VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Juha-Matti Rannanjärvi

YRITYKSEN SISÄINEN AD-SIIRTO

Liiketalous
2022

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Juha-Matti Rannanjärvi
Opinnäytetyön nimi	Yrityksen sisäinen AD siirto
Vuosi	2022
Kieli	Suomi
Sivumäärä	30
Ohjaaja	Antti Mäkitalo

Opinnäytetyön tarkoituksena oli raportoida, miten yrityksen Active Directory migraatioprojekti edistyi käyttäjän ja migraation toteuttajien näkökulmasta. Migraation aikana tutustuttiin Microsoft Active Directoryyn sekä sen hallinta- ja migraatiotyökaluihin.

Opinnäytetyö saatiin merkitsevältä osalta valmiiksi käyttäjäkohtaisten migraatioiden osalta. Kohdeyrityksen näkökulmasta opinnäytetyön tavoite oli ollut tarpeellinen jo vuosia ennen työn aloittamista ja sen oli suunniteltu valmistuvan vuoteen 2018 mennessä. Työn valmistumista hidastivat mm. kiireet asiakasprojektien kanssa sekä maailmanlaajuinen COVID-19-pandemia.

Tutkimustyön tuloksena syntyi kolme toteutustapaa migraation toteuttamiselle. Sopiva toteuttamistapa valittiin käyttäjäkohtaisesti riippuen muun muassa migraation kohteena olevan käyttäjän saavutettavuudesta, aikataulusta sekä hänen laitteistonsa iästä ja kunnosta.

Tutkimuksen teoreettisena viitekehyksenä toimi Microsoftin verkkopohjainen Active Directoryn dokumentaatio. Lisäksi tutkimus käsittelee migraatioprosessin kannalta keskeisiä käsitteitä, menetelmiä ja tutkimusaineistoa.

Avainsanat Active Directory, Migraatio, SCCM, Centero Carillon

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Juha-Matti Rannanjärvi
Title	Internal AD migration of a company
Year	2022
Language	Finnish
Pages	30
Name of Supervisor	Antti Mäkitalo

The objective of this thesis was to report how the Active Directory migration project of the subject company progressed from the point of view of the users and the migrator. The thesis project provides an introduction to Active Directory and to its management and migration tools.

The thesis was completed from the perspective of user migration. The goal of finishing this thesis had been on sights for the company for years before the thesis work was started and it was originally planned to be completed by the year 2018. Completion of the thesis was slowed down due to demanding customer projects and the worldwide COVID-19 pandemic.

The research work resulted in three different variants for doing the user migration. The suitable migration variant was decided on a per user basis. The deciding factors were for instance the availability of the user, The user's schedule, and by age and health of the user's device.

Microsoft Active Directory documentation was used as frame of reference. In addition, the thesis project includes terms, methods, and research materials relevant to the migration process.

Keywords Active Directory, Migration, SCCM, Centero Carillon

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

KÄSITE- JA LYHENNELUETTELO

ACL
Access Control List. Taulu, joka kertoo tietokoneen käyttöjärjestelmälle, mitkä käyttöoikeudet jokaisella käyttäjällä on tiettyyn järjestelmäobjektiin.

Active Directory
Microsoftin Windows-alustoille kehitetty käyttäjätietokanta, jonka tarkoitus on helpottaa keskitettyä käyttäjähallintaa ja tietoturvan ylläpitoa, sekä toimia hakemistopalveluna yrityksen ympäristössä.

AD
Lyhenne sanoista Active Directory.

AD DS
Active Directory Domain Service. Windows-palvelu, joka autentikoi kaikki käyttäjät ja tietokoneet Windows-verkkoympäristössä.

AD LDS
Active Directory Lightweight Directory Services. AD DS:lle tehty implementaatio LDAP:sta.

API
Application Programming Inferface eli yhteys tietokoneitten välillä tai tietokonesovellusten välillä.

Centero Carillon
Windows-laitteiden käyttäjätunnusten pääsynhallintaa varten luotu sovellus.

Domain
Toimialueverkko. Joukko Microsoft Windows -käyttöjärjestelmän omaavia tietokoneita, joita voi hallita keskitetysti yhdeltä tai useammalta Windows-palvelimelta.

DNS
Domain Name System eli Internetin nimipalvelujärjestelmä. DNS:n avulla ihmisille luontevat selkokieliset verkkotunnukset voidaan muuttaa tietokoneille sopiviksi numeerisiksi IP-osoitteiksi.

Forest
Usean toimialueverkon kokoelma. Jokaisessa kokoelmassa on omat pääkäyttäjänsä.

Group Policy
Ryhmäkäytäntö eli keskitetty oikeuksien hallinta Windows-ympäristöjen koneti-leille ja käyttäjille.

IP-osoite
Internet Protocol -osoite on numerosarja, jota käytetään IP-verkkoihin kytkettyjen verkkosovittimien yksilöitymiseen.

IT
Informaatiotekniikka. Digitaalisen tekniikan avulla tehtävää tietojenkäsittelyä.

LDAP
Hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla, jonka avulla hakemistoista voidaan noutaa tietoa.

Migraatio
Active Directoryn kontekstissa migraatio tarkoittaa siirtymistä yhdestä AD-ympäristöstä toiseen.

SCCM
System Center Configuration Manager on Microsoftin julkaisema sovellus, jota käytetään isojen koneryhmien hallintaan esimerkiksi etäyhteyskäyttöön, päivitystenhallintaan, sovellusjakeluihin ja verkkopääsynhallintaan.

SPN
Service Principal Name on nimi, jolla Kerberos identifioi palveluinstansseja Kerberoksen kohdekoneelle.

SSO
Single Sign-On eli menetelmä, jossa pääsy useisiin palveluihin toteutetaan yhdelle käyttäjän todennuksella.

Yliheitto
Tietoliikenneprojektissa käytetty termi, joka kuvaa käyttäjän siirtämistä Active Directorysta toiseen.

1 JOHDANTO

Tämän opinnäytetyön kohdeyritys hyödyntää ohjelmistoyritys Microsoftin Active Directory -hallintaohjelmistoa yrityksen verkkoresurssien keskitettyyn ylläpitoon. Active Directoryn (tästä eteenpäin AD) avulla voidaan määrittää tai rajata verkon käyttäjille käyttöoikeudet verkkoresursseihin, kuten esimerkiksi palvelimiin ja tulostimiin. AD:n rakenne tulee konfiguroida sitä hyödyntävän yrityksen tarpeisiin, jotta sieltä löytyvät kaikki yrityksen tarvitsemat käytettävyyteen, hallittavuuteen ja turvallisuuteen liittyvät ominaisuudet. Kohdeyrityksen käytössä oleva AD on konfiguroitu ajan saatossa vastaamaan yrityksen sen hetkisiä tarpeita. Lisääntynyt tarve tietoturvalle ja ylläpidon helppoudelle on luonut tarpeen muuttaa yrityksen AD:n rakennetta. Olemassa olevan AD:n uudelleenkonfigurointi on suhteellisen monimutkaista ja mahdollisista virheistä saattaisi aiheutua käyttökatkoja, jotka haittaavat yrityksen liiketoimintaa. Tämän vuoksi yrityksessä rakennetaan vanhan rinnalla täysin uusi AD-rakenne, joka sopii yrityksen nykyisiin tarpeisiin. Tämä opinnäytetyö käsittelee migraatioprosessia vanhasta AD-rakenteesta uuteen.

Opinnäytetyön tavoitteena on dokumentoida yrityksen Sisäinen AD:n migraatio uudelle palvelimelle käyttäjäprofiilien ja tiettyjen verkkoresurssien osalta. Työssä esitetään kolme eri migraatiotapaa, joita käytettiin projektin aikana yliheittoon. Opinnäytetyön aikana on perehdytty tarkemmin AD:n rakenteeseen sekä sovellukseen, jolla migraatioita tehtiin.

Kappale yksi on johdanto-osa. Kappale kaksi on teoriaosa, jossa kerrotaan muun muassa AD:sta. Kolmannessa kappaleessa kerrotaan suoritetun työn vaiheista ja käsitellään työn suorittamiseen hyödynnettyjä sovelluksia. Neljännessä kappaleessa pohditaan työn tuloksia.

2 ACTIVE DIRECTORY

Tässä osiossa käydään läpi tälle opinnäytetyölle keskeistä teoriaa Microsoftin Active Directory -hakemistopalvelusta. Osio esittelee Active Directorylle ominaisia rakenneosia, mahdollisuuksia ja käytäntöjä.

Active Directory on Microsoftin tarjoama hakemistopalvelu, joka säilyttää dataa Active Directoryn loppukäyttäjien ja järjestelmänvalvojien käytettäväksi. Active Directory säilyttää verkkoympäristön objekteista informaatiota ja tekee sen järjestelmänvalvojille sekä käyttäjille helposti löydettäväksi ja käytettäväksi. Active Directory hyödyntää strukturoitua datasäilöä peruspohjana hakemistotietojen loogiseen ja hierarkkiseen säilyttämiseen. Tämä datasäilö, jota kutsutaan myös directoryksi, sisältää tietoa Active Directoryn objekteista. (Active Directory Domain Services Overview 2017.)

Sisäänpääsy ja suojaus on toteutettu Active Directoryssa yksilöllisen salasanakirjautumisen avulla. Sisään kirjautumalla järjestelmänvalvojat voivat hallita directoryn dataa ja rakennetta verkon välityksellä. Verkkoympäristön käyttäjät saavat vuorostaan pääsyn resursseihin mistä tahansa organisaationsa verkossa. Group Policyihin perustuva järjestelmänhallinta helpottaa verkkoympäristön hallintaa isommissakin verkkoympäristöissä. Yrityksen sisäverkko voi koostua useasta Active Directory Domainista joiden muodostamaa kokonaisuutta kutsutaan Forestiksi. (Active Directory Domain Services Overview 2017)

2.1 Active Directory Domain Services Collection

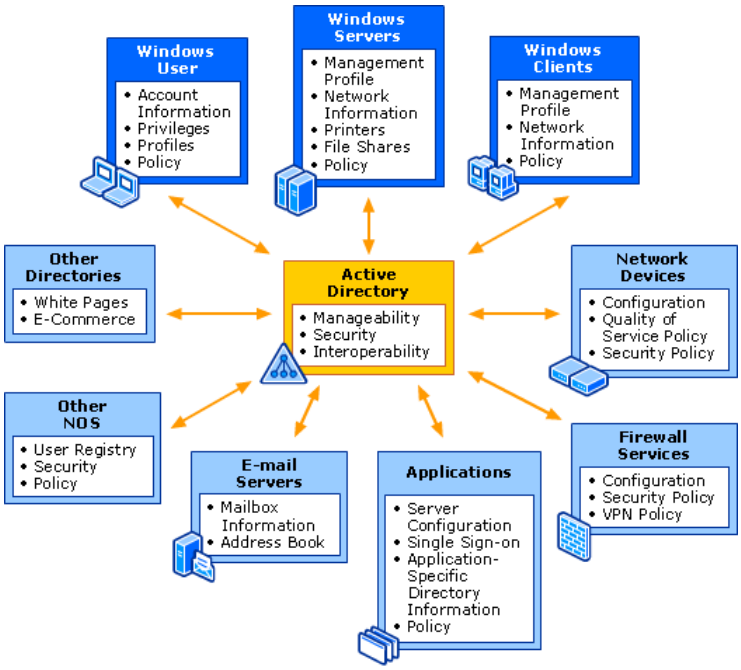
Active Directory Domain Services eli AD DS toimii informaatiokeskuksena käyttöjärjestelmälle, palvellen ominaisuuksillaan Active Directoryn käyttäjiä. Active Directoryn ominaisuuksia ovat muun muassa:

- Verkkoympäristön keskitetty hallinta ja laaja järjestelmänvalvojan oikeuksien delegointi. Active Directoryn avulla voidaan hallita verkkoympäristön

resursseja, laitteita, käyttäjiä, objektiryhmiä, Group Policyja ja turvallisuusominaisuuksia.

- Tietoturvallisuus ja mahdollisuus organisaation laajuiseen SSO:n hyödyntämiseen. Tehokas tietoturvaintegraatio vähentää tarvetta autentikoida käyttäjiä eri ohjelmistoympäristöjen välillä. Jokainen verkkoympäristön käyttäjä voidaan identifioida yksilöllisen käyttäjätunnuksen avulla. Tämä identifiointi seuraa käyttäjää ympäri verkkoa.
- Järjestelmän skaalautuvuus. AD DS sisältää yhden tai useamman toimialueen, joista jokaisessa on yksi tai useampi domain controller.
- Joustavuus ja järjestelmänlaajuinen etsintä. Käyttäjät ja järjestelmänvalvojat voivat hyödyntää työpöytätyökaluja resurssien etsimiseen AD DS:stä.
- Keskitetty sovellustietojen tallennus. AD DS tarjoaa keskitetyn sijainnin datan säilyttämiseen, mikä mahdollistaa sovelluksille sujuvan verkonlaajuisen tiedon jakamisen.
- Järjestelmällinen päivitysten jakelu. Ohjelmistopäivitykset voidaan jakaa verkon käyttäjille turvallisesti ja kustannustehokkaasti toimialueiden välillä.
- Etähallinta. Verkon sisällä olevia domain controllereita voidaan hallita miltä tahansa verkosta löytyvältä Windows-päätteltä.
- Yksi muokattava ja laajennettavissa oleva rakennekaavio. Kaavio on joukko objekteja ja sääntöjä, jotka määrittävät rakennevaatimukset AD DS objekteille. Kaavaa muokkaamalla voidaan toteuttaa uudenlaisia objekteja tai objektien ominaisuuksia.
- Objektinimien integrointi DNS:n kanssa. AD DS palvelut ja toimialueen kontrollerit ovat näin ollen paikannettavissa tavanomaisen internetprotokollan avulla sekä verkon sisällä että internetissä.
- Lightweight Directory Access Protocol (LDAP) tuki. LDAP on alan standardi hakemistoprotokolla, mikä tekee AD DS:stä helposti lähestyttävän hallinta- ja kyselysovelluksille. (AD DS on a Windows Server Network 2014.)

Kuviossa 1 nähdään Microsoftin laatima esimerkki siitä, miten AD DS toimii hallitsevana keskipisteenä Windows Server -verkkoympäristössä. Se hallinnoi resurssien identiteettejä ja välittää resurssien välisiä suhteita, jotta ne voivat toimia yhdessä. (AD DS on a Windows Server Network 2014.)

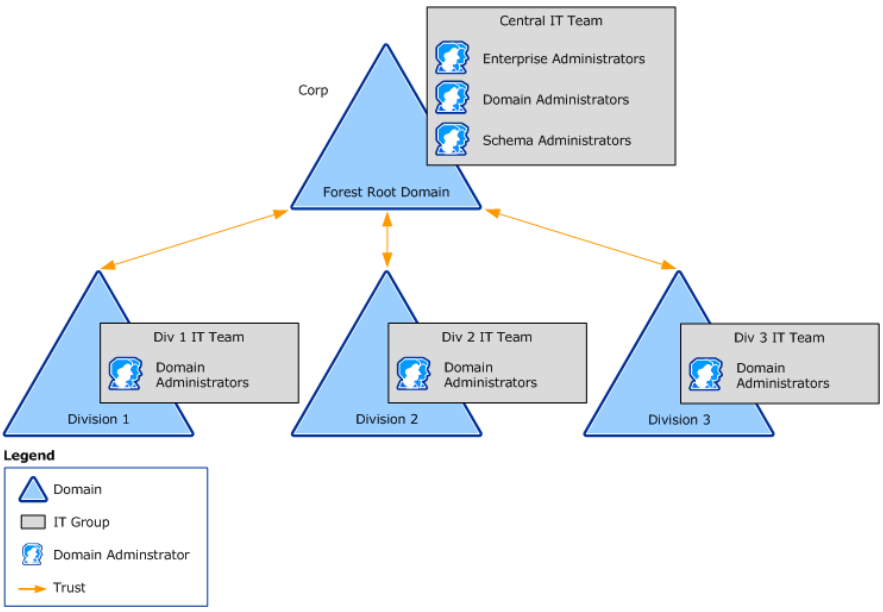


Kuvio 1. Active Directory Windows Server -ympäristössä. (AD DS on a Windows Server Network 2014.)

Active Directory Lightweight Directory Services (AD LDS) on hakemistopalvelu, jonka tarkoitus on täyttää tarpeet yritykselle, jotka eivät voi vain turvautua AD DS:ään hakemistopalvelujen tarjoamisessa hakemistoa tukeville sovelluksille. Vaikka AD DS tarjoaa monia etuja verkkoinfrastruktuurin hallinnassa, organisaatiot yleensä tarvitsevat joustavampaa hakemistopalvelua hakemistopohjaisten sovellusten tukemiseksi. AD LDS:n avulla tuodaan LDAP-palvelu hakemistoympäristöön. (What Is Active Directory Lightweight Directory Services? 2018.)

2.2 AD DS Rakenne, Roolit ja Käytäntöjä

AD DS:n looginen hierarkiarakenne muodostuu domaineista ja foresteista. Domainien avulla hallitaan yrityksen eri käyttäjäryhmiä, tietokoneita ja verkkoresursseja, kun taas forest edustaa ylintä loogista hierarkiatasoa sekä tietoturvarajaa AD DS:ssä. Toimialueiden sisältöä voidaan myös organisoida, mikäli toimialueen hallintaa halutaan jakaa pienempiin osiin. AD DS:n looginen rakenne voidaan kuvata hierarkiana, vaikka objektit itsessään on tallennettu yksinkertaiseksi miellettyyn niin kutsuttuun flat-file database -tiedostoon. Oman nimensä lisäksi jokainen objekti sisältää sen yläpuolella hierarkiassa olevan säilön nimen. Kyseinen säilö taas sisältää sitä ylemmän säilön nimen ja niin edelleen, kunnes saavutetaan hierarkiassa ylimpänä oleva säilö (Kuvio 2). Tällä tavalla luodaan looginen rakenne, jota voidaan tarkastella AD DS -työkaluja hyödyntämällä. Tämän hierarkkisen nimijärjestelmän ansiosta hierarkiapuun objekteja voidaan kuvata säilömässä toisia objekteja sisäänsä. (Structure and Storage Technologies 2014.)



Kuvio 2. Esimerkkikuva Domain Forest mallinnuksesta. (Using the Organizational Domain Forest Model 2021.)

Active Directoryn forestit ovat AD DS:n hierarkian ylin taso ja ne mahdollistavat järjestelmän keskitetyn hallinnan. Forestien sisällä pääkäyttäjät voivat hallita käyttäjien käyttöoikeuksia, määrätä ryhmäkäytäntöjä sekä asettaa resursseja eri käyttäjäryhmien tavoitettavaksi. Foresteja voidaan siis kuvailla eräänlaisena tietoturvarajana. Yhden forestin ominaisuudet riittävät useimmissa tapauksissa tarjoamaan organisaatiolle sen tarvitsemat toiminnallisuudet. Tarvittaessa organisaation järjestelmään voidaan kuitenkin luoda myös useampia foresteja toimimaan samanaikaisesti. Usean forestin järjestelmä vaatii enemmän ylläpitoa, mutta sen avulla voidaan erottaa organisaation sisäisten jaostojen järjestelmiä toisistaan. (Active Directory forest (AD forest) 2020.)

AD DS schema määrittelee hakemistopalvelun käytettävissä olevat objektit. Schema tallennetaan omaan erikoisosioonsa, joka myös on eräänlainen AD-objekti. AD DS:n attribuutit ja luokat tallennetaan schemaosioon hakemisto-objekteina, joita kutsutaan schemaobjekteiksi. Vaikka oletusarvoinen schema sisältääkin kaikki luokat ja määritteet, joita AD DS vaatii toimintaansa, voivat järjestelmänvalvojat tarvittaessa lisätä omia luokkiaan ja määritteitään olemassa olevaan objektityyppiin. (Structure and Storage Technologies 2014.)

AD:ssa oleviin tietoihin kohdistuvien muutoksien jakelu asiaan kuuluville domain controllereille tapahtuu automaattisesti AD DS -replikoinnin avulla. Replikoimalla tietoja hakemisto-osioiden mukaisesti AD DS tarjoaa tietovaraston, joka on samaan aikaan loogisesti keskitetty, eli sen hallinta tapahtuu yhdestä pisteestä, mutta fyysisesti hajautettu, eli sen tiedot on synkronoitu useille domain controllerille. (Structure and Storage Technologies 2014.)

2.2.1 Active Directory Roolit

Windows Server -palvelinta asennettaessa sille valitaan sen käyttötarkoitusta vastaava rooli. Windows Server -palvelinta, johon on asennettu AD DS, kutsutaan Domain Controlleriksi. Sen tehtävä on säilyttää sen toimialueen objektit, mihin se on asennettu. Lisäksi Domain Controller säilyttää tiedon koko ylätason forestin

rakenteesta. Luodun Domain Controllerin avulla on mahdollista luoda uusi forest tai toimialue, tai jakaa olemassa olevan toimialueen hallintaa. (Domain Controller Roles 2014.)

Joissain tilanteissa Domain Controllerilla voi olla myös erikoisrooleja. Esimerkiksi Global Catalog Serverin tehtävä on säilyttää oman toimialueen objektien lisäksi myös koko muun forestin objektit. Tämä toteutetaan replikoimalla forestin domainien objektit Global Catalog Serverille, mikä mahdollistaa tiedon hakemisen AD DS:stä ilman, että haku täytyy suorittaa usean palvelimen kautta. Usein forestin ensimmäinen Domain Controller määritetään Global Catalog Serveriksi. (Global Catalog Servers 2014.)

Domain Controller voidaan määrittää myös Operations Master -rooliin. Tässä roolissa oleva Domain Controller varmistaa, että AD:n sisällä tapahtuvassa tietokantaliikenteessä ei synny konflikteja. AD DS:n sisällä voi olla useita Operations Master -palvelimia, joille voidaan antaa erilaisia vastuualueita. (Operations Masters 2014.)

2.2.2 Replikointitekniikat

Kaikki AD:ssa olevat objektit kuuluvat jollekin domain controllerille ja jokaisen domain controllerin tiedot voidaan päivittää suoraan. AD DS -replikoinnissa on kyse tapahtumasta, jossa yhdelle domain controllerille tehdyt muutokset synkronoidaan automaattisesti muiden domain controllerien kanssa. Tietojen eheys varmistetaan seuraamalla muutoksia jokaisessa domain controllerissa ja päivittämällä muita domain controllereita systemaattisella tavalla. Oletusarvoisesti luotu AD DS replikointitopologia hyödyntää optimaalisesti fyysisiä verkkoyhteyksiä ja vapauttaa järjestelmänvalvojat tarpeesta päättää, mikä domain controller replikoi ja kenen kanssa. Tarvittaessa replikaatiotopologiat voidaan myös luoda myös manuaalisesti. AD DS -replikointi on suunniteltu maksimoimaan hakemistojen johdonmukaisuus ja minimoimaan verkkoliikenteen vaikutukset. (Replication Technologies 2014.)

2.2.3 Haku- ja julkaisutekniikat

AD DS -forestin toiminta perustuu siihen, että sen käyttäjät ja palvelut löytävät domain controllerin. AD DS hyödyntää DNS-palveluja verkon resurssien paikantamiseen ja domain controllerin onnistunut paikantaminen vaatii sen, että sijaintitieto on rekisteröity DNS-palveluun ja että tämä tieto on saatavilla. DNS:n avulla AD DS pystyy selvittämään tarvittavien verkossa olevien tietokoneiden IP-osoitteet. Toimialueverkon tietokoneissa ja domain controllereissa toimiva Net Logon -palvelu toimii niin sanottuna Locatorina ja on vastuussa Windows server -API:en ja DNS-palveluihin yhdistämisessä etsiessään tarvittuja domain controllereita. (Search and Publication Technologies 2014.)

Domain controllerin löydyttyä, tietojen noutamiseen käytetään LDAP:ia. LDAP on yksi AD DS:n perustoiminnoista ja suositeltu keino AD DS:n kanssa vuorovaikuttamiseen. LDAP:n avulla käyttäjät voivat hakea, luoda, päivittää ja poistaa AD DS:iin tallennettuja tietoja. (Search and Publication Technologies 2014).

Tietojen luomista, tallentamista ja ylläpitoa AD DS:ssä kutsutaan palvelujulkaisuksi. Hakemistopalvelut ja sovellukset voivat julkaista hyödyllistä tietoa, kuten palvelujen saatavuutta ja ominaisuuksia AD DS:ssä. Tämän avulla asiakasprosessit voivat etsiä ja muodostaa yhteyden mihin tahansa hakemistopalveluun tarpeen mukaan, ja verkkoasiakkaat ja järjestelmänvalvojat voivat löytää, muodostaa yhteyden ja hallita palveluita. (Search and Publication Technologies 2014).

2.2.4 Asennus-, päivitys- ja migraatiotekniikat

AD DS:n asentamista varten on olemassa ohjattu asennustoiminto, joka pystyy varmistamaan palvelimen yhteensopivuuden AD DS:n kanssa. Ohjattu asennustoiminto tarjoaa käyttöliittymän, jonka avulla kerätään AD DS:n asennuksen kannalta oleellista tietoa. Lisäksi asennustoiminto konfiguroi itse AD DS:n, jolloin palvelimesta muodostuu domain controller. Myös AD DS Scheman määrittely kuuluu

osaksi hakemiston määritystä ja siinä valitaan kaikki hakemistossa käytettävissä olevat luokat. (Installation, Upgrade, and Migration Technologies 2014.)

Onnistuneen AD DS:n asennuksen jälkeen luodaan joukko sääntöjä, jotka tarjoavat kokoonpanotuen AD DS -ominaisuuksille, määräävät ne Windows-käyttöjärjestelmäversiot, jotka voivat toimia kyseessä olevan toimialueen kanssa ja muun muassa varmistavat yhteensopivuuden vanhempien domain controllerien kanssa. (Installation, Upgrade, and Migration Technologies 2014.)

Riippuen siitä, kuinka AD DS on konfiguroitu, ja mihin suuntaan järjestelmää kehitetään, AD DS:n täysi uudelleenrakentaminen saattaa olla kokonaisuuden kannalta kannattavampaa AD-ympäristön päivittämisen sijasta. Varsinkin siirryttäessä kokonaan uudempaan järjestelmäversioon, saattaa tuottavuuden puolesta olla hyödyllisempää rakentaa koko AD DS uudestaan. Microsoft tarjoaa erilaisia työkaluja, joiden avulla AD siirtotehtäviä ja uudelleenkonfigurointeja voidaan automatisoida. Siirtotehtäviä ovat muun muassa käyttäjien, ryhmien, palvelutilien, tietokoneiden ja turvasäilöjen siirto. AD DS -ympäristö voidaan myös uudelleen järjestellä nimeämällä domain uudelleen. Lisäksi joustavuutta luo kyky tehdä nimimuutoksia tärkeille resursseille. (Installation, Upgrade, and Migration Technologies 2014.)

3 MIGRAATIOPROSESSI

Opinnäytetyön alussa huomasin, että migraatioprojektia oli lykätty useasti varsinaisten asiakasprojektien vuoksi. Sillä migraatio uuteen AD-ympäristöön kehittäisi yrityksen omaa toimintaa pitkällä aikavälillä, tuli projektiin edistämiseen valita henkilöitä, jotka eivät olisi sitoutuneita asiakasprojekteihin. Ongelmakohdaksi huomasin myös sen, että käyttäjien kanssa tuli saada sovittua aikataulut yliheittoon siten, että ne eivät vaikuttaneet negatiivisesti nykyisten ja tulevien asiakasprojektien etenemiseen. Opinnäytetyön alkaessa migraatioprojekti oli jo aluillaan, mutta sen eteneminen oli pysähtynyt muutaman vuoden ajaksi. Migraatiolle asetettiin uudeksi tavoiteaikatauluksi siirron saattaminen loppuun 2019 alussa. Osa käytetyistä työkaluista oli valmiiksi otettu käyttöön alkuperäisen migraatioprojektitiimin puolesta.

3.1 Käytetyt ohjelmistot

Tässä luvussa käydään läpi sovelluksia, jotka olivat tarpeellisia migraation aikana. Osa käytetyistä sovelluksista on Microsoftin kehittämiä ja ylläpitämiä.

Forensit on sovellus, jonka tarkoitus on helpottaa migraatioprosessia säilyttämällä siirrettävän käyttäjän kaikki Windowsiin sisältyvä profiilidata ja asetukset. Käyttäjäprofiilissa säilytetään Omat Tiedostot, Kuvat, Musiikki, Internetin Suosikit ja Evästeet. Tämä helpottaa migraatioprosessin taakkaa käyttäjälle sekä migraation tekijälle. (ForensIT 2021, 6)

LAPS on hallintatyökalu, jolla pystyt hallitsemaan lokaalin järjestelmänvalvojan salasanaa koneella, joka on liitetty toimialueeseen. Salasanat ovat Active Directoryssa suojattuna ACL:n takana, jotta vain asianmukaiset henkilöt pystyvät Lukemaan salasanoja. (Local Administrator Password Management Datasheet. 2018)

Microsoft Teams on Microsoftin Office 365 -ohjelmistopakettiin lisätty uusi viestintäalusta, joka tulee lähitulevaisuudessa korvaamaan aikaisemmin käytössä olleen Skype for Business -viestintäalustan. Sovellusta on käytetty projektin aikana

palaverien ylläpitämiseen ja loppukäyttäjille kommunikoinnissa migraation aikataulutuksesta.

Microsoft Planner on Microsoft Office 365 -ohjelmistopakettiin sisältyvä aikataulutussovellus. Sovellus on luotu projektien aikatauluttamiseen ja edistymisen seurantaan. Myös migraatioprojektin etenemistä seurattiin Plannerin avulla.

3.2 Toteutus

Yrityksellä on noin 50 työntekijää, joista suurin osa pyritään siirtämään uuteen ympäristöön. Projekti alkoi vuonna 2018, jolloin yrityksen käytössä olevan AD-rakenteen todettiin olevan kehittämisen tarpeessa. Yrityksen tarpeisiin sopivan uuden AD-rakenteen suunnittelu aloitettiin ja tämän opinnäytetyön tekijä valittiin suorittamaan migraatioprosessia sekä varmistamaan, että uusi AD-rakenne vastaa yrityksen tarpeita.

Migraatioprosessin aikataulutus oli projektin alkuvaiheessa hankalaa, koska projektin laajuus ei ollut täysin tiedossa. Yleinen näkemys kuitenkin oli, että projekti haluttiin saada suoritettua kohtuullisessa ajassa, jotta uuden AD:n hyödyt saataisiin käyttöön ja vanhan AD:n tietoturvahaasteet ratkaistua. Aikatauluun vaikuttivat merkittävästi käyttäjien työtilanne, etenkin yrityksen asiakasprojektien kanssa työskentelevien käyttäjien osalta sekä yliheittoon käytettävien toteutustapojen muuttuminen. Yliheittoja pyrittiin suorittamaan projektin edetessä noin yhdestä kahteen käyttäjää viikossa.

AD-yliheiton suorittaminen käyttäjän työasemalle vaati, että käyttäjän kanssa sovitaan ajankohta yliheiton suorittamiselle. Käyttäjän kanssa viestintään hyödynnettiin Microsoft Teams -viestintäalustaa ja aikataulujen sopimiseen Microsoft Planner -aikataulutussovellusta. Käyttäjille lähetettiin Teamsin avulla viesti, jossa ehdotettiin ajankohtia yliheiton toteuttamiselle. Käyttäjä on valinnut itselleen sopivan ajankohdan, joka on merkitty Planner-sovellukseen. Käyttäjän tehtäväksi

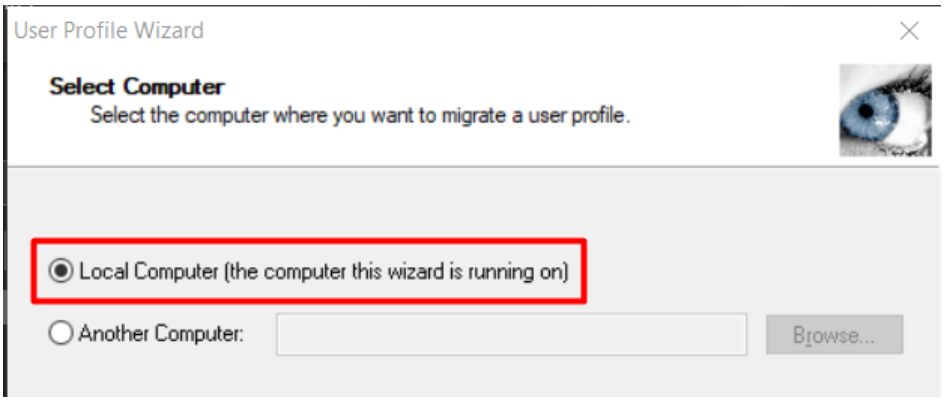
jää varmistaa, että työasemalla olevista tiedostoista on tehty tarpeelliset varmuuskopiot, jotta yliheitto ei vaikuta niihin.

Lisäksi opinnäytetyön tekijän tuli valita käyttäjän tarpeisiin sopiva siirtotapa. Yhteensä siirtotapoja syntyi kolme: A-tapa, B-tapa ja C-tapa. Käytettävä siirtotapa määräytyi sen mukaan, voitiinko käyttäjän työasema tyhjentää migraatioprosessin yhteydessä, vai tuliko käyttäjän työasemalle tallentamia tietoja säilyttää.

3.2.1 A-Tapa

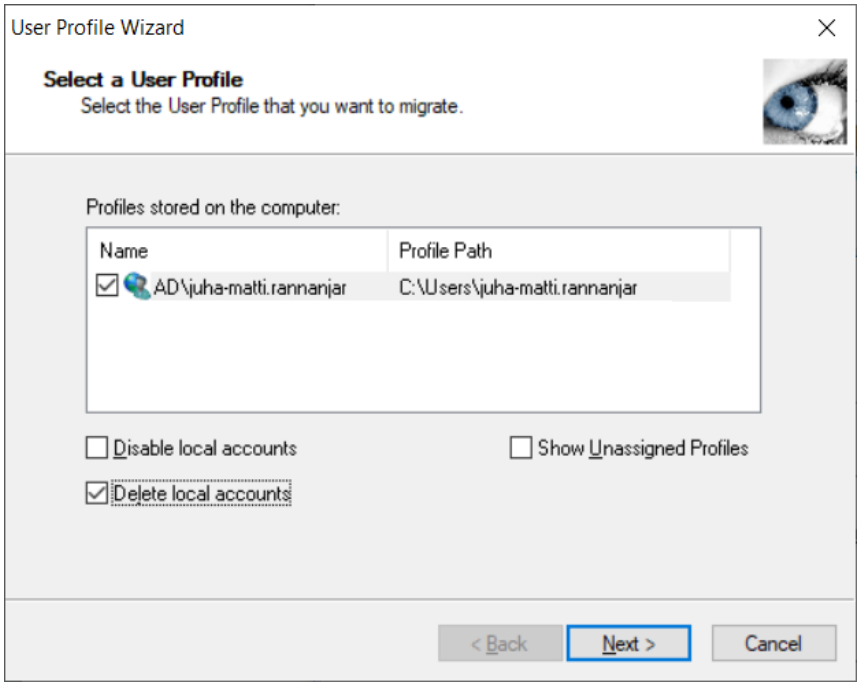
Siirtotapa A tehtiin käyttäjille, joiden oli hankala ottaa koneistaan varmuuskopioita tai joiden konetta ei ollut mahdollista tyhjentää migraatioprosessin yhteydessä. A-tapa keskittyi varmistamaan käyttäjän tiedostojen säilymisen, mutta oli siirtotavoista opinnäytetyön tekijälle työläin.

Siirtotapa A hyödyntää Forensit-ohjelmistoa työaseman alkuperäisten asetusten säilyttämiseen. Forensit ja sen tarvitsemat konfiguraatiotiedostot asennettiin käyttäjän koneelle, minkä jälkeen ohjelma kysyy mille koneelle siirto tehdään. Valintavaiheessa valitaan ”Local Computer” eli sillä hetkellä käytössä oleva työasema, jolle Forensit:n asennus on suoritettu (Kuvio 3).



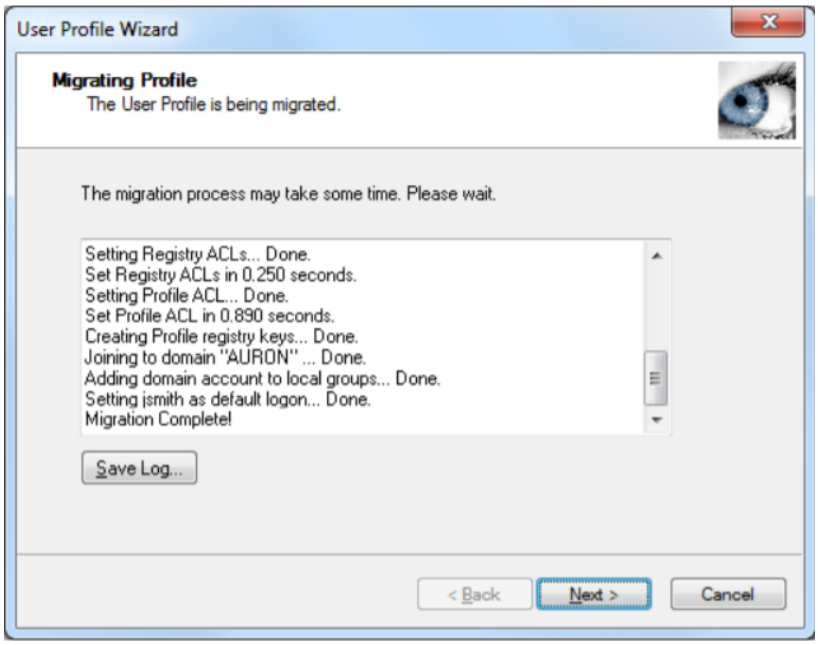
Kuvio 3. Kohteen valinta ForensiT-migraatio-ohjelmassa.

Seuraavaksi ohjelma kysyy, mille käyttäjälle siirto suoritetaan. Koneista siirretään vain käyttäjän päätili. Ylimääräiset paikalliset käyttäjätilit poistetaan siirron yhteydessä, jolla pyritään varmistamaan käyttöympäristön turvallisuus (Kuvio 4).



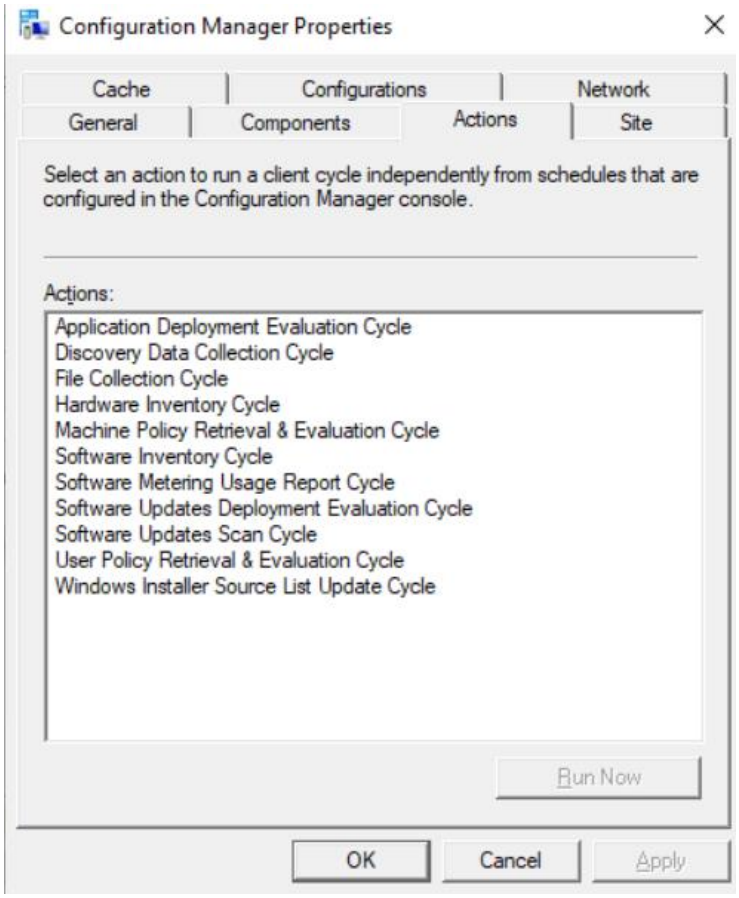
Kuvio 4. Käyttäjäprofiilin valinta ForensiT-migraatio-ohjelmassa.

Valinnan jälkeen ohjelma kysyy tunnuksia, joilla on oikeudet luvittaa toimialue siirto. Tämän jälkeen ohjelma tekee domain-siirron ja kopioi koneelle vanhan domainin profiilista uutta toimialuetta varten oman profiilin (Kuvio 5).
Suorituksen jälkeen kone bootataan ja käyttäjä pyydetään kirjautumaan uuden toimialueen tunnuksilla.



Kuvio 5. Migraatioprosessin käynnistäminen ForensiTi-migraatio-ohjelmassa.

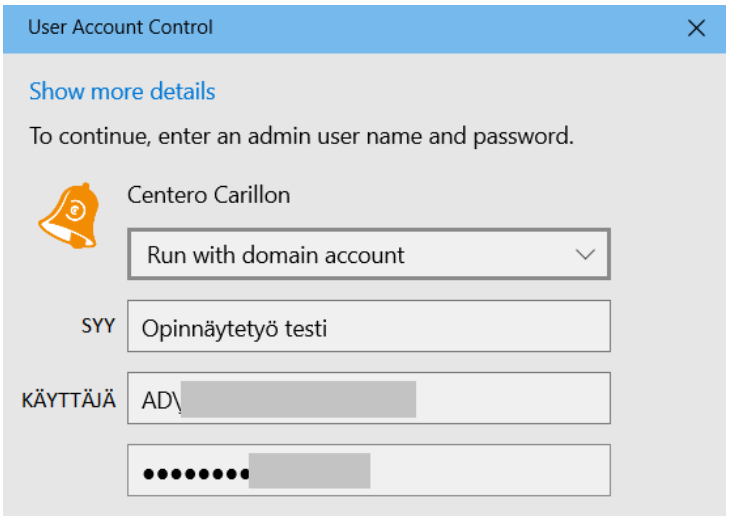
Uusi kone tehdään nimeämiskäytännöllä "KonePaikkakuntaKonenumero". Tämä tehdään numerojärjestyksessä sitä mukaa kuin uuteen ympäristöön tulee koneita. Esimerkiksi tunniste "LTOUL001" muodostuu laptop-tyyppistä eli kannettavaa tietokonetta kuvailevasta lyhenteestä "LT", Oulua tarkoittavista merkeistä "OUL" ja juoksevasta järjestysnumerosta "001". Koneen ja käyttäjän tulee olla vielä aluekohtaisissa ryhmissä, joiden avulla määrätään yrityksen toimialueen ryhmäkäytännöt. Koneelle asentuu automaattisesti SCCM-agentti ryhmäkäytäntöjen avulla. Vikatilanteissa, joissa SCCM-agentti ei asennu sen voi asentaa käsin palvelimelta. Jotta Software Center löytää asennettavia yrityksen sovelluksia on SCCM-agentin skannattava koneelta löytyvät sovellukset (Kuvio 6).



Kuvio 6. SCCM-konfigurointiavustin.

Kun SCCM-agentti on asennettu ja haut on ajettu ohjelman pitäisi näyttää sovelluksia. SCCM kautta pystyy asentamaan ja poistamaan yrityksen päättämiä ohjelmistojakeluja ilman järjestelmänvalvojan oikeuksia. Kaikki työskentelyyn tarvittavat sovellukset voidaan asentaa tämän kautta. Tietoturvan kanssa on luovuttu edeltävästä käytännöstä ja on päädytty siirtyä uuteen käytäntöön. Jokaiselle koneelle tulee ryhmäkäytäntöjen kautta Centero Carillon-sovellus, jolla hallinnoidaan pääkäyttäjäoikeuksia. Tähän on päädytty, jos esimerkiksi tietokone kaapataan ja se on jäänyt kirjautuneena sisälle. Tällöin koneella ei pääse tekemään paljoa tuhotöitä eikä sabotaasia. Tällä myös vähennetään yrityksen työtaakkaa, sillä käyttäjä pystyy asentamaan itse omat sovelluksensa Centero Carillonin kautta. Tässä vaiheessa vielä tarkistetaan, että käyttäjälle on asentunut kaikki tarpeelliset sovellukset. Tarkistetaan myös, että kone löytyy meidän hallintajärjestelmästämme.

Tässä vielä kaksi esimerkki kuvaa jossa (Kuvio 7) Näytetään miltä Carillonin luvitus näyttää ja (Kuvio 8) jossa näkyy, miten tämä tulee esille Carillonin auditoinnissa.



Kuvio 7. Kirjautuminen Centero Carillonin sovelluksen kautta.

Kuvio 8. Lokiin jäänyt merkintä kirjautumisesta Centero Carillonin sovelluksen kautta.

Tulostimien lisäys kuuluu myös koneen asentajalle. Nämä tulevat verkkojaoista.

3.2.2 B-Tapa

B-Tavassa lähdetään siltä pohjalla, jossa käyttäjä on suostuvainen koneen tyhjäykseen. Ajan sovittua kone formatoidaan ja Forensittia ei tarvita siirron

yhteydessä. Tämä säästää tuelta paljon enemmän aikaa ja siirrot onnistuivat vähemmillä virheillä.

B-Tavan suurin ongelma oli käyttäjien kanssa selvittelyt mitä dataa koneista pitää säilyttää ja mitkä saivat mennä formatoinnin mukana pois. Muutamassa tilanteessa työntekijä huomasi vasta kuukausien päästä, että joku X tiedosto ei ollutkaan Pilvessä ja koneen formatoinnin yhteydessä tiedostot olivat hävinneet.

B-Tapaa myös käytettiin tilanteissa, jossa käyttäjä oli esim. pitemmällä lomalla tai sairaana ja käyttäjä oli suostuvainen, että suoritin koneen tyhjäyksen ilman heidän seuraamistansa tilanteen etenemisestä.

3.2.3 C-Tapa

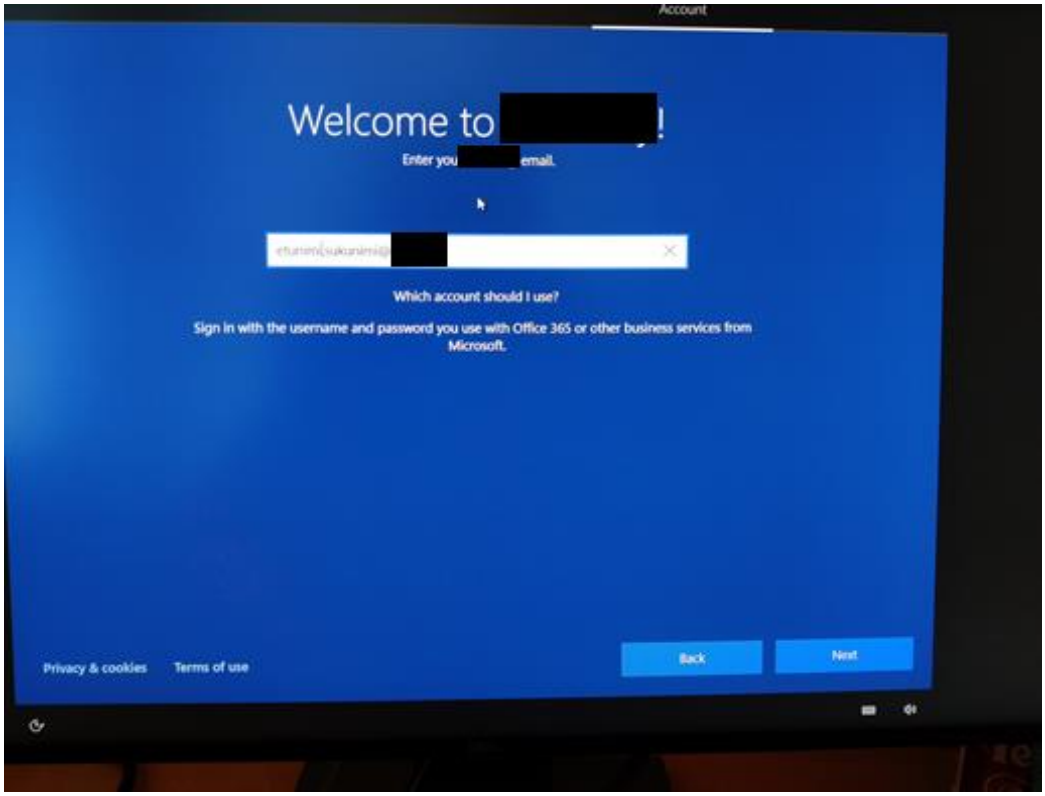
C-tapa on uusi tapa, joka on vasta hiljattain otettu käyttöön. Tässä kone rekisteröidään Windows Intunen hallinnan alaiseksi. Aika sovitaan käyttäjän kanssa samaan tapaan kuin muissa tavoissa. Ensimmäisenä käyttäjän koneelle ajetaan komento Power Shellissä, jolla saadaan koneen tarvittavat tiedot intuneen rekisteröintiä varten. Tämä koodin ajo luo käyttäjän koneelle CSV- tiedoston, jossa on kaikki tarvittavat tiedot intunen rekisteröintiä varten (Kuvio 9).

```
Device Serial Number,Windows Product ID,Hardware Hash,Group Tag,Assigned User
<serialNumber>,<ProductID>,<hardwareHash>,<optionalGroupTag>,<optionalAssignedUser>
```

Kuvio 9. Intune .csv tiedostossa käytetyt sarakkeet. (Manually register devices with Windows Autopilot 2022)

Power Shell komennon ajon jälkeen sinulla on tarpeelliset tiedot Intune rekisteröintiä varten. CSV-tiedosto siirretään Microsoftin Endpoint Manager sivustolle, jonka jälkeen käyttäjän kone näkyy Endpointin Autopilotoitavissa laitteissa. Kone vielä pitää vielä lisätä ryhmään, jotta Intune rekoisteröinti voi tehdä käyttäjän

koneella. Kone laitetaan resetoimaan itsensä tehdasasetuksiin. Kun kone on resetoitu ja käynnistetään uudelleen, kone rupeaa tyhjäämään itseään sekä asentamaan puhdasta Window-asennusta koneelle. Formatoinnin jälkeen kone toivottaa tervetulleeksi yrityksen ympäristöön ja käyttäjä voi kirjautua omilla uuden ympäristön tunnuksilla sisään. Käyttäjän ensimmäisellä kirjautumiskerralla Käyttäjältä kysytään varmennetta kännykältä. Näin saadaan varmennettua kyseisen käyttäjän olevan yrityksen sisäinen työntekijä (Kuvio 10).



Kuvio 10. Koneen käyttöönotto migraatioprosessin jälkeen.

Varmennuksen jälkeen koneelle tehdään viimeistelyt, jotka tehdään Intunen sääntöjen mukaan. Prosessin valmistumisen jälkeen (n.30minuuttia) käyttäjä kirjautuu koneelle uudestaan, jonka jälkeen koneelle alkaa ”tippumaan” Company Portaalista asennuksia. Työhön tarpeelliset sovellukset ”tippuvat” pakotetusti

koneelle, jotta työnteko saataisiin aloitettua nopeasti. Intune toimii samalla periaatteella kuin SCCM mutta Intunen hallinta on paljon selkeänpää.

4 YHTEENVETO

Opinnäytetyön aikana AD-migraatio saatiin merkitsevin osin, eli käyttäjäkohtaisten migraatioiden osalta suoritettua. Liityin projektiin vuonna 2017, jolloin sen alkuperäinen suunniteltu valmistumishetki oli 2018 vuoden lopussa. Projektin edetessä kohdattiin useita vastoinkäymisiä, jotka hidastivat projektin valmistumista. Muun muassa ihmistekijät vaikeuttivat käyttäjämigraation toteuttamista, koska käyttäjien kanssa tuli sopia henkilökohtaisesti heidän yksilölliset tarpeensa huomioon ottaen ajankohdat yliheitoille. Lisäksi vuoden 2020 koronavirus-pandemian tuoma laaja etätöiden lisääntyminen hidasti projektin etenemistä entisestään, koska loppukäyttäjien kanssa oli vaikeampi sopia tapaamisia, jossa olimme samassa tilassa tekemässä käyttäjämigraatiota.

Vastoinkäymisistä huolimatta käyttäjämigraatio saatiin vihdoin päätökseen vuoden 2020 loppupuolella. Vaikeuksia siis migraatioprosessin aikana oli useita, joista suurin osa johtui ympäristötekijöistä. Ratkaisuna osaan haasteista olisi ollut kiinteiden yliheittoaikojen hyödyntäminen, jolloin yliheiton kohteena olevan käyttäjän aikataulut eivät hankaloittaisi yliheiton suorittamista yhtä paljon. Lisäksi yliheiton kohteena olevan työntekijän työtehtävät voisi siirtää siirron ajaksi toiselle vastuuhenkilölle, jotta yliheitto ei vaikeuttaisi kohdehenkilön työntekoa. Kohdehenkilöiden tietokoneet olisi myös voitu tyhjentää olemassa olevista ohjelmista ja uudelleen konfiguroida, jolloin migraatiosta johtuvia ongelmia olisi ilmennyt vähemmän ja niiden selvittämisestä ilmennyt työmäärä olisi ollut kevyempi. Lisäksi huomattiin, että osalla työntekijöistä ei tietokoneen varmuuskopiointeja ollut suoritettu. Varmuuskopioiden suorittaminen ennen yliheittoa oli oleellista, minkä vuoksi niistä kertyi yliheiton suorittajalle ylimääräistä työtä.

Osalta käyttäjistä saatiin negatiivista palautetta käyttäjämigraation jälkeen mm. aiempaa rajoitetumpien pääkäyttäjäoikeuksien vuoksi. Käyttäjille oli kyllä tiedotettu tästä mutta tämä tuli silti esille uudestaan migraation jälkeen.

Käyttäjämigraation hyviä puolia oli uuden ympäristön suorituskyvyn parantuminen vanhaan verrattuna, sekä lisääntynyt tietoturvan taso. Näistä kumpikin olivat projektin pääasiallisia tavoitteita ja näin ollen projektia voidaan pitää onnistuneena.

LÄHTEET

Active Directory Domain Services Overview. 2022. Microsoft. Viitattu 15.1.2022. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Active Directory forest (AD forest). 2020. Brien Posey. Viitattu 9.2.2022 https://www.techtarget.com/searchwindowsserver/definition/Active-Directory-forest-AD-forest

AD DS on a Windows Server Network. 2014. Microsoft. Viitattu 19.10.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)#ad-ds-on-a-windows-server-network

Domain Controller Roles. 2014. Microsoft. Viitattu 6.11.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786438(v=ws.10)

Forensit User Profile Wizard Corporate Edition 3.1.6.1243. (ForensiT Limited 2021). Viitattu 30.8.2019. https://www.forensit.com/Downloads/User%20Profile%20Wizard%20Corporate%20User%20Guide.pdf

Global Catalog Servers. 2014. Microsoft. Viitattu 6.11.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786438(v=ws.10)#global-catalog-servers

Installation, Upgrade, and Migration Technologies. Microsoft. 2014 Viitattu 16.1.2022 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)#installation-upgrade-and-migration-technologies

LAPS_Datasheet (Local Administrator Password Solution (LAPS) Ohjeistus). Ohjeistusta päivitetty viimeksi 6.2018. Viitattu 16.01.2022. https://www.microsoft.com/en-us/download/details.aspx?id=46899

Operations Masters. 2014. Microsoft. Viitattu 6.11.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786438(v=ws.10)#operations-masters

Replication Technologies. 2014. Microsoft. Viitattu 6.11.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)#replication-technologies

Search and Publication Technologies. 2014. Microsoft Viitattu 16.1.2022 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)#search-and-publication-technologies

Structure and Storage Technologies. 2014. Microsoft. Viitattu 6.11.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)#structure-and-storage-technologies

Using the Organizational Domain Forest Model. 2021. Microsoft. Viitattu 16.1.2022 https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/using-the-organizational-domain-forest-model

What Is Active Directory Lightweight Directory Services? 2018. Microsoft. Viitattu 6.11.2021. https://docs.microsoft.com/en-us/previous-versions/windows/desktop/adam/what-is-active-directory-lightweight-directory-services