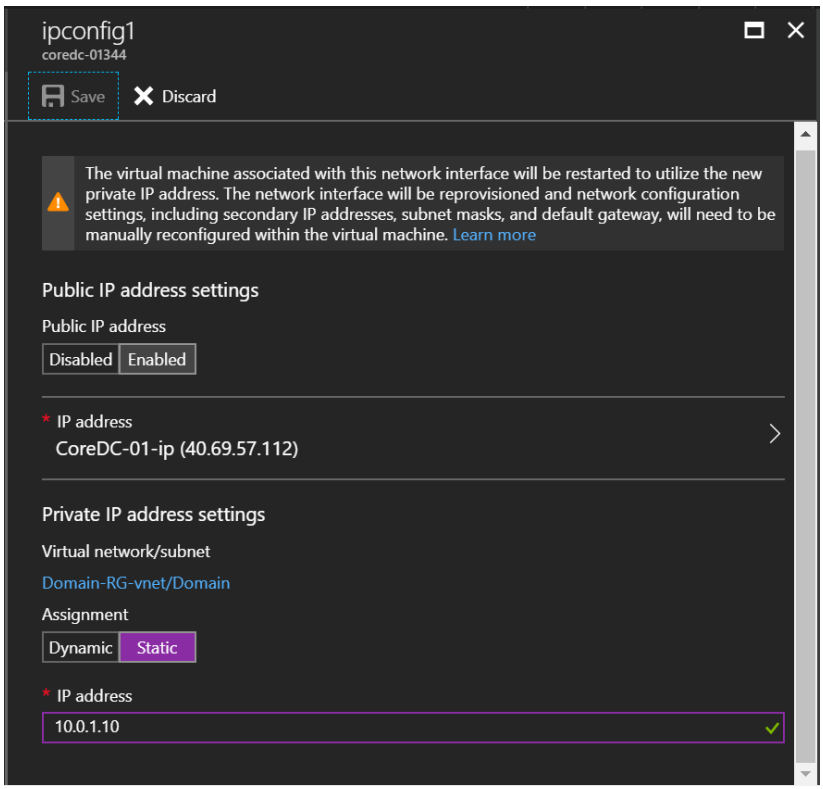
Kuva 81. Virtuaaliverkon luonti Azuressa.

Jos haluaa käyttää Azuren managed disk -palvelua, kannattaa käyttöjärjestelmäimageksi valita versio, jonka nimen alussa on smalldisk-tunniste, olettaen ettei käyttöjärjestelmälevyn kapasiteettia täytetä ylimääräisillä tiedostoilla ja sovelluksilla. Tällöin käyttöjärjestelmälevyn kooksi tulee 30 GB eikä 128 GB:n oletuskokoa. Managed disk -levyjen laskutus perustuu provisioitavan levyn kapasiteettiin eikä todelliseen tilan käyttöön, jolloin tällä imagella saavutetaan muutaman euron kuukausittainen säästö.

Ennen tiedostopalvelimen luomista käydään luomassa uusi palvelimet-niminen 10.0.2.0/24-aliverkko sovelluspalvelimille. Sen jälkeen luodaan 64,00 euroa kuussa maksava (64) F1-mallinen fileserver-01-virtuaalikone, jossa on yksi prosessori ja 2 GB keskusmuistia. Palvelin määritetään käyttämään luotua palvelimet-aliverkkoa ja samaa storage accountia, kuin toinen palvelinkin.

7.3 Toimialueen ja käyttäjien luominen

Active Directorya ei saa tietojen korruptoitumisen estämiseksi määrittää käyttämään välimuistia (cache) käyttävää levyä. Tätä varten lisätään CoreDC-01:lle 50 GB:n kokoinen datalevy ja määritetään Host Cache: None. Lisäksi määritetään myös virtuaalikoneen verkkokortin asetuksista kiinteä 10.0.1.10-IP-osoite (kuva 82) DNS-palvelun asennusta varten. IP-asetusten muuttamisen jälkeen virtuaalikone uudelleen käynnistyy, minkä jälkeen siihen voidaan muodostaa etätyöpöytäyhteys ja aloittaa Active Directoryn määritys.



Kuva 82. Virtuaalikoneen verkkokortin IP-asetukset.

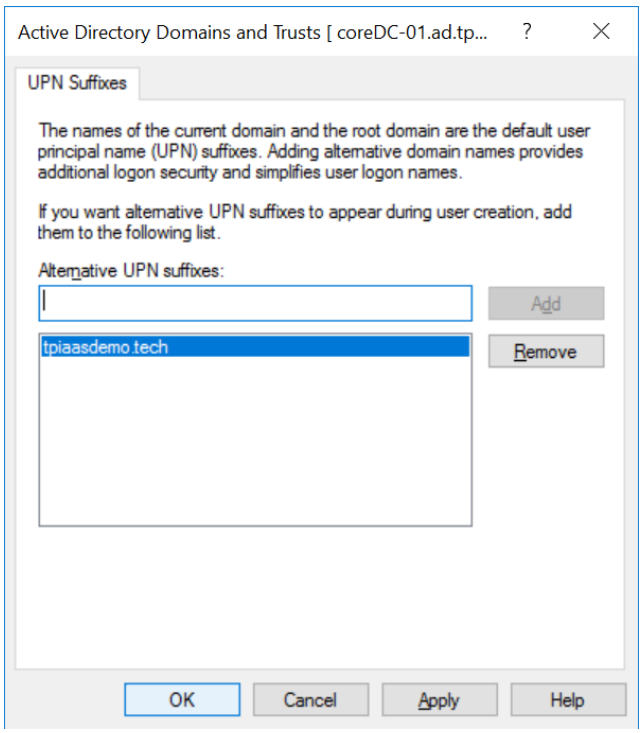
Azuresta tehtyjen esivalmistelujen ja etätyöpöytäyhteyden muodostamisen jälkeen voidaan aloittaa komentojen syöttäminen Server Coren komentoriviin. Get-Timezone-komennolla varmistetaan ensin, onko oikea aikavyöhyke määritetty, ja tarvittaessa määritetään se Set-Timezone-komennolla. Uusi kiintolevy otetaan käyttöön Diskpart-työkalulla ja annetaan sen asematunnukseksi F.

Active Directory asennetaan ensin komennolla install-windowsfeature AD-Domain-Services, jonka jälkeen asennetaan Windows Server 2016-tasoinen metsä ja toimialue komennolla

```
Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath “F:\AD\NTDS” -DomainMode “7” -DomainName “ad.tpiaasdemo.tech” -DomainNetbiosName “tpiaasdemo” -ForestMode “7” -InstallDns:$true -NoRebootOnCompletion:$false -SysvolPath “F:\AD\SYSVOL” -Force:$true
```

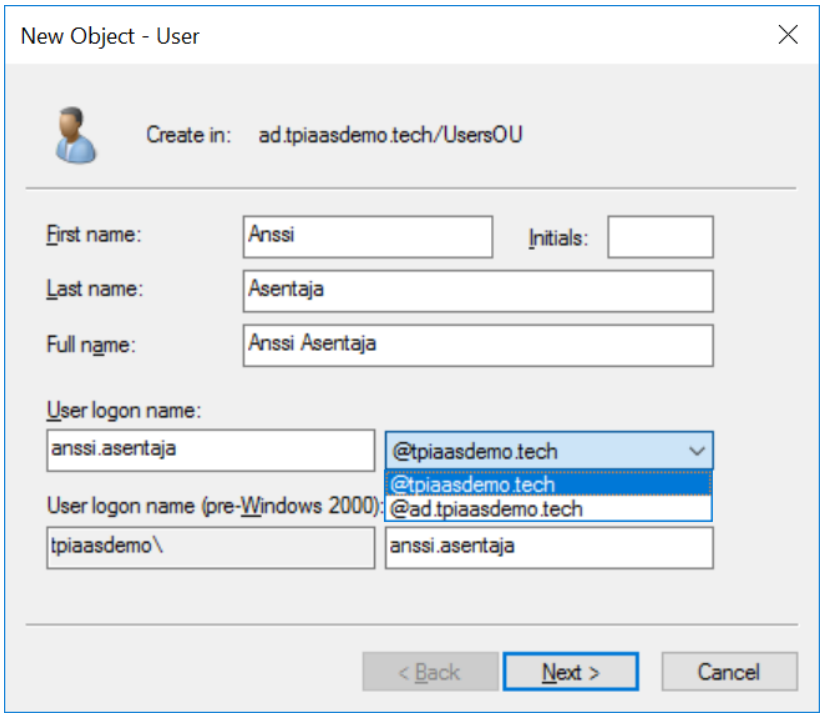
Active Directory on määritetty käyttämään lisättyä F-levyä ja toimialueesta luodaan ad.tpiaasdemo.tech-niminen. Toimialueen nimeämisen parhaiden käytäntöjen mukaan ei ole suositeltavaa nimetä toimialuetta suoraan internetissä käytössä olevan verkkotunnuksen mukaan, mutta kuitenkin sellaisen verkkotunnuksen mukaan, jonka omistaa. Komento määrittää palvelimesta myös DNS-palvelimen, ja tämä IP-osoite täytyy määrittää virtuaaliverkon DNS-servers-kohtaan, kuten ratkaisu 2:n kuvassa 57.

Käyttäjille lisätään UPN-jälkiliite (User Principal Name, UPN-suffix) Active Directory Domains and Trust -työkalulla. Jälkiliitteeksi annetaan yritykselle rekisteröity verkkotunnus (kuva 83), joka on otettu käyttöön Office 365:n palveluissa, ja näin käyttäjät voivat käyttää kirjautumiseen sähköpostiosoitettaan. Tunnus vastaa nyt Azure Active Directoryn vahvistamaa verkkotunnusta, joka on vaatimuksena AD:n ja Azure AD:n synkronoimisessa Azure AD Connectin kanssa.



Kuva 83. UPN-suffiksin lisääminen.

Kaikki esimerkkikäyttäjät luodaan Active Directory Users and Computers -työkalulla. Käyttäjien luontivaiheessa voidaan käyttäjät nyt määrittää käyttämään lisättyä UPN-jälkiliitettä (kuva 84).



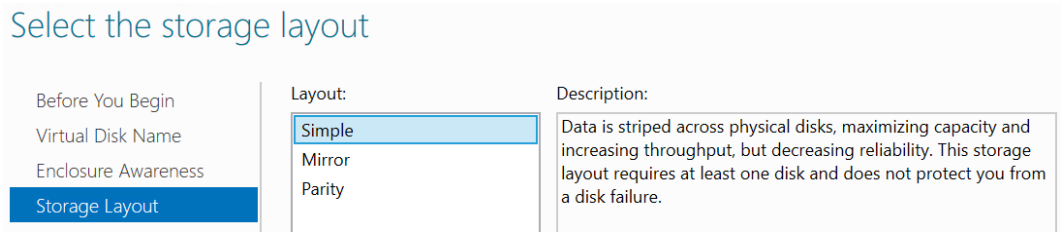
Kuva 84. Käyttäjän luominen Active Directoryyn.

7.4 Tiedostojaon ja Group Policyn määritys

Tiedostopalvelimelle määritetään myös virtuaalikoneen verkkokortin asetuksista kiinteä 10.0.2.10 IP-osoite. Tiedostojakoa varten lisätään kaksi 1 024 GB:n kokoista datalevyä, joiden kummankin kokoa voi tarvittaessa kasvattaa neljään tebitavuun.

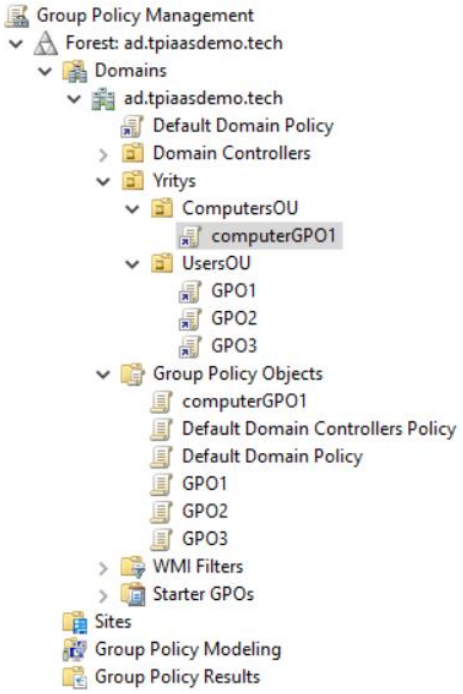
Sen jälkeen muodostetaan palvelimeen etätyöpöytäyhteys ja liitetään palvelin luotuun ad.tpiiasdemo.tech-toimialueeseen. Toimialueen ja DNS-palvelujen hallinta graafisilla työkaluilla onnistuu asentamalla Remote Server Administration Tools -toiminto, kuten luvussa 6.3 Tiedostopalvelin. Tiedostopalvelimeen asennetaan myös Group Policy Management -toiminto, jotta työasemia päästään hallitsemaan. Tiedostopalvelin voidaan myös määrittää DNS-palvelimeksi ja virtuaaliverkon DNS-asetuksiin määrittää toiseksi DNS-palvelimeksi tämän palvelimen IP-osoite.

Levyistä luodaan Windows Server 2016:n File and Storage Servicellä storage pool. Storage poolista luodaan koko levykapasiteetin käyttävä virtuaalinen Simple-levy (kuva 85), ja siitä luodaan koko kapasiteetin käyttävä osio, johon verkkojaot määritellään. Sama prosessi on kuvattu ratkaisussa 2:ssa, ja luvussa 6.3 Tiedostopalvelin on lyhyesti kerrottu verkkojakojen luomisesta.



Kuva 85. Storage poolin virtuaalisen kiintolevyn konfigurointi.

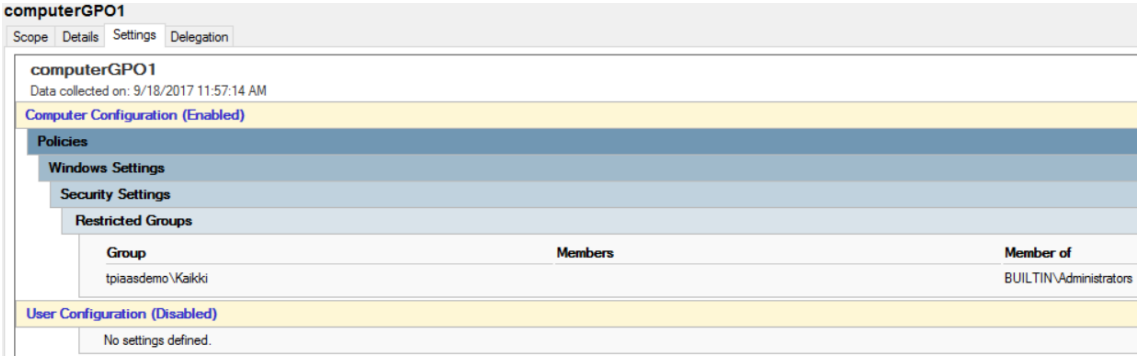
Group Policyjä ei voi kohdistaa konetunnusten oletus-Computers-säilöön, vaan tätä varten ne pitää siirtää johonkin luotuun OU:hun. Tätä varten luotiin AD:hen Yritys OU, jonka alle luotiin ComputersOU- ja UsersOU-säilöt Group Policyjä varten (kuva 86).



Kuva 86. Group Policyn rakenne.

Toimialueeseen liittyvien työasemien konetunnusten automaattinen ohjaaminen ComputersOU:hun toteutettiin ajamalla redircmp-komento tiedostopalvelimessa, ja kaikki käyttäjät siirrettiin UsersOU:n alle manuaalisesti Active Directory Users and Computers -työkalulla. Molemmat OU:t ovat Yritys-OU:n alla, jolloin Yritys-OU:hun kohdistetut Group Policyt vaikuttavat sen sisällä oleviin ComputersOU ja UsersOU:hun.

Tässä ratkaisussa käyttäjät suorittavat toimialueeseen liittymisen omilla tunnuksillaan, ja heidät lisätään koneiden paikallisiksi järjestelmänvalvojiksi. Group Policy -objekti, joka lisää kaikki-ryhmän jäsenet työasemiin paikallisiksi järjestelmänvalvojiksi, on kohdistettu ComputersOU:hun, ja sen määritykset näkyvät kuvassa 87. Tämä Group Policy -objekti täytyy prosessoida toimialueeseen liittyvässä työasemassa, jotta käyttöönotto onnistuu tässä ratkaisussa kuvatulla tavalla.

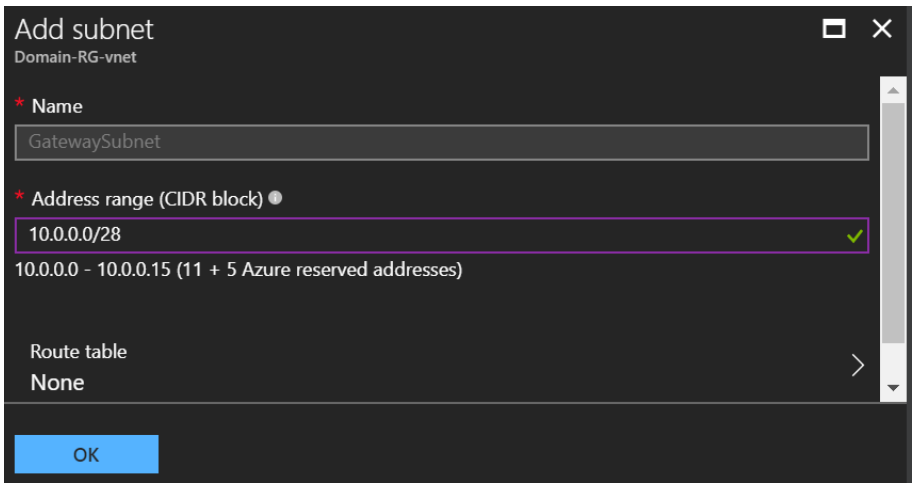


Kuva 87. Group Policy objektin määritykset.

UsersOU:hun on testauksen vuoksi luotu Group Policy -objekti, joka lisää käyttäjille Yhteiset-verkkojaon. Group Policy toimii VPN:n kautta ja näin ollen sitä voi käyttää tekemään muitakin määrityksiä käyttäjien koneisiin. Group Policy suoritetaan käyttäjän kirjautuessa työasemalla, mikä ei tässä kohtaa toimi, koska silloin ei VPN-yhteyttä ole vielä muodostettu. Group Policy päivittyy myös taustalla tietyin väliajoin ja se voidaan pakottaa päivittymään gpupdate /force -komennolla.

7.5 Point-to-Site-VPN-yhteyden määritys portaalista

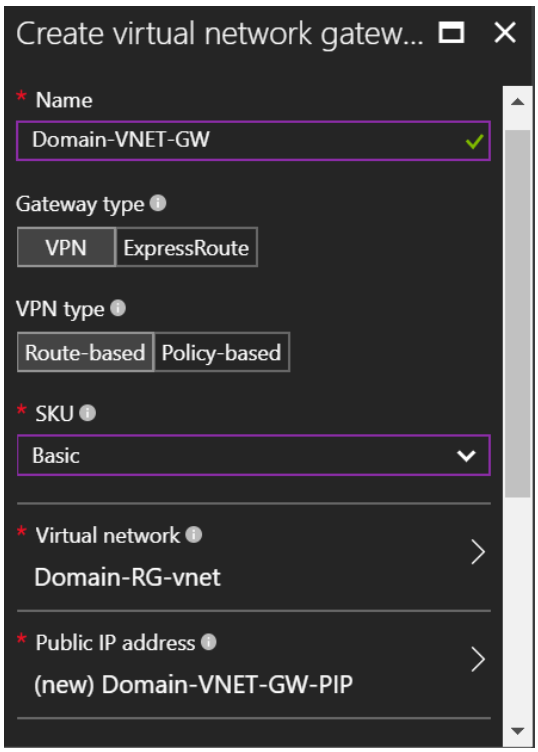
VPN-yhdyskäytävän käyttöönoton ensimmäinen vaihe on tehdä luotuun virtuaaliverkkoon oma aliverkko VPN-yhdyskäytävälle. Tämä onnistuu VNETin Subnets-kohdasta painamalla + Gateway Subnet -painiketta. Azureen suositellaan aliverkon luomista vähintään 27 tai 28 -bitin maskilla, jotta aliverkossa on riittävästi osoitteita tulevaisuuden tarpeita varten. Kuvassa 88 luodaan 10.0.0.0/22-verkkoon 10.0.0.0/28 GatewaySubnet -aliverkko VPN-yhdyskäytävälle.



Kuva 88. Yhdyskäytävä-aliverkon luominen Azuressa.

Kun DNS-palvelimen (CoreDC-01) IP-osoite on määritetty virtuaaliverkon asetuksiin ja tarvittava aliverkko luotu, voidaan virtuaaliverkon VPN-yhdyskäytävä luoda Azuren plus-painikkeesta ja valitsemalla Virtual network gateway. Yhdyskäytävän tyypiksi valitaan SKU-pudotusvalikosta 100 Mbps:n (Megabit per second, megabittiä sekunnissa) nopeudella toimiva Basic-vaihtoehto. Tätä mallia ei suositella tuotantokäyttöön, mutta sen 22,59 euron kuukausihinta tekee siitä houkuttelevan vaihtoehdon testikäyttöön. Basicista seuraavaksi halvin vaihtoehto on 119,21 euroa kuukaudessa maksava VpnGw1, joka toimii 650 Mbps:n nopeudella. (61.)

VPN-yhdyskäytävän luonnissa pitää sen tyypiksi valita Route-Based, määrittää, mihin virtuaaliverkkoon se luodaan, ja luoda yhdyskäytävälle uusi julkinen IP-osoite (kuva 89). VPN:lle täytyy määrittää myös datakeskus, johon se luodaan, ja sen täytyy olla sama kuin missä virtuaaliverkko sijaitsee. Näiden valintojen jälkeen voidaan yhdyskäytävä luoda Create-painikkeesta.

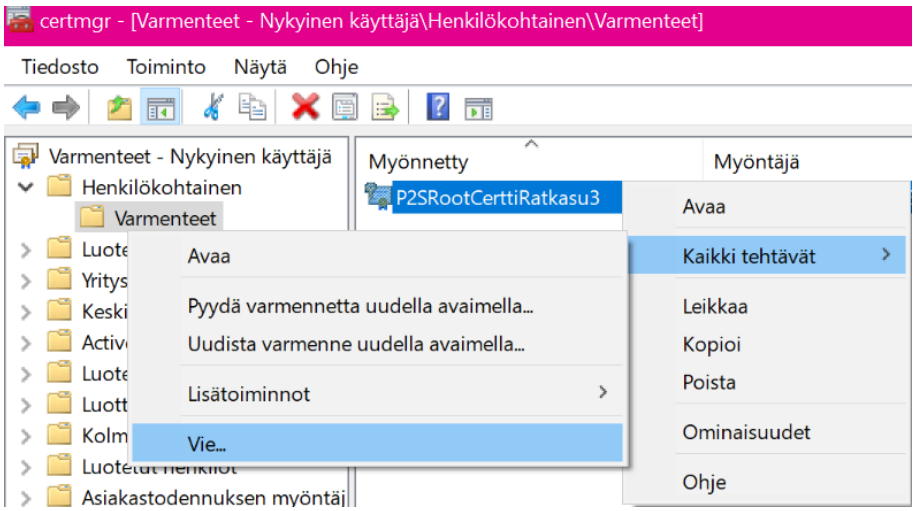


Kuva 89. VPN-yhdyskäytävän luominen Azuressa.

VPN:n autentikointi täytyy konfiguroida julkisella ja yksityisellä avaimella. Tämä voidaan toteuttaa yrityksen olemassa olevalla julkisten avainten hallintaratkaisulla (Public Key Infrastructure, PKI) tai luoda sertifikaatit Windows 10:n PowerShellilla. Seuraava PowerShell-komento luo julkisen avaimen sisältävän juuri sertifikaatin:

```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SRootCerttiRatkasu3" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage
CertSign
```

Julkinen avain täytyy ladata Azuren VPN-konfiguraatioon. PowerShellissa luodun sertifikaatin julkinen avain saadaan vietyä työaseman Certificate Managerista, hiiren kakkospainikkeen valikosta, kuvan 90 osoittamalla tavalla.



Kuva 90. Varmenteiden hallinnasta sertifikaatin vieminen.

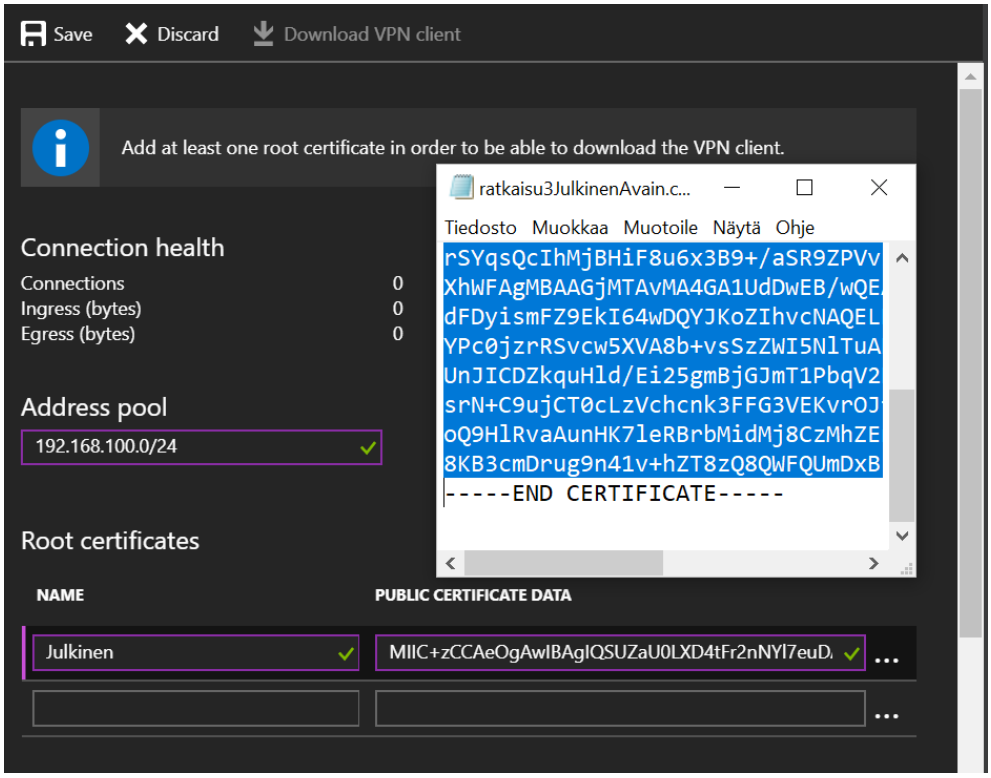
Viemisprosessissa kysytään, halutaanko myös yksityinen avain viedä, mihin vastataan tässä vaiheessa kieltävästi. Sen jälkeen valitaan käytettäväksi muodoksi ”Base64-koodattu X.509 (.cer)”. Sitten valitaan tallennussijainti, ja lopuksi luodaan avain valmis-painiketta painamalla.

Tämän jälkeen luodaan yksityinen avain tai avaimia, jotka täytyy asentaa käyttäjien työasemille, jotta VPN-yhteyden autentikointi ja itse yhteys toimivat. Kaikille käyttäjille voidaan käyttää samaa avainta tai luoda jokaiselle oma muuttamalla PowerShell-komennossa luotavan avaimen nimeä. Seuraava komento luo samasta PowerShell-sessiosta, jossa julkinen avain on tallennettu cert-muuttujaan, yksityisen avaimen kahden vuoden voimassaoloajalla.

```
New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SChildCertti1Ratkasu3" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-NotAfter (Get-Date).AddMonths(24) `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

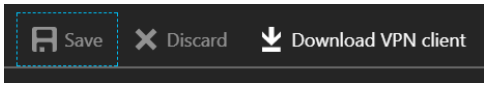
Komento luo suorittavaan työasemaan yksityisen avaimen, josta se viedään kuten julkinen avainkin ja jaetaan edelleen käyttäjien työasemille. Avaimen vientiprosessissa vastataan yksityisen avaimen viemiseen tällä kertaa myönteisesti, suojataan avain salasanalla ja valitaan tallennussijainti. Nyt koneella pitäisi olla tiedostoina .cer-päätteinen julkinen avain ja .pfx-päätteinen yksityinen avain.

Kun Azure on luonut VPN-yhdyskäytävän, täytyy sen Point-to-site configuration -valikosta määrittää VPN-yhteyden jakelemat osoitteet ja kopioida julkisen avaimen sisältämä tieto public certificate data -kohtaan. Julkisen avaimen voi avata esimerkiksi muistiolla ja kopioida datan rivien -----BEGIN CERTIFICATE----- ja -----END CERTIFICATE----- välistä kuvan 88 mukaisesti.



Kuva 91. Azuren VPN-yhdyskäytävän Point-to-Site-konfiguraatio.

VPN-yhteys on nyt määritetty loppuun Azuressa ja VPN-clientin asennuspainike on muuttunut aktiiviseksi, jolloin se voidaan ladata ja asentaa työasemille (kuva 92).



Kuva 92. VPN-clientin latauspainike.

VPN-yhteyden määritys manuaalisesti työasemalla

Ratkaisu 2:n luvussa 6.4 Point-to-Site-VPN-yhteyden määritys PowerShellilla kuvataan VPN-clientin autentikointiongelmia ja VPN-yhteyden määrittämistä. Ongelmana on, että

Azuresta ladattavalla VPN-clientin yhteydellä ei päästä käsiksi tiedostojakoihin virheellisen autentikoinnin takia, minkä takia VPN-yhteys pitää määrittää manuaalisesti.

VPN-yhteyden luomiseen olen kokeillut neljää vaihtoehtoa. Yksinkertaisin vaihtoehto on Azuresta ladattava VPN-clientti, jonka kanssa olen onnistunutkin liittymään toimialueeseen. Kuten ratkaisu 2:ssa todetaan, tällä yhteydellä konfiguraatiotiedostoon jää UseRasCredentials=1, joka aiheuttaa virheellisen autentikoinnin ainakin verkkojakoa käytettäessä. Vaikka parametrin muuttaisi nollaksi, VPN-yhteyden muodostamisen jälkeen se on ylikirjoitettu konfiguraatiotiedostossa aikaisempaan arvoonsa.

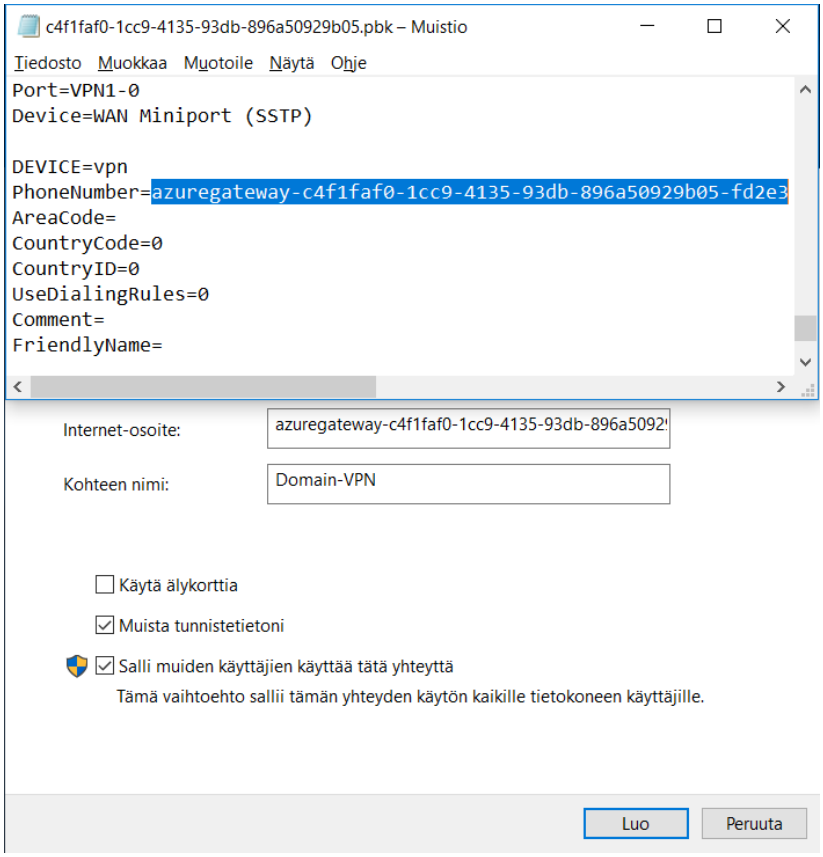
Loin myös Connection Manager Administration Kit (CMAK):lla konfiguroidun VPN-yhteyden, jossa kaikki yhteyden asetukset pääsee määrittämään haluamikseen. Sillä on mahdollista määrittää myös käyttäjän reititystaulukkoon lisättäviä reittejä ja asennuksen jälkeen suoritettavia tapahtumia. Tässäkin tuntui UseRasCredentials-parametrin arvo muuttuvan, vaikka se välillä säilyikin ja Group Policy välittyi VPN:n läpi.

Muokkasin myös Azuresta ladatun ja puretun VPN-clientin asennustiedostoja määrittämällä muun muassa konfiguraatiotiedostoon UseRasCredentials=1. Tämä parametri ylikirjoitettiin jälleen asennusvaiheessa nollaksi ja konfiguraatiotiedostoon tehdyt muutokset asennuksen jälkeen eivät säilyneet VPN-yhteyden uudelleenmuodostamisen jälkeen.

Onnistuin kuitenkin komentorivillä käynnistämään ohjelman toisena käyttäjänä ja onnistuin lisäämään verkkojaon valitsemalla "Muodosta yhteys eri tunnistetiedoilla", johon annoin Anssi Asentajan käyttäjätunnukset. Verkkoasema ei kuitenkaan ollut enää käytettävissä uudelleenkäynnistyksen jälkeen, joten tätä ei voi pitää toimivana ratkaisuna ilman jonkinlaista ylimääräistä lisäskriptiä. Kaiken kaikkiaan tulokset vaihtelivat, Group Policyjen päivitys toimi epäsäännöllisesti ja ratkaisut olivat muutenkin huonosti toimivia. Näitä kaikkia ratkaisuja yhdistää VPN-yhteyden erillinen yhdistä-ikkuna, jonka epäilen olevan syypää konfiguraatiotiedoston ylikirjoittamiseen.

Useiden yritysten ja kokeilujen jälkeen totesin toimivimmaksi ratkaisuksi luoda VPN-yhteys manuaalisesti, kuten ratkaisussa 2. Tällä kertaa ei asenneta ollenkaan VPN-yhteyttä, vaan tehdään VPN-yhteys manuaalisesti käyttäen Azuren VPN-asennuspaketista saatavaa tunneliosoitetta.

Anssi Asentajan OneDriveen on siirretty yksityisen avaimen sisältävä .pfx-tiedostomuodossa oleva sertifikaatti, joka täytyy asentaa Anssin työasemalle ennen VPN-yhteyden ominaisuuksien määritystä. Uuden luotavan VPN-yhteyden internetosoitteeksi syötetään esimerkiksi VPN-clientin asennuspaketin .pbk-tiedostosta selvitetty tunneliosoite (kuva 93).

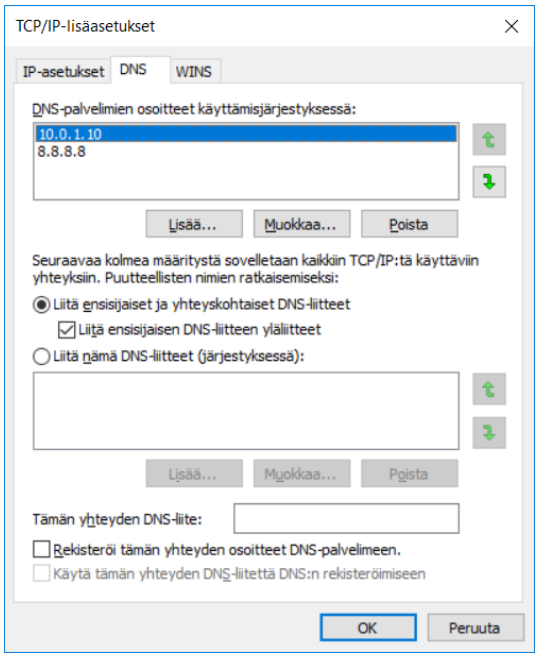


Kuva 93. Uuden VPN-yhteyden luonti Verkko- ja jakamiskeskuksen kautta.

Kun VPN-yhteys on määritetty, muokataan VPN:n verkkosovittimen asetuksia kuten luvussa 6.4 Point-to-Site-VPN-yhteyden määritys PowerShellilla. Tässä ratkaisussa ei ole asennettu ollenkaan valmista VPN-clienttia, joten autentikointiin käytettävän sertifikaatin nimi näkyy luodun juuri sertifikaatin nimenä eikä Azuregateway-nimisenä, kuten ratkaisu 2:n kuvassa 70.

VPN-yhteyden luoman verkkokortin IP-asetuksiin täytyy määrittää DNS-palvelimeksi Azuren virtuaaliverkossa toimivan DNS-palvelimen osoite. Myös kohtaan ”Tämän yhteyden DNS-liite” täytyy määrittää toimialueen täydellinen toimialuenimi (Fully Qualified Domain Name, FQDN), joka tässä tapauksessa on ad.tpiaasdemo.tech.

Lisäksi työaseman verkkokortin asetuksiin määritin kuvan 94 mukaisesti ensisijaiseksi nimipalvelimeksi Azuren DC/DNS-palvelimen osoitteen ja muuta internetin nimenselvennystä varten toissijaiseksi nimipalvelimeksi Googlen vapaassa käytössä olevan nimipalvelimen.



Kuva 94. Työaseman verkkokortin TCP/IP-lisäasetukset.

Toimialueeseen liittyminen ei onnistu, jos verkkokortin asetuksiin määritellä Azuren DNS-palvelinta. Nslookup toimi myös näillä asetuksilla, kun olin DNS-palvelimelle määrittänyt reverse lookup zonen ja palvelimia vastaavat PTR-tietueet.

Työaseman liittäminen toimialueeseen

Työaseman liittäminen Azuressa sijaitsevaan toimialueeseen Point-to-Site-VPN-yhteyttä käyttäen ei ole suoraviivainen operaatio. Olen onnistunut kuitenkin tekemään tämän useasti ja selvittänyt sen onnistuvan käyttäen seuraavia vaiheita:

1. Asenna sertifikaatti.

2. Luo VPN-yhteys ja määritä verkkokorttien DNS-palvelimien ja DNS-liitteiden asetukset.

3. Muuta VPN-yhteyden rasphone.pbk-konfiguraatiotiedostoon UseRasCredentials=0.

4. Luo ajoitettu tehtävä, joka havaitsee VPN-yhteyden käynnistymisen ja käynnistää PowerShell-skriptin päivittämään reititystaulukon vastaamaan VPN-yhteyden jakamaa IP-osoitetta.

5. Liity toimialueeseen, uudelleenkäynnistä kone ja kirjaudu uudestaan paikallisella tunnuksella.

6. Yhdistä VPN:n ja päivitä Group Policy gpupdate /force -komennolla, jolloin toimialueen käyttäjä tai ryhmä tulee työaseman paikalliseksi järjestelmänvalvojaksi. Group Policy -objekti on määritetty luvussa 7.4 Tiedostojaon ja Group Policyn määritys

7. Vaihda käyttäjätiliä ja kirjaudu sisään käyttäen toimialueen käyttäjätunnusta. VPN-yhteys täytyy olla käynnissä paikallisella tunnuksella tässä vaiheessa.

8. Asenna sertifikaatti. Jos asennuksessa tulee virheilmoitus, vaihda paikalliseen tunnukseen ja yhdistä VPN uudelleen. Vaihda takaisin toimialuetunnukseen ja yritä sertifikaatin asennusta uudelleen.

9. Muuta VPN-yhteyden rasphone.pbk-konfiguraatiotiedostoon UseRasCredentials=0.

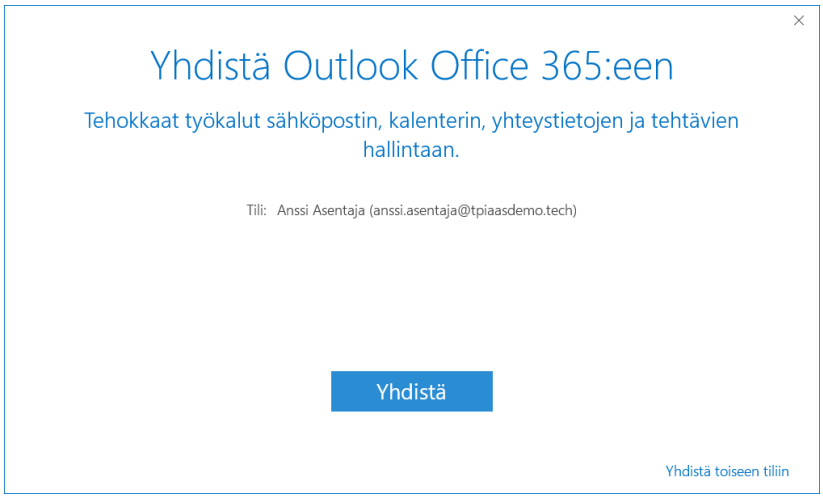
Näitä vaiheita noudattaen olen onnistunut luomaan toimivan VPN-yhteyden toimivalla autentikoinnilla toimialuetunnukselle. Verkkoaseman lisäävä Group Policykin suoritettiin onnistuneesti työasemassa ja lisäsin myös Anssi Asentajalle oman IT-verkkojaon manuaalisesti. Lisättyjen verkkoasemien autentikointi pysyi toiminnassa, kunhan VPN-yhteys oli päällä. Esimerkiksi uudelleenkäynnistyksen jälkeen täytyy näillä määrityksillä VPN-yhteys yhdistää manuaalisesti, jotta verkkojaot ovat käytettävissä.

7.6 Office 365 -palveluiden asennus työasemalla

Käyttäjät voivat asentaa Office 365 -sovellukset itsepalveluna Officen portaalista (kuva 95). 64-bittisen version latauslinkin löytää Muut asennukset -painikkeesta.

Kuva 95. Office 365 -työpöytäsovelluksien lataaminen Officen portaalista.

Officen asentamisen jälkeen, Outlook-postilaatikon saa käyttöön avaamalla ohjelman ja valitsemalla yhdistä-painikkeen (kuva 96). Salasanaa ei tarvinnut syöttää ollenkaan kuten ratkaisu 2:ssa.



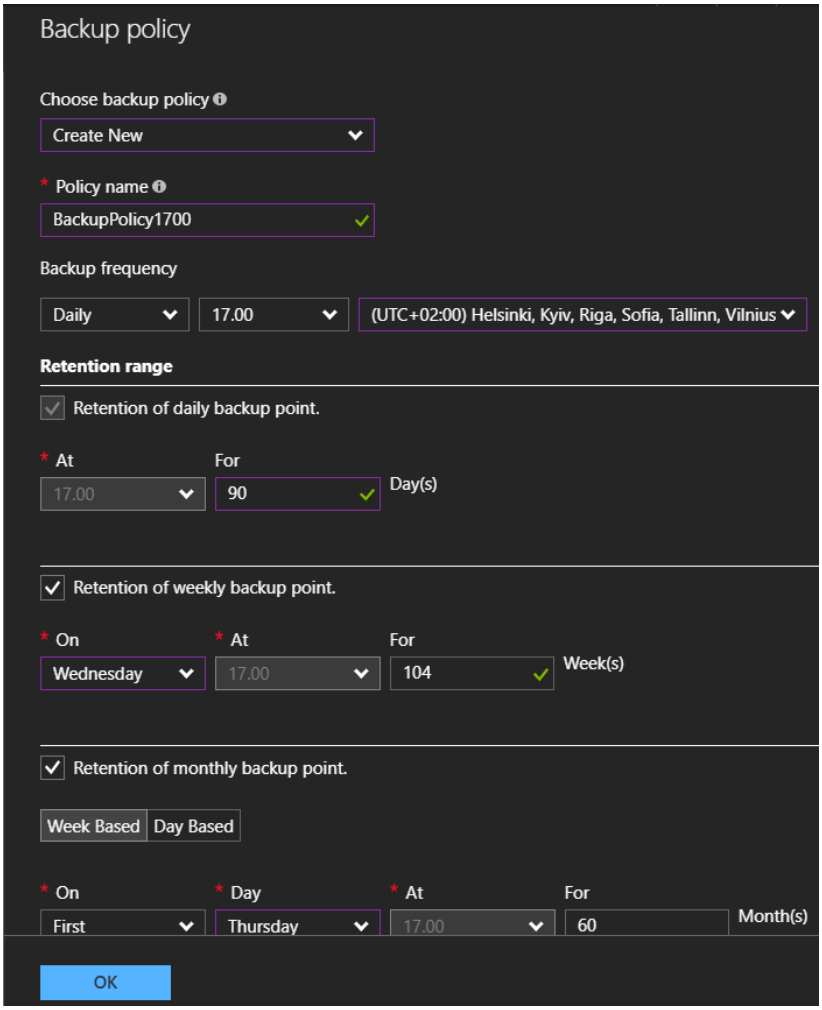
Kuva 96. Outlook-tilin määrittäminen.

7.7 Varmuuskopiointi

Varmuuskopiointi toteutetaan Azuren Recovery Services vaults -palvelulla. Ensin luodaan uusi Recovery Services vault, joka täytyy luoda samaan sijaintiin varmuuskopioitavien virtuaalikoneiden kanssa. Oletuksena käytössä on Geo-Redundant-replikointi, jolloin varmuuskopiot replikoidaan datakeskuksen vastaparin kanssa (aihetta käsitelty luvussa 4.1 Microsoft Azure -pilvipalvelualusta). Palvelussa on muutama käyttöä vaikuttava tekninen rajoitus: olemassa olevan virtuaalikoneen korvaaminen varmuuskopiosta ei ole tuettu ja palvelu voi varmuuskopioida vain alle 1 023 GB:n kokoisia levyjä.

Varmuuskopioinnin määritys

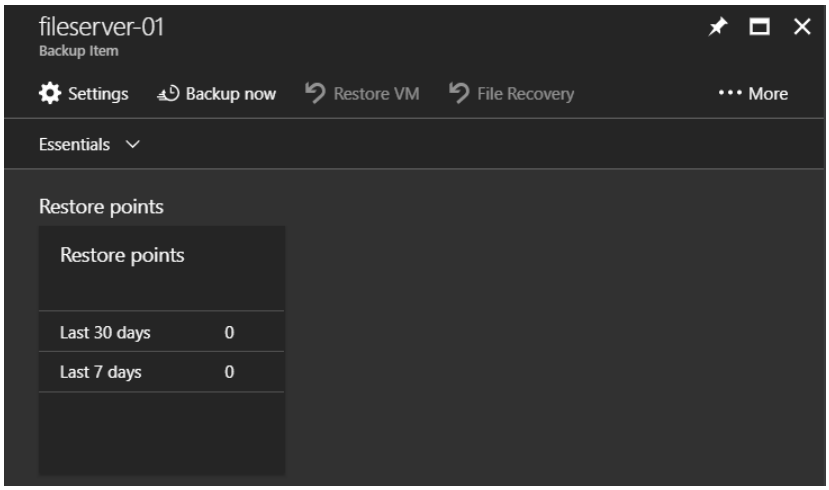
Varmuuskopioinnin määrittämisessä ensimmäinen askel on määrittää, sijaitsevatko varmuuskopioinnin kohteet Azuressa vai On-Premisessä. Tähän valitaan Azuressa, minkä jälkeen voi käyttää joko oletusvarmuuskopiointi-policya tai luoda oman policyn. Kuten kuvasta 97 huomaa, policylla määritetään varmuuskopiointien aikatauluja ja säilytysaikoja. Azuren virtuaalikoneista voi tehdä enintään yhden varmuuskopioinnin päivässä.



Kuva 97. Azuren Recovery Services vaultin varmuuskopiointi-policy.

Policyn määrityksen jälkeen valitaan, mitä kohteita varmuuskopioidaan. Azure näyttää listan virtuaalikoneista, jotka sijaitsevat samassa datakeskuksessa, kuin missä Recovery Services vault sijaitsee, ja jotka eivät ole minkään toisen vaultin varmuuskopioinnin piirissä.

Tämän jälkeen varmuuskopiointi on konfiguroitu, ja virtuaalikoneet varmuuskopioidaan määritellyn aikataulun mukaisesti. Varmuuskopioinnin voi käynnistää myös manuaalisesti, esimerkiksi Recovery Services vaultin Backup now -painikkeella (kuva 98).

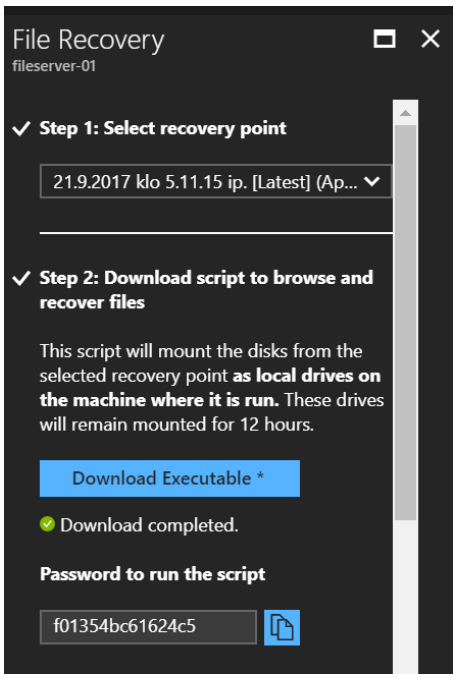


Kuva 98. Virtuaalikoneen hallinta Recovery Services vaultissa.

Tiedostojen palauttaminen varmuuskopiosta

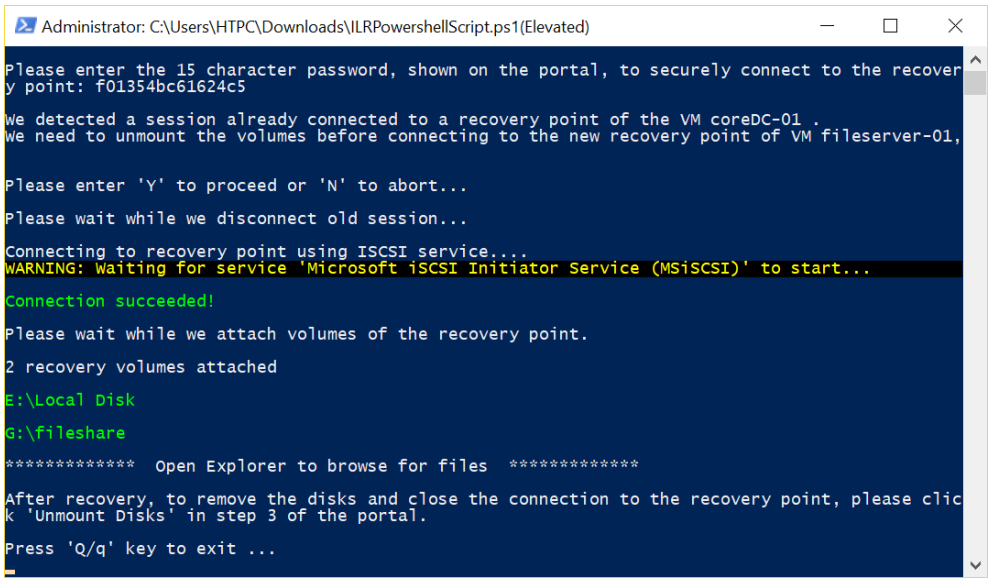
Recovery Services vaultilla tehtyjen Azuren virtuaalikoneiden varmuuskopioiden palautusvaihtoehtoja on kaksi. File Recovery -toiminnolla voidaan tarkastella ja kopioida varmuuskopioidun levyn tiedostoja. Tällä toiminnolla voidaan varmuuskopioituja levyjä käyttää kohdekoneessa kuten muitakin levyasemia, jolloin tiedostojenpalautus on mahdollista kopioi-liitä-menetelmällä. Restore VM -toiminnolla voidaan varmuuskopiosta luoda uusi virtuaalikone.

Tiedostojenpalautus onnistuu Recovery Services vaultin kohdasta Backup Items > Azure Virtual machine > *Varmuuskopioinnin kohde* > File Recovery. Valitaan haluttu palautuspiste ja ladataan levyaseman yhdistävä skripti (kuva 99). Kuten kuvasta huomaa, levyasema on käytössä vain 12 tuntia tietoturvasyistä.



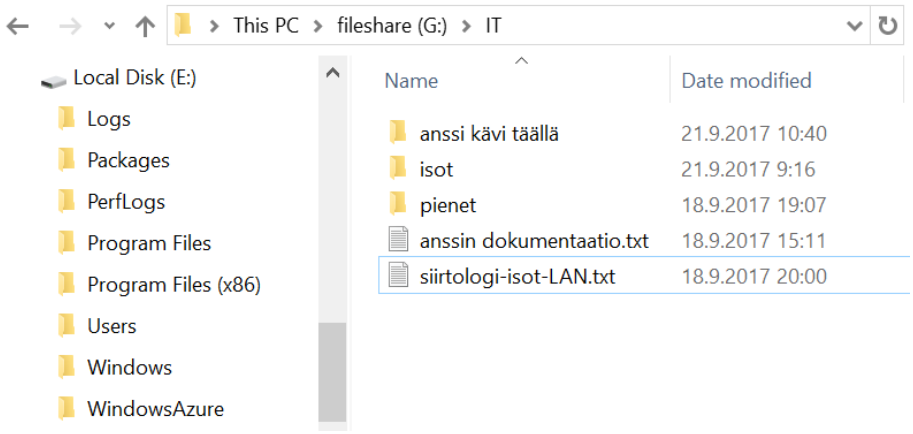
Kuva 99. Tiedostojen palautus Recovery Services vaultissa.

Skriptin voi suorittaa jollain palvelimella tai työasemalla, tai joissakin tilanteissa palautus voidaan suorittaa suoraan varmuuskopioidussa palvelimessa. Skriptin käynnistäminen aukaisee PowerShell-ikkunan, johon syötetään portaalin antama salasana (kuva 100).



Kuva 100. Tiedostojenpalautusskriptin suortittaminen työasemassa.

Kuten kuvasta 101 huomaa, varmuuskopion tiedostoja voi käsitellä kuten muitakin levyaseman tiedostoja. Skriptin suorittaneelle työasemalle tuli E-asemaksi tiedostopalvelimen C-levy. G-asemaksi tuli File and Storage Servicellä luotu kahden kiintolevyn kapasiteetin yhdistävä levy.

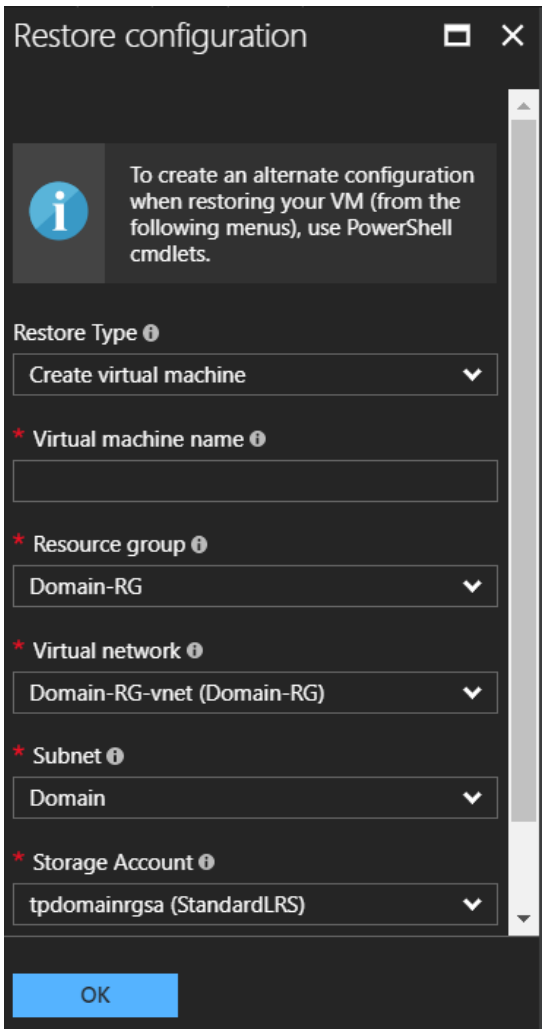


Kuva 101. Palautettavien tiedostojen avaaminen työasemassa.

Virtuaalikoneen palauttaminen varmuuskopiosta

Varmuuskopiosta voi palauttaa vain uuden erinimisen virtuaalikoneen. Jos halutaan luoda samaniminen virtuaalikone, kuin varmuuskopion alkuperäinen lähde, täytyy alkuperäinen virtuaalikone poistaa Azuresta ennen palautusoperaatiota.

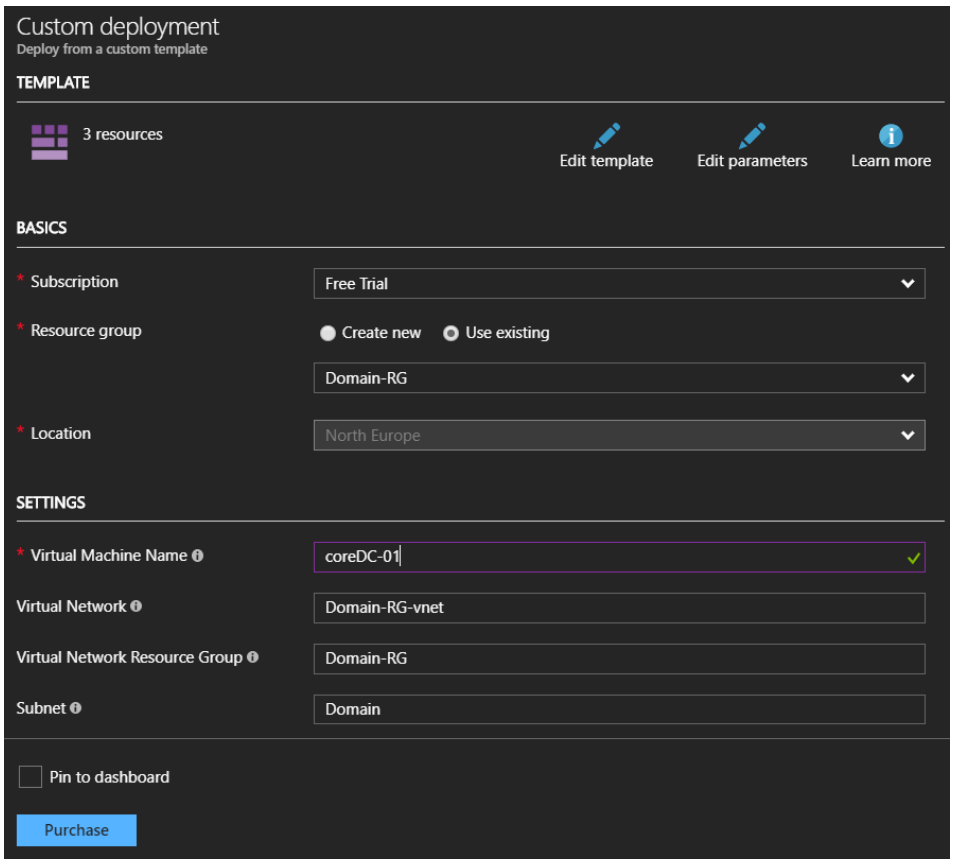
Virtuaalikoneen palautus käynnistetään Recovery Services vaultin kohdasta Backup items > Azure Virtual machine > *Varmuuskopioinnin kohde* > Restore VM > Select restore point: *Haluttu varmuuskopio*. Valitsemalla palautuksen tyypiksi ”Create virtual machine”, voidaan resurssien oletusnimillä luoda palautuspisteestä uusi virtuaalikone (kuva 102).



Kuva 102. Virtuaalikoneen palautus Recovery Services vaultissa.

Valitsemalla palautuksen tyypiksi”Restore disks” Azure palauttaa pelkästään levyt, jolloin voidaan portaalista muuttaa uuden luotavan virtuaalikoneen resurssien nimiä. PowerShellilla voidaan palautetusta levystä luoda halutunkaltainen virtuaalikone, jolloin on mahdollista määrittää uusi kone käyttämään vanhan koneen NSG:tä, verkkokorttia ja IP-osoitetta.

Varmuuskopiointi- ja palautusoperaatioita voi seurata Recovery Services vaultin Jobs > Backup Jobs -kohdasta. Valitsemalla listasta valmistuneen Recovery disks -palautusoperaation ja sen Deploy template -painikkeen voidaan luoda uusi virtuaalikone muokattavilla valinnoilla ja resurssien nimillä, tai vaihtoehtoisesti koko palautuksen templatea voidaan muokata (kuva 103).



Kuva 103. Virtuaalikoneen luominen Recovery Services vaultin palauttamasta levystä.

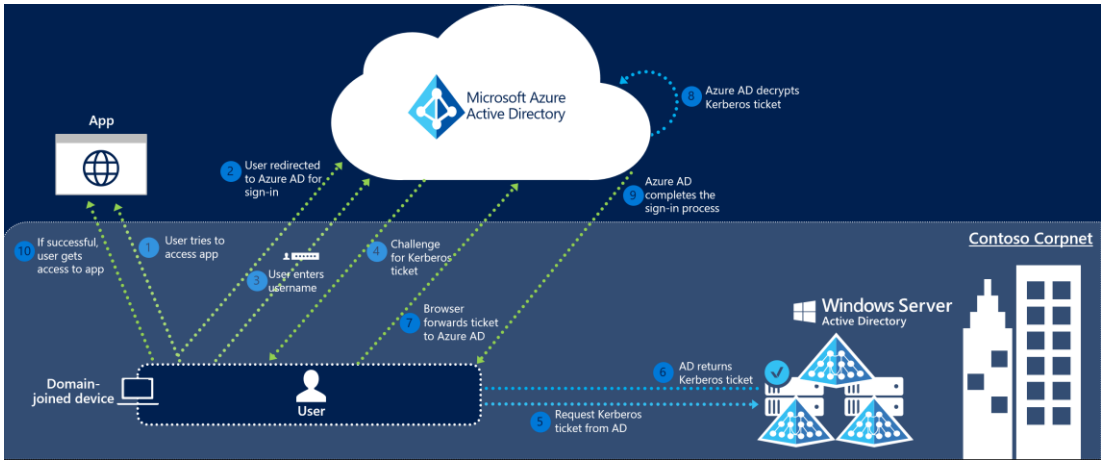
Palauttamisen jälkeen voidaan uusi virtuaalikone manuaalisesti määrittää käyttämään vanhan virtuaalikoneen NSG:tä ja julkista IP-osoitetta ja syöttää kiinteä yksityinen IP-osoite.

7.8 Yhden tunnuksen käyttäminen ja kertakirjautuminen

Azure AD Connect -työkalulla voidaan paikallinen Active Directory synkronoida Azure AD:n kanssa. Näin voidaan mahdollistaa käyttäjille yhden identiteetin ja salasanan käyttäminen AD-ympäristössä ja pilvipalveluissa ja myös kertakirjautumisominaisuuksien (Single sing-on) käyttöönotto.

Kertakirjautumisella tarkoitetaan käyttäjän kirjautumista vain kerran. Käyttäjän kirjautuessa työasemaan hänen identiteettinsä on vahvistettu, joten periaatteessa sitä ei tarvitsisi tietoturvamielessä enää vahvistaa eri verkkopalveluissa. Toisaalta suuremman tietomäärän asettaminen yhden kirjautumisen taakse, tuottaa se yhden tunnuksen paljastumiselle isommat riskit.

Active Directoryn synkronoiminen pilveen mahdollistaa saman tunnuksen ja kertakirjautumisen käyttämisen Azure AD:hen liitetyissä SaaS-sovelluksissa. Tässä insinöörityössä ei oteta käyttöön ylimääräisiä sovelluksia ja kertakirjautuminen todennetaan Microsoftin omilla sivustoilla, jotka hakevat käyttäjän identiteetin Azure Active Directorysta. Koko autentikointi on prosessina esitetty kuvassa 104.

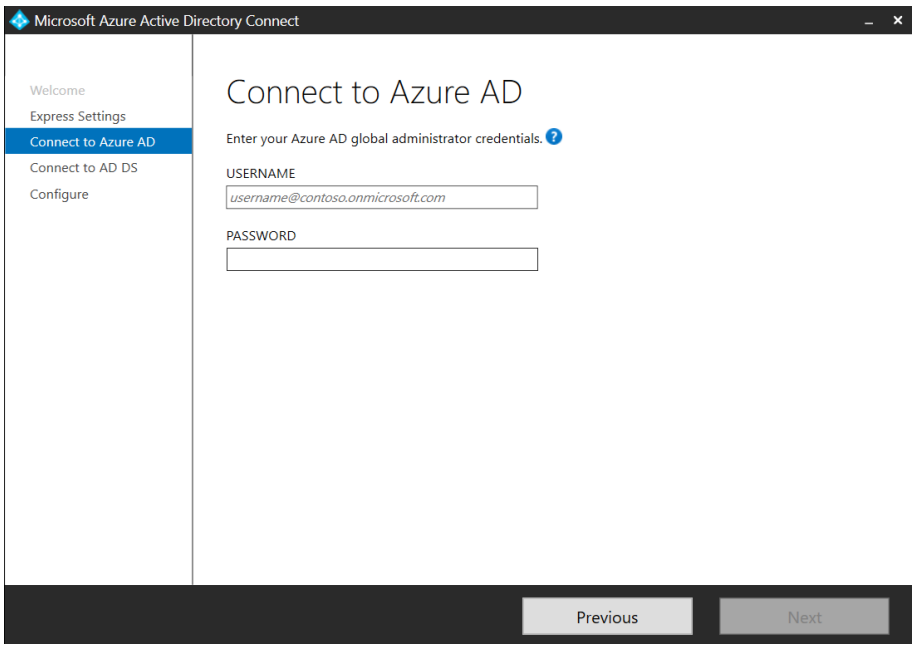


Kuva 104. Azure Active Directory Seamless single sign-on -autentikoinnin toiminta (65).

Paikallisen Active Directoryn synkronoiminen Azure AD:n kanssa

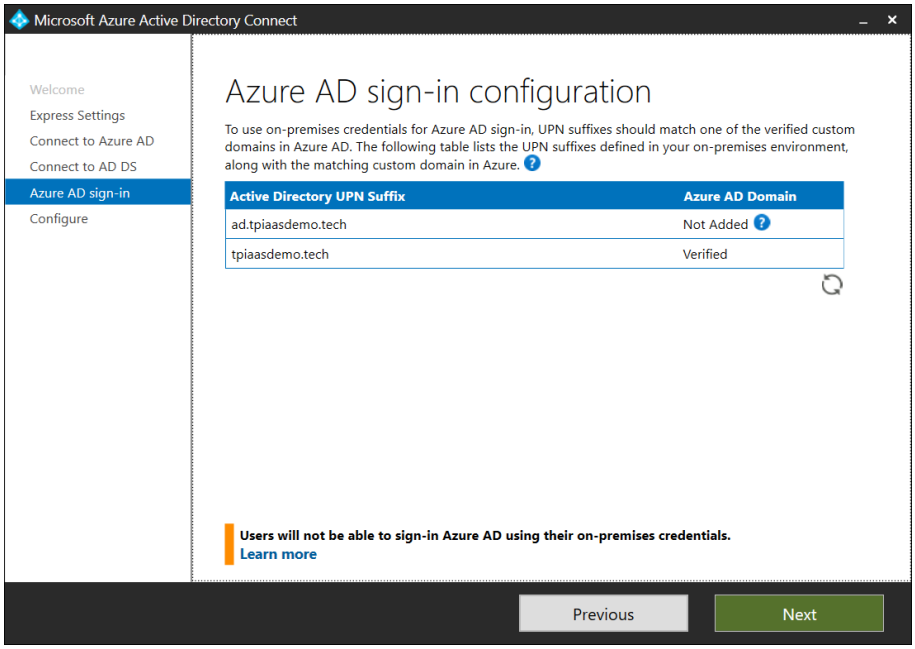
Microsoftin dokumentaation mukaan Azure AD Connect täytyy asentaa koneeseen, jossa on vähintään 4 GB keskusmuistia. Erikseen mainitaan myös, että Azuressa käytettävän virtuaalikoneen mallin täytyy olla suorituskyvyltään vähintään A2:n veroinen. Tähän tarkoitukseen käytetään Fileserver-01-virtuaalikonetta, jonka malliksi päivitetään virtuaalikoneen Size-valikosta 2 vCPU:lla ja 4 GB:n keskusmuistilla varustettu A2_V2. Malli tukee myös neljää datalevyä ja maksaa 81,56 euroa kuukaudessa. (64; 66.)

Azure AD Connectin asennuspaketin saa ladattua Microsoftin sivuilta, ja lataamisen jälkeen käynnistetään Azure AD Connectin asennus käyttäen Use express settings -valintaa. Custom install -valinnalla voidaan konfiguraatiota määrittää edistyksellisemmin, muun muassa multi-domain-ympäristöjen synkronoinnin suhteen. Express settings -valinnan jälkeen täytyy asennusohjelmalle syöttää Azure AD:n järjestelmänvalvojan tunnus (kuva 105), joka tässä tapauksessa on anssi.asentaja@tpiaasdemo.tech.



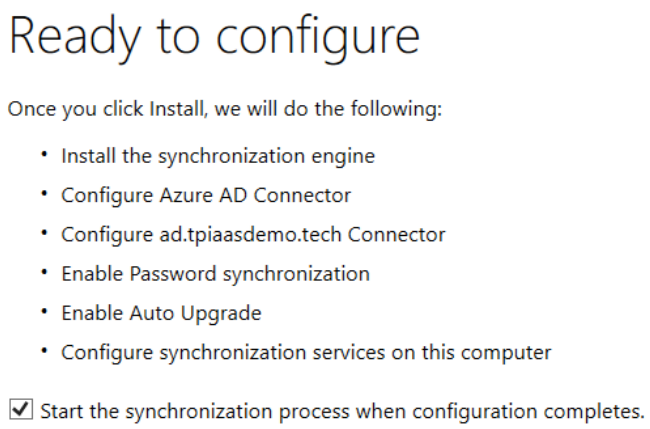
Kuva 105. Azure AD Connectin määritys 1.

Seuraavassa kohdassa täytyy syöttää paikallisen Active Directoryn Enterprise Administrator -tunnus, ja sitä seuraavassa kohdassa (kuva 106) näytetään paikalliseen Active Directoryyn määritetyt UPN-jälkiliitteet. Synkronoitavien käyttäjien UPN-jälkiliitteen täytyy vastata Azure AD:ssa vahvistettua verkkotunnusta, jotta käyttäjät voivat käyttää samoja tunnuksia kirjautumiseen molemmissa ympäristöissä. Tämän takia määritettiin käyttäjille UPN-jälkiliite aikaisemmin.



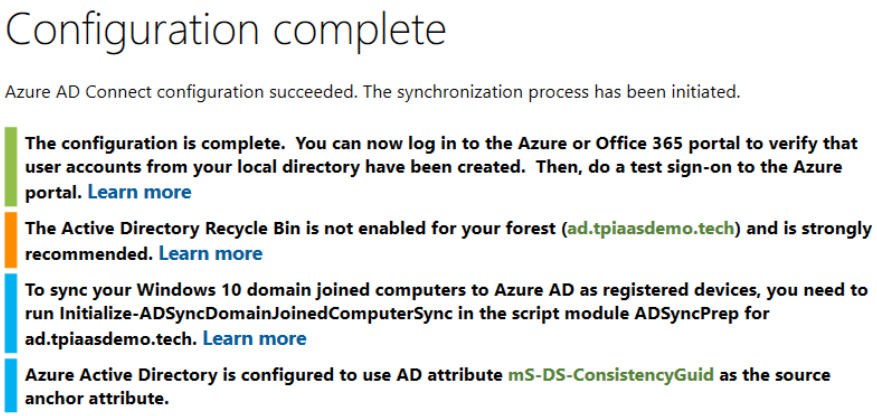
Kuva 106. Azure AD Connectin määritys 2.

Näiden määritysten jälkeen Azure AD Connect on valmis asennettavaksi. Kuvassa 107 asennusohjelma näyttää vielä yhteenvedon asennuksen määrityksistä ennen asennuksen käynnistämistä.



Kuva 107. Azure AD Connectin asennuksen käynnistämisikkuna.

Ohjelman asennuksen jälkeen näytetään vielä lisätietoja asennukseen ja synkronointiin liittyen ja mahdollisesti suositeltavia toimenpiteitä. Kuten kuvasta 108 näkee, on suositeltavaa ottaa käyttöön Azure Active Directory Recycle Bin.



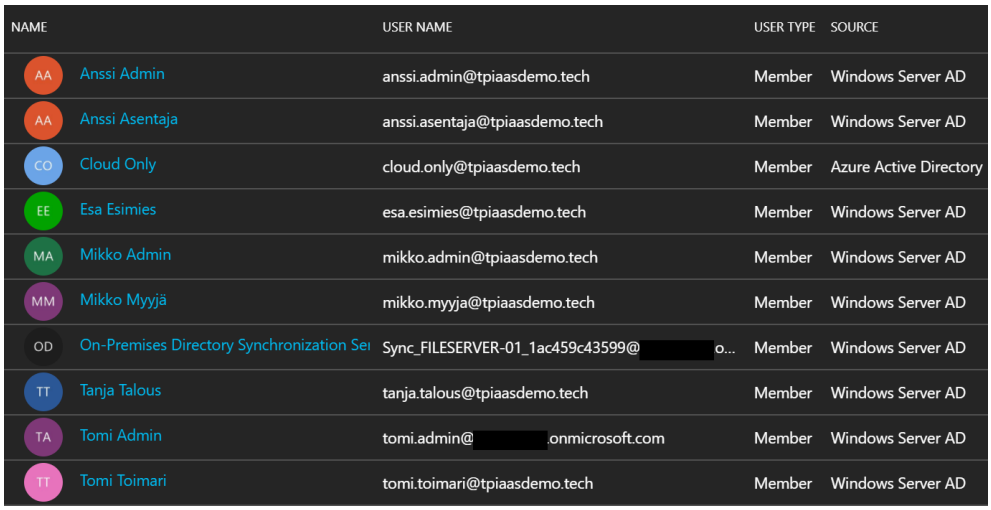
Kuva 108. Valmistuneen Azure AD Connectin asennuksen yhteenvetoikkuna.

Muutama huomio tunnusten hallitsemisesta synkronoinnin jälkeen:

- Paikallisessa Active Directoryssa sijaitseva eri UPN-jälkiliitteellä oleva tunnus replikoituu Azure AD:hen microsoftonline.com-jälkiliitteellä, kuten kuvassa 109 Tomi Admin -tunnus.

- Azure AD:n puolella tehdyt tunnukset eivät replikoidu paikalliseen AD:hen, vaan synkronointi on yksisuuntainen, kuten kuvassa 109 Cloud Only -tunnus.

- Synkronoituja objekteja hallitaan vain yhdestä hakemistosta. Paikallisessa AD:ssa sijanneiden tunnusten hallitseminen säilyy paikallisessa AD:ssa. Kuvassa 109 näkyy Azure Active Directoryn All users -näkymä, jossa Source-sarakkeessa näkyy hakemisto, josta kutakin tunnusta hallitaan.

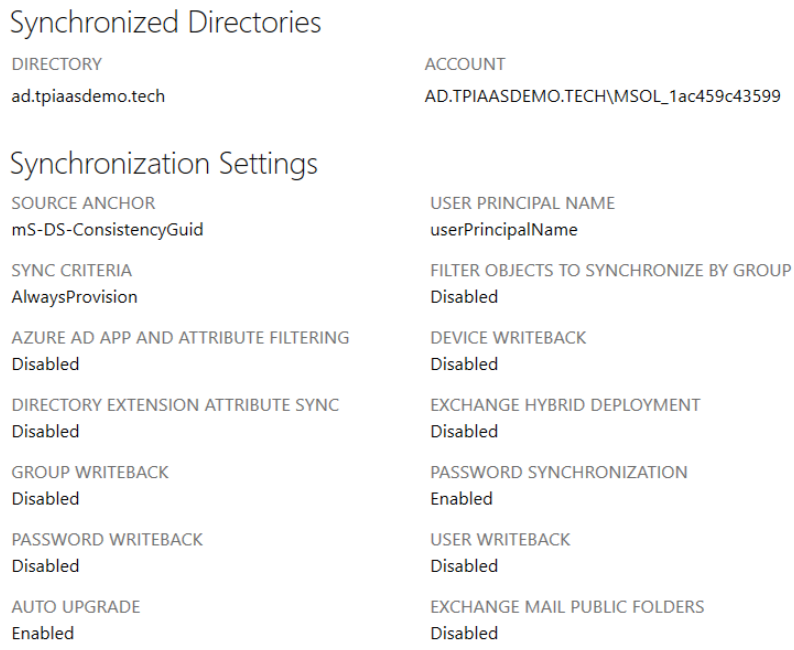


NAME	USER NAME	USER TYPE	SOURCE
AA Anssi Admin	anssi.admin@tpiaasdemo.tech	Member	Windows Server AD
AA Anssi Asentaja	anssi.asentaja@tpiaasdemo.tech	Member	Windows Server AD
CO Cloud Only	cloud.only@tpiaasdemo.tech	Member	Azure Active Directory
EE Esa Esimies	esa.esimies@tpiaasdemo.tech	Member	Windows Server AD
MA Mikko Admin	mikko.admin@tpiaasdemo.tech	Member	Windows Server AD
MM Mikko Myyjä	mikko.myyja@tpiaasdemo.tech	Member	Windows Server AD
OD On-Premises Directory Synchronization Ser	Sync_FILESERVER-01_1ac459c43599@ [redacted] o...	Member	Windows Server AD
TT Tanja Talous	tanja.talous@tpiaasdemo.tech	Member	Windows Server AD
TA Tomi Admin	tomi.admin@ [redacted] .onmicrosoft.com	Member	Windows Server AD
TT Tomi Toimari	tomi.toimari@tpiaasdemo.tech	Member	Windows Server AD

Kuva 109. Azure AD:n käyttäjät synkronoinnin käyttöönoton jälkeen.

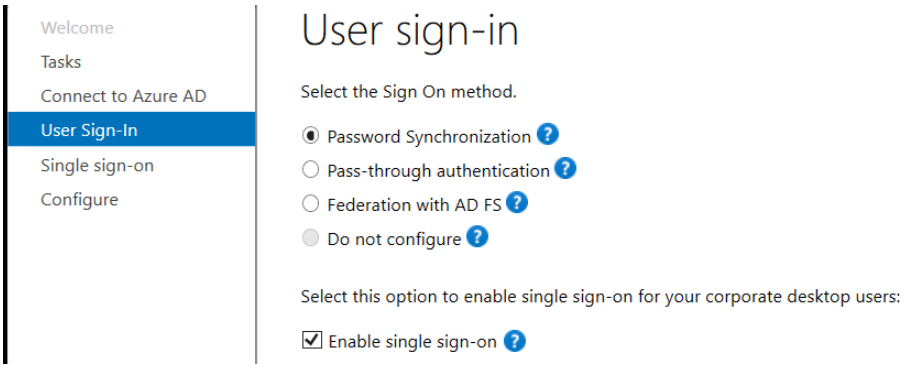
Kertakirjautumisen käyttöönotto

Kertakirjautumisen konfiguroimiseksi avataan Azure AD Connect ja valitaan configure, jolloin avautuu valittavaksi erilaisia konfigurointivaihtoehtoja. Täältä voi myös valita View current configuration, jolloin saa näkymän nykyisen synkronoinnin asetuksista kuvan 110 mukaisesti. Kertakirjautumisen voi konfiguroida myös kerralla Custom install -asennuksella, mutta tämä tapa on yksinkertaisempi demonstroida.



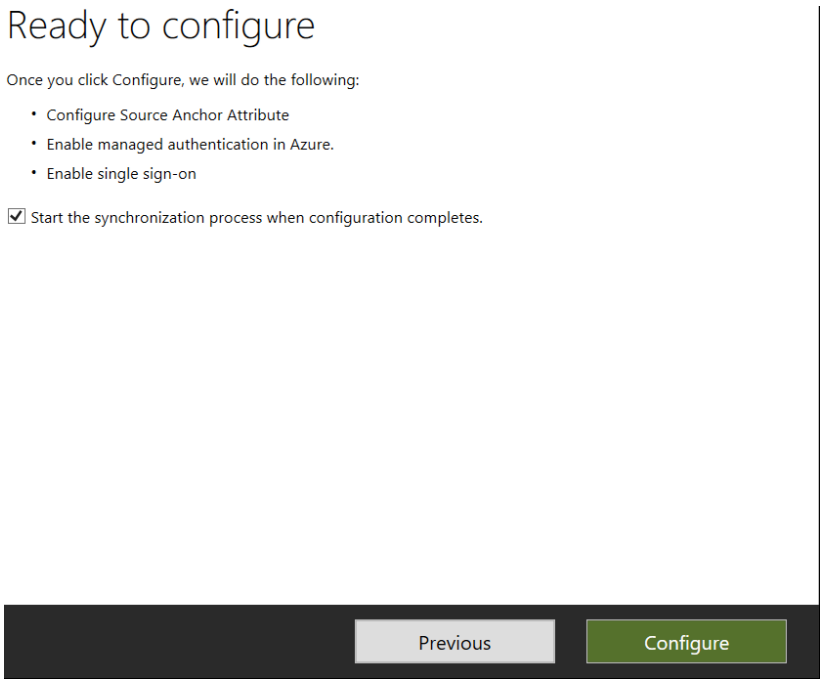
Kuva 110. Azure AD Connectin konfiguraatio.

Kertakirjautumisen konfiguroimiseksi valitaan Azure AD Connectista Change User Sing-in ja syötetään Azure AD:n järjestelmänvalvojan tunnus. Tämän jälkeen laitetaan valinta Enable single sign-on -ruutuun ja jatketaan eteenpäin (kuva 111).



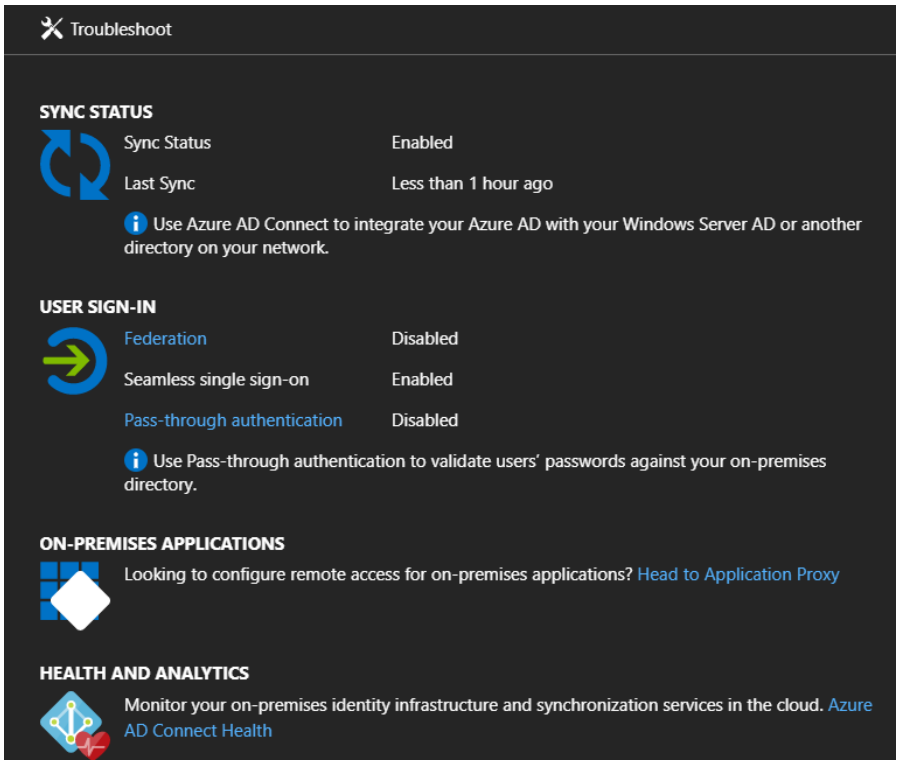
Kuva 111. Kertakirjautumisen konfigurointi Azure AD Connectissa.

Seuraavassa kohdassa täytyy antaa toimialueen järjestelmänvalvojan tunnukset, minkä jälkeen ohjelma ilmoittaa, mitä muutoksia tehdään (kuva 112). Muutokset otetaan käyttöön configure-painikkeella.



Kuva 112. Kertakirjautumisen käyttöönotto Azure AD Connectissa.

Konfiguroinnin jälkeen kertakirjautumisen tilan voi tarkistaa Azure AD:sta valitsemalla Azure AD Connect -valikon, joka näyttää tietoja Azure AD Connectin tilasta. Kuten kuvasta 113 huomaa, Seamless single sing-on on nyt tilassa enabled.



Kuva 113. Azure Active Directoryn Azure AD Connect -valikko.

Tällä tavalla käyttöönotetun kertakirjautumiseen mahdollistamiseksi tarvitsee käyttäjän olla kirjautuneena yrityksen laitteeseen, jolla on yhteys Domain Controlleriin ja jolla on lisättynä seuraavat osoitteet intranetvyöhykkeeseen: https://autologon.microsoftazuread-sso.com ja https://aadg.windows.net.nsatc.net.

Tällä hetkellä Anssi Asentaja kirjautuu työasemalle, jonka konetunnus on olemassa Active Directoryssa, käyttäen toimialueen tunnusta, ja yhteys DC:hen on olemassa VPN:n ollessa päällä. Viimeinen vaatimus voidaan täyttää luomalla Group Policy -objecti, joka lisää mainitut sivustot intranetvyöhykkeeseen. Tämän määrityksen pystyy tekemään GPO:n polusta ”User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Site to Zone Assignment List” ja määrittämällä ”Value name” -kohtaan internetosoitteen ja määrittämällä ”Value” -kohtaan arvon 1 kertomaan vyöhykkeen, johon osoitteet halutaan lisätä.

Kun GPO oli luotu ja työasema pakotettu päivittämään Group Policyt gpupdate /force -komennolla, päivittyi työasemaan kertakirjautumisen viimeinen vaatimus. Tämän jälkeen toiminnallisuutta voi testata esimerkiksi menemällä portal.office.com-osoitteeseen. Sivustolla syötin Anssi Asentajan käyttäjänimen, minkä jälkeen siirryttiin salasanan syöttämiseen, josta selain ohjautui suoraan palveluun, ilman että salasanaa tarvitsi syöttää. Kertakirjautuminen oli siis toiminnassa, ja testasin sen myös toimivan Chrome-selaimella, ilman lisä konfigurointia.

7.9 Vikasietoisuus

Kahdelle samassa availability set -palvelussa sijaitsevalle virtuaalikoneelle, Microsoft lupaa vähintään yhdelle virtuaalikoneelle 99,95 %:in SLA:n. Kahden virtuaalikoneen konfiguroiminen samaan availability setiin tuo lisää kapasiteettia palvelemaan käyttäjien pyyntöjä, mutta samaa virtuaalikonemallia käytettäessä hinta kaksinkertaistuu.

Microsoft lupaa 99,9 %:in SLA:n yhdelle virtuaalikoneelle, jonka käyttöjärjestelmälevy ja datalevyt käyttävät premium storagea. Jotta SLA:n voisi saavuttaa yhdellä Domain Controllerilla ja yhdellä tiedostopalvelimella, täytyisi kaikkien datalevyjenkin levyjen käyttää premium storagea. (67).

Premium storagessa laskutetaan provisioidusta kapasiteetista eikä todellisen tilan käytön mukaan. Käyttöjärjestelmälevyksi valikoituisi oletuksena 128 GB:n kapasiteetilla varustettu P10-levy, joka maksaa 18,29 € ja tiedostopalvelimella datalevyksi yksi 2 TB:n kapasiteetilla varustettu P40-levy, joka maksaa 218,46 €. Näin ollen tiedostopalvelimen yksi P10-levy ja yksi P40-levy maksaisivat 236,7 €/kk.

Standardissa storage accountissa hinnoittelu on käytön mukaista. Paikallisen datakeskuksen replikointikonfiguraatiolla (Locally redundand Storage, LRS) yksi gigatavu maksaa 0,0422 €, jolloin koko premium storage accountissa luotava kapasiteetti maksaisi noin 92 €/kk. (64.) Tämän hintaeron takia ratkaisussa ei käytetty premium storage accountia, eikä myöskään availability set -palvelua SLA:n saavuttamiseksi.

Vaikkei tällä konfiguraatiolla saadakaan virtuaalikoneille Microsoftin lupaamaa SLA:ta, on Azure rakennettu vikasietoiseksi ja Microsoft lupaa Storagelle 99,9 %:in SLA:n, jolloin virtuaalikoneiden levyjen data säilyy ja on saatavissa, vaikkei virtuaalikone olisikaan käytettävissä (67).

Azuren alustan havaitessa infrastruktuurin vikaantumisen käynnistyy virtuaalikoneiden live-migraatio toimivalle isäntäkoneelle (host), jolloin virtuaalikone on hetken aikaa pysäytettynä. Odottamattomassa infrastruktuurin vikaantumisessa virtuaalikoneet uudelleenkäynnistetään osana automaattista migraatiota toimivalle isäntäkoneelle.

Azuren infrastruktuurille voidaan tehdä suunniteltuja huoltotoimenpiteitä, joissa virtuaalikone pysäytetään 30 sekunniksi, ilman ilmoitusta käyttäjälle. Uudelleenkäynnistystä vaativissa huoltotoimenpiteissä ilmoitetaan käyttäjälle ja käyttäjä voi manuaalisesti siirtää virtuaalikoneen jo päivitetylle isäntäkoneelle, tai odottaa huoltoikkunan alkamista, jolloin virtuaalikone uudelleenkäynnistetään pakotetusti. Virtuaalikoneille on portaalissa myös redeploy-painike, jolla virtuaalikone voidaan migroida toiseen isäntäkoneeseen, esimerkiksi käyttäjän kohdatessa ongelmia virtuaalikoneen käynnistämisessä. (68; 69.)

Varmuuskopion palautuksella voidaan Domain Controller palauttaa takaisin toimintakuntoon esimerkiksi virheellisen konfiguraation tai datan korruptoitumisen jäljiltä. Varmuuskopiolla ja Geo-redundant-replikoinnilla konfiguroidulla storage accountilla voidaan virtuaalikone myös luoda toiseen datakeskukseen esimerkiksi datakeskuksen ollessa laajan häiriön tai katastrofin vaikutuksen alaisena. Microsoftilla on myös omia toimintatapoja datakeskuksen resurssien siirtämisestä sen vastapariin, mutta näillä ei ole SLA:ta, eikä käyttäjä pysty vaikuttamaan operaation aikatauluun.

Varmuuskopiosta voidaan luoda uusi virtuaalikone tai luoda samanniminen virtuaalikone korvaamaan alkuperäinen, poistamalla ensin alkuperäinen. Virtuaalikoneen luomista varmuuskopiosta kannattaa harjoitella ja testata ja myöskin luoda toimintatapa minkälaisessa tilanteessa palautus toteutetaan. Palautus voidaan käynnistää nopeasti ja suunnitellusti esimerkiksi PowerShell skriptillä, joka luo varmuuskopioidun virtuaalikoneen levystä uuden virtuaalikoneen vanhan tilalle ja ottaa vanhan virtuaalikoneen verkkokortin, IP-osoitteen ja NSG:n omiksi resursseikseen.

8 Yhteeveto

Insinöörityössä luotiin pilvipalvelujen avulla kolme erilaista ratkaisua vastaamaan mikroyrityksen perusinfrastruktuuritarpeita. Kaikissa ratkaisussa pystyttiin luomaan keskitetysti hallittavat käyttäjätunnukset ja tiedostonjakoratkaisu. Ensimmäisessä ratkaisussa ei luoda ollenkaan virtuaalipalvelimia eikä VPN-yhdyskäytävää, mikä vähentää kuukausittaisia kustannuksia ja myös ylläpitotyötä. Tiedostonjakoratkaisuna käytettävää SharePoint Onlinea pystytään käyttämään missä vain, milloin vain, millä tahansa laitteella, eikä se tarvitse samanlaista ylläpitoa kuin palvelin, mutta sen muutostöihin ja hallintaan tarvitaan kuitenkin henkilöresurssia. Ratkaisu 2:ssa taas Domain Controllereita ei tarvitse ylläpitää, mutta luotavasta tiedostopalvelimesta tai muista luotavista palvelimista kertyy ylläpitotyötä.

Ensimmäisessä ja toisessa ratkaisussa käyttäjätunnuksia hallitaan Azure Active Directoryn kautta ja työasemia Intunen kautta. Azure AD on helppokäyttöinen, mutta Intunen haltuunotto vaatii käyttäjältä osaamista, ja monimutkaisemmat työasemien määritykset vaativat vielä enemmän osaamista. Intunen työasemien hallinnan kyvykkyys omiin tarpeisiin kannattaa määrittää ja kartoittaa tarkasti. Kuten muutkin Microsoftin pilvipalvelut, on Intune jatkuvan kehityksen alla ja sen OMA-URI-arvoilla pystytään toteuttamaan laajasti erilaisia määrityksiä ja käytäntöjä. Intuneen on hiljattain lisätty myös muun muassa tuki suorittaa PowerShell-skriptejä Windows 10 -työasemissa, jolloin työasemien hallinnan mahdollisuudet laajentuvat entisestään.

Ratkaisu 3 taas on puhdas IaaS-toteutus, jolloin joutuu ylläpitämään Domain Controlleria sekä muita palvelimia, mutta käyttäjien ja laitteiden hallintatavat ovat ylläpitäjille tuttuja perinteisestä maailmasta. Ratkaisu 3:ssa pystytään työasemia hallitsemaan Group Policyilla tai käyttämään jotain muuta ratkaisua perinteisessä toimialue-ympäristössä.

Käyttäjä voi ottaa työaseman itsepalveluna käyttöön kahdessa ensimmäisessä ratkaisussa, mutta ratkaisu 2:n VPN-yhteys ja tiedostojaot täytyy käyttäjän määrittää itse tai selvittää niiden toteutus esimerkiksi Intunella. Myös ratkaisu 3:ssa täytyy määrittää manuaalisesti VPN-yhteys ja työaseman käyttöönotto on paljon hankalampi prosessi toimialueeseen liittymisen takia, minkä vuosi tässä ei voida puhua itsepalvelukäyttöönotosta. Site-to-Site-VPN-yhteydellä liittyminen olisi helpompaa, mutta sitä ei ajanpuutteen takia toteutettu tässä insinöörityössä. Näiden puutteiden takia ratkaisuissa on vielä kehittämisen varaa. Site-to-Site-VPN-yhteys on todennäköinen avaintekijä ratkaisu 3:n itsepalvelukäyttöönoton tai ylipäätänsä käyttöönoton yksinkertaistamiseksi.

Kaikissa kolmessa ratkaisussa suoritettiin tiedonsiirtonopeustestejä työaseman ja tiedostojaon välillä. Lataus- ja lähetysnopeutta testattiin yhdellä isolla tiedostolla ja suurella määrällä pieniä tiedostoja, mutta ratkaisu 2:n lataustesti jäi tekemättä. Isona tiedostona käytettiin noin 350 MB:n kokoista vmdk-tiedostoa, ja pieninä tiedostoina käytettiin eri tiedostomuotoisia dokumentteja ja kuvia, yhteensä noin 350 MB:n edestä. Tiedonsiirtoon käytetty aika mitattiin ratkaisu 1:n nopeustesteissä sekuntikellolla ja ratkaisu 2:ssa ja 3:ssa käytettiin Robocopy-komentorivityökalun luomaa lokitiedostoa.

Tiedonsiirtonopeustestit tehtiin 100/10 Mbps -nopeuksisella, langallisella internetyhteydellä. Testille ei luotu mitenkään erityisen häiriöttömiä olosuhteita, mutta lopputuloksena (taulukko 3) käytettiin useamman testin keskiarvoa. Laskelmasta poistettiin silmämääräisestä keskiarvosta paljon poikkeavat tulokset satunnaisten poikkeamien vaikutusten kumoamiseksi. Ratkaisu 2:n virtuaalikoneet sijaitsivat Länsi-Euroopan datakeskuksessa, ja ratkaisu 3:ssa Pohjois-Euroopassa. Taulukossa esitellyissä tuloksista on nähtävissä, että ratkaisu ykkösen Sharepoint Onlinen synkronoinnilla vaikuttaa olevan tehokas kyky käsitellä pieniä dokumentteja, kun vertaa tiedonsiirtonopeuksia muihin ratkaisuihin. Länsi-Euroopan datakeskuksella näyttää myös olevan nopeampi yhteys Suomeen kuin Pohjois-Euroopan datakeskuksella.

Taulukko 3. Kaikkien ratkaisujen tiedonsiirtonopeustestien keskiarvot.

	Ratkaisu 1	**Ratkaisu 2**	**Ratkaisu 3**
Lataus			
Pienet tiedostot	1 min 29 s	-	8 min 41 s
Iso tiedosto	0 min 57 s	-	1 min 4 s
lähetys			
Pienet tiedostot	6 min 16 s	9 min 21 s	11 min 32 s
Iso tiedosto	6 min 0 s	2 min 26 s	2 min 53 s

Insinöörityö tehtiin mikroyritysnäkökulmasta viidelle käyttäjälle, ja tämän takia valittiin edulliset ja matalalla suorituskyvyllä varustetut resurssit. Virtuaalikoneiden mallia voi vaihtaa ja määrää lisätä vastaamaan suurempaa käyttäjämäärää, ja Azureen saa muodostettua myös hyvinkin nopeita VPN- ja ExpressRoute-yhteyksiä, jos suorituskyky alkaa riippua verkon kapasiteetista. Ratkaisu 1:ssä käytetään automaattisesti skaalautuvia pilvipalveluita, joiden suorituskykyä ei määritellä. Näin ollen ratkaisu 1:n skaalautuu sellaisenaan isoillekin käyttäjämäärille, tosin SharePoint Online ei välttämättä tässä vaiheessa ole hyvä tuote tiedostojakoon.

Ratkaisu 3:ssa käytetty A0:n suorituskyky riitti testikäyttöön, mutta tuotantokäytön kuormituksessa tilanne voi olla erilainen. Jaetun suorittimen käyttö ei myöskään ole kovin perusteltua vajaan 30 euron kuukausittaiseen säästöön nähden. Myös toisessa ja kolmannessa ratkaisussa käytetyn F1-mallin suorituskyky oli riittävä, eikä tiedonsiirtonopeuksiin vaikuttanut suurimman osan keskusmuistista vievän Wiresharkin suorittaminen taustalla. Jossain tilanteissa voi 2 GB:n keskusmuisti kuitenkin jäädä pieneksi ja virtuaalikonemalli täytyy päivittää tehokkaammaksi.

Azuressa kertyy kustannuksia sen datakeskuksesta ulospäin kulkevasta verkkoliikenteestä ensimmäisen ilmaisen 5 gigatavun jälkeen 0,075 € jokaisesta gigatavusta, ja virtuaalikoneiden kiintolevyille suoritettavasta jokaisesta 10 000 operaatiosta (transaktio, luku ja kirjoitus) veloitetaan 0,000304 €. Käytännössä operaatioista ei aiheudu kustannuksia, eikä niitä ole huomioitu laskelmissa. Taulukossa 4 on esitetty eri ratkaisujen kuukausi- ja vuosihinnat viidelle käyttäjälle. Laskettaessa hintaa muille käyttäjämäärille voi laskelmassa muuttaa lisenssimääriä vastaamaan haluttua käyttäjämäärää, jos suorituskyky ja verkon kapasiteetti riittää laskennalliselle käyttäjämäärälle. Laskelmissa on käytetty esimerkkinä 100 GB:n verkkoliikennettä ja 100 GB:n kokoista tiedostojakoa ja käyttöjärjestelmälevyjen tilan käyttö on laskettu suurin piirtein minimikäytön mukaan. Azure AD Connectin vaatimaa tehokkaampaa virtuaalikonetta ei ole huomioitu kustannuksissa, mutta sen vaatimaa suorituskykyä varten voi tiedostopalvelimen päivittää tarvittaessa A2_v2:ksi (80,25 €/kk). Hinnat perustuvat Azure Pricing calculator -sivuston käyttämään 732 tunnin (30,5 vuorokautta) hintaan. Jos esimerkiksi tiedostopalvelinta ei tarvitse pitää päällä ympärivuorokauden jokaisena päivänä, vaan ainoastaan arkisin 12 tuntia, virtuaalikoneen kustannuksia saadaan laskettua alle 40 %:iin alkuperäisestä hinnasta. (64.)

Taulukko 4. Insinöörityössä tehtyjen ratkaisujen vähimmäiskustannukset (64).

	Ratkaisu 1		**Ratkaisu 2**		**Ratkaisu 3**	
	Tuote	Hinta	Tuote	Hinta €	Tuote	Hinta €
Domain Controller	-	-	AAD DS	96,20	A0	12,35
Tiedostopalvelin	-	-	F1	63,58	F1	63,58
Käyttöjärjestelmien levytila (LRS)	-	-	14 GB	0,60	24 GB	1,00
Tiedostojaon tiedostot	sis. hintaan	-	100 GB	4,22	100 GB	4,22
VPN	-	-	Basic	22,23	Basic	22,23
VPN:n tiedonsiirto	-	-	100 GB	7,03	100 GB	7,03
EMS E3 7,40 €	5:lle käyttäjälle	37,00	-	0,00	-	0,00
Office 365 Business Premium 10,50 €	5:lle käyttäjälle	52,50	5:lle käyttäjälle	52,50	5:lle käyttäjälle	52,50
Recovery Services vault (varmuuskopiot)	-	-	Instanssit	8,43	Instanssit	12,65
Varmuuskopioiden levytila (GRS)	-	-	114 GB	4,62	124 GB	5,02
Kuukausihinta	89,50 €		259,41 €		180,58 €	
Vuosihinta	1 074,00 €		3 112,96 €		2 166,96 €	

Taulukossa 5 esitetään korkeampaa suorituskykyä edustavat tuotteet. Jaetun suorittimen A0-virtuaalikonemalli on vaihdettu A1:een, tiedostopalvelimeksi on valittu enemmän muistia sisältävä D1_V2, ja VPN-yhdyskäytäväksi on vaihdettu 650 Mbps-nopeudella toimiva VpnGw1.

Taulukko 5. Insinöörityössä tehtyjen ratkaisujen korkeamman suorituskyvyn kustannukset (64).

	Ratkaisu 1		**Ratkaisu 2**		**Ratkaisu 3**	
	Tuote	Hinta €	Tuote	Hinta €	Tuote	Hinta €
Domain Controller	-	-	AAD DS	96,20	A1	55,56
Tiedostopalvelin	-	-	D1_V2	84,70	D1_V2	84,70
Käyttöjärjestelmien levytila (LRS)	-	-	14 GB	0,60	24 GB	1,00
Tiedostojaon tiedostot	sis. hintaan	-	100 GB	4,22	100 GB	4,22
VPN	-	-	VpnGw1	117,29	VpnGw1	117,29
VPN:n tiedonsiirto	-	-	100 GB	7,03	100 GB	7,03
EMS E3 7,40 €	5:lle käyttäjälle	37,00	-	0,00	-	0,00
Office 365 Business Premium 10,50 €	5:lle käyttäjälle	52,50	5:lle käyttäjälle	52,50	5:lle käyttäjälle	52,50
Recovery Services vault (varmuuskopiot)	-	-	Instanssit	8,43	Instanssit	12,65
Varmuuskopioiden levytila (GRS)	-	-	114 GB	4,62	124 GB	5,02
Kuukausihinta	89,50 €		375,59 €		339,97 €	
Vuosihinta	1 074,00 €		4 507,12 €		4 079,64 €	

Taulukosta 4 on nähtävissä, että 5 hengen mikroyritykselle voidaan toteuttaa täysin palveliton infrastruktuuritratkaisu alle 100 euron kuukausihinnalla (ratkaisu 1). Alle 200 euron kuukausihinnalla voidaan toteuttaa vaihtoehto konesalikapasiteetin ostamiselle (ratkaisu 3), tosin työskentelyn sujuvoittamiseksi tähän täytyy laskea palomuurin ostohinta mukaan, jolla voidaan toteuttaa Site-to-Site-VPN-yhteys.

Insinöörityössä esitellyillä ratkaisuilla voidaan hyvin korvata ainakin yksinkertainen pieni palvelininfrastruktuuri, jossa käyttäjien työasemia ei ole suuremmin rajoitettu. Ratkaisuja käytiin tavallaan konsepti- ja demo mielessä läpi, ja ratkaisujen käyttökokemusta ei tutkittu oikeassa ympäristössä, jossa yrityksen käyttämä infrastruktuuri siirretään pilveen. Ensimmäisessä ratkaisussa käytetään SaaS-sovelluksia, jolloin palvelinten toiminnalla ei ole vaikutusta ratkaisuun.

Insinöörityössä luotuja mikroyrityksen laite- ja identiteetinhallintaratkaisuja voi teknisesti hyödyntää vastaavissa tilanteissa, ja työssä saatiin selvitettyä näiden ratkaisujen hinnat. Ratkaisuista saa kattavamman kokemuksen integroimalla SaaS-sovelluksia Azure AD:hen, ja ottamalla sovelluspalvelimia käyttöön Azuren virtuaaliverkkoon. Ratkaisuja voi jalostaa enemmän automatisoidussa käyttöönotossa.

Lähteet

1 What is Identity and Access Management? Verkkoaineisto. Karin Group. <http://www.karingroup.com/eng/about/what_is_identity.pdf>. Luettu 30.5.2017.

2 Niemi, Kalle. Identiteetin ja pääsynhallinta (IAM). Verkkoaineisto. <https://www.itewiki.fi/opas/kayttajahallinta-iam/>. Luettu 30.5.2017.

3 Linden, Mikael. 2015. Identiteetin- ja pääsynhallinta. Verkkoaineisto. Tampere University of Technology. Department of Pervasive Computing. Report, Vuosikerta. 6, Tampere University of Technology. <https://tutcris.tut.fi/portal/files/3087873/linden_identiteetin_ja_paasynhallinta.pdf>. Luettu 30.5.2017.

4 Roll out password reset for users. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-best-practices>. Luettu 31.5.2017.

5 Setting up Azure Active Directory for self-service group management. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management>. Luettu 31.5.2017.

6 Managing owners for a group. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-managing-group-owners>. Luettu 31.5.2017.

7 What is Azure Active Directory? 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis>. Luettu 31.5.2017.

8 Forest: Implementation of All Trees. Verkkoaineisto. Microsoft. <https://technet.microsoft.com/en-us/library/cc978004.aspx>. Luettu 1.6.2017.

9 What Are Domains and Forests? 2014. Verkkoaineisto. Microsoft. <https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx>. Luettu 1.6.2017.

10 McDonough, Michele. 2015. Understanding Active Directory Containers. Verkkoaineisto. <http://www.brighthub.com/computing/windows-platform/articles/33795.aspx>. Luettu 1.6.2017.

11 Clerk, Jan De. 2007. Comparing Windows Kerberos and NTLM Authentication Protocols. Verkkoaineisto. <http://windowsitpro.com/security/comparing-windows-kerberos-and-ntlm-authentication-protocols>. Luettu 2.6.2017.

12 Protocols and Interfaces to Active Directory. Verkkoaineisto. Microsoft. <https://technet.microsoft.com/en-us/library/cc961766.aspx>. Luettu 2.6.2017.

13 Supported Authentication Methods. Verkkoaineisto. Microsoft. <https://msdn.microsoft.com/en-us/library/cc223498.aspx>. Luettu 2.6.2017.

14 Fundamentals of Azure identity management. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/identity-fundamentals#connect-on-premises-active-directory-with-azure-ad-and-office-365>. Luettu 31.5.2017.

15 Azure Active Directory Pricing. Verkkoaineisto. Microsoft. <https://azure.microsoft.com/en-us/pricing/details/active-directory>. Luettu 12.7.2017.

16 How to provide secure remote access to on-premises applications. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/active-di rectory-application-proxy-get-started>. Luettu 2.6.2017.

17 Panettieri, Joe. 2017. Cloud Market Share 2017: Amazon AWS, Microsoft Azure, IBM, Google. Verkkoaineisto. <https://www.channele2e.com/2017/02/09/cloud-market-share-2017-amazon-microsoft-ibm-google/>. Julkaistu 9.2.2017. Luettu 7.6.2017.

18 Castrillo, Ileana & Rountree Derrick. The Basics of Cloud Computing. E-kirja. USA: Syngress.

19 Azure subscription and service limits, quotas, and constraints. 2017. Verkkoaineisto. <https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits>. Luettu 7.6.2017.

20 Caithness, Neil ; Drescher, Michel & Wallom David. 2017. Journal of Cloud Computing; Advances, Systems and Applications. Verkkoaineisto. <https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-017-0084-1>. Julkaistu 5.6.2017. Luettu 8.6.2017.

21 SLA summary for Azure services. 2017. Verkkoaineisto. Microsoft. <https://azure.microsoft.com/en-gb/support/legal/sla/summary>. Luettu 7.7.2017.

22 Grance,Timonthy & Mell, Peter. 2011. The NIST Definition of Cloud Computing. Verkkoaineisto. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Luettu 7.6.2017.

23 Stamey, Laura. 2017. IaaS vs. PaaS vs. SaaS Cloud Models (Differences & Examples). Verkkoaineisto. <http://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas>. Julkaistu 30.5.2017. Luettu 8.6.2017.

24 Koskinen, Ernesto. 2016. Palvelut pilvessä, so what? Osa 2/2. Verkkoaineisto. <https://www.emce.fi/blog/palvelut-pilvessa-so-what-osa-22/>. Luettu 8.6.2017.

25 Rouse, Margaret. 2016. Microsoft Azure (Windows Azure). Verkkoaineisto. <http://searchcloudcomputing.techtarget.com/definition/Windows-Azure>. Päivitetty 23.2.2016 Luettu 6.7.2017.

26 Microsoft operation management suite. 2017. Microsoftin webinaari 5.7.2017.

27 Azure Resource Manager vs. classic deployment: Understand deployment models and the state of your resources. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-deployment-model>. Luettu 6.7.2017.

28 Azure Datacenters. 2017. Verkkoaineisto. Microsoft. <https://azure.microsoft.com/en-us/overview/datacenters>. Luettu 5.7.2017.

29 Azure Regions. 2017. Verkkoaineisto. Microsoft. <https://azure.microsoft.com/en-us/regions>. Luettu 5.7.2017.

30 Regions and availability for virtual machines in Azure. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/regions-and-availability> Luettu 7.6.2017.

31 Dantison, John. 2015. Using Organizational Accounts for Azure Subscription Administration. Verkkoaineisto. <https://www.cardinalsolutions.com/blog/2015/05/organizational-accounts-for-azure-subscription-admin>. Julkaistu 20.5.2015. Luettu 6.7.2017.

32 Marko, Kurt. 2016. How to set up and manage Azure subscriptions. Verkkoaineisto. <http://searchcloudcomputing.techtarget.com/tip/How-to-set-up-and-manage-Azure-subscriptions>. Luettu 6.7.2017.

33 Get started with Role-Based Access Control in the Azure portal. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-what-is> Luettu 7.7.2017.

34 Lock resources to prevent unexpected changes. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources> Luettu 7.7.2017.

35 Resource policy overview. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-policy>. Luettu 7.7.2017

36 How Azure subscriptions are associated with Azure Active Directory. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-how-subscriptions-associated-directory>. Luettu 7.7.2017.

37 Conway, Andrew. 2016. Introducing Enterprise Mobility + Security. Verkkoaineisto. <https://blogs.technet.microsoft.com/enterprisemobility/2016/07/07/introducing-enterprise-mobility-security>. Luettu 12.7.2017.

38 Enterprise Mobility + Securityn hinnoittelu. Verkkoaineisto. Microsoft. <https://www.microsoft.com/fi-fi/cloud-platform/enterprise-mobility-security-pricing>. Luettu 12.7.2017.

39 How to buy Microsoft Intune. Verkkoaineisto. Microsoft. <https://www.microsoft.com/fi-fi/cloud-platform/microsoft-intune-pricing>. Luettu 12.7.2017.

40 What is Intune? 2017.Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/intune/device-profiles>. Luettu 12.7.2017.

41 What are Microsoft Intune device profiles? 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/intune/introduction-intune>. Luettu 13.7.2017.

42 Protect your enterprise data using Windows Information Protection (WIP). 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/fi-fi/windows/threat-protection/windows-information-protection/protect-enterprise-data-using-wip>. Luettu 13.7.2017.

43 Rouse, Margaret. 2013. Mobile device management (MDM). Verkkoaineisto. <http://searchmobilecomputing.techtarget.com/definition/mobile-device-management>. Päivitetty 11.5.2013 Luettu 12.7.2017.

44 Sign up for an Office 365 subscription with your Azure account. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/billing/billing-use-existing-azure-account-for-office-365-subscription>. Julkaistu 3.4.2017. Luettu 19.7.2017.

45 Hanki paras hyöty Officesta Office 365:n avulla. Verkkoaineisto. Microsoft. <https://products.office.com/fi-fi/compare-all-microsoft-office-products?tab=2>.Luettu 17.7.2017.

46 Hanki Office 365:n uusimmat kehittyneet ominaisuudet. Verkkoaineisto. Microsoft. <https://products.office.com/fi-fi/business/compare-more-office-365-for-business-plans>.Luettu 17.7.2017.

47 Valitse Office. Verkkoaineisto. Microsoft. <https://products.office.com/fi-FI/buy/compare-microsoft-office-products?tab=opc>. Luettu 18.7.2017.

48 Hoffman, Chris. 2017. What’s the Difference Between Office 365 and Office 2016? Verkkoaineisto. <https://www.howtogeek.com/136343/whats-the-difference-between-office-365-and-office-2013>. Julkaistu 2.3.2017. Luettu 18.7.2017.

49 Rouse, Margaret. 2016. Microsoft Office 365 suite. Verkkoaineisto. <http://searchenterprisedesktop.techtarget.com/definition/Microsoft-Office-365-suite>. Päivitetty 8.2016 Luettu 18.7.2017.

50 Exchange Online Limits. 2017. Verkkoaineisto. Microsoft. <https://technet.microsoft.com/en-us/library/exchange-online-limits.aspx>. Päivitetty 30.5.2017. Luettu 17.7.2017.

51 Exchangen avulla yritystason sähköposti. Verkkoaineisto. Microsoft. <https://products.office.com/fi-fi/exchange/compare-microsoft-exchange-online-plans>. Luettu 17.7.2017.

52 Allan, Darren. 2017. Microsoft is pushing Office 2016 users towards Office 365. Verkkodokumentti. <http://www.techradar.com/news/microsoft-is-pushing-office-2016-users-towards-office-365>. Julkaistu 21.4.2017. Luettu 18.7.2017.

53 Office 365 Plan Options. 2017. Verkkoaineisto. Microsoft. <https://technet.microsoft.com/fi-fi/library/office-365-plan-options.aspx>. Päivitetty 30.5.2017. Luettu 17.7.2017.

54 Add a custom domain name to Azure Active Directory. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-add-domain>. Päivitetty 13.7.2017. Luettu 20.7.2017.

55 Simon, Alex. 2015. Windows 10, Azure AD and Microsoft Intune: Automatic MDM enrollment powered by the cloud! Verkkoaineisto. <https://blogs.technet.microsoft.com/enterprisemobility/2015/08/14/windows-10-azure-ad-and-microsoft-intune-automatic-mdm-enrollment-powered-by-the-cloud>. Julkaistu 14.8.2015. Luettu 10.6.2017.

56 Smith, Russell. 2016. Microsoft Intune: Windows 10 Device Enrollment. Verkkoaineisto. https://www.petri.com/microsoft-intune-windows-10-device-enrollmen. Julkaistu 23.12.2016. Luettu 12.6.2017.

57 How to assign Office 365 ProPlus 2016 apps to Windows 10 devices with Microsoft Intune. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/fi-fi/intune/apps-add-office365>. Päivitetty 26.7.2017. Luettu 28.7.2017.

58 Customize your Office 365 team site for file storage and sharing. Verkkoaineisto. Microsoft. <https://support.office.com/en-us/article/Customize-your-Office-365-team-site-for-file-storage-and-sharing-70a62f09-45ea-4968-8482-43cddfb8cc01?ui=en-US&rs=en-US&ad=US>. Luettu 28.7.2017.

59 Enable Azure Active Directory Domain Services using the Azure classic portal. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-getting-started-create-group>. Päivitetty 14.5.2017. Luettu 20.6.2017.

60 Virtual Network Pricing. Verkkoaineisto. Microsoft. <https://azure.microsoft.com/en-us/pricing/details/virtual-network>. Luettu 20.6.2017.

61 VPN Gateway Pricing. Verkkoaineisto. Microsoft. <https://azure.microsoft.com/en-us/pricing/details/vpn-gateway>. Luettu 20.6.2017.

62 McDaniel, Drew. 2016. New F-Series VM Sizes. Verkkoaineisto. <https://azure.microsoft.com/en-us/blog/f-series-vm-size>. Julkaistu 8.6.2016. Luettu 7.8.2017.

63 Azure compute unit (ACU). 2017. Verkkoaineisto. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/acu>. Luettu 7.8.2017.

64 Pricing calculator. Verkkoaineisto. Microsoft. <https://azure.microsoft.com/en-us/pricing/calculator>. Luettu 7.8.2017.

65 Azure Active Directory Seamless Single Sign-On: Technical deep dive. 2017. Verkkoaineisto. Microsoft. https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-how-it-works. päivitetty 19.9.2017. Luettu 29.9.2017.

66 Prerequisites for Azure AD Connect. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-prerequisitest. päivitetty 12.7.2017. Luettu 29.9.2017.

67 Azure resiliency technical guidance: Recovery from local failures in Azure. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/architecture/resiliency/recovery-local-failures>. Päivitetty 18.8.2017. Luettu 29.9.2017.

68 Manage the availability of Windows virtual machines in Azure. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>. Päivitetty 21.3.2017. Luettu 29.9.2017.

69 Planned maintenance for virtual machines in Azure. 2017. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/fi-fi/azure/virtual-machines/windows/maintenance-and-updates>. Päivitetty 15.9.2017. Luettu 29.9.2017.