KARELIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutusohjelma

Tuomas Kuittinen

ACTIVE DIRECTORYN SUUNNITTELU JA KÄYTTÖÖNOTTO PIENYRITYKSESSÄ

Opinnäytetyö
Huhtikuu 2018

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Huhtikuu 2018** **Tieto- ja viestintätekniikan koulutusohjelma** Karjalankatu 3 80200 JOENSUU (013) 260 600

Tekijä
Tuomas Kuittinen

Nimeke
Active Directoryn suunnittelu ja käyttöönotto pienyrityksessä

Toimeksiantaja
Process Genius Oy

Tiivistelmä

Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa Active Directoryn käyttöönotto pienyrityksessä. Työn toimeksiantajana on joensuulainen ohjelmistoalan yritys Process Genius Oy.

Tavoitteena oli luoda Process Genius Oy:n käyttötarpeisiin soveltuva Active Directory -ympäristö ja liittää se käytössä olevaan Office 365 -ympäristöön. Active Directoryllä haluttiin korvata myös yrityksen Linux-pohjainen tiedostonjakopalvelin.

Teoriaosuudessa on käsitelty Active Directoryn rakennetta ja toiminnallisuutta yleisellä tasolla. Lisäksi on selvitetty, mitä tulisi huomioida Active Directoryn suunnittelussa ja käyttöönotossa pienyrityksen kannalta. Teoriaosuudessa käsitellään myös joitakin Microsoftin suosituksia Active Directoryn käyttöönoton osalta.

Käytännönosuudessa on kerrottu, millä tavalla Active Directory -ympäristö toteutettiin Process Genius Oy:lle, mitkä asiat vaikuttivat toteutukseen ja miten integrointi Office 365 -ympäristöön tehtiin. Projekti alkoi keväällä 2017 ja toteutus tehtiin vuoden 2018 alkupuolella.

Kieli	Sivuja 41 Liitteet 0 Liitesivumäärä
suomi	

Asiasanat

Active Directory, Active Directory Domain Services, Windows Server

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
April 2018
Degree Programme in Information and Communication technology

Karjalankatu 3
80200 JOENSUU
(013) 260 600

Author
Tuomas Kuittinen

Title
Designing and Implementing Active Directory in an SME.

Commissioned by
Process Genius Oy

Abstract

The purpose of this thesis was to design and implement an Active Directory environment for SME. The project was commissioned by a software company Process Genius Oy in Joensuu.

The aim of the thesis was to create an Active Directory environment appropriate to the needs of Process Genius Oy and to integrate it with the existing Office 365 environment. Active Directory was also to replace the company's Linux-based file server.

The theory part addresses the structure and functionality of Active Directory at a general level. In addition, it was studied what should be taken into consideration when planning and implementing Active Directory for an SME. The theoretical part also addresses some of Microsoft's recommendations regarding the implementation of Active Directory.

The practical part describes how the Active Directory environment was implemented for Process Genius Oy, which factors influenced the implementation choices and how the integration into the Office 365 environment was done. The project started in spring 2017 and the implementation was carried out in early 2018.

Language
Finnish

Pages 41
Appendices 0
Pages of Appendices 0

Keywords
Active Directory, Active Directory Domain Services, Windows Server

Sisältö

Käsitteet

Active Directory	Aktiivihakemisto. Microsoftin hakemistopalvelu.
AD CS	Active Directory Certification Services. Palvelinrooli varmenteiden luomiseen ja hallintaan.
AD DS	Active Directory Domain Services. Palvelinrooli, joka määrittää palvelimen ohjauskoneeksi.
Aliverkko	IP-osoitteista muodostuvan verkon osa.
Azure AD	Azure Active Directory. Azure -pilvipalvelussa toimiva Microsoftin ylläpitämä aktiivihakemistopalvelu.
CA	Certificate Authority. Varmenteen myöntävä taho.
DHCP	Dynamic Host Configuration Protocol. Protokolla, jota käytetään IP-osoitteiden jakamiseen.
DNS	Domain Name Services. Nimipalvelin järjestelmä, joka muuttaa verkkotunnukset IP-osoitteiksi.
Hakemistopalvelu	Directory Services. Hakemistopalvelu sisältää tietoja käyttäjistä, tietokoneista ja verkon resursseista.
IP	Internet Protocol. Protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta verkossa.
Kaava	Schema. Hakemistopalvelussa oleva malli miten tieto on tallennettu hakemistoon ja niiden välisistä suhteista.
Kontti	Container. Organisaatioyksikköä yksinkertaisempi säiliö Active Directoryssä.
Käyttäjätili	User account. Active Directoryn objektityyppi, jota käytetään käyttäjätietojen tallennukseen.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen käyttämä verkkoprotokolla.
Objekti	Hakemistopalvelussa oleva tallennettu kohde. Toimialue, käyttäjätili, tietokonetili tai käyttäjäryhmä ovat kaikki objekteja.
Ohjauskone	Domain Controller. Palvelintietokone, joka ylläpitää tietoa Active Directorystä.
Organisaatioyksikkö	Organizational Unit (OU). Objekti, jonka avulla voidaan ryhmittää muita objekteja Active Directoryssä.
Palvelinrooli	Server Role. Windows Server -käyttöjärjestelmässä asennettava palvelinrooli.
Ryhmäkäytäntö	Group Policy. Sääntö jolla voidaan hallita käyttäjien ja tietokoneiden asetuksia.
SID	Security identifier. Toimialueen sisällä yksilöllinen tunniste toimialueen jokaisella käyttäjälle, tietokoneelle ja käyttäjäryhmälle.
Säiliö	Container. Organisaatioyksikkö ja kontti ovat säiliöitä. Voivat sisältää muita objekteja.

Tietokonetili	Computer Account. Active Directoryn objektityyppi, jota käytetään tietokonetietojen tallennukseen.
Toimialue	Domain. Tietokone- ja käyttäjätileistä muodostuva kokonaisuus.
Toimialuemetsä	Domain Forest. Toimialueiden ja toimialuepuiden muodostama kokonaisuus.
Toimialuepuu	Domain Tree. Toimialueen ja sen alitoimialueiden muodostama kokonaisuus.
Toimipaikka	Site. Aliverkoista muodostuva kokonaisuus.
UPN	User Principal Name. Käyttäjän pääasiallinen kirjautumisnimi. Yksilöllinen toimialuemetsässä.
Varmenne	Certificate. Tunniste jolla voidaan todentaa kohteen identiteetti.
Verkkotunnus	Domain. IP-osoitteen sijaan käytettävä helpommin muistettava tapa viitata verkkoon kytkettyyn koneeseen. kts. DNS.
VPN	Virtual Private Network. Virtuaalinen erillisverkko. Lähiverkkojen välille Internetin ylitse muodostettava verkko.

1 Johdanto

Opinnäytetyön aiheena oli Active Directoryn suunnittelu ja käyttöönotto pienyrityksessä. Opinnäytetyössä perehdyttiin Active Directoryn ominaisuuksiin ja mahdollisuuksiin pienyrityksen näkökulmasta sekä niihin asioihin, joita Active Directoryn käyttöönotossa tulee huomiota pienyrityksen tapauksessa. Työssä käsitellään myös Active Directoryn kanssa liitettäviä palveluita siltä osin kuin ne olennaisesti esiintyivät projektissa.

Työ on tehty Joensuulaiselle Process Genius Oy:lle tarkoituksena päivittää IT-ympäristö paremmin ylläpidettäväksi ja käytettäväksi hakemistopalvelun avulla. Opinnäytetyö painottuu Active Directoryn osalta Process Genius Oy:lle olennaisiin ominaisuuksiin, jotka ovat osittain sovellettavissa muihinkin pienyrityksiin.

Opinnäytetyön teoriaosuudessa perehdyttiin Active Directoryn rakenteeseen ja ominaisuuksiin yleisellä tasolla sekä minkälaisiin asioihin tulisi kiinnittää huomiota Active Directoryn suunnittelussa ja käyttöönotossa pienyrityksen kannalta. Käytännönosuudessa käytiin läpi, miten Active Directory -ympäristö toteutettiin ja mitkä tekijät vaikuttivat toteutukseen. Työn lopussa käytiin läpi lyhyesti Azure Active Directoryn teoriaa, sen integroimista paikalliseen Active Directory -ympäristöön ja millä tavalla integrointi toteutettiin Process Genius Oy:n tapauksessa.

2 Process Genius Oy

Process Genius Oy on Joensuunlainen vuonna 2012 perustettu ohjelmistoalan yritys, joka keskittyy ”Digital Twin” -ratkaisuiden tarjoamiseen teollisuudelle. Digital Twinillä tarkoitetaan fyysisen ympäristön luomista virtuaalisovellukseen, esimerkiksi tuotantolaitoksen mallintaminen ja laitoksen datan visualisointi digitaalisessa mallissa. Digital Twinin lisäksi Process Genius on erikoistunut esineiden internetiin (Internet of Things – IoT), 3D-mallinnukseen sekä lisättyyn ja virtuaaliseen todellisuuteen liittyviin ratkaisuihin.

Process Geniuksella työskentelee kirjoittamishetkellä 31 henkilöä, joista suurin osa Joensuun toimistossa, mutta muutamia henkilöitä Helsingissä ja yksi Tampereella. Yrityksessä rohkaistaan etätyöhön ja liikkuvuuteen, joka on otettava huomioon myös Active Directoryn suunnittelun kannalta. Yrityksessä pääasiallisina kielinä käytetään englantia ja suomea.

Yrityksen organisaatiorakenne on joustava, mutta karkeasti voisi rajata yrityksessä olevan seuraavat osastot:

- Production Team
- Management
- Research & Development
- Sales & Marketing
- IT

Production Team käsittää työntekijöiden valtaosan, ohjelmistokehittäjistä mallintajiin. Production Team:in puolestaan muodostavat sen sisällä olevat Developers Team ja UX Team, joista jälkimmäinen sisältää mallintajat, käyttöliittymäsuunnittelijat ja käyttökokemuksesta vastaavat henkilöt. Management-ryhmä sisältää hallintoon liittyvät henkilöt ja operatiivisen johdon. Research & Development -ryhmään kuuluu teknologiajohtajan lisäksi muut tuotteen kehityksestä vastaavat henkilöt. Sales & Marketing -ryhmän muodostavat myyntiin ja markkinointiin erikoistuneet henkilöt. IT-ryhmä sisältää yrityksen sisäisestä tietotekniikasta vastaavan henkilöstön.

Process Genius on nopeasti kasvanut yritys ja tämä on tuonut omat haasteet organisaation ja tietotekniikan ylläpidolle. Yrityksessä on ollut puhetta Active Directoryn tai vastaavan palvelun käyttöönotosta jo ennen tätä opinnäytetyötä.

3 Active Directory

Active Directory on Microsoftin kehittämä hakemistopalvelu, joka pohjautuu LDAP-protokollaan ja tuli käyttöön ensimmäisen kerran Windows 2000 -käyttöjärjestelmässä. Hakemistopalvelulla tarkoitetaan palvelua, johon tallennetaan erilaisia objekteja ja niille voidaan liittää ominaisuuksia.

Active Directory mahdollistaa koko yrityksen laajuisen tiedon tehokkaan hallinnan keskitetystä palvelusta, joka voidaan jakaa maailmanlaajuisesti. Active Directoryssä oleva tieto voidaan saattaa yrityksen laajuisesti saataville, tai rajatummalle joukolle. [1, s. 1]

3.1 Active Directoryn rakenne

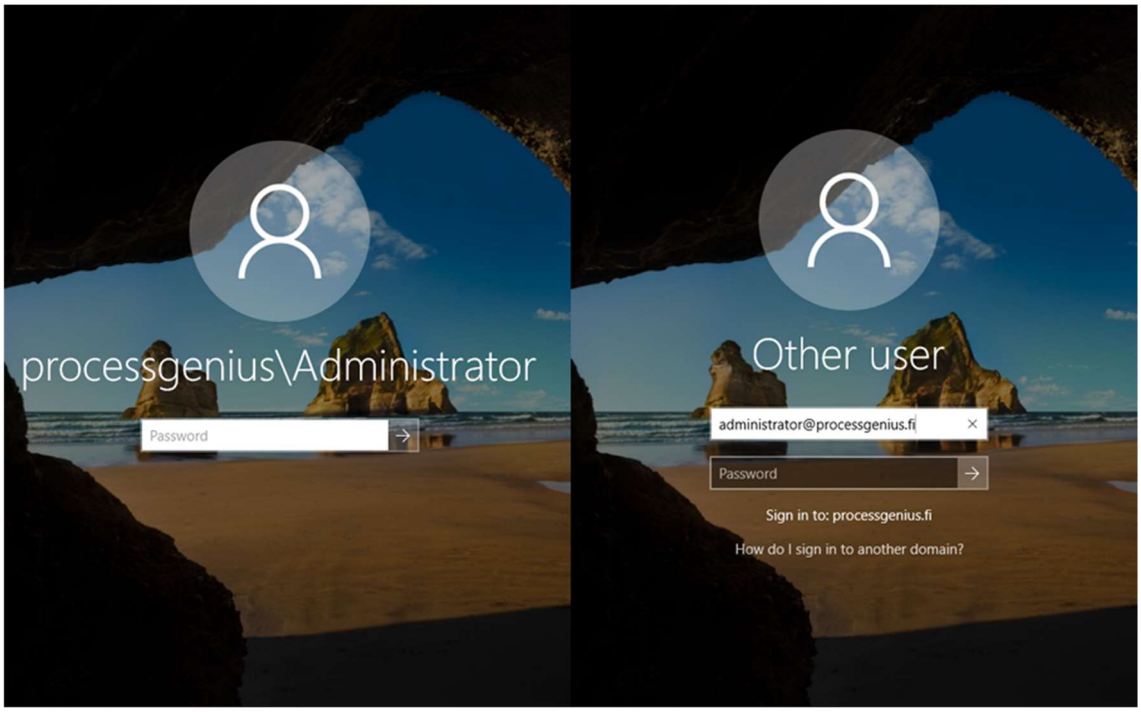
Active Directoryssä tieto on tallennettu hierarkkisesti objekteihin. Objektit, joita kutsutaan myös lehtisolmuiksi (leaf nodes), ovat joko säiliöitä (containers) tai eisäiliöitä (non-containers). Säiliöt voivat sisältää toisia säiliöitä tai lehtisolmuja, mutta lehtisolmut eivät voi sisältää muita objekteja. [1, s. 5]

Kaikilla objekteilla Active Directoryssä on maailmanlaajuisesti yksilöllinen 128-bittinen tunnistetieto, joka määritetään objektin luomisvaiheessa. Tätä tunnistetietoa kutsutaan nimellä ”globally unique identifier” eli GUID. Objektin GUID pysyy muuttumattomana, vaikka itse objekti nimettäisiin uudelleen tai siihen tehtäisiin muita muutoksia.

Objekteilla on GUIDin lisäksi myös yksiselitteinen nimi ”distinguished name” (DN) -tunnistetieto, joka on helpompi muistaa ja käsitellä kuin GUID. LDAP-protokolla määrittelee yksiselitteisen nimen normaaliksi tavaksi viitata objektiin hakemistossa. RDN:n eli ”relative distinguished namen” avulla voidaan viitata kyseisen säiliön (container) sisällä olevaan objektiin. Saman säiliön sisällä ei voi olla useampia objekteja samalla RDN-tunnistetiedolla, mutta eri säiliössä olevilla objekteilla voi olla sama RDN-tunnistetieto. [1, s. 7-8]

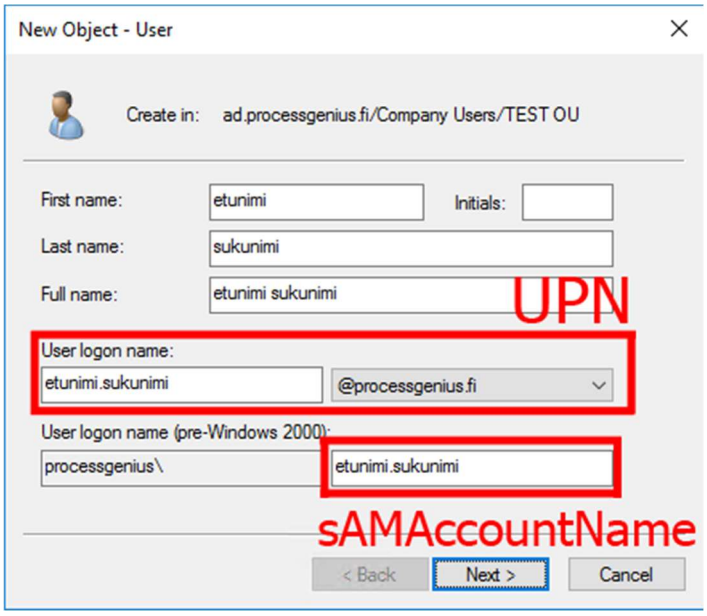
Käyttäjäobjektilla on attribuutti ”sAMAccountName”, joka on käyttäjän kirjautumisnimi. Tämän kirjautumisnimen pitää olla yksilöllinen toimialueessa. Kirjautumisnimi voi olla esimerkiksi muotoa ”matti.meikalainen”. Perinteisen kirjautumisnimen lisäksi käyttäjäobjektilla on toinen kirjautumisnimi attribuutti ”UPN” eli UserPrincipalName (käyttäjän pääasiallinen kirjautumisnimi). UPN näyttää muodoltaan sähköpostiosoitteelta ja on syytä olla yksilöllinen koko toimialuemetsässä.

Käyttäjä voi kirjautua toimialuemetsään tietokoneella perinteisen kirjautumisnimen (sAMAccountName) ja toimialueen nimen avulla tai vaihtoehtoisesti käyttämällä UPN-kirjautumisnimeä (Kuva 1).



Kuva 1. Kirjautuminen

Active Directoryssä UPN-päätteen ei tarvitse olla toimialueen nimi, vaan se voi olla mikä tahansa RFC 5322 -standardin mukainen osoite. UPN-päätteitä voidaan lisätä Active Directoryyn jälkikäteen ja jokaiselle käyttäjälle määritetään käytössä oleva UPN-pääte. Käyttäjätunnusta luodessa määritetään UPN ja sAMAccountName -attribuutit (Kuva 2).



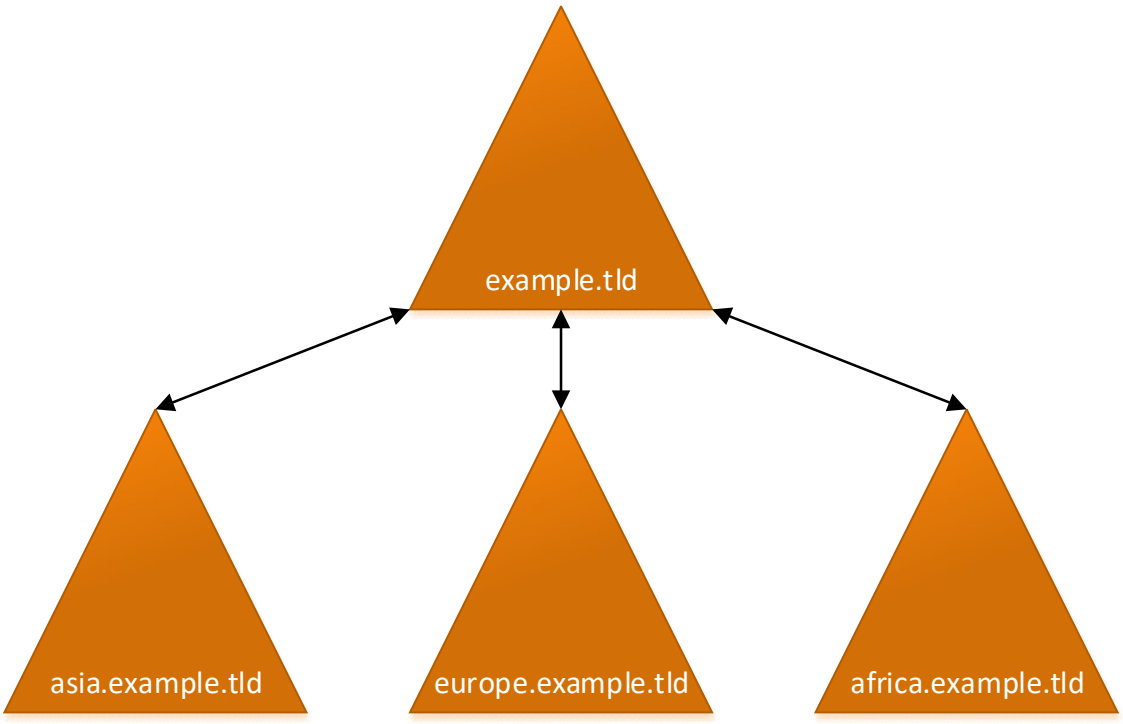
Kuva 2. Uuden käyttäjän luominen

3.1.1 Toimialue

Active Directory koostuu toimialueista ja toimialue sisältää säiliöitä ja objekteja. Toimialueelle on määritetty yksilöllinen DNS-nimiavaruus. Ohjauskone (Domain Controller) voi kuulua vain yhteen toimialueeseen, mutta toimialueella voi olla useampi ohjauskone. [1, s. 9]

Toimialuepuu muodostuu toimialuekokonaisuuksista, jotka on luotu juuritoimialueen alle alitoimialueina samalle nimiavaruudelle. Esimerkiksi example.tld-toimialueelle luodaan alitoimialueet asia.example.tld, europe.example.tld ja africa.example.tld. Toimialueella ja alitoimialueilla voi olla useita alitoimialueita ja tätä hierarkkista rakennetta kutsutaan toimialuepuuksi. Toimialuepuu nimetään juuritoimialueen mukaan, tässä esimerkissä example.tld (Kuva 3).

Kaikkien toimialuepuussa olevien toimialueiden välillä on kaksisuuntainen transitiivinen luottamussuhde ”Two-Way Transitive Trust” [2] , joka tarkoittaa, että toimialueiden välinen kaksisuuntainen luottamussuhde laajennetaan automaattisesti muihin toimialueisiin, johon kyseinen toimialue luottaa. Käyttäjän autentikoidessa esimerkiksi asia.example.tld toimialueessa voidaan hänelle antaa muiden example.tld toimialuepuun resurssit käyttöön ilman erillistä autentikointia jokaiselle toimialueelle. [1, s. 10]



Kuva 3. Toimialuepuu example.tld

Siinä missä toimialuepuu on kokoelma toimialueita, muodostuu toimialuemetsä yhdestä tai useammasta toimialuepuusta. Toimialuemetsän sisällä olevien toimialuepuiden välillä on samanlainen luottamussuhde kuin toimialuepuun toimialueiden välillä. Toimialuemetsä nimetään automaattisesti ensimmäisen toimialueen mukaan (Forest Root Domain), eikä toimialuemetsän juuritoimialuetta pysty poistamaan Active Directorystä tuhoamatta koko toimialuemetsää. Toimialuemetsän sisällä kaikki toimialueet jakavat toimialueen kaavan (Schema). [1, s. 11]

Eri toimialuemetsissä olevien toimialueiden välille voidaan luoda luottamussuhde, joka voidaan määrittää yksisuuntaiseksi tai kaksisuuntaiseksi. Eri toimialuemetsissä olevien toimialueiden luottamussuhde on aina ”non-transative trust”, eli luottamussuhde on vain tiettyjen toimialueiden välinen, eikä laajennu automaattisesti muihin toimialueisiin. [3]

3.1.2 Toimipaikat

Toimipaikkojen (Sites) tarkoituksena Active Directoryssä on määrittää verkon fyysistä rakennetta käyttäen aliverkkoja. Active Directory käyttää toimipaikkatietoa hakemistotiedon replikointia varten ja ohjaa käyttäjät käyttämään lähimmän toimipaikan saatavilla olevia resursseja. Toimipaikkojen välille määritetään yhteydet, joiden avulla Active Directory pystyy replikoimaan tiedot tehokkaasti.

Päätelaitteen toimipaikka tunnistetaan laitteen IP-osoitteen perusteella ja tämän mukaan määritetään, minkä toimipaikan resursseja laitteen tulisi käyttää. Mikäli toimipaikkoja ja aliverkkoja ei määritetä erikseen, kuuluvat kaikki IP-avaruudet oletustoimipaikkaan.

3.1.3 DNS ja toimialueen nimi

DNS-järjestelmä (nimipalvelinjärjestelmä) määrittää DNS-protokollan, jolla verkkotunnukset muutetaan IP-osoitteiksi. DNS ei ole varsinaisesti Active Directoryn

osa, mutta Active Directory on tiiviisti sidottu DNS-järjestelmään. Active Directory on riippuvainen DNS:stä ohjauskoneiden sijainnin paikantamisessa ja DNS vaikuttaa toimialueen nimeämiseen. [4]

Microsoft suosittelee Active Directoryn kanssa käytettäväksi yritykselle rekisteröidyn verkkotunnuksen aliverkkotunnusta ja välttämään aikaisemmin yleisessä käytössä olleita epävirallisia ylätason verkkotunnuspäätteistä ”.lan”, ”.local” ja ”.internal”. Myöskin testaamiseen ja dokumentointiin käytettäviä päätteitä ”.test”, ”.example”, ”.invalid” ja ”.localhost” tulisi välttää oikeassa tuotantoympäristössä. [5]

Toimialueen nimi ei ole sama asia kuin DNS-nimi. Toimialueen nimen avulla luokitellaan resursseja ja DNS-nimen avulla haetaan resursseja. Active Directory käyttää DNS:n mukaista nimeämiskäytäntöä toimialueille ja tietokoneille sekä tallentaa näiden tiedot DNS hierarkiaan. [6]

Active Directoryn kannalta on suositeltavaa käyttää DNS-roolia Active Directoryssä sen sijaan, että käytettäisiin erillistä DNS-palvelinta. Tätä ratkaisua kutsutaan nimellä ”Active Directory-Integrated DNS”. [7]

3.1.4 Global Catalog

Global Catalog (GC) on tärkeä osa Active Directoryä, koska Global Catalogissa säilytetään vain-luku-listaus kaikista toimialuemetsän objekteista. Toimialuemetsässä on pakollista olla vähintään yksi Global Catalog -palvelu ja uutta toimialuemetsää luodessa ensimmäiselle ohjauskoneelle tulee palvelu pakosti käyttöön.

Tavallisesti toimialueen ohjauskoneella on tieto pelkästään kyseisessä toimialueessa olevista objekteista, joten useamman toimialueen toimialuemetsässä objektien toimialuetieto haetaan Global Catalog -palvelusta.

Useamman toimialueen toimialuemetsässä on syytä määrittää jokaiselle toimialueelle vähintään yksi Global Catalog -palvelu. Global Catalog -palvelua ylläpitävät ohjauskoneet replikoivat Global Catalog -palvelun normaalin Active Directory replikaatiojärjestelmän kautta.

3.2 Flexible Single Master Operation (FSMO) roolit

Active Directory on rakenteeltaan multimaster replication -tyylinen, eli tietokanta on tallennettu usealle palvelintietokoneelle, joista jokainen pystyy tekemään päivityksiä tietokantaan. Kaikki palvelimet vastaavat tarvittaessa asiakastietokoneiden pyyntöihin ja ovat vastuussa replikoinnin onnistumisesta. Tällä rakenteella varmistetaan tietokannan toimivuus, vaikka osa palvelintietokoneista lopettaisi toiminnan. Active Directoryssä ohjauskoneet toimivat palvelintietokoneina ja pitävät yllä Active Directory tietokantaa.

Vaikka Active Directory käyttää multimaster replication -rakennetta on Active Directoryssä poikkeustapauksia, joissa vain yksi ohjaintietokone saa toimia hallintapalvelimena tietyille rooleille. Näitä rooleja on viisi kappaletta ja niitä hallitsevia ohjauskoneita kutsutaan Flexible Single Master Operation (FSMO) role owner,

eli FSMO-roolin omistajiksi. Näistä viidestä roolista kolme roolia on yksilöllisiä jokaisessa toimialueessa ja kaksi roolia on yksilöllisiä toimialuemetsäkohtaisesti. [1, s. 14]

Schema master -rooli on toimialuemetsäkohtainen. Roolin omistava ohjauskone on ainoa ohjauskone, joka voi tehdä Active Directoryn toimialuemetsän kaavaan muutoksia. Mikäli jokin muu kuin roolin omistava ohjauskone yrittää tehdä kaavaan muutosta, ohjataan pyyntö roolin omistavalle ohjauskoneelle käsiteltäväksi.

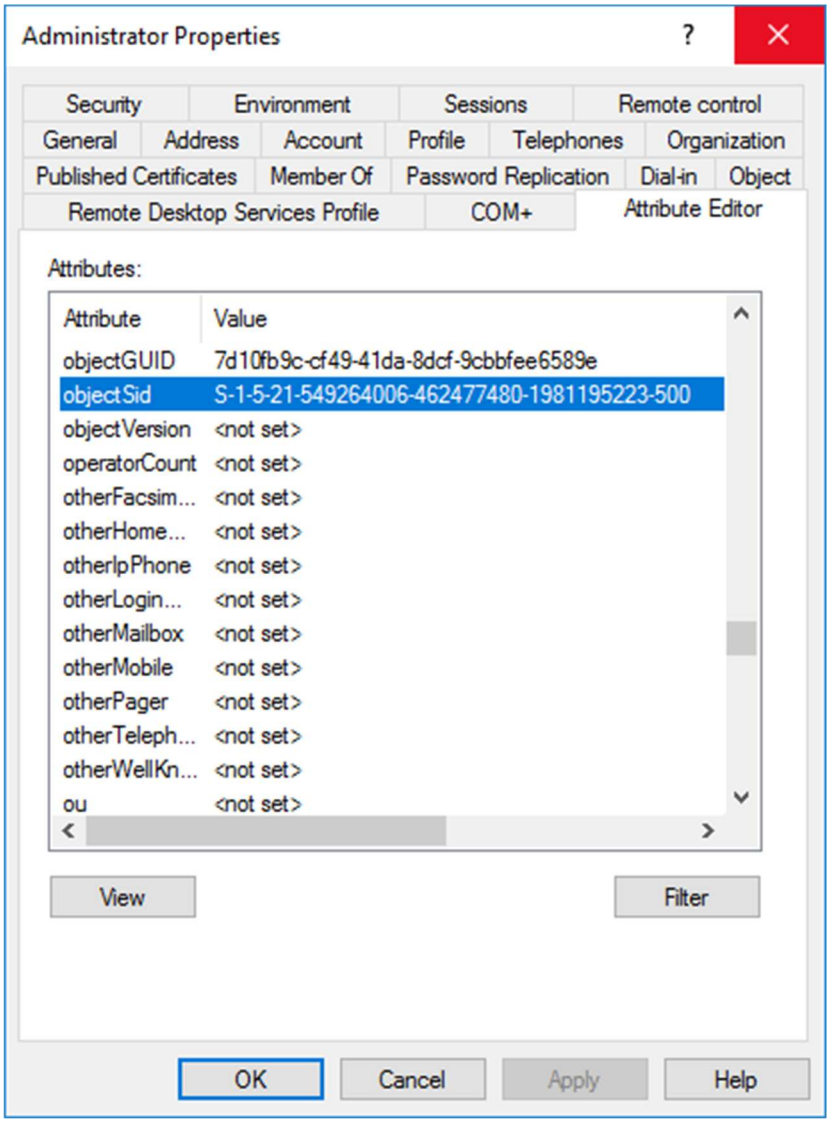
Domain naming master -rooli on myös toimialuemetsäkohtainen ja roolilla kontrolloidaan muutoksia toimialuemetsän nimiavaruuteen. Roolin omistava ohjauskone lisää ja poistaa toimialueita sekä uudelleen nimeää ja siirtää toimialueita toimialuemetsässä. Roolilla kontrolloidaan myös ”application partitions” osiota Active Directoryssä, joka sisältää tiedon Active Directoryyn liitetyistä applikaatioista kuten DNS-palvelimesta.

PDC emulator -rooli on toimialuekohtainen ja roolin tarkoitus on toimia Windows NT primary domain controllerina (PDC) yhteensopivuussyistä ja aikapalvelimena toimialueelle. PDC emulator -roolin omistavan ohjauskoneen tehtävä on myös ylläpitää tietoa viimeisimmistä salasanoista. Esimerkiksi mikäli käyttäjä haluaa vaihtaa salasanaa, ohjataan salasananvaihtopyyntö toimialueen ohjauskoneelle joka ylläpitää PDC emulator -roolia. Mikäli toimialueen ohjauskone ei pysty varmentamaan salasanaa kirjautumisvaiheessa niin pyyntö varmistetaan toimialueen PDC emulator -roolin pitäjältä. Ryhmäkäytäntöjen muokkaaminen tapahtuu myös PDC emulator -roolin ohjauskoneen kautta, jotta varmistetaan ettei useampi pääkäyttäjä tee muutoksia samaan ryhmäkäytäntöön eri ohjauskoneilla.

RID (relative identifier) master -rooli on toimialuekohtainen rooli, jonka tehtävä on huolehtia toimialueen RID -tiedon ylläpidosta. Security Identifier (SID) on toimialueen sisällä yksilöllinen tunniste toimialueen jokaisella security principalilla eli käyttäjällä, ryhmällä ja tietokoneella (Kuva 4). SID-tunniste luodaan security principalin luomisvaiheessa ohjauskoneen toimesta. Ryhmien kohdalla SID pysyy aina samana, mutta käyttäjien ja tietokoneiden SID luodaan uudelleen, mikäli nämä siirtyvät toimialueesta toiselle.

SID-tunnisteen viimeiset numerot muodostuvat RID -tiedosta, jotka security principalin luonut ohjauskone määrittää. Jokaiselle ohjauskoneelle on varattu ennalta 500 RID-tietoa käytettäväksi RID master -roolin ylläpitävän ohjauskoneen toimesta. Kun RID-tietoja on käytetty yli 50 % ohjaintietokone pyytää automaattisesti RID master -roolin ohjauskoneelta lisää tietueita. Tämä varmistaa, ettei samaa RID-arvoa esiinny toimialueella useampaa kertaa.

Käyttäjän autentikoituessa toimialueelle luodaan käyttäjälle pääsyoikeus (access token), joka sisältää käyttäjän nykyisen ja vanhat SID-tunnisteet sekä kaikkien käyttäjäryhmien SID-tunnisteet, joihin käyttäjä on liitetty. Käyttäjän yrittäessä käyttää resursseja Active Directoryssä verrataan pääsyoikeudessa olevia SID-tunnisteita resurssin pääsylistalla oleviin SID-tunnisteisiin ja tämän perusteella käyttäjälle joko myönnetään tai estetään oikeus resurssiin.



Kuva 4. Käyttäjätilin SID

Infrastructure master -rooli on toimialuekohtainen ja sen tehtävänä on ylläpitää viittauksia objekteihin, jotka ovat toisissa toimialueissa. Roolia ylläpitävä ohjauskone huolehtii myös viittauksista objekteihin toimialueessa ja tarkistaa tiedon Global Catalog -palvelimelta.

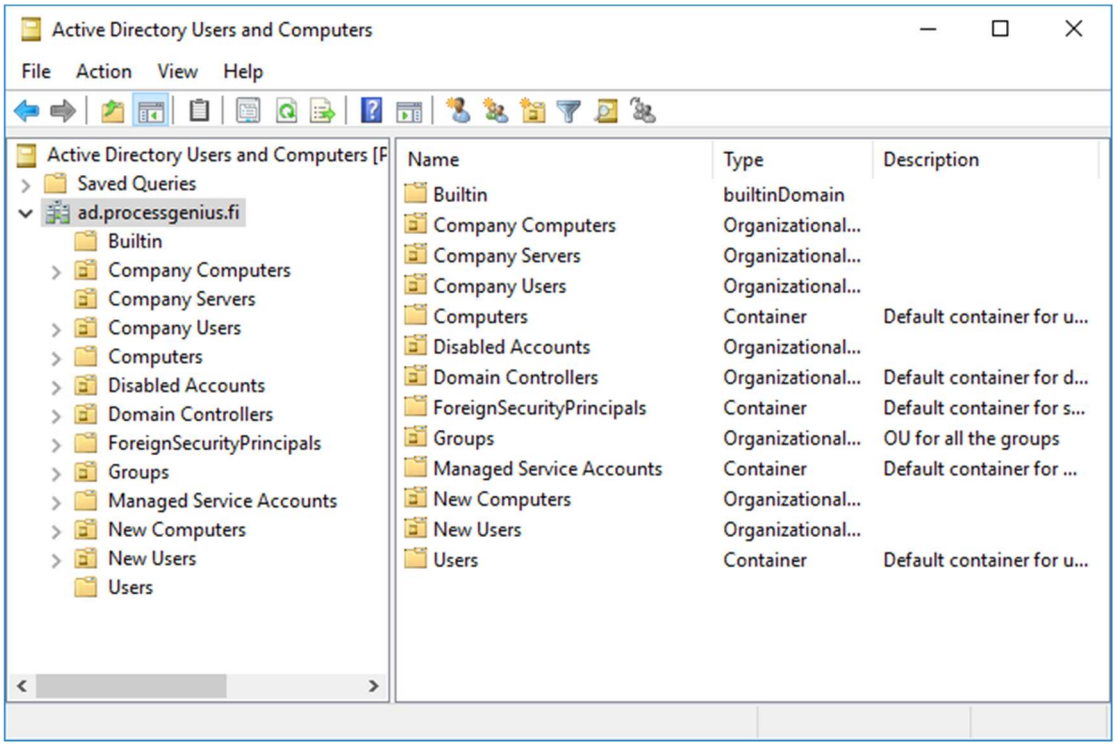
Kaikki FSMO roolit on mahdollista siirtää ohjauskoneelta toiselle tarvittaessa. FSMO roolit eivät siirry automaattisesti toiselle ohjauskoneelle, mikäli alkuperäinen roolia ylläpitävä ohjauskone ei ole enää käytettävissä, vaan siirto vaatii ylläpitäjän tekemään muutoksen.

3.3 Organisaatioyksikkö

Organisaatioyksikkö on Active Directoryssä oleva säiliötyyppi, jonka sisälle voidaan laittaa toimialueen objekteja: käyttäjätilejä, tietokonetilejä ja käyttäjäryhmiä. Organisaatioyksikkö voi sisältää myös muita organisaatioyksiköitä ja organisaatioyksikkö ei näy loppukäyttäjälle.

Organisaatioyksiöiden tulisi perustua yrityksen rakenteeseen ja tarpeisiin. Organisaatioyksiköiden avulla voidaan delegoida ylläpito-oikeuksia koskemaan vain tiettyjä organisaatioyksikön objekteja. Active Directoryn objekti voi kuulua vain yhteen organisaatioyksikköön ja objekteja voidaan siirtää organisaatioyksiköstä toiseen Active Directoryn Users and Computers -konsolissa (Kuva 5).

Organisaatioyksikön lisäksi toinen säiliötyyppi on kontti (container), mutta kontti ei tue ryhmäkäytäntöjä eikä oikeuksien delegointia. Onkin suositeltavaa aina käyttää organisaatioyksiköitä konttien sijaan nykyaikaisessa Active Directory ympäristössä. [1, s. 13]



Kuva 5. Active Directory Users and Computers -konsoli

3.4 Käyttäjäryhmät

Active Directoryssä on kahden tyyppisiä käyttäjäryhmiä ”distribution” ja ”security” joista ensimmäistä käytetään pääasiassa sähköpostituslistoja muodostamaan ja Security -tyyppisiä ryhmiä käyttöoikeuksien hallinnassa.

Active Directoryssä käyttäjäryhmillä on kolme eri laajuutta: Domain Local, Global ja Universal. Käyttäjäryhmät tukevat sisäkkäisiä käyttäjäryhmiä (nested groups), jonka avulla käyttäjäryhmä voi olla toisen käyttäjäryhmän jäsen. Käyttäjäryhmän ominaisuudet riippuvat sille määritetystä laajuudesta, joka määritetään käyttäjäryhmän luomisvaiheessa (Kuva 6).

Kaikki käyttäjäryhmätyypit voivat sisällyttää käyttäjä- ja tietokonetilejä saman toimialueen sisältä. Mikäli käytössä on useampi kuin yksi toimialue riippuu käyttäjäryhmätyypistä mitä objekteja siihen voidaan sisällyttää (Kuva 7) (Kuva 8).

Laajuus	Voi sisältää Domain Local	Voi sisältää Global	Voi sisältää Universal
Domain Local	Kyllä	Kyllä	Kyllä
Global	Ei	Kyllä	Ei
Universal	Ei	Kyllä	Kyllä

Kuva 6. Käyttäjäryhmätyypit

Laajuus	Voi sisältää käyttäjä- ja tietokonetilejä		Voi sisältää Domain Local ryhmiä	
	Samasta toimialueesta	Toisesta toimialueesta	Samasta toimialueesta	Toisesta toimialueesta
Domain Local	Kyllä	Kyllä	Kyllä	Ei
Global	Kyllä	Ei	Ei	Ei
Universal	Kyllä	Kyllä	Ei	Ei

Kuva 7. Käyttäjä- ja tietokonetilit ja Domain Local -ryhmät usean toimialueen toimialuemetsässä.

Laajuus	Voi sisältää Global ryhmiä		Voi sisältää Universal ryhmiä	
	Samasta toimialueesta	Toisesta toimialueesta	Samasta toimialueesta	Toisesta toimialueesta
Domain Local	Kyllä	Kyllä	Kyllä	Kyllä
Global	Kyllä	Ei	Ei	Ei
Universal	Kyllä	Kyllä	Kyllä	Kyllä

Kuva 8. Global ja Universal -ryhmät usean toimialueen toimialuemetsässä.

3.5 Ryhmäkäytännöt

Ryhmäkäytännöt ovat Active Directoryssä objekteja, joihin voidaan tallentaa ylläpitäjän määrittämiä asetuksia. Ryhmäkäytännöillä voidaan määrittää mm. tietokoneiden- ja käyttäjien asetuksia, suojauksia, ajettavia skriptejä ja asennettavia ohjelmia.

Kaikki ryhmäkäytännöt muodostuvat kahdesta osasta: tietokone- ja käyttäjäosasta. Tietokonekäytännöt vaikuttavat vain tietokonetiliobjekteihin ja käyttäjäkäytännöt vaikuttavat käyttäjätiliobjekteihin. Yhdessä ryhmäkäytännössä voi olla tietokonekäytäntöjä, käyttäjäkäytäntöjä tai molempia yhtä aikaa.

Ryhmäkäytännöt ovat itsenäisiä objekteja Active Directoryssä, jotka voidaan linkittää yhteen tai useampaan seuraavista kohteista: toimialueeseen, toimipaikkaan tai organisaatioyksikköön. [1, s. 290]

Ryhmäkäytännöt prosessoidaan seuraavassa järjestyksessä:

- Paikalliset ryhmäkäytännöt (Local Group Policy Objects)
- Toimipaikan ryhmäkäytännöt
- Toimialueen ryhmäkäytännöt
- Organisaatioyksikön ryhmäkäytännöt

Linkitetyt ryhmäkäytännöt vaikuttavat kaikkiin objekteihin, jotka sijaitsevat linkitetyn kohteen alla hierarkiassa. Esimerkiksi toimialuetasolle linkitetty ryhmäkäytäntö tulee voimaan kaikille ryhmäkäytäntöä koskeville objekteille toimialueella. Ryhmäkäytännöt prosessoidaan niin, että mikäli samaan asetukseen vaikuttaa useampi ryhmäkäytäntö tulee voimaan viimeisenä prosessoitu, eli mikäli toimialue-tasolle on määritetty ryhmäkäytäntö ja samaan asetukseen vaikuttava ryhmäkäytäntö on määritetty myös organisaatioyksikköön, jää organisaatioyksikössä määritetty asetus voimaan. Mikäli jotain asetusta ei määrätä ryhmäkäytäntöjen avulla erikseen, niin voimaan jää oletusasetus.

Ryhmäkäytännöt voidaan estää periytymästä tietylle organisaatioyksikölle määrittämällä organisaatioyksille periytymisen esto (Block Inheritance) asetus päälle. Vastaavasti ryhmäkäytäntö voidaan määrittää pakotetuksi (Enforced), jolloin se periytyy estosta huolimatta. Ryhmäkäytäntöjen ”security filtering” ominaisuutta muuttamalla on mahdollista rajoittaa ryhmäkäytäntöjen toiminta esimerkiksi tietylle käyttäjälle tai tietokoneelle.

Käyttämällä ryhmäkäytäntöjen ”Loopback Merge Mode” ja ”Loopback Replace Mode” ominaisuuksia voidaan luoda ryhmäkäytäntöjä, jotka ovat voimassa esimerkiksi käyttäjälle vain kun hän kirjautuu tietylle tietokoneelle. Mikäli tietokoneelle on asetettu Loopback Merge Mode -käytäntö päälle, käsitellään kirjautuvan käyttäjän ryhmäkäytännöt normaalisti, mutta tämän jälkeen käsitellään vielä käyttäjäkäytännöt, jotka vaikuttavat kyseiseen tietokoneobjektiin. Loopback Replace Modea käyttäessä käyttäjää koskevat ryhmäkäytännöt jätetään kokonaan käsittelemättä ja käsitellään vain tietokoneobjektille määritetyt käyttäjäkäytännöt.

Loopback -käytännöllä voidaan siis luoda tilanne, jossa esimerkiksi yleisessä käytössä olevalle tietokoneelle voidaan asettaa Loopback Replace Mode ja luoda ryhmäkäytäntöjä, jotka rajoittavat koneen käyttöä. Näin ollen riippumatta käyttäjän omista ryhmäkäytännöistä, tulee hänelle aina voimaan kyseiselle tietokoneobjektille määritetyt käyttäjäkäytännöt tälle tietokoneelle kirjautuessa.

3.6 Active Directory Domain Services

Active Directory Domain Services on palvelu, joka käytännössä muodostaa Active Directoryn. Usein kuitenkin Active Directory sanalla tarkoitetaan kokonaisuutta, joka sisältää Domain Servicesin lisäksi muitakin palveluita.

Active Directory Domain Services -roolin asennus Windows-palvelimelle ylentää palvelimen ohjauskoneeksi (Domain Controller), jonka yhteydessä palvelin voidaan liittää olemassa olevaan toimialuemetsään tai luoda uusi toimialuemetsä.

3.7 Active Directory Certificate Services

Active Directory Certificate Services (AD CS) on palvelinrooli, joka mahdollista julkisen avaimen infrastruktuurin (Public Key Infrastructure – PKI) luomisen ja tarjoaa käyttöön julkisen avaimen salauksen, digitaalisia varmenteita ja digitaalisia allekirjoituksia Active Directory -ympäristössä. [8]

AD CS ei ole pakollinen osa Active Directoryä, mutta on tehokas, turvallinen ja kustannustehokas tapa hallita varmenteiden jakamista ja käyttöä. AD CS mahdollistaa palvelimen käyttämisen ”certification authority” (CA) roolissa, jolloin palvelimen luodulla päävarmenteella (root certificate) voidaan allekirjoittaa varmenteita esimerkiksi lähiverkkoon liitetyille palvelimille. Ryhmäkäytäntöjen avulla Active Directoryyn liitetyille laitteille voidaan automaattisesti lisätä luotu päävarmenne luotetuksi varmenteiden myöntäjäksi. Tällä tavalla Active Directoryssä oleva tietokone joka yhdistää palvelimeen, millä on käytössä päävarmenteen allekirjoittamaa varmenne, luottaa automaattisesti tämän palvelimen varmenteeseen. [8] AD CS rooli sisältää myös työkalut joiden avulla voidaan luoda ja ottaa käyttöön automaattisesti varmenteita käyttäjille, tietokoneille ja verkkolaitteille.

3.8 Active Directory Federation Services

Active Directory Federation Services (AD FS) esiteltiin ensimmäisen kerran Windows Server 2003 R2 -käyttöjärjestelmässä ja on siitä lähtien ollut saatavilla kaikille Windows Server -käyttöjärjestelmille. AD FS mahdollistaa kertakirjautumisen (single sign-on; SSO) toimialuetunnuksilla verkkosovelluksiin, jotka ovat toisten organisaatioiden hallinnoimia, ilman luottamussuhteen muodostamista toisen toimialueen kanssa. [9, s. 657]

AD FS:n avulla erotetaan käyttäjän autentikointi (Authentication) ja valtuutus (Authorization) eri prosesseihin. Käyttäjä autentikoidaan yhden organisaation palvelun kautta ja tämä palvelu välittää tiedon kolmannelle osapuolelle, että käyttäjä on se kuka väittää olevansa. Kolmannen osapuolen palvelin tarjoaa palveluita sen perusteella mitä oikeuksia käyttäjälle on asetettu. Näiden kahden organisaation välistä suhdetta kuvataan termillä ”Federation Trust”. [9, s. 657]

3.9 Windows-palvelimen muut roolit

Windows-palvelimelle voidaan asentaa monia muitakin rooleja, jotka eivät ole suoranaisesti osa Active Directoryä. Näitä palveluita kuitenkin käytetään usein Active Directoryn kanssa ja ne voidaan monissa tapauksissa integroida osaksi Active Directory -ympäristöä. Esimerkkinä näistä rooleista DHCP (Dynamic Host configuration Protocol) -palvelin ja Windows-palvelimen File and Storage Services -palvelut.

3.9.1 DHCP Server

DHCP-palvelin jakaa IP-osoitteita lähiverkkoon kytketyille laitteille DHCP-protokollan avulla. IP-osoitteen lisäksi laitteille voidaan jakaa oletusyhdyskäytävän ja nimipalvelimien IP-osoitetiedot.

DHCP-palvelin ei ole pakollinen osa Active Directory -ympäristöä, vaan voidaan toteuttaa esimerkiksi erillisellä reitittimellä, palomuurilla tai palvelimella. Mikäli DHCP-palvelin rooli asennetaan toimialueelle on siihen määritettävä osoitealue (DHCP Scope), jonka mukaan IP-osoitteet jaetaan. Lisäksi palvelin tulee asettaa valtuutetuksi palvelimeksi.

3.9.2 File and Storage Services

File and Storage Services -kategoria sisältää useita tiedostojen ja tallennustilan jakamiseen liittyviä palveluita.

File Server -roolin avulla voidaan luoda palvelimelle jaettuja kansioita, joihin voidaan määrittää käyttäjille käyttöoikeuksia. Jaettuihin kansioihin voidaan määrittää pääsyoikeudet käyttäjä, tietokone tai ryhmäkohtaisesti. Käyttöoikeudet käyttävät SID-tunnisteita.

File Server Resource Manager -roolilla voidaan luoda tiedostoraportteja, luokitteluja sekä kiintiöitä tallennustilaan. Kiintiöiden avulla voidaan määrittää levyasemien ja kansioiden käytettävissä olevat koot.

Work Folders -roolin tarkoitus on synkronoida käyttäjän paikallisia tiedostoja palvelimelle. Work Folders -teknologia on ollut käytössä Windows Server 2012 R2 -käyttöjärjestelmästä lähtien ja sen tarkoitus on korvata aikaisemmin yleisesti käytössä ollut Folder Redirection ja Offline Files -ominaisuuksien yhteiskäyttö.

Folder Redirectionin ja ryhmäkäytäntöjen avulla on voitu määrittää esimerkiksi käyttäjän työpöydältä tietyn kansion sijaitsevan toimialueella olevalla tiedostonjakopalvelimella, jolloin käyttäjän tallentaessa tiedostoja kyseiseen kansioon ne on tallennettu paikallisen koneen sijaan tiedostonjakopalvelimelle. Ongelma syntyy esimerkiksi kannettavien tietokoneiden kanssa, kun käyttäjä haluaa käyttää palvelimella olevia tiedostoja ilman verkkoyhteyttä tai hitaalla verkkoyhteydellä virtuaalisen erillisverkon (VPN) yli. Hitaalla yhteydellä suurien tiedostojen käsittely palvelimelta käsin on ongelmallista ja ilman verkkoyhteyttä mahdotonta.

Ratkaisuna tähän on käytetty Offline Files -teknologiaa yhdessä Folder Redirectionin kanssa. Offline Filesin avulla voidaan määrittää tiettyjä tiedostojakoja käytettäväksi ilman verkkoyhteyttä tähän tiedostonjakopalvelimeen. Käytännössä Offline Files synkronoi tiedostot palvelimelta käyttäjän tietokoneelle. Folder Redirection ja Offline Files yhdistelmän kanssa voi tulla ongelmatilanteita synkronoinnin kanssa, kuten jos käyttäjä tallentaa tiedoston kansioon joka sijaitsee Folder Redirectionin takia verkkolevyllä, mutta katkaisee yhteyden verkkoon ennen kuin Offline Files -ominaisuus ehtii synkronoida tiedot paikalliselle tietokoneelle takaisin.

Work Foldersin on tarkoitus tarjota parempi ja luotettavampi tapa taata käyttäjille pääsy tiedostoihinsa erilaisilla laitteilla. Toisin kuin Offline Files -teknologia, Work Folders tukee synkronointia internetin yli ilman erillistä etäkäyttötekniikka ja lisäksi Work Folders tukee perinteisten tietokoneiden lisäksi Android ja iOS -laitteita. Work Folders toimii myös Folder Redirection ja Offline Files yhdistelmään nähden toisinpäin; käyttäjä tallentaa tiedostot paikalliselle laitteelle ja ne synkronoidaan siitä palvelimelle verkkoyhteyden niin salliessa. Näin viimeisin versio tiedostoista on aina käyttäjän laitteella.

4 Active Directoryn suunnittelu

Microsoftin ohjeistuksen mukaisesti Active Directoryn suunnittelu tulee aloittaa loogisen rakenteen suunnittelusta, eli millä tavalla objektit halutaan organisoida. Loogisen rakenteen suunnittelu sisältää toimialuemetsän suunnittelun, toimialueiden suunnittelun jokaiseen toimialuemetsään, DNS-infrastruktuurin ja organisaatioyksiköiden suunnittelun. Loogisen rakenteen suunnittelun jälkeen tulee suunnitella ohjauskoneiden sijoittelu ja toimipaikat sekä toimipaikkojen väliset yhteydet. [10]

4.1 Suunnittelussa huomioitavaa

Active Directoryn käyttöönottoa varten yritys tarvitsee palvelimen, Windows Server -käyttöjärjestelmän ja tarvittavat käyttäjä- tai laitelisenssit. Pienyrityksen tapauksessa näistä voi muodostua yrityksen kannalta huomattava aloituskustannus ja tämä tulee ottaa huomioon Active Directoryn käyttöönottoa suunnitellessa. Nykyisin monia Active Directoryn ominaisuuksia pystytään korvaamaan esimerkiksi Azure Active Directoryä käyttäen. Pilvipalvelujen avulla ei kuitenkaan yleisesti pystytä tarjoamaan yhtä hyvää päätelaitteiden hallintaa, eikä korvaamaan esimerkiksi paikallista tiedostonjakopalvelinta.

Active Directoryn käyttöönotto jo toiminnassa olevaan yritysympäristöön täytyy suunnitella huolellisesti, ettei käyttöönotosta synny ylimääräisiä katkoksia ympäristöön. Active Directory vaatii muutoksia yrityksen verkkoinfrastruktuuriin ja tietokoneisiin, jotka liitetään Active Directoryyn. Tarvittaessa on hyvä suunnitella testiympäristö, jossa tarvittavia ominaisuuksia ja palveluita voi testata ennen lopullista Active Directoryn käyttöönottoa.

4.1.1 Verkkoinfrastruktuuri

Suunnittelussa on huomioitava yrityksen käytössä oleva verkkoinfrastruktuuri ja sen soveltuvuus ja muokattavuus Active Directoryä varten. Mikäli sisäinen verkkoinfrastruktuurin ylläpito on ulkoistettu kolmannelle osapuolelle, voi muutoksien tekeminen Active Directoryä varten olla hankalampaa ja aiheuttaa lisäkustannuksia.

Active Directoryn kannalta on olennaista suunnitella yrityksen sisäverkon DHCP-palvelimen ja DNS-palvelimen soveltuvuus sekä selvittää mahdollisuus siirtää DNS-palvelin toimimaan Active Directoryn ohjauskoneelle Microsoftin suosituksien mukaisesti.

Mikäli käytössä on fyysisesti erillään olevia toimipisteitä, jotka haluaan liittää Active Directoryyn tulee suunnitella millä tavalla toimipisteiden välillä ohjauskoneet kommunikoivat.

4.1.2 Palvelimet, roolit ja lisensointi

Active Directoryn kannalta käytännössä pakolliset roolit ovat Active Directory Domain Services (AD DS) ja DNS-palvelin. Näiden roolien lisäksi kuitenkin usein halutaan myös esimerkiksi tiedostonjakorooli. Microsoft suosittelee, ettei Active

Directory Domain Services -palvelun kanssa asenneta muita rooleja samalle ohjauskoneelle, kuin korkeintaan DNS-palvelin. [11]

Microsoftin suosituksien perusteella olisi syytä asentaa AD DS ja DNS-palvelin -roolit yhdelle Windows Server -palvelimelle ja muut roolit toiselle tai toisille palvelimille. Microsoftin Windows Server 2016 -lisenssiä on saatavilla kahdenlaisia: Standard ja Datacenter. Lisenssiehtojen mukaisesti yhdellä lisenssillä voi käyttää yhtä tai useampaa Windows Server 2016 -palvelinta samalla fyysisellä palvelimella. Standard-lisenssillä tämä on rajoitettu kahteen palvelimeen per lisenssi ja Datacenter-lisenssillä rajattomaan määrään. [12] Käytännössä tämä tarkoittaa, että hankkimalla Datacenter-lisenssin yhdelle fyysiselle palvelimelle voi tällä palvelimella käyttää rajatonta määrä Windows Server 2016 -palvelimia virtualisoinnin avulla.

Datacenter-lisenssi on Standard-lisenssiä paljon kalliimpi ja pienyrityksen tapauksessa Standard-lisenssi voi olla järkevämpi vaihtoehto. Tämä kuitenkin tarkoittaa, että yhdellä fyysisellä palvelimella voi käyttää vain kahta Windows Server 2016 -palvelinta. Windows Server 2016 -lisensoinnissa tulee ottaa huomioon myös edellisistä käyttöjärjestelmistä poikkeava prosessoriydinkohtainen lisensointi (Core-based) jos palvelimessa on käytössä moniytimisiä prosessoreja. Hankkimalla useampia Standard-lisenssejä on mahdollista käyttää useampia virtuaalisia Windows Server 2016 -palvelimia samalla fyysisellä palvelimella; kahdella lisenssillä neljää, kolmella lisenssillä kuutta virtuaalista palvelinta jne. Käyttöjärjestelmän lisenssin lisäksi yrityksen tulee hankkia CAL-lisenssejä (Client Access License) jotka ovat joko käyttäjä- tai laitemäärän mukaan valittavissa.

Noudattamalla Microsoftin suositusta pitämällä AD DS ja DNS-palvelimen roolit omalla Windows Server 2016 -palvelimellaan ja käyttämällä edullisinta Standard-lisenssiä tarkoittaa tämä, että kaikki muut palvelinroolit asennettaisiin keskenään samalle Windows Server 2016 -palvelimelle. Yrityksen toimipisteiden määrä ja käytettävät palvelinroolit vaikuttavat miten monia palvelimia ja minkälaisella lisensoinnilla on järkevää hankkia.

4.2 Toimialuemetsän suunnittelu

Active Directoryn rakenne on suositeltavaa pitää yksinkertaisena, jotta hallinnointi on helpompaa. Parhaiden käytäntöjen mukaista uudelle toimialuemetsälle on luoda vain yksi toimialue toimialuemetsään. [1, s. 12]

Mikäli yrityksellä on toimintaa useassa maassa tai maanosassa, voi olla järkevää suunnitella toimialueet maa- tai maanosakohtaisesti helpottamaan toimialuemetsän hallintaa.

4.2.1 Toimialueiden suunnittelu

Microsoft suosittelee, että Active Directoryn toimialueen nimenä käytetään käytössä olevan verkkotunnuksen aliverkkotunnusta, esimerkiksi example.org jolloin toimialueen nimenä olisi ad.example.org. Aliverkkotunnus kannattaa olla semmoinen, jolle ei ole käyttöä Active Directoryn ulkopuolella, jotta DNS-tietojen ylläpito on helpompaa. [5]

4.2.2 Toimipaikkojen suunnittelu

Toimipaikkojen määrään vaikuttaa lähinnä yrityksen fyysiset toimipisteet. Mikäli yrityksellä on toimipisteitä useassa kaupungissa ja näihin toimipisteisiin halutaan ohjauskoneet, kannattaa fyysiset toimipisteet erotella Active Directoryssä erillisiksi toimipaikoiksi.

Toimipaikkojen suunnittelun osalta tulee ottaa huomioon, ettei useammassa toimipisteessä ole käytössä sama aliverkko, koska tällöin laitteet eivät tiedä mihin toimipaikkaan kuuluvat. Yhden fyysisen toimipisteen yritys ei lähtökohtaisesti tarvitse useampaa toimipaikkaa.

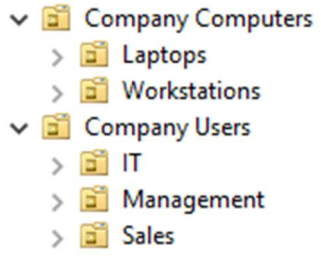
4.3 Organisaatioyksiköiden suunnittelu

Organisaatioyksikköjen suunnittelussa kannattaa ottaa pohjaksi yrityksen organisaatio ja luoda sitä vastaava tai yksinkertaistettu malli organisaatioyksiköille. Organisaatioyksikköjen mukaan voidaan delegoida oikeuksia, eli esimerkiksi voidaan erottaa tavalliset tietokoneet ja palvelimet omiin organisaatioyksiköihin ja antaa tietyille työntekijöille oikeus muokata vain tietokoneita organisaatioyksikössään.

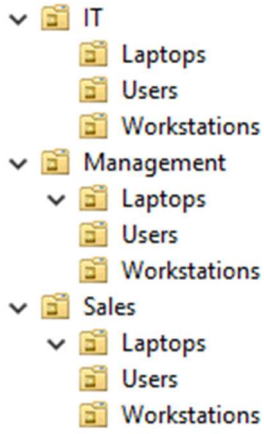
Ryhmäkäytännöt voidaan myös osoittaa tiettyyn organisaatioyksikköön, joten organisaatioyksiköiden suunnittelussa on hyvä huomioida millä tavalla ryhmäkäytäntöjä halutaan kohdistaa. Esimerkiksi pöytätietokoneet ja kannettavat voidaan erotella omiin organisaatioyksiköihin eri ryhmäkäytäntöjä varten.

Oletusarvoisesti Active Directoryssä uudet käyttäjätilit menevät konttiin nimeltään ”Users” ja tietokonetilit konttiin nimeltään ”Computers” toimialueen juuressa. Kontteihin ei voi osoittaa ryhmäkäytäntöjä, eikä delegoida oikeuksia, joten on suositeltavaa tehdä näiden konttien sijaan jonkinlainen toinen rakenne.

Esimerkkinä on kaksi erilaista rakennetta, joista ensimmäisessä on luotu tietokonetilejä varten ”Company Computers” organisaatioyksikkö, jonka alle on tehty organisaatioyksiköt ”Laptops” ja ”Workstations”. Käyttäjätilit ovat organisaatioyksikön ”Company Users” alle luoduissa osastokohtaisissa organisaatioyksiköissä (Kuva 9). Toisessa esimerkissä jokaiselle osastolle on luotu oma organisaatioyksikkö ja osastokohtaisen organisaatioyksiköiden alle omat yksiköt ”Laptops”, ”Users” ja ”Workstations” (Kuva 10). Active Directoryn ylläpitämisen kannalta on suositeltavaa, ettei samaan organisaatioyksikköön laiteta tietokone- ja käyttäjätilejä.



Kuva 9. Organisaatioyksikkö esimerkki 1



Kuva 10. Organisaatioyksikkö esimerkki 2

4.4 Käyttäjäryhmien ja käyttöoikeuksien suunnittelu

Microsoft suosittelee hyödyntämään sisäkkäisiä ryhmiä, koska sillä helpotetaan käyttöoikeuksien hallintaa ja vähennetään ylimääräistä verkkoliikennettä monen toimialueen toimialuemetsässä. [13]

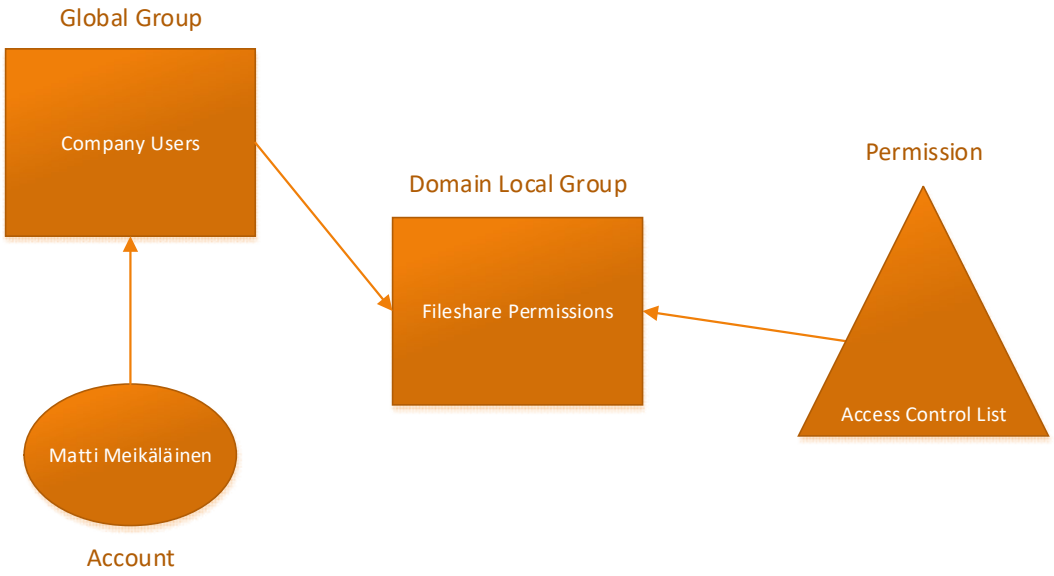
Sisäkkäisten ryhmien periaatteella kun ryhmälle käyttäjiä halutaan antaa oikeudet tiedostonjakopalvelimelle, toimitaan esimerkiksi seuraavasti (Kuva 11):

1) Ylläpitäjä luo Domain Local Group -ryhmän nimellä ”Fileshare Permissions”.
2) Ylläpitäjä antaa tiedostonjakoon tarvittavat oikeudet käyttäjäryhmälle ”Fileshare Permissions”.
3) Ylläpitäjä luo Global Group -ryhmän nimellä ”Company Users” johon lisätään halutut käyttäjät.
4) Ylläpitäjä lisää ”Company Users” ryhmän jäseneksi ”Fileshare Permissions” -ryhmään.

Käyttöoikeudet on helppo tarkistaa katsomalla Domain Local Group -ryhmän (”Fileshare Permissions”) jäsenet, tai vaihtoehtoisesti voidaan helposti tarkistaa käyttäjäryhmän oikeudet tarkistamalla minkä ryhmien jäsenenä Global Group -ryhmä (”Company Users”) on. Esimerkin mukaista järjestystä kutsutaan kirjainyhdistelmällä AGDLP sanojen **account**, **global**, **domain local**, **permissions** mukaisesti. Kirjainyhdistelmällä kuvataan järjestystä, miten käyttäjäryhmät ja oikeudet muodostuvat. Käyttäjätili (account) lisätään Global Group -ryhmään, joka lisätään Domain Local Group -ryhmään ja lopulta käyttöoikeudet resurssiin annetaan Domain Local Groupille. [13]

Antamalla käyttöoikeuksia pelkästään Domain Local Group -ryhmille on käyttöoikeuksien valvominen helpompaa, kun ei tarvitse tarkistaa resurssikohtaisesti mille käyttäjille tai käyttäjäryhmille on annettu oikeuksia resurssiin. Käyttäjän oikeudet nähdään helposti tarkistamalla käyttäjäryhmät, joihin käyttäjä kuuluu. Tällä vältytään tilanteelta, että jollekin käyttäjälle jäisi oikeuksia resursseihin joihin ei ole enää tarvetta.

AGDLP-mallia voidaan laajentaa käyttämällä Universal Group -ryhmiä, jolloin käytetään niin kutsuttua AGUDLP-mallia. AGUDLP-malli noudattaa AGDLP-mallin logiikkaa, mutta Global Group -ryhmät kuuluvat Universal Group -ryhmään ja Universal Group -ryhmät lisätään Domain Local Group -ryhmiin käyttöoikeuksia varten. Universal Group -ryhmille ja AGUDLP-mallille ei yleisesti ottaen ole tarvetta ympäristöissä, joissa ei ole useampaa toimialuetta samassa toimialuemetsässä. Kuten edellä kuvatussa esimerkissä käy ilmi, tulisi käyttäjäryhmät suunnitella käyttöoikeuksia huomioon ottaen.



Kuva 11. AGDLP-malli

4.5 Ryhmäkäytäntöjen suunnittelu

Ryhmäkäytännöillä voidaan säädellä Active Directoryssä olevien päätelaitteiden asetuksia hyvinkin tarkkaan. Ryhmäkäytännöillä voidaan määrittää seuraavia asetuksia:

- Registery settings
- Security settings
- Group policy preferences
- Software installation

Ryhmäkäytäntöjen käsittely hidastaa aina päätelaitetta. Tietokonetileihin vaikuttavat ryhmäkäytännöt käsitellään tietokoneen käynnistyessä ja käyttäjätileihin vaikuttavat käyttäjän kirjautuessa. Mikäli käytössä on liian monia ryhmäkäytäntöjä, hidastuu nämä operaatiot. Ryhmäkäytäntöjä suunnitellessa onkin hyvä pyrkiä välttämään kaikkien asetuksien ennalta määrittämistä ja määrittää vain välttämättömät yrityksen tietoturvan ja käyttäjän käytettävyyden kannalta.

Ryhmäkäytäntöjä tulisi pääasiassa linkittää haluttuihin organisaatioyksiköihin ja välttää ylimääräisiä ryhmäkäytäntöjen pakottamisia (Enforce) ja periytymisen es-

toja (Block Inheritance), koska nämä asetukset muuttavat ryhmäkäytäntöjen oletusarvoista toimintaperiaatetta ja voivat vaikeuttaa vikatilanteiden selvittämistä. [1, s. 296]

Listassa on muutamia esimerkkejä, mitä ryhmäkäytäntöjen avulla voidaan tehdä ja joita kannattaa miettiä suunnitteluvaiheessa:

- lisätään käyttäjälle automaattisesti verkkosijainti verkkolevyksi
- määritetään tietokoneen virta-asetukset ja näytönsäästäjän asetukset
- tehdään automaattisia rekisterimuutoksia päätelaitteille
- sallitaan päätelaitteen etäkäyttö Remote Desktop -ohjelmistolla
- määritetään päätelaitteen palomuurin asetukset
- tehdään muutoksia päätelaitteen paikallisiin käyttäjiin/käyttäjäryhmiin.

4.6 Muiden palveluiden suunnittelu

Suunnitteluvaiheessa on syytä kartoittaa mille palveluille ympäristössä on tarvetta. Active Directory Certificate Services on hyödyllinen, mikäli ympäristössä on tarvetta varmenteiden myöntämiselle ja hallinnalle. Varmenteita voidaan käyttää esimerkiksi samassa lähiverkossa sijaitsevilla verkkolaitteilla ja palvelimilla muodostamaan salattu yhteys. DHCP-palvelin ja tiedostonjako -roolien tarpeellisuus riippuu yrityksen tarpeista ja onko ne toteutettu jo jollakin toisella palvelimella.

Active Directoryyn on myös mahdollista liittää muita palveluita Active Directory Federation Services -roolin avulla sekä käyttämällä LDAP-protokollaa. Suunnitteluvaiheessa onkin hyvä kartoittaa, että mitä palveluita on käytössä, voiko ne liittää Active Directoryyn ja onko liittämiselle tarvetta. Liittämällä palvelut Active Directoryyn käyttäjien ja oikeuksien hallinta voidaan toteuttaa keskitetysti, mikä helpottaa ylläpitoa ja tietoturvaa.

5 Active Directoryn toteutus

Active Directoryn perusrakenne on pysynyt samanlaisena vuosikymmeniä, mutta vuosien saatossa ominaisuuksia ja palveluita on tullut lisää, sekä parhaat käytännöt (best practices) ovat muuttuneet joiltakin osin hyvin suuresti. Hyvänä esimerkkinä tästä aikaisemmin käytössä ollut Folder Redirection ja Offline Files -ominaisuuksien käyttö, joka nykyisin suositellaan korvaamaan uudemmalla Work Folders -ominaisuudella.

5.1 Lähtötilanne

Lähtötilanteessa selvitettiin yrityksen tarpeet ja vaatimukset Active Directorylle. Palvelun käyttöönotosta oli yrityksessä ollut puhetta jo aikaisemmin ja projektin alkuvaiheessa tultiin siihen tulokseen, että palvelu oli yritykselle hyödyllinen. Esi-

merkiksi pilvipalveluvaihtoehdot karsiutuivat pois, koska yrityksellä oli tarvetta tiedostonjakopalvelimelle ja suurelle määrälle tallennettua tietoa, jonka siirtäminen ja tallentaminen Internet-yhteyttä käyttäen olisi ollut epäkäytännöllistä.

Yrityksen käytössä oli tiedostonjakopalvelin ja testipalvelimia asiakasprojekteja varten paikallisella palvelimella, joten oli luontevaa lähteä suunnittelemaan olemassa olevan ratkaisun päivittämistä. Keskusteluissa tultiin tulokseen, että Active Directoryn avulla voidaan toteuttaa nykyinen ratkaisu paremmin ja lisäksi helpottaa tietokoneiden ja käyttöoikeuksien hallintaa. Suurin osa Process Genius Oy:n työntekijöistä on Joensuun toimipisteellä, eikä erillisten ohjauskoneiden hankintaa muille toimipisteille nähty kustannustehokkaana muutaman työntekijän takia. Lisäksi työntekijöiden liikkuvuuden takia etäyhteys Joensuun toimistoon oli välttämätöntä toteuttaa muutenkin.

Alkuselvityksen aikana luotiin projektille aikataulu-arvio ja suunnitelmaa projektin toteuttamisesta. Suunnitteluvaiheessa tultiin siihen tulokseen, että käyttäjät ja laitteet haluttiin liittää pienissä osissa Active Directory -palveluun mahdollisten ongelmien välttämisessä.

Projektin alkuvaiheessa selvitin yrityksen tarpeet ja minkä tyyppisille ominaisuuksille yrityksellä olisi käyttöä. Tämän jälkeen tutustuin Active Directoryn ominaisuuksiin ja selvitin millä tavalla Active Directoryn avulla pystytään toteuttamaan yrityksen tarvitsemat palvelut. Palveluita ja ominaisuuksia testattiin ensin testiympäristössä, joka toteutettiin yrityksen verkossa erillisessä virtuaalilähiverkossa (VLAN).

Process Geniuksen kannalta tärkeimmiksi käyttötarpeiksi Active Directorylle rajautui:

- nykyisen tiedostojakopalvelimen korvaaminen
- tietokoneiden ja käyttöoikeuksien hallinnan ja ylläpidon helpotettavuus
- GDPR (EU:n tietosuoja uudistus)
- varmuuskopiointi
- muihin järjestelmiin integrointimahdollisuus tulevaisuus.

Tiedostonjakopalvelin oli Linux-pohjainen Samba-palvelin, johon työntekijöille oli luotu tarvittaessa käyttäjätunnus ja määritetty oikeus tiedostonjakoihin. Eri käyttäjäryhmiä ja erilaisia oikeuksia ei ollut, eikä myöskään automaattista varmuuskopiointia.

Process Genius Oy:n kaikki tietokoneet olivat aikaisemmin paikallisesti hallittuja niin, että jokaisella työntekijällä oli käyttäjä omalle tietokoneelleen ylläpitäjäoikeuksilla. Joillekin tietokoneelle oli tehty yhteisiä käyttäjätunnuksia ja välillä työntekijät lainasivat omia käyttäjätunnuksiaan toisten käyttöön. Tähän haluttiin parannusta tietoturvan ja yksityisyydensuojan takia voimaan tulevan GDPR:n takia.

Process Genius Oy:llä on käytössä Office 365:nen, joten käytännössä tiedostojen varmuuskopiointi oli toteutettu käsin Microsoftin One Drive for Business ja Sharepoint -palveluihin tai ulkoiselle tallennusmedialle. Tähän haluttiin parannus, että varmuuskopiot saatiin tehtyä automaattisesti ja paremmin kuin pilvipalveluun.

5.2 Laitteisto ja sisäverkon toteutus

Process Genius Oy:n sisäverkko muodostuu yhdestä palomuuri-reitittimestä, kytkimistä sekä WLAN-tukiasemista. Käytössä on kolme erillistä virtuaalilähiverkkoa: työntekijöille, vierailijoille ja verkon- ja palvelimien ylläpidolle. Virtuaalilähiverkot on määritetty palomuuri-reitittimeen, joka hoitaa verkkojen välisen reitityksen. Active Directoryä varten luotiin oma virtuaalilähiverkko erillään muista.

Lähtötilanteessa yrityksen palomuuri-reititin toimi DHCP- ja DNS-palvelimena. Yhtenä haasteena oli toteuttaa projekti aiheuttamatta käyttökatkoksia olemassa oleviin palveluihin ja verkkoon.

Active Directoryn käytön kannalta päädyttiin suunnitelmaan, että palomuuri-reititin toimii DHCP- ja DNS-palvelimena jatkossakin, mutta Active Directoryyn integroidaan oma DNS-palvelin. Palomuuri-reitittimeen määritettiin Active Directoryllä käytössä oleva nimiavaruus ohjautumaan Active Directoryn DNS-palvelimelle ”Domain override” asetuksella, jolloin kaikki kyseiseen nimiavaruuteen tulevat kyselyt ohjataan Active Directoryn DNS-palvelimelle.

Käytännössä siis kaikki verkossa olevat laitteet saavat IP-osoitteen palomuuri-reitittimen DHCP-palvelimelta ja käyttävät tätä palvelinta DNS-palvelimena, paitsi yhdistäessä nimiavaruuteen, joka on käytössä Active Directoryssä. Tällöin nimipalvelukysely ohjataan Active Directoryn DNS-palvelimeen. Tällä ratkaisulla pystyttiin pitämään nykyinen verkkoinfrastruktuuri käytössä, kunnes kaikki laitteet on siirretty Active Directory -ympäristöön. Tällöin kaikki DNS-liikenne voidaan vaihtaa ohjautumaan Active Directoryn DNS-palvelimelle.

5.3 Palvelimien asennus

Process Genius Oy:n vanhan palvelimen korvaajaksi hankitun palvelimen mukana hankittiin yksi kappale Microsoft Windows Server 2016 Standard -lisenssejä sekä tarvittava määrä Windows Server CAL -lisenssejä kaikille yrityksen työntekijöille.

Virtuaalisointikäyttöjärjestelmäksi valittiin Microsoft Hyper-V Server 2016, koska yrityksessä oli aikaisempaa kokemusta Microsoft Hyper-V Server -käyttöjärjestelmästä ja Microsoft Hyper-V Server -käyttöjärjestelmä on ilmainen käyttää. Hyper-V -palvelimelle asennettiin projektissa tarvittavat palvelimet virtuaalikoneina.

Microsoft Windows Server 2016 Standard -lisenssi sallii kahden virtuaalisen Windows Server 2016 käytön samalla fyysisellä palvelimella virtuaalisointikäyttöjärjestelmästä riippumatta. Palvelimelle luotiin kaksi virtuaalikonetta: **PRD-DC-01** ohjauskoneeksi ja **PRD-FS-01** tiedostonjakopalvelimeksi.

5.4 Roolien asennus

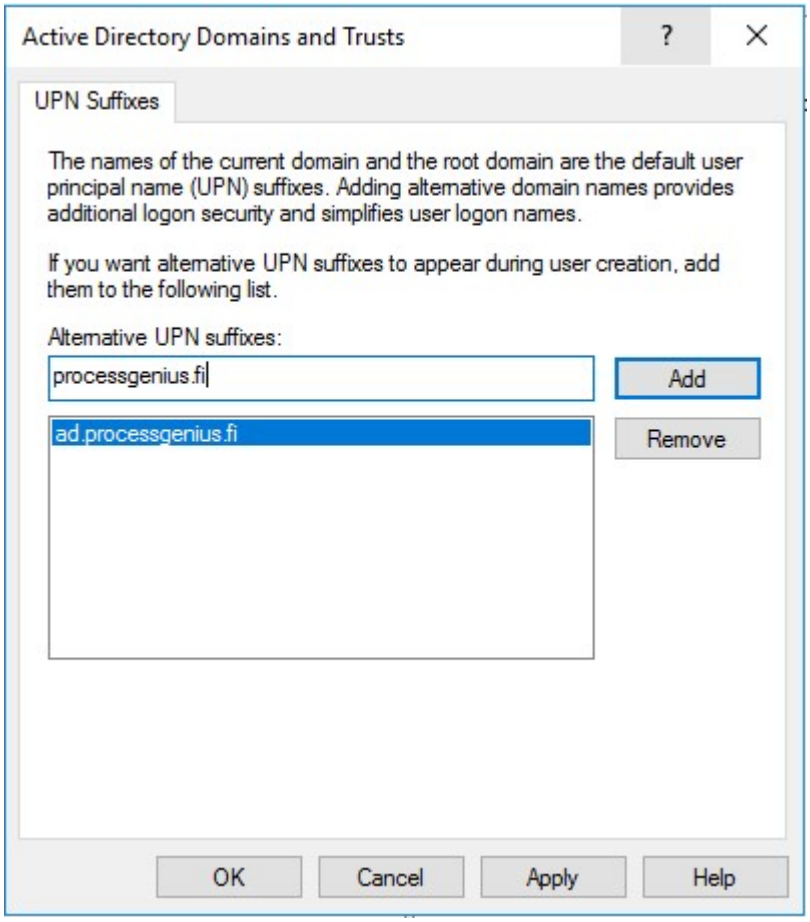
Microsoftin suosituksien mukaisesti ohjauskoneelle PRD-DC-01 asennettiin pelkästään Active Directory Domain Services ja DNS-palvelin roolit. Myöhemmin palvelimeen lisättiin myös Azure AD Connect liitokseen Azure AD:hen.

Toiselle virtuaalipalvelimelle (PRD-FS-01) asennettiin muut tarvittavat roolit. Yhdelle palvelimelle monen roolin keskittämisen sijaan harkittiin vaihtoehtoa jakaa roolit kahden virtuaalisen palvelimen välillä tasaisemmin, mutta lopulta päädyttiin ohjauskoneen pitämisen mahdollisimman suosituksien mukaisena ilman lisäroolеja. Tulevaisuudessa rooleja voidaan kuitenkin siirtää tiedostonjakopalvelimelta muille palvelimille, mikäli tarvetta tälle tulee ja hankitaan lisää palvelinlisenssejä.

5.5 Toimialuemetsän toteutus

5.5.1 Toimialueen toteutus

Process Genius Oy:n pääasiallisena verkkotunnuksena on käytössä ”processgenius.fi”, joka on myös käytössä käyttäjien sähköpostiosoitteissa. Ympäristön koon ja parhaiden käytäntöjen mukaisesti luotiin yksi toimialuemetsä ja siihen yksi toimialue ”ad.processgenius.fi”. Toimialueelle lisättiin UPN-päätteeksi ”processgenius.fi” (Kuva 12), jotta kirjautumista varten voitiin käyttää ”etunimi.sukunimi@processgenius.fi” muotoa. Tällöin oli helppo ohjeistaa työntekijöitä käyttämään samaa tunnusta, kuin heidän sähköpostissa on käytössä.



Kuva 12. UPN-päätteen lisääminen

Active Directory Domain Services -roolia asentaessa määritettiin myös NetBIOS -nimeksi ”PROCESSGENIUS” oletusarvoisen ”AD” sijaan. Oletusarvoinen NetBIOS -nimi muodostuu toimialueen nimen vasemman puoleisimmasta osasta, eli ”ad.processgenius.fi” tapauksessa ”AD”. Käyttäjillä on mahdollisuus kirjautua joko käyttämällä ”DOMAIN\sAMAccountName” -muotoista tunnusta, tai vaihtoehtoisesti pelkkää UPN-kirjautumisnimeä käyttäen.

5.5.2 Toimipaikan toteutus

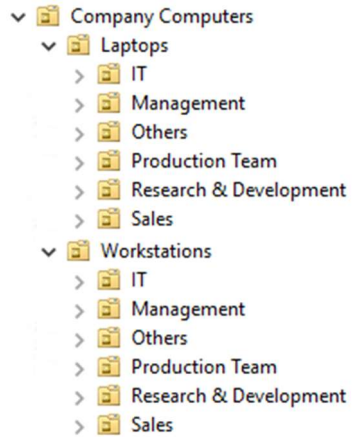
Suunnitteluvaiheessa päätettiin, että Active Directoryyn tulee vain yksi toimipaikka ja muihin toimipisteisiin ei asenneta ohjauskonetta tässä vaiheessa. Active Directory mahdollistaa tulevaisuudessa uusien toimipaikkojen lisäämisen, mikäli ohjauskoneita halutaan ottaa käyttöön muissa toimipisteissä.

Active Directoryn oletustoimipaikka nimettiin ”Joensuu” toimipaikaksi ja siihen liitettiin käytössä olevat aliverkot. Active Directory toiminnan kannalta tällä muutoksella ei ole väliä, mutta mikäli uusia toimipaikkoja lisätään olisi Joensuun toimipisteen aliverkot jouduttu määrittämään joka tapauksessa. Tulevaisuudessa jos Helsingin toimipisteelle halutaan ottaa ohjauskone käyttöön, luodaan Active Directoryyn uusi toimipaikka ”Helsinki” ja määritetään siihen kuuluvat aliverkot.

5.6 Organisaatioyksiköiden toteutus

Organisaatioyksiköiksi luotiin uusille käyttäjille ”New Users” ja vastaavasti uusille tietokoneille ”New Computers” organisaatioyksikkö. Uudet käyttäjät ja tietokoneet asetettiin automaattisesti menemään näihin organisaatioyksiköihin oletusarvoisten konttien ”User” ja ”Computers” sijaan. Tällä järjestelyllä on helppo löytää uudet käyttäjät ja tietokoneet ja siirtää ne oikeisiin organisaatioyksiköihin. Käyttämällä organisaatioyksiköitä konttien sijaan mahdollisestaan myös ryhmäkäytäntöjen ajamisen suoraan uusille käyttäjille ja tietokoneille. Esimerkkinä voidaan luoda ryhmäkäytäntö, joka estää tietokoneelle kirjautumisen ja liittää se ”New Computers” organisaatioyksikköön. Näin varmistetaan, että vaikka tietokone saataisiin liitettyä toimialueeseen niin se pitää siirtää pois oletusyksiköstä oikeaan organisaatioyksikköön ennen käyttöä.

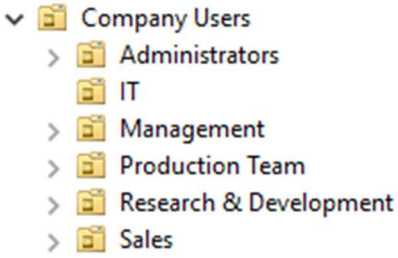
Toimialueeseen luotiin tietokoneita varten organisaatioyksikkö ”Company Computers” jonka alle tehtiin ”Laptops” ja ”Workstations” organisaatioyksiköt. Molempiin organisaatioyksiköihin tehtiin omat organisaatioyksiköt osastoittain (Kuva 13). Tällä organisoinnilla mahdollistetaan ryhmäkäytäntöjen helppo kohdistaminen esimerkiksi pelkästään myyjien kannettaviin tietokoneisiin.



Kuva 13. Company Computers

Toimialueelle luotiin organisaatioyksikkö ”Company Servers”, jota käytetään kaikille muille palvelimille paitsi ohjauskoneille, jotka ovat omassa ”Domain Controllers” organisaatioyksikössä microsoftin suosituksen mukaisesti. [14]

Käyttäjiä varten luotiin organisaatioyksikkö ”Company Users”, minkä alle tehtiin tarvittavat organisaatioyksiköt osastoittain (Kuva 14). Tämän organisaatioyksikön alle luotiin myös ”Administrators” yksikkö, johon tehtiin ”Domain Administrators” ja ”Server Administrators” yksiköt. ”Domain Administrators” yksikkö sisältävät ”Domain Admins” ryhmässä olevat käyttäjät ja ”Server Administrators” yksikössä on muut käyttäjätunnukset, joita käytetään hoitamaan Active Directoryn ylläpitoa. Ylläpitäjäroolit on erotettu muista osastoista selkeyden vuoksi sekä mahdollistamaan oikeuksien rajoittamista niin, ettei tavallinen ylläpitäjä voi tehdä muutoksia ”Domain Administrators” yksikössä oleviin käyttäjätileihin.



Kuva 14. Company Users

Käyttäjäryhmiä varten luotiin organisaatioyksikkö ”Groups” johon tehtiin organisaatioyksiköt ”Domain Local Groups”, ”Global Groups”, ”Domain Administrators Groups” ja ”AD Administrator Groups” (Kuva 15). ”Domain Local Groups” ja ”Global Groups” sisältävät nimensä mukaiset ryhmät ja ”Domain Administrators Groups” sisältää ryhmät joihin halutaan vain ”Domain Admins” ryhmässä olevien pystyvän tekemään muutoksia. Vastaavasti ”AD Administrator Groups” yksikkö sisältää ryhmät, joihin tavalliset ylläpitäjät pääsevät muokkaamaan.

Kuva 15. Groups

Käytöstä poistettuja tilejä varten luotiin ”Disabled Accounts” organisaatioyksikkö johon voidaan siirtää käytöstä poistetut tilit. Tällöin käytöstä poistetut tilit eivät jää käytössä olevien käyttäjien yksiköihin ja voidaan tehdä kohdennettuja ryhmäkäytäntöjä tälle yksikölle.

5.7 Käyttäjäryhmien ja käyttöoikeuksien toteutus

Active Directoryn oletuskäyttäjäryhmä siirrettiin organisaatioyksikköön ”AD Administrator Groups” ja vastaavasti ryhmät joihin haluttiin antaa oikeus vain ”Domain Admins” -käyttäjäryhmän jäsenille siirrettiin ”Domain Administrator Groups” organisaatioyksikköön. ”Domain Administrator Groups” yksikön alle siirretyt ryhmät sisälsivät ”Domain Admins”, ”Schema Admins” ja ”Enterprise Admins” sekä siihen liittyvät ryhmät. Myöskin kaikki Azure Active Directoryyn liittyvät ryhmät siirrettiin myöhemmässä vaiheessa ”Domain Administrator Groups” organisaatioyksikköön.

Process Genius Oy:n tapauksessa päädyin käyttämään AGDLP -käyttöoikeusmallia, koska Universal Group -ryhmille ei nähty tarvetta yhden toimialueen toimialuemetsässä. ”Global Groups” organisaatioyksikköön luotiin tarvittavat käyttäjäryhmät Global Groups -tyyppisenä etuliitteellä ”AD”, jotta käyttäjäryhmät erottuvat Azure AD:ssa olevista ryhmistä näiden yhdistyttyä. Käyttäjäryhmiä luotiin tarvittaville osastoille ja lisäksi luotiin ”AD Help Desk” -niminen ryhmä, jolle voitiin antaa käyttöoikeuksia esim. käyttäjien salasanan resetoimiseen. ”AD Administrator Groups” alle luotiin ”AD Administrators” -käyttäjäryhmä, joka toimii Active Directoryn ylläpitäjien ryhmänä.

”Domain Local Groups” organisaatioyksikön alle luotiin ”Domain Local” -tyyppisinä tarvittavat käyttäjäryhmät käyttöoikeuksien jakamista varten. Luotuja käyttäjäryhmiä oli esimerkiksi tiedostojakopalvelinta varten ”Storage Drive Read-Write Permission” ja ”IT Storage Drive Read-Write Permission”. ”Storage Drive Read-Write Permission” ryhmään lisättiin jäseneksi ”Domain Users” -käyttäjäryhmä, johon oletusarvoisesti kaikki uudet käyttäjät liitetään Active Directoryssä. Tällä saavutettiin haluttu tilanne, että kaikki Active Directoryn käyttäjät pääsivät käyttämään tiedostonjakopalvelinta.

5.8 Ryhmäkäytäntöjen toteutus

Process Genius Oy:n tapauksessa ryhmäkäytännöillä haluttiin helpottaa ylläpidettävyyttä ja lisätä tietoturvaa sen sijaan, että haluttaisiin rajoittaa liikaa käyttä-

jän oikeuksia. Ryhmäkäytäntöjen avulla Active Directoryn ominaisuuksien käytettävyyttä pystyttiin parantamaan, esimerkiksi Work Folders -ominaisuutta varten tehtiin tarvittavat ryhmäkäytännöt, jonka ansiosta käyttäjän ei tarvitse ottaa erikseen ominaisuutta käyttöön vaan se tehdään automaattisesti käyttäjän puolesta. Vastaavasti ryhmäkäytäntöjen avulla lisättiin käyttäjille automaattisesti tiedostojakopalvelin levyasemaksi.

Tietoturvan parantamisen osalta luotiin ryhmäkäytännöt, joiden avulla BitLockerin asetukset olivat ennalta määritetty halutunlaiseksi ja BitLockerin palautusavain tallentuu automaattisesti Active Directoryyn. Käyttäjien tietokoneille pakotettiin asetus ryhmäkäytäntöjen avulla, että mikäli tietokone on käyttämättömänä 5 minuuttia, niin tietokone menee lukitusruutuun ja käyttäjän pitää syöttää salasanansa käyttääkseen tietokonetta.

6 Muiden roolien ja palveluiden toteutus

Active Directoryn kannalta tärkeimmät roolit Active Directory Domain Services ja DNS-palvelin asennettiin PRD-DC-01 -palvelimelle, mutta kaikki muut roolit asennettiin tiedostopalvelimelle PRD-FS-01. Myöhemmässä vaiheessa myös Azure AD connect -työkalu asennettiin PRD-DC-01 -palvelimelle.

6.1 Active Directory Certificate Services

Tiedostopalvelimelle asennettiin Active Directory Certificate Services (AD CS) -rooli, jotta pystyttiin luomaan varmenteita toimialueeseen liitetyille tietokoneille ja palvelimille. Roolin asennuksen yhteydessä tiedostopalvelimelle luotiin ”self-signed certificate authority”, jota pystyttiin käyttämään varmenteita luodessa päävarmenteena allekirjoittamaan muut myönnetyt varmenteet. Ryhmäkäytäntöjen avulla tiedostopalvelimen päävarmenne asetettiin luotetuksi varmenteen myöntäjäksi kaikille toimialueeseen liitetyille tietokoneille.

Active Directory Certificate Services -rooli oli tarpeellinen Work Folders -roolia varten, jotta käyttäjien tietokoneiden ja tiedostopalvelimen välinne liikenne saatiin salattua. Toinen tärkeä syy Active Directory Certificate Services -roolin asentamiselle oli mahdollisuus luoda ryhmäkäytäntö, jolla kaikille toimialueeseen liitetyille tietokoneille pystyttiin automaattisesti luomaan ja jakamaan tietokonekohtainen varmenteita. Tietokonekohtaista varmennetta haluttiin käyttää OpenVPN-palvelun kanssa.

OpenVPN on avoimen lähdekoodin VPN-ohjelma, joka on saatavilla monille käyttöjärjestelmille mm. Windows, macOS ja Linux. Process Genius Oy:llä oli käytössä OpenVPN-palvelin palomuuri-reitittimessä etäyhteyttä varten. Palvelimelle oli luotu käyttäjätunnukset tarvittaville työntekijöille, joilla oli tarvetta muodostaa yhteys Joensuun toimiston verkkoon esimerkiksi tiedostonjakoja varten.

OpenVPN:ää haluttiin hyödyntää Active Directoryn kanssa niin, ettei työntekijöiden tarvitse erikseen kirjautua tunnuksilla VPN-ohjelmaan ja muodostaa yhteyttä

esimerkiksi kotoa työskennellessä. OpenVPN oli mahdollista asettaa käynnistymään tietokoneen käynnistyksen yhteydessä ennen käyttäjän kirjautumista tietokoneelle. Tällä mahdollistettiin se, että tietokone hakee aina uusimmat toimialueen ryhmäkäytännöt ohjauskoneelta ja ottaa ne voimaan käyttäjän kirjautuessa.

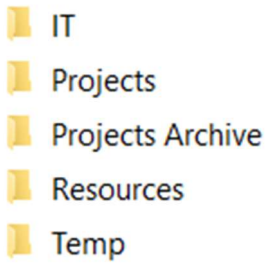
VPN-yhteyden ollessa muodostettu ennen käyttäjän kirjautumista, tapahtuu käyttäjän kirjautuminen tietokoneelle toimialueen ohjauskoneen kautta sen sijaan, että käytettäisiin paikallisessa välimuistissa olevia tunnuksia.

Active Directory Certificate Services -roolin luomia tietokonekohtaisia varmenteita hyödynnettiin OpenVPN:n kanssa, jotta tietokoneet yhdistävät palvelimeen käyttäen tietokonekohtaista varmennetta todentamaan henkilöllisyyden aikaisemman käyttäjän käsin syöttämän käyttäjätunnuksen ja salasanan sijaan.

Käytännössä AD CS:n avulla saavutettiin haluttu tilanne, että Active Directoryyn liitetyt tietokoneet saivat automaattisesti varmenteen palvelimelta ja OpenVPN-palvelun avulla tietokoneet saatiin yhdistämään turvallisesti toimialueeseen toimiston verkon ulkopuolelta, ilman tarvetta käyttäjän tehdä mitään.

6.2 File Server

Tiedostopalvelimelle asennettiin tiedostojakoon roolit ”File Server” ja ”File Server Resource Manager” sekä luotiin 3,75 teratavun levyosio tiedostojakoja varten. Levyosiolle luotiin kansio ”Storage” johon luotiin tarvittavat kansiot tiedostojakoihin (Kuva 16).



Kuva 16. Tiedostonjaon kansiorakenne

Kansioiden ”Projects”, ”Projects Archive”, ”Resources” ja ”Temp” oikeudet muokattiin niin, että aikaisemmin luodulla Domain Local -käyttäjäryhmällä ”Storage Drive Read-Write Permission” oli luku-, kirjoitus- ja muokkausoikeudet kansioihin. Kansiolle ”IT” määritettiin samanlaiset oikeudet ryhmälle ”IT Storage Drive Read-Write Permission”. Tiedostojaon juurihakemistoon estettiin kansioiden ja tiedostojen luonti-, sekä juurihakemistossa olevien edellä mainittujen kansioiden poisto tai muokkaus. Näin varmistettiin, että tiedostojaon juuri pysyy järjestyksessä ja käyttäjät käyttävät alikansioita juurikansion sijaan tiedostojen tallennuspaikkana.

Tiedostopalvelimelle otettiin käyttöön ”Shadow Copy” -ominaisuus, joka ottaa jaetuista tiedostoista versiohistoriasta varmuuskopion ennalta määritettynä aikana. Shadow Copyn avulla voidaan palauttaa tiedosto aikaisemmasta versiosta, mikäli käyttäjä poistaa tai muokkaa tiedostoa vahingossa.

6.3 Work Folders

Work Folders otettiin käyttöön tiedostonjakopalvelimella ja palvelua varten luotiin oma 1 teratavun levyosio. Levyosiolle tehtiin WorkFolders -niminen kansio jonka sisälle palvelu luo automaattisesti käyttäjäkohtaiset kansiot. Palvelua varten palvelimelle asennettiin IIS manager, jotta pystyttiin luomaan varmenteen allekirjoituspyyntö (Certificate Signing Request) Work Foldersia varten. Varmennepyyntö allekirjoitettiin tiedostopalvelimen varmenteen myöntäjän toimesta ja allekirjoituksen jälkeen lisättiin palvelimelle. Tämän avulla Work Folders -palvelun liikenne oli salattu.

Work Folders -kansiolle määritettiin käyttäjäkohtainen 10 gigatavun tallennuskiintiö. Work Folders -kansiolle otettiin käyttöön myös Shadow Copy -ominaisuus.

6.4 LAPS – Local Administrator Password Solution

LAPS on Microsoftin ohjelma joka mahdollista tietokoneiden paikallisen ylläpitäjäkäyttäjän salasanan tallentamisen Active Directory -palveluun. LAPS mahdollistaa myös paikallisten ylläpitäjäkäyttäjien salasanan muuttamisen satunnaiseksi kirjain-numero-yhdistelmäksi ja tämän tallentamisen Active Directoryyn. LAPS mahdollistaa tietokonekohtaisten paikallisten ylläpitäjäkäyttäjien salasanojen etsimisen Active Directorystä toimialueen ylläpitäjien toimesta esimerkiksi tilanteessa, jossa käyttäjällä ei ole verkkoyhteyttä tietokoneessa ja on tarvetta ylläpitäjätilin oikeuksiin.

LAPSin käyttöönotto vaati Active Directoryn kaavan muutosta, koska tietokone -objekteille haluttiin lisätä attribuutit paikallisen ylläpitäjäkäyttäjän salasanaa ja sen vanhenemisaikaa varten. LAPSia varten luotiin myös kaksi ryhmäkäytäntöä. Toinen ohjelman asennusta varten ja toinen käyttöä varten. LAPS-ohjelman asennus tapahtui tiedostonjakopalvelimen jaetulta verkkolevyltä. LAPS määritettiin ”Administrator” käyttäjälle ja salasanan vaikeudeksi 14 merkkiä ja vanhenemisajaksi 30 päivää.

Luotiin LAPSin salasanojen lukemista varten Domain Local -käyttäjäryhmä nimeltään ”LAPS Read Password Permission” ja salasanan nollaamista varten vastaava ”LAPS Reset Password Permission”. Näille ryhmille delegoitiin tarvittavat oikeudet lukea ja muuttaa LAPSin tallentamaa tietoa Active Directoryssä. Active Directoryn käyttäjäryhmä ”Domain Admins” lisättiin molempiin ryhmiin jäseneksi.

6.5 BitLocker

BitLocker on Microsoftin kehittämä kiintolevyn tai ulkoisen tallennusmedian salausohjelma. BitLocker on käytettävissä Windows Vista -käyttöjärjestelmästä lähtien ammattikäyttöön ja yrityksille suunnatuissa versioissa.

BitLockeria varten luotiin tarvittavat ryhmäkäytännöt, että BitLockeria käyttöönottaessa käyttäjälle on jo valmiiksi määritetty halutut asetukset kuten salausalgoritmin valinta jne. Ryhmäkäytännöillä määritettiin myös BitLockerin palautusavaimen tallennus Active Directoryyn tietokone objekteihin.

BitLockeria ei pakotettu käyttöön tietokoneille, vaan ryhmäkäytännöillä haluttiin asettaa yhteneväiset asetukset kaikille koneille, joille BitLocker tulevaisuudessa otetaan käyttöön.

6.6 Karsitut ominaisuudet

Suunnitteluvaiheessa harkittiin Process Genius Oy:lle käyttöön Windows Deployment Servicesiä (WDS) ja Microsoft Deployment Toolkitiä (MDT), mutta tarkemmin tarpeita kartoittaessa tultiin siihen tulokseen, etteivät nämä ominaisuudet olleet tässä vaiheessa tarpeelliset ja vaatisi enemmän työtä kuin mitä hyötyä ominaisuudet olisivat tuoneet. WDS on hyödyllisempi suuremmalla määrällä tietokoneita, joita tarvitsee asentaa ja tietokoneet ovat identtisempiä. WDS rooli on mahdollista ottaa käyttöön myöhemmin, mikäli nähdään tarpeelliseksi.

Windows Server Update Services (WSUS) käyttöönottoa harkittiin, mutta tämä karsittiin projektin alkuvaiheissa liian työläänä ja tarpeettomana tässä vaiheessa. Päivityksien keskitetyn hallinnan hyödyllisyyttä ei koettu tässä vaiheessa, kun käytössä olevat tietokoneet ja ohjelmistot eivät ole määritetty tiettyyn konfiguraatioon.

Active Directory Federation Serviceä ei myöskään otettu käyttöön tässä vaiheessa, koska se ei ollut tarvittava Azure Active Directoryn integrointiin. Azure Active Directory mahdollista Federation Servicen käyttämistä Azure-pilvipalvelussa ja näiden kahden vertailu ja testaaminen on oma projektinsa.

7 Azure Active Directoryn integrointi

Projektin yhtenä isona asiana oli tehdä integrointi paikallisen Active Directory ympäristön ja Azure-pilvipalvelussa olevan Azure Active Directoryn välillä. Process Genius Oy:llä on ollut jo pitkään käytössä Microsoftin Office 365 -pilvipalvelu jonka taustalla käyttöoikeudet on toteutettu Azure Active Directoryn avulla. Integrointi paikallisen Active Directoryn ja Azure Active Directoryn välillä haluttiin toteuttaa, että käyttäjien hallinta on helpompaa ja voidaan keskittää paremmin.

7.1 Azure Active Directory

Azure Active Directory (Azure AD) on Microsoftin tarjoama hakemistopalvelu pilvipalvelussa. [15] Azure AD toimii hakemistopalveluna ja käyttöoikeuksien hallintaan Microsoftin pilvipalveluissa kuten Office 365 ja Microsoft Azure -pilvipalvelussa.

Azure Active Directory ei tarjoa täysin samoja ominaisuuksia kuin perinteinen Active Directory, mm. ryhmäkäytännöt ovat paljon rajatummat Azure Active Directoryssä. Pienemmille yrityksille kuitenkin pelkkä Azure Active Directory voi olla houkutteleva palvelu, varsinkin jos yrityksellä on jo käytössä esimerkiksi Office 365. Azure Active Directory ei vaadi mitään paikallista palvelinta, mutta Microsoft

tarjoaa työkalut paikallisen Active Directoryn ja Azure Active Directoryn liittämiseksi.

7.2 Integroinnin suunnittelu

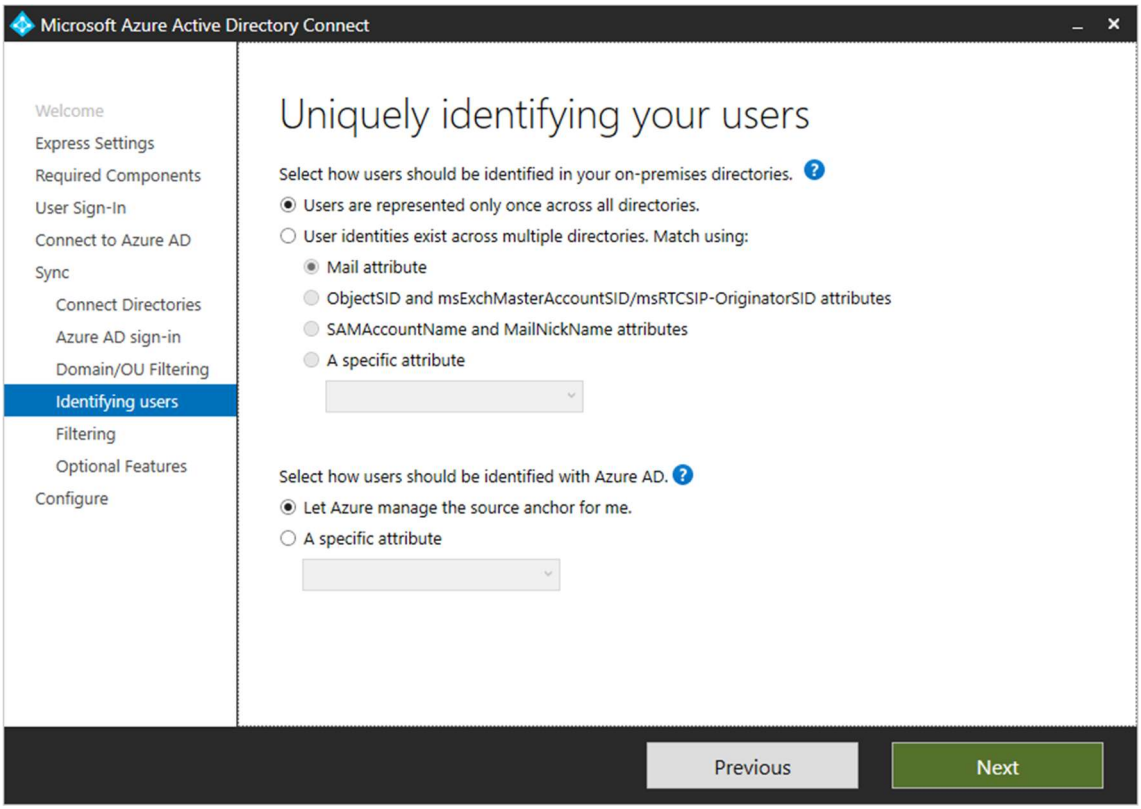
Process Geniuksella oli Azure Active Directory päivittäisessä käytössä Office 365:sen kautta, joten integrointi piti suunnitella ja testata erittäin huolellisesti, ettei katkoksia tai tiedonhäviämistä tapahdu integrointia tehdessä.

Tutustuin Azure Active Directoryn ja paikallisen Active Directoryn integrointiin Azure AD Connect -työkalulla, joka on Microsoftin suosittelema työkalu integrointiin. Vanhempia integrointityökaluja on Windows Azure Active Directory Sync (DirSync) ja Azure AD Sync, mutta ne eivät ole enää tuettuja. [16]

Azure AD Connectin tutustumista varten loin muusta testiympäristöstä erillisen testiympäristön ja tein uuden Azure Active Directory ilmaisversiona. Ilmaisversio mahdollisti integroinnin paikalliseen toimialueeseen ja tarvittavat ominaisuudet palvelun testaamista varten.

Palveluun tutustumisen jälkeen liitin palvelun testiympäristöön jossa testasin ja dokumentoin palvelun toimintaa erilaisissa skenaarioissa, kuten mikäli käyttäjä on jo olemassa Azure AD:ssa ja palvelu synkronoi käyttäjän paikallisesta Active Directorystä. Nämä skenaariot olivat tärkeitä miettiä ja testata etukäteen ennen palvelun liittämistä tuotantoympäristön Azure AD:hen, ettei käyttäjien tai käyttäjien tiedon häviämistä tapahdu.

Azure AD Connectilla ympäristöjen synkronointia varten tulee määrittää millä tavalla työkalu osaa tunnistaa Active Directoryn käyttäjät ja liittää ne Azure AD:hen. Yhden toimialuemetsän ja toimialueen tapauksessa tilanne on helppo, koska käyttäjät ovat vain yhdessä toimialuemetsässä (Kuva 17).



Kuva 17. Azure AD Connect

7.3 Integroinnin toteutus

Ympäristöjen integroinnin suunnittelun ja testaamisen jälkeen integrointi toteutettiin oikeassa ympäristössä. Paikalliseen Active Directoryyn ei ollut luotu käyttäjätunnuksia yrityksen työntekijöille, koska mikäli nämä olisi luotu valmiiksi olisi käyttäjien olemassa olevat Azure Active Directory käyttäjätunnuksen salasanat ylikirjoitettu.

Azure Active Directoryn liittäminen paikalliseen Active Directoryyn oli hyvin yksinkertainen prosessi Azure AD Connect -työkalulla. Integraatiota varten tarvitsi pääkäyttäjäoikeudet Azure Active Directory ympäristöön ja paikalliseen Active Directory ympäristöön, jotka haluttiin liittää keskenään. Integraatiota tehtäessä käytettiin ”Password hash synchronization” ja ”Password writeback” lisäasetuksia sekä sallittiin kertakirjautuminen (single sign-on). Näiden avulla paikallisen Active Directoryn käyttäjien salasanat ylikirjoitettiin Azure Active Directoryyn ja tämän jälkeen molemmat ympäristöt käyttivät samaa salasanaa. Mikäli käyttäjä vaihtaa salasanan Azure AD ympäristössä tai paikallisella Active Directoryyn liitetyllä tietokoneella synkronoituu se toiseenkin palveluun lähes välittömästi. Käyttäjien UPN-tunnuksen ollessa muotoa ”etunimi.sukunimi@processgenius.fi” eli sama kuin käyttäjien sähköpostin, on hyvin helppoa käyttäjille käyttää paikallisen Active Directory ympäristössä olevia koneita ja pilvipalveluita, koska molempiin voi kirjautua käyttäen samassa muodossa olevaa käyttäjätunnusta ja salasanaa.

Integroinnin jälkeen toteutettiin käyttäjien siirtäminen Active Directory ympäristöön luomalla heille käyttäjätunnus paikalliseen ympäristöön ja ohjeistamalla käyttäjä kirjautumaan paikalliseen Active Directory ympäristöön ja luomalla itselleen salasanan. Tämän jälkeen salasana synkronoitui Azure Active Directoryyn ja käyttäjä pystyi käyttämään normaalisti samaa käyttäjätunnusta ja salasanaa kummassakin ympäristössä.

Process Genius Oy:n tapauksessa synkronointi oli hyvin yksinkertainen, koska oli käytössä vain yksi paikallinen toimialuemetsä jossa yksi toimialue, eikä käytössä ollut paikallista sähköpostipalvelinta.

8 Kehitettävää

Ympäristö toteutettiin käyttämällä vain yhtä ohjauskonetta. Tämä oli tietoinen ratkaisu tässä vaiheessa, koska tulevaisuudessa yrityksen ympäristöön on tarkoitus lisätä toinen palvelin, johon luodaan myös toinen ohjauskone. Tällä voidaan parantaa ympäristön vikasietoisuutta ja varmistaa ympäristöön kirjautumisten onnistuminen, vaikka pääasiallinen ohjauskone vikaantuisi.

Projektin aiheen ulkopuolelle jäi varmuuskopioiden toteutus. Yritykselle toteutetaan erillinen varmuuskopiointiratkaisu tulevaisuudessa, joten tämän opinnäytetyön osalta varmuuskopiointiratkaisuun ei tarvinnut ottaa kantaa.

Tiedostopalvelimen rakenne on pyritty kuitenkin suunnittelemaan varmuuskopiointia ajatellen, että käyttäjien tiedostot sijaitsevat erillään projektitiedostoista. Lisäksi kaikissa tiedostonjaoissa on käytössä Shadow Copy ominaisuus, joka ei varsinaisesti ole varmuuskopiointia, mutta voi pelastaa tärkeitä tiedostoja, mikäli käyttäjä ne vahingossa poistaa.

9 Yhteenveto

Active Directory on hyvin laaja ja monimutkainen aihealue. Opinnäytetyössäni pyrin tutustumaan Active Directoryn mahdollisuuksiin ja luomaan toimivan ja hyvän pohjan pienyritykselle Active Directoryn käyttöä varten. Active Directoryn toteutus riippuu hyvin paljon yrityksen koosta ja tarpeista, mutta palvelun perusperiaate on joka tapauksessa kaikissa tapauksissa sama.

Process Genius Oy:lle toteutetun Active Directory ympäristön pohjalta on hyvä lähteä rakentamaan laajempaa ympäristöä lisäämällä tarvittavia palveluita sitä mukaan, kun yritykseen tarpeet kasvavat.

Lähteet

[1] B. Desmond, J. Richards, R. Allen ja A. G. Lowe-Norris, Active Directory: Designing, Deploying, and Running Active Directory 5th Edition, USA: O'Reilly Media, 2013.

[2] Microsoft Corporation, ”Microsoft Docs - Trust Relationships,” 7 Heinäkuu 2012. [Online]. Available: https://technet.microsoft.com/en-us/library/cc977993.aspx. [Haettu 20 Maaliskuu 2018].

[3] Microsoft Corporation, ”Microsoft TechNet - How Domain and Forest Trusts Work,” 2018. [Online]. Available: https://technet.microsoft.com/pt-pt/library/cc773178(v=ws.10).aspx. [Haettu 12 Helmikuu 2018].

[4] Microsoft Corporation, ”Microsoft Docs - DNS Support for Active Directory Technical Reference,” 19 Marraskuu 2014. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781627(v=ws.10). [Haettu 12 Helmikuu 2018].

[5] P. Geelen, ”Microsoft TechNet - Active Directory: Best Practices for Internal Domain and Network Names,” 24 April 2017. [Online]. Available: https://social.technet.microsoft.com/wiki/contents/articles/34981.active-directory-best-practices-for-internal-domain-and-network-names.aspx. [Haettu 12 February 2018].

[6] Microsoft Corporation, ”Microsoft Docs - Active Directory Domain Names,” 18 Heinäkuu 2012. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc977988(v=technet.10). [Haettu 12 Helmikuu 2018].

[7] Microsoft Corporation, ”Microsoft Docs - Best Practice Active Directory Design for Managing Windows Networks,” 12 Joulukuu 2009. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727085(v=technet.10). [Haettu 12 Helmikuu 2018].

[8] Microsoft Corporation, ”Microsoft Docs - Active Directory Certificate Services Overview,” 31 Elokuu 2016. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11). [Haettu 24 Helmikuu 2018].

[9] B. Svidergol ja R. Allen, Active Directory Cookbook 4th Edition, USA: O'Reilly Media, 2013.

[10] Microsoft Corporation, ”Microsoft Docs - AD DS Design Requirements,” 31 Toukokuu 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/ad-ds-design-requirements. [Haettu 24 Helmikuu 2018].

[11] Microsoft Corporation, ”Microsoft Docs - Active Directory Domain Services Overview,” 31 Elokuu 2016. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831484(v%3dws.11). [Haettu 24 Helmikuu 2018].

[12] Microsoft Corporation, ”Microsoft.com - Pricing and licensing for Windows Server 2016,” [Online]. Available: https://www.microsoft.com/fi-fi/cloud-platform/windows-server-pricing. [Haettu 7 Huhtikuu 2018].

[13] Microsoft Corporation, ”Microsoft Developer Network - Nested Groups,” [Online]. Available: https://msdn.microsoft.com/en-us/library/cc246068.aspx. [Haettu 8 Huhtikuu 2018].

[14] Microsoft Corporation, ”Microsoft Docs - Administration of Default Containers and OUs,” 6 Kesäkuu 2011. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc728418(v=ws.10). [Haettu 24 Maaliskuu 2018].

[15] Microsoft Corporation, ”Microsoft Azure - What is Azure Active Directory?,” 9 Huhtikuu 2018. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis. [Haettu 15 Huhtikuu 2018].

[16] Microsoft Corporation, ”Microsoft Azure - Integrate your on-premises directories with Azure Active Directory,” 19 Maaliskuu 2018. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect. [Haettu 15 Huhtikuu 2018].

[17] J. Talvivaara, ”Verkon nimi- ja hakemistopalvelut,” [Online]. Available: http://www2.amk.fi/mater/tietotekniikka/nimipalvelut/.