ADVANCED GROUP POLICY MANAGEMENT

Case Oulun Tietotekniikka

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittely

Visamäki, syksy 2014

Tiina Kela

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

VISAMÄKI
Tietojenkäsittely

Tekijä Tiina Kela **Vuosi** 2014

Työn nimi Advanced Group Policy Management, Case Oulun Tietotekniikka

TIIVISTELMÄ

Tämän opinnäytetyön toimeksiantajana oli liikelaitos Oulun Tietotekniikka, joka on osa Oulun kaupunkiorganisaatiota. Työn tavoitteena oli asentaa ryhmäkäytäntöjen hallintatyökalu Advanced Group Policy Management toimeksiantajan Active Directory Domain Services -tuotantoympäristöön ja löytää toiminnot sekä tavat, joilla ryhmäkäytäntöjen hallintaa saadaan tehostettua.

Työssä tutkittiin yleisellä tasolla Active Directoryn palveluita sekä rakennetta ja perehdyttiin ryhmäkäytäntöjen toimintaan sekä hallintaan. Lähdemateriaalina käytettiin aiheeseen liittyvää alan kirjallisuutta sekä www-sivustoja. Myös työn kirjoittajan omaa kokemusta ja osaamista hyödynnettiin opinnäytetyön teossa.

Teoriaosuuden tavoitteena oli selvittää lisäarvot, joita Advanced Group Policy Managementin liittäminen nykyiseen ryhmäkäytäntöhallintaan tuo. Työn käytännön osassa keskityttiin Advanced Group Policy Managementin asennuksen vaatimuksiin, asennukseen, toimintojen testaamiseen sekä työkalun käyttöönottoon tarkoituksena löytää ratkaisu ryhmäkäytäntöjen käsittelyn selkeyttämiseksi.

Opinnäytetyön tuloksena saatiin Oulun Tietotekniikan tuotantotoimialueelle apuväline keskitettyyn hallintaan käytettävien ryhmäkäytäntöjen käsittelyyn. Varsinainen käyttöönotto tapahtuu lähitulevaisuudessa. Suurissa ympäristöissä Advanced Group Policy Management on yksinkertaisuudestaan huolimatta varteenotettava apuväline ryhmäkäytäntöjen ylläpitoon. Sen avulla ylläpito-oikeuksien määrittely on selkeämpää ja itse ylläpito turvallisempaa, kuin perinteistä hallintatyökalua Group Policy Management Consolea käytettäessä.

Avainsanat aktiivihakemisto, keskitetty hallinta, ryhmäkäytännöt

Sivut 35 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Visamäki
Degree Programme in Business Information Technology

Author Tiina Kela **Year** 2014

Subject of Bachelor's thesis Advanced Group Policy Management, Case Oulun Tietotekniikka

ABSTRACT

This thesis was commissioned by the Oulu Information Technology which is part of the City of Oulu organization. The goal of this thesis was to install the Advanced Group Policy Management tool in the client's Active Directory Domain Services production domain and find the features and ways which improve management of group policies.

The services and structure of Active Directory were examined on a general level during the writing of this thesis. The operations and management of Group Policies were also studied. Literature related to the field and Internet pages were used as source material. Experience and knowledge of the writer were also utilized in writing this thesis.

The aim of the theoretical part was to find out added value of the Advanced Group Policy Management integration in the current Group Policy management. The practical section focused on the Advanced Group Policy Management installation requirements, the installation, operations, testing, and deployment of the tool in order to find a solution to clarify the processing of Group Policies.

As a result of this thesis Advanced Group Policy Management was installed in the domain of Oulu Information Technology. It was found to be of great assistance in managing Group Policies which are used in centralized management. The actual deployment will take place in the near future. In large environments Advanced Group Policy Management is a considerable add-on in the administration of Group Policies, in spite of its simplicity. Managing Group Policies by means of Advanced Group Policy Management is more explicit and safer than using the traditional management tool Group Policy Management Console.

Keywords Active Directory, centralized management, Group Policy

Pages 35 p.

AD - Active Directory. Kokoelma Windows-ympäristön palveluita.

AD CS - Active Directory Certificate Services. Active Directoryn varmennepalvelu.

AD DS - Active Directory Domain Services. Windows-toimialueen hakemistopalvelu ja käyttäjätietokanta. Active Directory -palveluiden ydin.

AD FS - Active Directory Federation Services. Active Directoryn kertakirjautumispalvelu.

AD LDS - Active Directory Lightweight Domain Services. Active Directoryn kevennetty hakemistopalvelu ilman autentikointivelvoitetta.

AD RMS - Active Directory Rights Management Service. Active Directoryn palvelu dokumenttien suojaamiseen.

Administrative Template - Ryhmäkäytännön ominaisuus. ADMX-mallitiedosto, jolla helpotetaan rekisteripohjaisten ryhmäkäytäntöjen hallintaa. Lisätään Group Policy Management Consoleen. Mahdollistaa esimerkiksi kolmannen osapuolen sovelluksen asetusten keskitetyn hallinnan.

AGPM - Advanced Group Policy Management. Liitännäinen Group Policy Management Console -työkaluun, jolla hallitaan ryhmäkäytäntöjä.

Class Store - Palvelimella sijaitseva tietovarasto, joka on olemassa sovellusten julkaisu- ja liittämistoimintoja tarjoavia sovelluksia, rajapintoja ja ohjelmointirajapintoja varten.

CSE - Client-Side Extension. Kohdetietokoneiden ryhmäkäytäntöjä määrittävä ryhmäkäytäntölaajennus, joka tulkitsee koneille levitettyä ryhmäkäytäntöä ja tekee ympäristöön tarvittavat muutokset.

DMZ - Demilitarized Zone. Verkkoalue, joka sijaitsee organisaation sisäverkon ja julkisen internetin välillä.

EFS - Windowsin ominaisuus tiedostojen salaamiseen.

FQDN - Fully Qualified Domain Name. Tietokoneen täydellinen toimialuenimi, esimerkiksi tietokone.toimialue.fi.

FRS - File Replication Service. Palvelu, jonka avulla ryhmäkäytäntöobjektit ja jaetut tiedostot jaellaan.

GP - Group Policy, ryhmäkäytäntö.

GPP - Group Policy Preferences. Ryhmäkäytäntölaajennus, jonka tuomat asetukset tallennetaan samoihin rekisteripolkuihin kuin käyttöjärjestelmän ja sovellusten asetukset.

GPC - Group Policy Container. Ryhmäkäytännön tietosäiliö.

GPMC - Group Policy Management Console. Ryhmäkäytäntöjen hallintatyökalu.

GPME - Group Policy Management Editor. Ryhmäkäytäntöjen muokkaustyökalu.

GPO - Group Policy Object. Ryhmäkäytäntöobjekti.

GUID - Globally Unique Identifer. Uniikki referenssinumero, jota käytetään tietojen tunnisteena tietokoneohjelmistoissa.

IPsec - IP Security Architecture. Tietoliikenneprotokolla, jolla turvataan inernet-yhtyeksiä.

Iso-tiedosto - CD- tai DVD-levyn näköistiedosto.

LDAP - Verkkoprotokolla hakemistopalveluille. Käytetään yleensä käyttäjien autentikointiin ja käyttöoikeuksien tarkastamiseen.

MDOP - Microsoft Desktop Optimization Pack. Microsoftin Software Assurance -asiakkaille saatavilla oleva kokoelma työkaluja Windows-ympäristöjen hallintaan ja ylläpitoon.

Microsoft Exchange - Microsoftin kehittämä sähköpostijärjestelmä.

MMC - Microsoft Management Console. Käyttöliittymä Windowsin MMC-laajennuksille.

Office 365 - Microsoftin sopimustuote. Yritysasiakkaille sopimus tarjoaa pilvipalveluina sähköpostin ja verkkoyhteisöpalveluita.

OU - Organization Unit, organisaatioyksikkö. Organisaatioyksiköillä muodostetaan toimialueelle loogisesti hallittava rakenne. Niihin jaotellaan toimialueeseen kuuluvia objekteja, kuten käyttäjiä ja koneita.

Pilvipalvelu - Internetin yli tarjottava palvelu. Yrityksillä myös omia pilviä, ns. privaattipilvi.

PowerShell - Windows-käyttöjärjestelmille kehitetty komentotulkki. Mahdollistaa järjestelmien hallinnan tekstipohjaisilla komennoilla.

RODC - Read-Only Domain Controller. Vain lukuoikeudet omaava toimialueen ohjauskone. Sisältää kaikki toimialueen sisältämät objektit ja attribuutit pois lukien käyttäjätunnusten salasanat.

S/MIME - Secure Multipurpose Internet Mail Extension. Sähköpostin salaus ja digitaalinen allekirjoitus varmennetta käyttämällä.

SMTP - Simple Mail Transfer Protocol. Sähköpostipalvelimien viestinvälitysprotokolla.

Snap-in - Lisäosa tai liitännäinen sovellukseen. Ei toimi ilman isäntäsovellusta.

Skripti - Komentosarja, jolla automatisoidaan tehtäviä.

TAPI - Telephony Application Programming Interface. Windowsin ohjelmointirajapinta, joka mahdollistaa puhelintoimintojen käyttämisen tietokoneen ja puhelimen välillä.

TSL - Transport Layer Security. Aiemmin SSL, Secure Sockets Layer. Tietoliikenteen suojausprotokolla.

VPN - Virtual Private Network. Tapa, jolla julkisen verkon yli voidaan yhdistää kaksi tai useampi verkko toisiinsa.

WMI-suodatin - Windows Management Instrumentation -suodatin. Sen avulla voidaan kerätä ryhmäkäytännöstä laite- ja käyttäjätietoja.

SISÄLLYS

1 JOHDANTO

Kuten monen muun yrityksen ja kunnan, myös Oulun Tietotekniikan hallinnoima Oulun kaupungin IT-ympäristö tukeutuu pitkälti Microsoftin tuotteisiin, kuten Windows-toimialueisiin sekä niiden Active Directory Domain Services -käyttäjätietokantoihin ja -hakemistopalveluihin. Ryhmäkäytäntöjen, eli Group Policyjen avulla voidaan Active Directory Domain Services -hakemistoihin kuuluvia objekteja hallita keskitetysti.

Ympäristöön kuuluu kaksi Windows-toimialuetta: koulut sekä hallinto. Tällä toimialuejaottelulla eriytetään selkeät vaatimuserot omaavat hallintokunnat toisistaan. Tämän opinnäytetyön tavoitteena on ottaa hallintopuolen toimialueelle testauksen kautta käyttöön Advanced Group Policy Management -työkalu, jolla toimialueen ryhmäkäytäntöjen hallintaan saadaan kaivattuja lisäominaisuuksia. Näihin ominaisuuksiin kuuluvat esimerkiksi version- ja muutoksenhallinta.

Työn sisältö koostuu sekä teoriaosuudesta että käytännön osuudesta. Aihe syntyi Oulun Tietotekniikan tarpeesta kehittää jatkuvasti laajentuvan IT-infrastruktuurin hallintaa ja prosesseja. Tällä hetkellä Oulun Tietotekniikka käyttää ryhmäkäytäntöjen hallintaan tähän tarkoitettua perustyökalua, Group Policy Management Consolea. Ympäristön kasvun sekä työntekijöiden määrän lisääntymisen myötä kyseinen työkalu ei enää tarjoa tarpeeksi kattavia ominaisuuksia sujuvaan ja turvalliseen ryhmäkäytäntöjen ylläpitoon.

Tämän opinnäytetyön tutkimuskysymyksiä ovat:

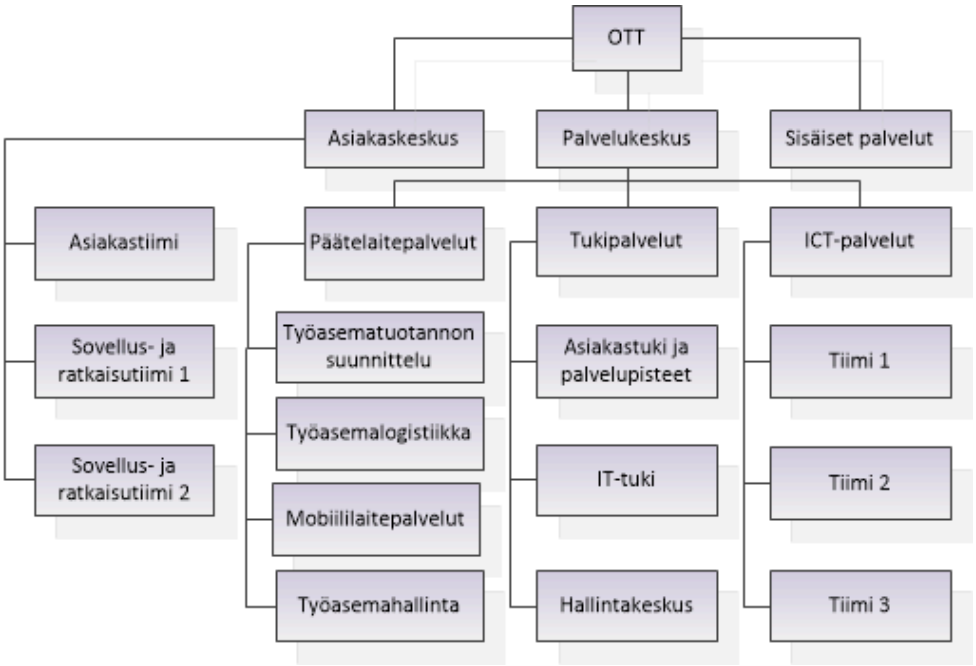
- Miten ryhmäkäytäntöjä ja niiden ylläpitoa hallitaan järkevästi?
- Mitä etuja Advanced Group Policy Management tarjoaa Group Policy Management Consoleen verrattuna?

Opinnäytetyö pohjautuu lähteisiin, joita ovat www-sivustot sekä alan kirjallisuus. Työn kirjoittamisessa hyödynnetään myös työn tekijän Windows-ympäristöjen parissa kertynyttä työkokemusta ja tietoa.

2 OULUN TIETOTEKNIIKKA

Oulun Tietotekniikka on Oulun kaupungin konserniin kuuluva liikelaitos, joka tuottaa Oulun kaupungille IT-palveluita. Oulun Tietotekniikka vastaa esimerkiksi työasemien, oheislaitteiden ja mobiililaitteiden hankinnasta, toimituksesta, ylläpidosta ja tukipalveluista. Näiden runkona on toimintavarman ICT-infrastruktuurin tuottaminen. Tuo infrastruktuuri pitää sisällään muun muassa tietoliikenneverkot, palvelimet, levyjärjestelmät ja palomuurin. Suurimmat asiakkaat ovat sivistys- ja kulttuuripalvelut sekä hyvinvointipalvelut. (Oulun Tietotekniikka n.d.a.)

Oulun Tietotekniikan historia yltää 1970-luvulle. Vuonna 1976 perustettiin Oulun kaupungin atk-osasto ja vuonna 1979 valmistui konesali. Työasemapalvelutuotanto käynnistyi 1985. Nykyinen liikelaitosmuotoinen toiminta alkoi vuonna 2000. Organisaatio koostuu asiakaskeskuksesta, palvelukeskuksesta ja sisäisistä palveluista. Asiakaskeskus vastaa tietojärjestelmien ja sovellusten ylläpidosta, versiopäivityksistä, kehittämisestä, integraatioista sekä niihin liittyvistä suunnittelu- ja käyttöönottoprojekteista. Palvelukeskus on jaettu kolmeen eri palvelulinjaan. Päätelaitepalveluiden vastuulla on esimerkiksi päätelaitteiden elinkaarenhallinta, asennusten automatisointi, päätelaitteiden vakiointi ryhmäkäytäntöjen ja jakelujen avulla sekä laitteiden toimitukset asiakkaille. Tukipalveluiden päätehtävänä on hoitaa asiakkaiden vikatilanteet ja palvelupyynnöt. ICT-palvelut tuottavat tietoturvallisen ja toimintavarman ICT-infrastruktuurin. Kuvio 1 kuvaa Oulun Tietotekniikan organisaatiorakenteen. (Oulun Tietotekniikka n.d.)



Kuvio 1. Oulun Tietotekniikan organisaatiorakenne.

Päätelaitteita Oulun Tietotekniikan IT-ympäristössä on lähes 17 000. Palvelimia löytyy yli 450, ja niiden virtualisointiaste on 85 %. Joulukuussa 2013 hallinnon toimialueella oli yli 12 000 käyttäjätunnusta sekä lisäksi koulujen toimialueella noin 25 800 käyttäjätunnusta. Vuonna 2013 Oulun

Tietotekniikka käsitteli 58 800 palvelupyyntöä joista 50 % ratkaistiin 0,42 päivässä. Kuva 1 esittää Oulun Tietotekniikan toiminnan keskeisimmän tunnusluvut. (Oulun Tietotekniikka 2014.)

	2012	2013
Päätelaitteiden määrä	15 972	16 540
Runkoverkon saatavuus	99,6	99,81
Palvelupyyntöjen määrä	53 011	58 800
Palvelimia (kuvaa sovellusten määrän kehittymistä)	323	452
Palvelinten virtuaalisointiaste %	83	85
Liikevaihto / henkilö	154 000	162 000
Sähköisen asioinnin osuus yhteydenotoista %	46	49
Keskimääräinen aika jona 80% palvelupyynnöistä ratkaistu (pv)	4,33	3,81
Keskimääräinen aika jona 50% palvelupyynnöistä ratkaistu (pv)	0,48	0,42

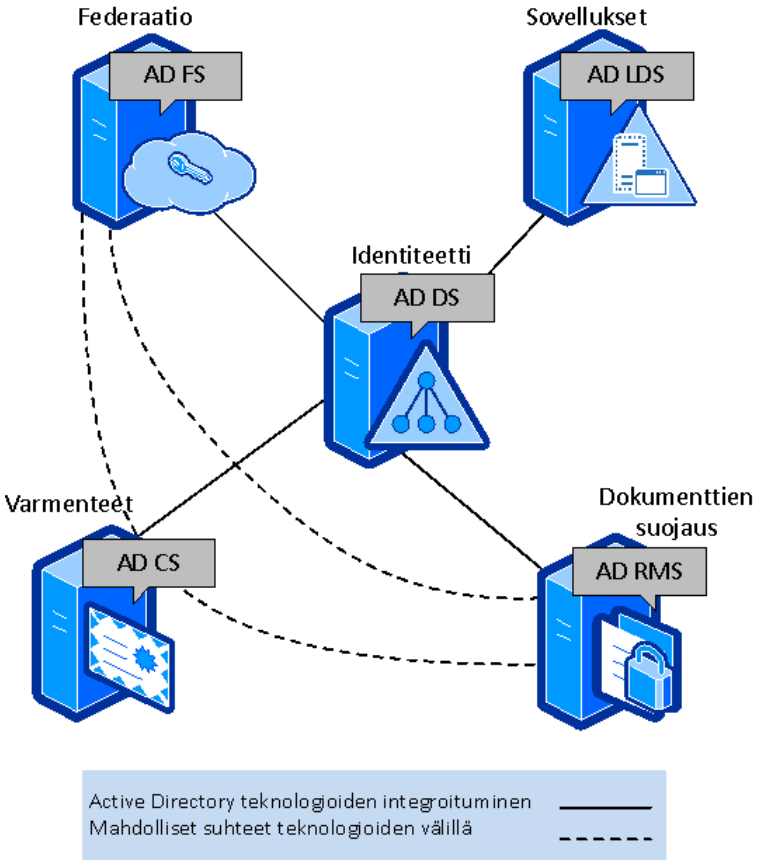
Kuva 1. Oulun Tietotekniikan toimintaa kuvaavat tunnusluvut. (Oulun Tietotekniikka 2014.)

3 ACTIVE DIRECTORY

Ensimmäisen kerran Active Directory, eli tuttavallisemmin AD, julkaistiin Windows 2000 Server -käyttöjärjestelmän mukana. Windows 2008 -versio toi muutoksen, sillä AD muutettiin sateenvarjotermiksi ja sen alle tuotiin lisää tekniikoita. Nykyisellään AD on kokoelma teknologioita, joilla hallitaan Windows-ympäristöjä. (Seitsonen 2014.)

AD-teknologioiden ja niiden sisältämien roolien asennusmahdollisuus riippuvat Windows-palvelinkäyttöjärjestelmän versiosta. Käyttöjärjestelmän Windows Server 2012 versiot Datacenter sekä Standard sisältävät kaikki AD:n ominaisuudet. Versiot Foundation ja Essentials sisältävät AD-rooleja vajain ominaisuuksin. Käyttöjärjestelmän Windows Server 2008 kohdalla versiot Enterprise ja Datacenter sisältävät AD:n kokonaisuudessaan, versiot Standard ja Foundation osittaiset AD:n ominaisuudet, kun puolestaan versiot Itanium ja Web eivät sisällä lainkaan AD:n tekniikoita.

AD muodostuu viidestä roolista. Kaiken keskustana on Active Directory Domain Services (AD DS), johon linkittyy Active Directory Certificate Services (AD CS), Active Directory Federation Services (AD FS), Active Directory Lightweight Directory Services (AD LDS) sekä Active Directory Rights Management Services (AD RMS). Kuva 2 kertoo AD-komponenttien suhteesta toisiinsa. (Holme, Ruest, D. & Ruest, N. 2008, 5.)



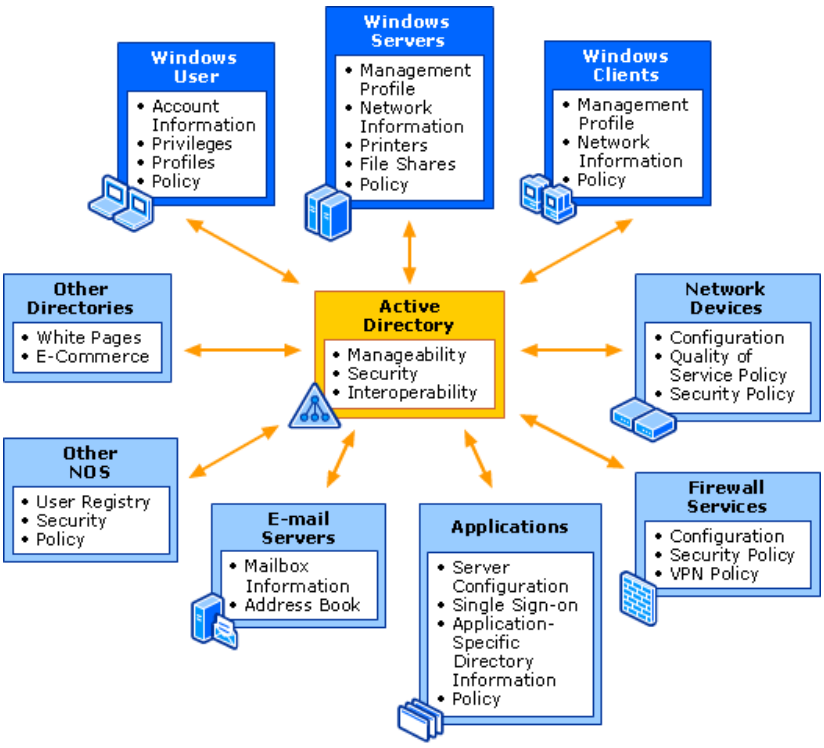
Kuva 2. Active Directoryyn kuuluvat teknologiat. (Mukaillen Holme ym. 2008, 5.)

3.1 Active Directory Domain Services

Active Directory Domain Services (AD DS), joka tunnettiin ennen Windows Server 2008 -versiota nimellä Active Directory (AD), on Microsoftin kehittämä työkalu Windows-toimialueiden hakemistopalveluksi. Hakemistopalvelu tarjoaa keskitetyn paikan tietojen tallentamiseen hajautetussa ympäristössä. Tällaista tietoa ovat esimerkiksi käyttäjät, verkkolaitteet ja palvelut. Hakemistopalvelu tarjoaa myös työkalut, jotka tuovat nämä tiedot käyttäjien, työasemien sekä sovellusten saataville. (Seitsonen 2014; Microsoft n.d.a.)

AD DS:ä voisi kuvailla erityiskäyttöiseksi tietokannaksi. Se on suunniteltu käsittelemään suuret määrät luku- ja hakuoperaatioita sekä pienempää määrää muutoksia ja päivityksiä. Sen data on hierarkkista, replikoitua ja laajennettavissa. (Microsoft n.d.a)

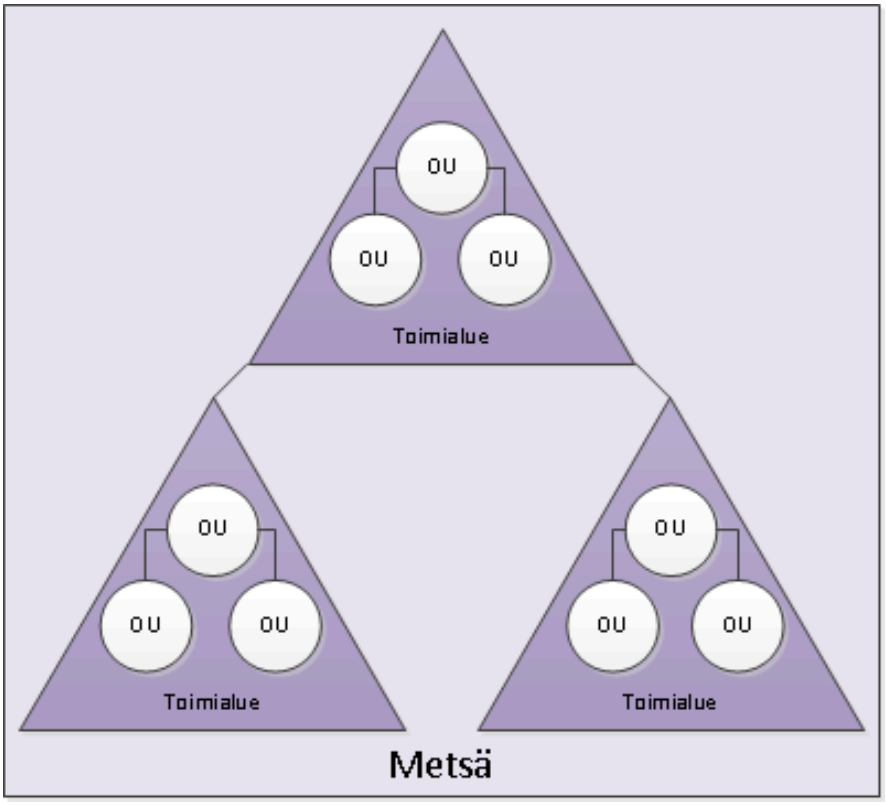
AD DS on käytössä yleensä jostain edellä mainituista syistä. Sisäisenä hakemistona: Käytetään käyttäjä- ja resurssitietojen julkaisuun yrityksen sisällä. Yrityksen työntekijöillä voi olla pääsy sisäiseen hakemistoon ulkoverkosta esimerkiksi VPN-yhteyden avulla, mutta ulkopuolisilla henkilöillä ei ole siihen pääsyä. Ulkoisena hakemistona: Nämä hakemistot sijaitsevat yleensä DMZ-verkkoalueella, eli yrityksen sisäisen ja julkisen verkon välissä. Ulkoisiin hakemistoihin tallennetaan usein tietoa asiakkaista ja yhteistyökumppaneista, jotka käyttävät ulkoisia sovelluksia ja palveluita. Sovellushakemistona (Application directory): Tallentaa tietoa, joka on relevanttia sovelluksille. Esimerkiksi TAPI-tiedot (Telephony Application Programming Interface) tallennetaan kyseiseen hakemistoon. Kuva 3 esittelee AD DS:n käyttötapoja. (Microsoft n.d.f.)



Kuva 3. Active Directory Domain Services Windows -palvelinverkossa. (Microsoft n.d.f.)

3.2 Active Directory Domain Services -rakenne

AD DS -metsään kuuluu yksi tai useampi AD DS -toimialue. Ensimmäisellä metsään asennetulla toimialueella, eli juuritoimialueella (forest root domain), on muihin metsän toimialueisiin verrattuna laajemmat oikeudet sekä tärkeämpi merkitys. Jokainen AD DS -toimialueen ohjauskone voi olla vain yhden toimialueen jäsen. Saman toimialueen kaikki ohjauskoneet, lukuun ottamatta Read-Only Domain Controllereita (RODC), sisältävät saman informaation. RODC on ohjauskone, joka ainoastaan lukee toimialueen tietoja. Se on kehitetty pääasiallisesti parantamaan sivutoimipisteiden tietoturvaa. Samaan metsään, mutta eri toimialueeseen kuuluvat ohjauskoneet jakavat saman tiedot konfiguraation sekä kaavan (schema) osalta. Kuviossa 2 nähdään esimerkki AD DS:n rakennekaaviosta. (Kivimäki 2005, 51; Holme ym. 2008, 374–375; Microsoft m.d.c.)



Kuvio 2. AD DS rakenne. (Mukaillen m.d.b.)

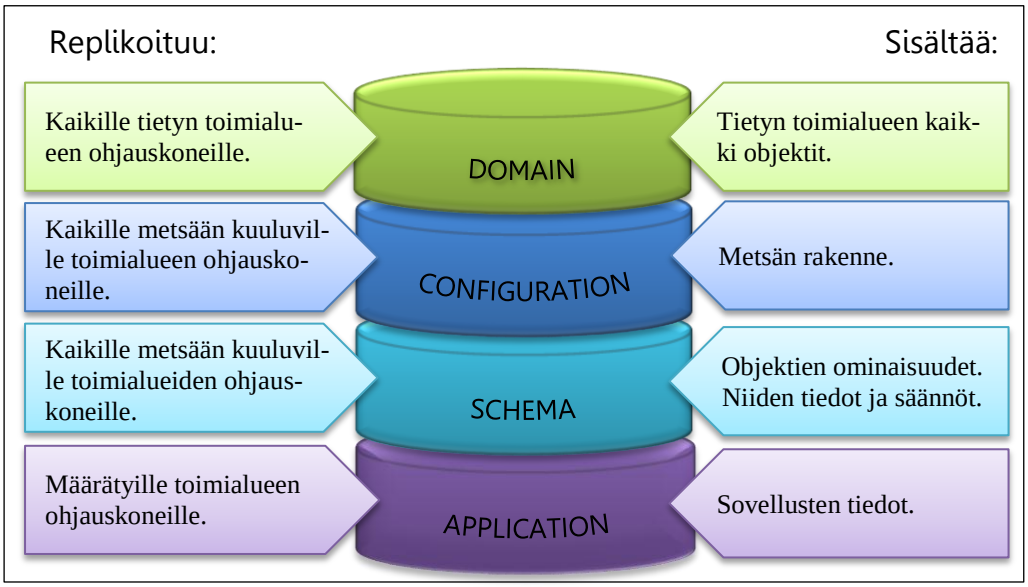
Kun toimialueet esitetään yleensä loogisen tai hallinnollisen rakenteen mukaan, toimipaikat (site) puolestaan kuvastavat verkon fyysistä rakennetta. Toisin sanoen ne jaotellaan usein maantieteellisen sijainnin mukaan ja niiden rajoiksi on asetettu sama verkkoavaruus, kuin lähiverkolla (LAN) tai laajaverkolla (WAN). Tällä rakenteella voidaan esimerkiksi nopeuttaa käyttäjän kirjautumista työasemalle. Kun kirjautumispyyntö annetaan, työasema pyrkii löytämään toimialueen ohjauskoneen saman toimipaikan sisältä. Yksi toimipaikka voi sisältää useita toimialueita, kun myös toimialue voi sisältää useita toimipaikkoja. (Kivimäki 2005, 10.)

Organisaatioyksiköt (OU, Organization Unit) ovat näkyvä osa toimialueiden rakennetta. Niillä pyritään muodostamaan toimialueelle organisaation

omaa rakennetta peilaava kokonaisuus. Organisaatioyksiköiden avulla voidaan rajata käyttöoikeuksia ja niihin voidaan linkittää ryhmäkäytäntöjä. (Kivimäki 2005, 10.)

3.3 Active Directory Domain Services -tietokanta

AD DS:n tietokanta on tallennettu tiedostoon Ntds.dit. Käytännössä tietokanta on kuitenkin jaettu kuviossa 3 näkyviin osioihin (Directory Partitions), jotta saavutettaisiin mahdollisimman toimiva replikointi sekä tehokas hallinta. Domain Partition sisältää tiedot toimialueen objekteista ja se replikoidaan pelkästään oman toimialueensa ohjauskoneille. Jokaista toimialuetta kohti on siis oma Domain Partition. Configuration Partition puolestaan tallettaa tiedot koko metsän rakenteesta, kuten esimerkiksi mitä toimialueita ja toimipaikkoja on olemassa, sekä mitkä palvelut metsässä on olemassa. Tämä osio replikoidaan kaikille metsässä sijaitseville toimialueen ohjauskoneille. Myös Schema Partition tallennetaan kaikille ohjauskoneille ja Configuration Partitionin tapaan niitä on metsässä vain yksi. Schema Partition sisältää tiedot jokaisesta objektista ja ominaisuudesta, joita hakemistoon voidaan luoda sekä säännöt niiden luomiseen ja muokkaamiseen. Application Partition sisältää sovellusten tallettamaa tietoa. Se voi sisältää mitä tahansa objekteja, paitsi suojausasetuksia. Sovellukset määrittävät itse mitä tietoa osiossa säilytetään ja millä tavalla se tapahtuu. Application Partition voidaan määrittää replikoitumaan mille tahansa metsään kuuluville toimialueen ohjauskoneille. (Microsoft n.d.c.)



Kuvio 3. AD DS Directory Partition.

3.4 Active Directory Domain Services -yleinen luettelo

Yleinen luettelo (Global Catalog) on kokoelma kaikista AD DS -metsän objekteista. Yleinen luettelo sijaitsee toimialueen ohjauskoneella. Kyseinen ohjauskone tallentaa täyden kopion oman toimialueensa objekteista.

Muiden, samaan metsään kuuluvien toimialueiden objekteista, se säilöö osittaisen lukutilassa olevan kopion. Mitä osittaisia tietoja tallennetaan, määritellään kaavassa sekä niiden tietojen perusteella, mitä yleisimmin käytetään suoritettaessa hakuja luetteloon. Yleinen luettelo luodaan automaattisesti uuden metsän ensimmäiselle toimialueen ohjauskoneelle. Seuraaville ohjauskoneille yleinen luettelo voidaan halutessa lisätä. Ominaisuus voidaan myös poistaa tarvittaessa. Yleistä luetteloa tarvitaan esimerkiksi silloin, kun suoritetaan hakutoiminto, jossa kohteena on koko AD DS -metsä. Muita yleisiä käyttötapauksia ovat Universal Group -ryhmään kuuluvien käyttäjien kirjautuminen sekä Microsoft Exchangen osoitekirjahaut. (Microsoft n.d.g.)

3.5 Muut Active Directory -roolit

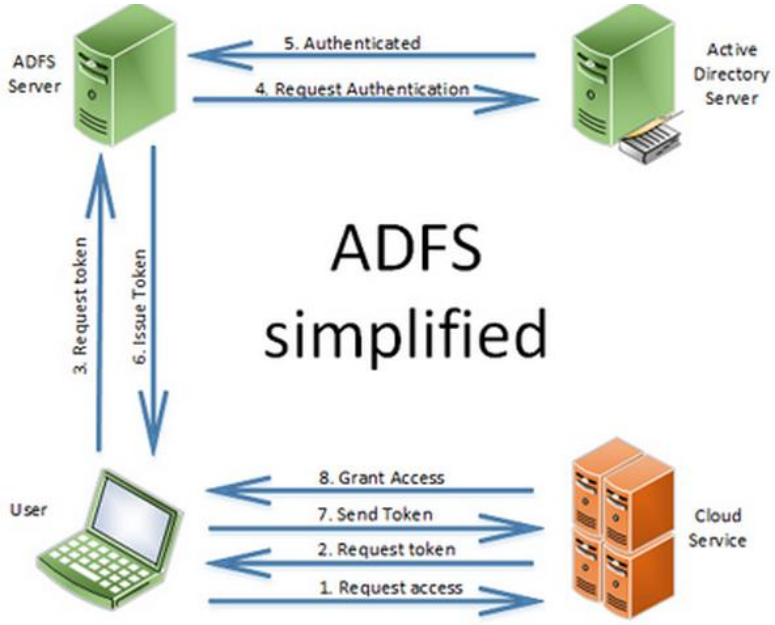
Active Directory Certificate Services (AD CS) tarjoaa työkalut sertifikaattien, eli varmenteiden hallintaan. Varmenteiden avulla voidaan mahdollistaa tietoturvallinen viestintä järjestelmien ja palveluiden kesken. AD CS:n tukemiin standardeihin ja protokolliin kuuluu esimerkiksi Secure/Multipurpose Internet Mail Extensions (S/MIME), suojatut langattomat verkot, virtuaaliset erillisverkot (Virtual Private Network, VPN), IP Security Architecture (IPsec), Encrypting File System (EFS), älykorttikirjautuminen, digitaaliset allekirjoitukset sekä Transport Layer Security (TSL, entinen Secure Sockets Layer eli SSL). AD CS:n komponentit voidaan asentaa yhdelle palvelimelle, mutta komponenttien jaottelu omille palvelimilleen on hyvin yleistä. Taulukossa 1 on eritelty AD CS:n komponentit ja niiden tehtävät. (Holme ym. 2008, 6, 730–732.)

Taulukko 1. AD CS:n komponentit.

Komponentti	Tehtävä
CA Web enrollment	Yhdistää käyttäjät sertifikaatin myöntäjään www-selaimen avulla.
Certification authorities (CAs)	Sertifikaattien hallinnointi ja myöntäminen.
Certificate Enrollment Policy Web Service	Sallii tietokoneiden ja käyttäjien noutaa tietoa siitä, millaisia sertifikaatteja voidaan anoa ja mitkä sertifikaattien hallinnoijat voivat niitä myöntää.
Certificate Enrollment Web Service	Mahdollistaa tietokoneiden ja käyttäjien rekisteröidä sertifikaatteja.
Network Device Enrollment Service	Sallii toimialueeseen kuulumattomien verkkolaitteiden noutaa sertifikaatteja.
Online Responder	Vastaa kyselyihin, jotka koskevat sertifikaattien tilaa.

Active Directory Federation Services (AD FS) on palvelu, joka mahdollistaa turvatun jakamisen identiteettitiedoille luotettujen tahojen välillä. Tätä luottosuhdetta voidaan kutsua federaatioksi. Kun käyttäjän täytyy päästä

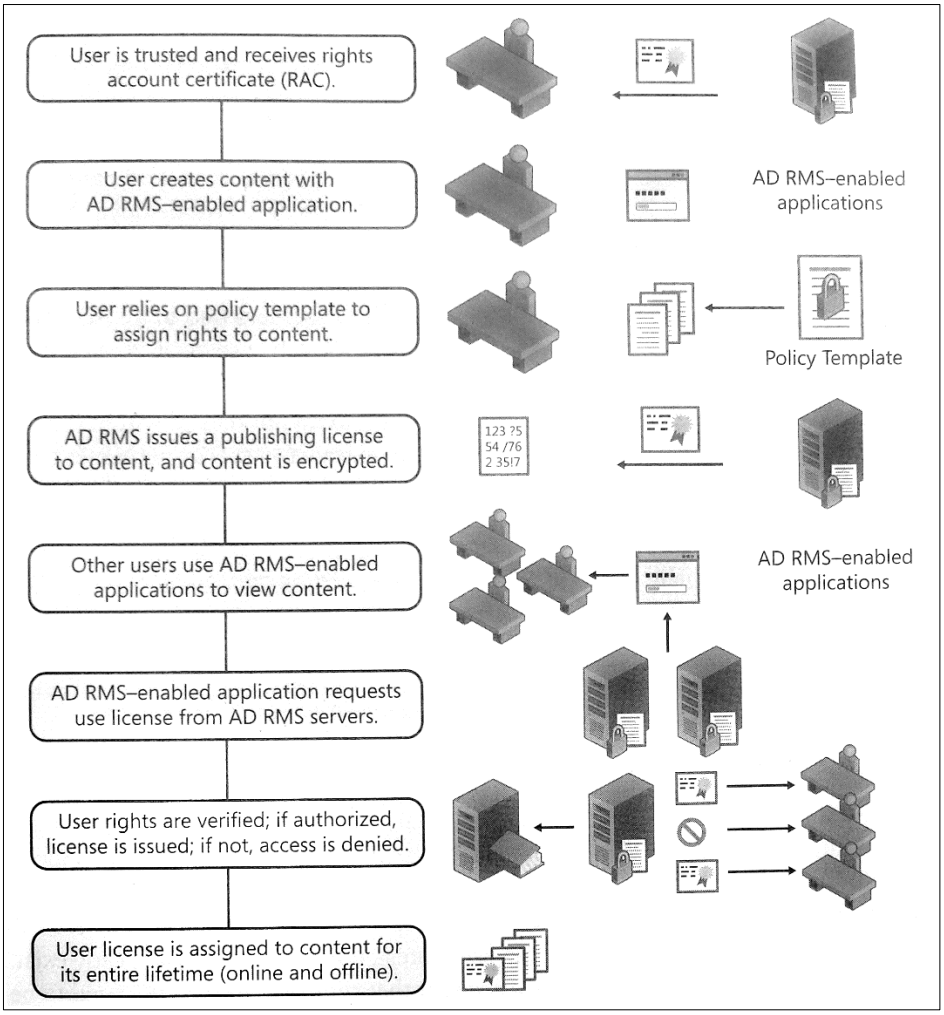
federaatiokumppanin tarjoamaan selainpohjaiseen sovellukseen, käyttäjän oma organisaatio on vastuussa käyttäjän autentikoinnista ja sovelluksen vaatimien identiteettitietojen luovuttamisesta kumppanille. Kaikki AD FS -palveluiden välinen liikenne on suojattua ja salattua. Suhteellisen tunnettu esimerkki on Microsoftin tarjoama palvelu Office 365. Kuvassa 4 on esitetty AD FS:n toimintaperiaate yksinkertaistettuna pilvipalvelussa. (Holme ym. 2008, 7, 825, 827–828.)



Kuva 4. AD FS:n yksinkertaistettu toimintaperiaate pilvipalvelussa. (AgileIT n.d.a.)

Active Directory Lightweight Directory Services (AD LDS) on LDAP-hakemistopalvelu. Se tarjoaa joustavan tuen hakemistopohjaisille sovelluksille, kuitenkin ilman AD DS:n vaatimia riippuvuuksia. AD LDS sisältää paljon samoja toimintoja, kuin AD DS, mutta se ei vaadi toimialueiden tai toimialueiden ohjauskoneiden käyttöönottoa. Yhdessä koneessa voi ajaa useita AD LDS -instansseja, joilla on itsenäisesti hallitut kaavat. AD LDS ei vaadi tai ole riippuvainen AD DS -palvelusta, mutta ympäristöissä, joissa AD DS on käytössä, AD LDS voi käyttää AD DS:ä autentikoitumiseen Windowsin suojausasetuksia (Security Principals) käyttäen. (Microsoft 2012.)

Active Directory Rights Management Services (AD RMS) on rooli, jonka avulla voidaan suojata dokumentteja käyttämällä sisältöoikeuksien hallintaa (IRM, Information Rights Management). Näiden tekniikoiden avulla käyttäjät ja ylläpitäjät voivat määritellä oikeuksia tiedostoihinsa sisältöoikeuksien käytäntöjen kautta. Kun dokumentin suojausoikeudet ovat käytössä, ne ovat voimassa aina siellä, missä dokumentti on, sillä oikeudet sijaitsevat tiedostossa itsessään. Käyttäjälle AD RMS näkyy sovelluksena, jolla hän pystyy suojaamaan haluamansa dokumentit. Kyseinen sovellus tulee Windows käyttöjärjestelmien mukana automaattisesti. Kuvassa 5 on esitetty esimerkkitilanne dokumentin julkaisusta AD RMS:n avulla. (Holme ym. 2008, 7, 788–790.)



Kuva 5. Esimerkki dokumentin julkaisusta AD RMS:n avulla. (Holme ym. 2008, 791.)

4 RYHMÄKÄYTÄNNÖT

Windows 2000 -käyttöjärjestelmä toi mukanaan ryhmäkäytännöt. Ne ovat objekteja (Group Policy Object, GPO), joihin tallennetaan käyttäjien ja työasemien asetuksia. Nuo objektit voidaan linkittää AD DS:ssä valittuihin objekteihin, kuten toimialueisiin, organisaatioyksiköihin, toimipaikkoihin tai ryhmiin. Keskitetysti hallittavien työasemien tulee kuulua toimialueeseen, sekä käyttäjätunnusten oltava toimialuetunnuksia.

Ryhmäkäytäntöjä voidaan hyödyntää myös yksittäisillä Windows-työasemilla paikallista ryhmäkäytäntöeditoria (Local Group Policy, LGP) käyttämällä. Mikäli toimialueeseen kuuluvalle koneelle määritellään paikallisia ryhmäkäytäntöjä, toimialueen ryhmäkäytännöt ohittavat ne.

Kuten mainittiin, ryhmäkäytännöt on jaettu kahteen eri joukkoon, jotka ovat käyttäjä- ja tietokoneasetukset. Tietokoneasetukset käsitellään silloin, kun käyttöjärjestelmä käynnistyy. Käyttäjäasetukset tulevat puolestaan voimaan, kun käyttäjä kirjautuu tietokoneelle. Tämän jälkeen, kun asetukset on kertaalleen hyväksytty, ne päivitetään automaattisesti määrätyin väliajoin. Oletusasetuksilla toimialueiden ohjauskoneiden ryhmäkäytännöt päivitetään viiden minuutin välein. Työasemien sekä palvelimien ryhmäkäytännöt päivitetään puolestaan 90 minuutin välein. Käytännössä aikaväli voi kasvaa 120 minuuttiin. Tämä tapahtuu, jotta vältytään ohjauskoneiden liialliselta kuormittamiselta useilla yhtäaikaisilla päivityspyynnöillä. Ryhmäkäytäntöjen päivitysväli on kuitenkin maksimissaan 16 tuntia, jolloin ne päivitetään vaikka muutoksia ryhmäkäytäntöasetuksiin ei ole tehty. (Mar-Elia, Melber & Stanek 2005, 5.)

Windows Server 2008 -käyttöjärjestelmän mukana Microsoft esitteli Group Policy Preferences -ominaisuudet. Niiden pääeroavaisuus perinetisin ryhmäkäytäntöihin verrattuna on se, että asetukset ovat muokattavissa kohdekoneilla jälkeenpäin. Group Policy Preferencejä ei kirjoiteta ryhmäkäytäntörekistereihin, vaan ne tallentuvat samoihin rekisteriosioihin, mihin käyttöjärjestelmä- ja sovellusasetukset tallentuvat. Niiden avulla voidaan jakaa esimerkiksi jaettujen verkkolevyjen asetukset. Taulukko 2 kuvaa Group Policy Preferences -asetusten ja ryhmäkäytäntöjen eroavaisuudet. (Honeycutt 2007.)

Taulukko 2. Group Policy Preferences -asetusten ja ryhmäkäytäntöasetusten eroavaisuudet. (Honeycutt 2007.)

	Group Policy Preferences	Group Policy Settings
Enforcement	• Preferences are not enforced • User interface is not disabled • Can be refreshed or applied once	• Settings are enforced • User interface is disabled • Settings are refreshed
Flexibility	• Easily create preference items for registry settings, files, and so on • Import individual registry settings or entire registry branches from a local or a remote computer	• Adding policy settings requires application support and creating administrative templates • Cannot create policy settings to manage files, folders, and so on
Local Policy	• Not available in local Group Policy	• Available in local Group Policy
Awareness	• Supports non-Group Policy-aware applications	• Requires Group Policy-aware applications
Storage	• Original settings are overwritten • Removing the preference item does not restore the original setting	• Original settings are not changed • Stored in registry Policy branches • Removing the policy setting restores the original settings
Targeting and Filtering	• Targeting is granular, with a user interface for each type of targeting item • Supports targeting at the individual preference item level	• Filtering is based on Windows Management Instrumentation (WMI) and requires writing WMI queries • Supports filtering at a GPO level
User Interface	• Provides a familiar, easy-to-use interface for configuring most settings	• Provides an alternative user interface for most policy settings

4.1 Ryhmäkäytöobjektin rakenne

Ryhmäkäytäntöobjekti (GPO), on tallennuspaikka ryhmäkäytäntöasetuksille. Se koostuu kahdesta komponentista: ryhmäkäytäntöjen säiliö (Group Policy Container, GPC) ja ryhmäkäytäntöjen malli (Group Policy Template, GPT).

Ryhmäkäytäntöjen säiliö löytyy AD DS -toimialueen System-säiliöstä. Sillä ei ole nimeä, vaan yksilöllinen GUID (Globally Unique Identifier). Kunkin ryhmäkäytäntöobjektin ryhmäkäytäntöjen säiliöstä löytyy esimerkiksi versiotieto, täydellinen toimialuenimi (FQDN), vastaavan ryhmäkäytäntöjen mallin polku, asiakkaan ryhmäkäytäntölaajennukset (CSE:t), sovelluksia koskevat luokkavarastotiedot (Class Store) sekä tilatiedot, jotka kertovat, onko ryhmäkäytäntöobjekti käytössä vai poistettu käytöstä. (Microsoft 2010, 17; Kivimäki 2005, 536.)

Ryhmäkäytäntöjen malli tallennetaan kansioon SYSVOL\Policies, eli mallin polku on %systemroot%\SYSVOL\domain\Policies\policyGUID, jossa domain on toimialueen nimi ja policyGUID ryhmäkäytännön GUID. Tämä sama kansio löytyy jokaiselta kyseisen toimialueen ohjauskoneelta, joille mallin tiedot replikoituvat File Replication Servicen (FRS) välityksellä. Ryhmäkäytäntöjen malliin tallentuu mallin versiotieto, Administrative Templatet, ryhmäkäytännön skriptit sekä käyttäjä- ja työasemaasetukset. (Kivimäki 2005, 536–537.)

4.2 Ryhmäkäytäntöjen suunnittelu

Jo AD DS:n rakennetta suunniteltaessa on ryhmäkäytännöt otettava huomioon. Yleensä organisaatiorakenteen mukainen AD DS:n rakenne on hyvä ratkaisu myös ryhmäkäytäntöjen kannalta. Organisaatioyksiköiden alla on järkevää eriyttää käyttäjätunnukset ja laitteet toisistaan, jolloin myös ryhmäkäytäntöjen kohdistaminen tulee loogisemmaksi. Ryhmäkäytäntöjen määrä tulisi pitää kohtuullisena, joten mikäli mahdollista, on järkevää yhdistää ryhmäkäytäntöobjekteja isommiksi kokonaisuuksiksi. Mikäli ympäristössä on olemassa suuria tai monimutkaisia ryhmäkäytäntöobjekteja, jotka usein vaativat muutoksia, on niille suositeltavaa luoda omat objektit. (Microsoft 2009.)

Suunnitteluvaiheessa kannattaa käydä läpi ryhmäkäytäntöjen jaottelua, kuten mitkä asetukset ovat samat kaikille toimialueen käyttäjille tai koneille. Jokaisen ryhmäkäytännön tarve on pohdittava tarkoin, kuten myös kohde niiden linkittämiselle. Ryhmäkäytäntöjen Default Domain Policy sekä Default Domain Controller Policy muokkaamista tulee välttää. Niiden muokkaamisen sijaan suositellaan uuden ryhmäkäytännön luomista toimialuetasolle ja määritellä se yliajamaan toimialueen oletuskäytännöt. On hyvin yleistä, että toimialueeseen kuuluu kahden tai jopa kolmen käyttöjärjestelmätason työasemia sekä palvelimia. Esimerkiksi Windows Server 2012 sisältää sellaisia ryhmäkäytäntöasetuksia, joita Windows Server 2008 ei omaa. Näissä ympäristöissä tulisi ryhmäkäytäntöjä hallita uusimmalla palvelinversiolla. Vanhemmat käyttöjärjestelmät yksinkertaisesti jättävät ne ryhmäkäytäntöasetukset huomioimatta, joita eivät tue. Toinen vaihtoehto on lisätä uudemman käyttöjärjestelmän Administrative Template vanhaan käyttöjärjestelmään. (Microsoft 2009.)

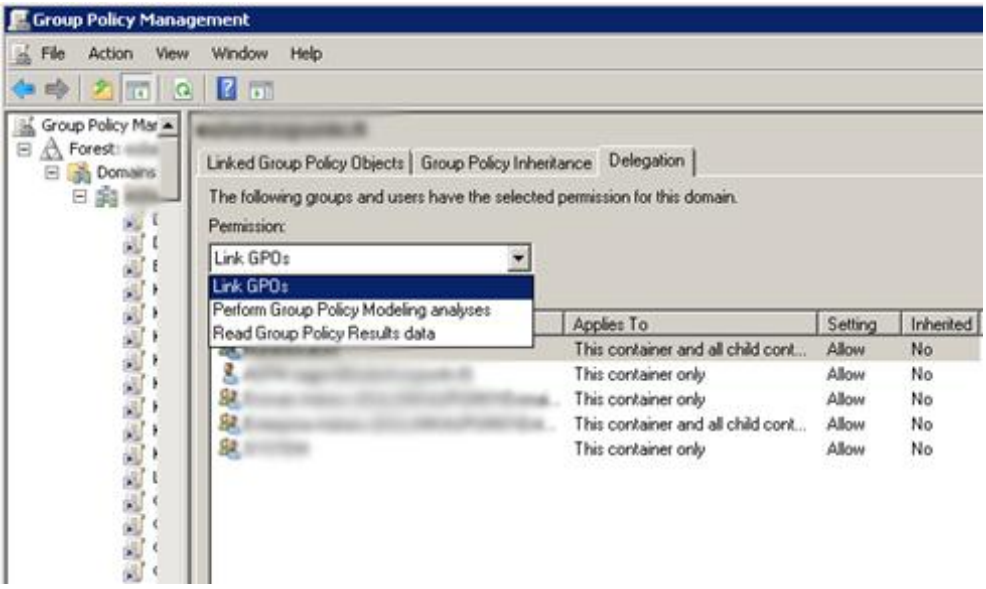
5 RYHMÄKÄYTÄNTÖJEN HALLINTATYÖKALUT

Ryhmäkäytäntöjen hallintaan käytetään yleensä Group Policy Management Consolea. Suurempien ympäristöjen avuksi on kehitetty Advanced Group Policy Management. Tässä luvussa keskitytään niiden ominaisuuksiin sekä eroavaisuuksiin.

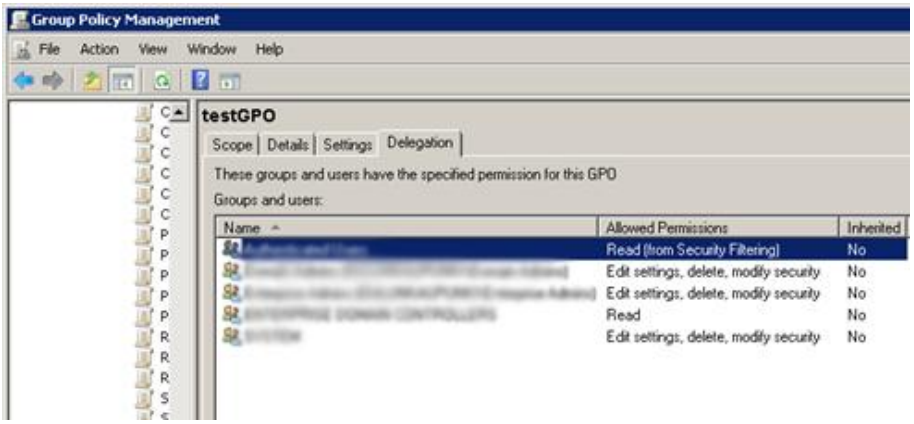
5.1 Group Policy Management Console

Group Policy Management Console (GPMC) on perustyökalu ryhmäkäytäntöjen hallintaan. Se on Microsoft Management Consolen (MMC) liitännäinen (snap-in). Windows palvelinkäyttöjärjestelmäversioiden Windows Server 2008 ja Windows Server 2012 mukana GPMC tulee automaattisesti, mutta ominaisuus pitää aktivoida käyttöön. Windows-työasemakäyttöjärjestelmille GPMC on saatavilla Remote Server Administration Tools -työkalupaketin (RSAT) mukana. RSAT mahdollistaa Windows-palvelimille asennettujen roolien ja ominaisuuksien hallinnan Windows-työaseman kautta.

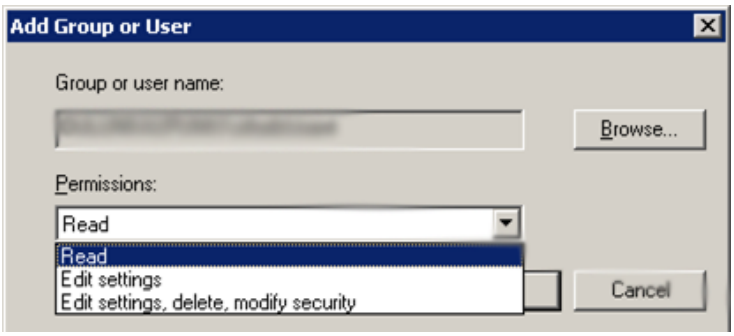
GPMC:n avulla voidaan tuoda, viedä, kopioida, liittää ja etsiä ryhmäkäytäntöjä sekä varmistaa ja palauttaa niitä. Hyvin tärkeä ominaisuus on ryhmäkäytäntöjen mallinnus, jolla voidaan selvittää ryhmäkäytäntöjen vaikutus käyttäjätunnukseen, konetiliin tai organisaatioyksikköön. Myös Windows Management Instrumentation -suodattimia (WMI) voidaan käyttää GPMC:ssa. GPMC:n Delegation-välilehdellä, joka sijaitsee GPMC:n jokaisella tasolla, voidaan käsitellä hallintaoikeuksia. Säiliöiden, kuten toimialueen tai organisaatioyksikön kohdalla voidaan määrittää millä tunnuksella tai ryhmällä on oikeudet sen sisältämiin ryhmäkäytäntöihin. Kuvassa 6 nähdään toimialuetasolla näkyvät oikeusmäärittelyt. Oikeudet voi periyttää ylemmältä tasolta ja ne pystytään levittämään alemman tason säiliöihin. Mikäli yksittäisille ryhmäkäytännöille on tarpeen antaa poikkeavia oikeuksia, tapahtuu se kyseessä olevan ryhmäkäytännön Delegation-välilehden kautta, kuten kuvassa 7 nähdään. WMI-suodattimien käsittelyyn on myös omat oikeusmäärittelynsä. AD DS -ryhmien Domain Admins, Enterprise Admins ja Group Policy Creator Owner jäsenillä on automaattisesti täydet oikeudet ryhmäkäytäntöjen käsittelyyn. Kuvassa 8 nähdään oikeustasovaihtoehdot, jotka tunnukselle tai ryhmälle voidaan tyhmäkäytäntöjen käsittelyyn määrittää. (Microsoft 2010.)



Kuva 6. Toimialuetason oikeusmäärittelyt.



Kuva 7. Ryhmäkäytännön oikeusmäärittelyt.



Kuva 8. Oikeustasot, jotka tunnukselle tai ryhmälle voidaan myöntää ryhmäkäytännön käsittelyyn.

GPMC ei sisällä versionhallintaa. Kun ryhmäkäytäntöön tehdään muutos tai luodaan uusi, se tulee välittömästi voimaan. Hyvä käytäntö onkin linkittää ryhmäkäytäntö ensin käyttöön ainoastaan testausta varten olemassa olevaan organisaatioyksikköön, jolloin uutta tai muokattua ryhmäkäytäntöä voidaan testata. Realistinen käyttökokemus saadaan kuitenkin vasta siinä vaiheessa, kun ryhmäkäytäntö otetaan tuotantoon. Mikäli muokatussa ryhmäkäytännössä esiintyy ongelmia, ei päästä helposti aikaisempaan

tilanteeseen, vaan tehdyt muutokset täytyy käydä ryhmäkäytännön sisällä palauttamassa aiempiin asetuksiin. Kun ryhmäkäytäntö avataan muokkausta varten, avautuu Group Policy Management Editor joka nähdään kuvassa 9.

Kuva 9. Group Policy Management Editor.

5.2 Advancd Group Policy Management

Advanced Group Policy Management (AGPM) tulee Microsoft Desktop Optimization Packn (MDOP) mukana. MDOP on kokoelma työkaluja, jotka on suunniteltu IT-alan ammattilaisten avuksi Windowsin virtualisointiin, suojaukseen ja hallintaan. Se on osa Software Assurance -sopimusta, joka on saatavilla Microsoftin voluumilisenssiasiakkaille. AGPM koostuu palvelinohjelmasta sekä asiakasohjelmasta. Taulukossa 3 on esitetty Software Assurancen hankintaväylät.

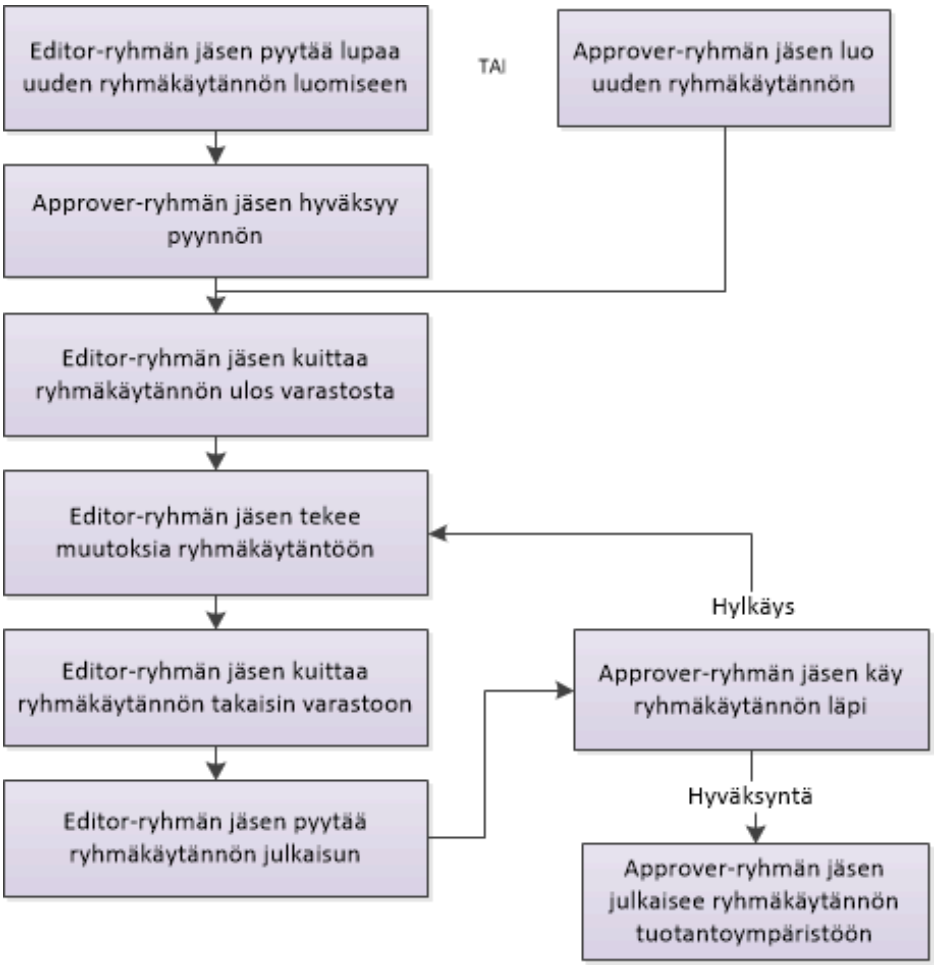
Taulukko 3. Microsoft Software Assurancen saatavuus. (Microsoft n.d.d.)

	Enterprise Agreement	Microsoft Products and Services Agreement (MPSA)	Open Value	Open License	Enrollment for Education Solutions
Software Assurance included	✓		✓		✓
Software Assurance optional		✓		✓	

AGPM:n yksi tärkeimmistä ominaisuuksista on ryhmäkohtaiset hallintaoikeudet. Ryhmään Reviewer kuuluvat voivat katsella ja vertailla ryhmäkäytäntöjä, mutta heillä ei ole oikeuksia muokata tai julkaista niitä. Ryhmän Editor jäsenet voivat pyytää luvan uuden ryhmäkäytännön luomiselle, kuitata ryhmäkäytännön muokattavaksi, tehdä siihen muutoksia ja muutoksien tekemisen jälkeen pyytää niille hyväksynnän. Käyttäjät, jotka kuuluvat ryhmään Approver, voivat hyväksyä ryhmäkäytäntöjen luomista ja muokkausta koskevat pyynnöt. He voivat myös itse tehdä muutoksia ryhmäkäytäntöihin, luoda uusia käytäntöjä sekä poistaa olemassa olevia ryhmäkäy-

täntöjä. Ryhmän Administrator jäsenet luonnollisesti omaavat täydet oikeudet järjestelmään. He voivat määrittää mihin hallintaoikeusryhmään käyttäjä tai käyttäjäryhmä kuuluu. (Honeycutt 2009.)

AGPM tarjoaa erillisen arkiston ryhmäkäytännöille. Kun olemassa olevaa ryhmäkäytäntöä halutaan muokata, se kuitataan ulos arkistosta muokkaustilaan, jolloin tiedosto lukitaan muilta käyttäjiltä. Tuolloin kukaan muu ei voi tehdä samaan ryhmäkäytäntöön yhtäaikaisia muutoksia. Kun ryhmäkäytäntöön tehdään muutos, se ei automaattisesti tule voimaan, vaan kuitataan takaisin arkistoon ja pyydetään ryhmäkäytännölle tarkastus. Muutokset hyväksyvän ryhmän jäsen tarkistaa ryhmäkäytännön ja hyväksyy sen tuotantoon. AGPM:ssa on versionhallinta, eli se säilyttää ryhmäkäytännön muutoshistorian. Näin mahdollistetaan paluu ryhmäkäytännön aikaisempaan versioon sekä ominaisuuksien vertailu eri versioiden välillä. Kuviossa 4 nähdään esimerkki ryhmäkäytännön käsittelytavasta AGPM:lla. (Honeycutt 2009.)



Kuvio 4. Esimerkki ryhmäkäytännön käsittelytavasta AGPM:lla.

AGPM:n haku- ja suodatintoiminnon avulla voidaan määrittää, mitkä ryhmäkäytännöt halutaan AGPM:n näkymässä näkyvän. Hakukenttään voidaan pelkän hakusanan lisäksi määrittää hakusanaksi se sarake, josta hakusanaa halutaan hakea. Tällöin haun muoto on ”sarakkeen nimi: hakusana”. (Honeycutt 2009.)

AGPM tukee käyttöjärjestelmien osalta osittain sekaympäristöä, mutta Microsoft vahvasti suosittelee koneen, jolle AGPM-asiakasohjelma on asennettu ja AGPM-palvelimen käyttävän samaa käyttöjärjestelmälinjaa. Esimerkiksi, jos asiakasohjelmaa käytetään Windows 8.1 -käyttöjärjestelmän päällä, tulisi palvelimen käyttöjärjestelmän olla Windows Server 2012 R2. Muita käyttöjärjestelmäpareja ovat muun muassa Windows 8 ja Windows Server 2012 sekä Windows 7 ja Windows Server 2008. Kaikki AGPM:n versiot voivat käsitellä vain niitä ryhmäkäytäntöasetuksia, jotka tulivat sen käyttöjärjestelmän mukana, tai aiemmassa käyttöjärjestelmäversiossa, jolle AGPM-asiakasohjelma tai palvelin on asennettu. Tällä hetkellä uusin AGPM-versio on 4.0 SP2. (Microsoft 2013a.)

5.3 PowerShell

Microsoft suosittelee nykyään PowerShellin hyödyntämistä hallintatyökaluna, eikä ryhmäkäytäntöjen hallinta ole tässä poikkeus. PowerShellin avulla voidaan automatisoida useita ryhmäkäytäntöihin liittyviä tehtäviä. Jotta PowerShelliä voidaan käyttää ryhmäkäytäntöjen hallintaan, tulee siihen lisätä ryhmäkäytäntömoduuli. Tällä hetkellä kyseinen moduuli sisältää 25 eri komentoa (cmdlet), joilla voidaan esimerkiksi luoda, poistaa, kopioida ja uudelleen nimetä ryhmäkäytäntöjä, luoda ja poistaa ryhmäkäytäntöobjektin linkitys, sekä luoda raportteja tietystä tai kaikista toimialueen ryhmäkäytännöistä. PowerShellin ryhmäkäytäntöjen hallintakomennot vastaavat GPMC:ssa tehtyjä toimintoja. (Microsoft n.d.h.)

5.4 Vertailu

Vaikka AGPM on käytännössä vain lisänäkymä GPMC:n sisään, ovat AGPM:n mukana tulevat ominaisuudet selkeästi kehitetty vastaamaan tarpeeseen. Ympäristöissä, joissa ylläpitäjiä on useita, on kasvanut riski inhimillisten virheiden tekemiseen. AGPM:n tarjoamilla hallintaryhmillä saadaan helposti selkeytettyä ylläpitorakennetta, jonka avulla virhetilanteita voidaan vähentää. Versiohallinnan avulla nopea palaaminen aikaisempaan tilanteeseen on selkeä etu AGPM:n eduksi. GPMC on käyttöjärjestelmän mukana tuleva työkalu, joka on myös saatavilla ilmaiseksi Microsoftin www-sivuilta. AGPM puolestaan on saatavilla vain erillisen sopimuksen mukana. Mikäli kyseinen sopimus on olemassa, on AGPM:n käyttöönotto yksinkertaista ja sen tuomat edut ryhmäkäytäntöjen ylläpitoon helposti saavutettavissa.

6 ADVANCED GROUP POLICY MANAGEMENT ASENNUS, TESTAUS JA KÄYTTÖÖNOTTO

AGPM:n asennusta varten on kerättävä tietoja, jotka vaikuttavat asennusvaiheisiin ja asennettaviin komponentteihin. AD DS -ympäristön rakenteesta on selvitettävä metsien määrä, löytyykö yhteysongelmia toimialueiden välillä, keskitetyn hallinnan taso ja ryhmäkäytäntöjen määrä hallittavissa toimialueissa. Näiden tietojen avulla voidaan päätellä, kuinka monta AGPM-palvelinta ympäristöön asennetaan ja kuinka paljon hallittavia ryhmäkäytäntöjä on olemassa. (Microsoft 2013.)

Ennen asennusta on tarpeellista suunnitella ryhmäkäytäntöjen hallintaoikeusrakenne, jotta AGPM:ia käyttäville henkilöille saadaan määritettyä oikea ryhmäjäsenyys. Kyseisiä ryhmiä käsiteltiin kappaleessa 5.2. AD DS:en luodaan tunnus AGPM-palvelua varten. AGPM-palvelin voidaan asentaa toimialueen ohjauskoneelle tai jollekin muulle toimialueeseen kuuluvalle palvelimelle. Mikäli AGPM-palvelin asennetaan koneelle, joka ei ole toimialueen ohjauskone, täytyy AGPM-palvelutunnus lisätä koneen paikallisiin järjestelmänvalvojiin. Tunnukselle täytyy antaa myös tarvittavat oikeudet AD DS:en. Ne voidaan yksinkertaisemmillaan myöntää liittämällä tunnus AD DS:n ryhmään Domain Admins. Mikäli oikeuksia halutaan rajata tarkemmin ja tunnukselle ei myönnetä Domain Admins -ryhmän oikeuksia, täytyy se lisätä jokaisen AGPM-palvelimen hallinnoiman toimialueen ryhmiin Group Policy Creator Owner sekä Backup Operators. Lisäksi tunnus tarvitsee täydet oikeudet paikalliseen temp-kansioon, joka yleensä sijaitsee polussa %windir%\temp, täydet oikeudet kaikkiin niihin ryhmäkäytäntöihin, joita AGPM:lla aiotaan hallita sekä täydet oikeudet AGPM:n arkistokansioon. AD DS:en on luotava myös tunnus tai ryhmä AGPM:n arkistoa varten. Tuo tunnus tai ryhmä on ensimmäinen AGPM:n Administrators-ryhmän jäsen. (Microsoft 2013.)

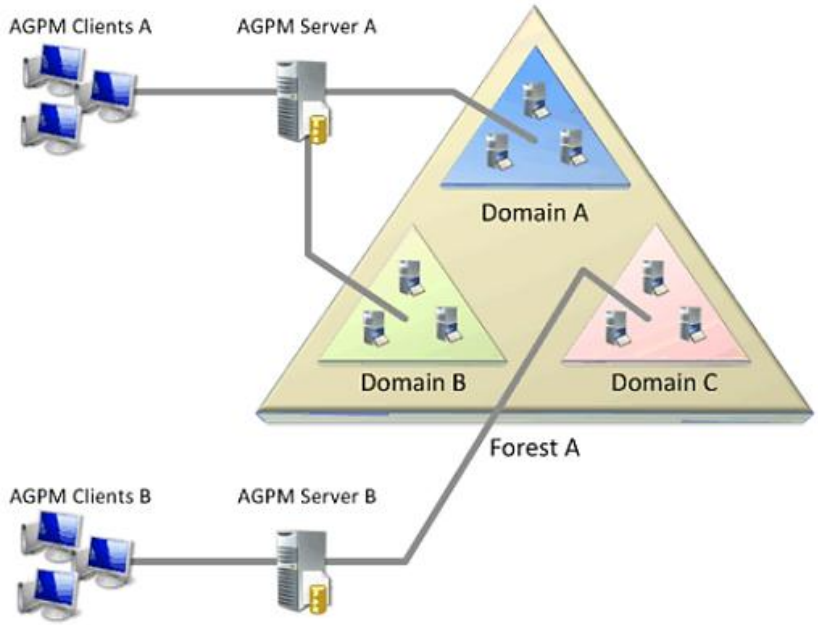
Ryhmäkäytännön uloskuittausprosessin aikana ryhmäkäytännöstä luodaan arkistosta otettu kopio aiemmin mainittuun temp-kansioon. Tästä arkistokopiosta luodaan palautusta käyttämällä [AGPM]-etuliitteen omaava offline-ryhmäkäytäntö. Uloskuittausprosessin toimintatavasta johtuen AGPM:n hallintaan tuotua ryhmäkäytäntöä ei ole suositeltavaa käsitellä GPMC:lla, sillä GPMC:lla tehdyt muutokset katoavat kun ryhmäkäytäntöä muokataan seuraavan kerran AGPM:lla. (Wright 2011.)

AGPM-palvelin lähettää sähköpostiviestin esimerkiksi silloin, kun ryhmäkäytännölle pyydetään tarkistusta. Jotta palvelin voi lähettää postia, täytyy sille kertoa lähtevän postin palvelimen, eli SMTP-palvelimen täydellinen toimialuenimi (FQDN). Mikäli SMTP-palvelimen lähetysoikeudet on rajattu konekohtaisiksi nimen tai IP-osoitteen perusteella, tulee kaikki AGPM-palvelimet lisätä sallittuihin lähettäjiin. Jos lähettävän postin palvelimen ja AGPM-palvelimen välissä on palomuuri, täytyy SMTP-liikenne sallia muurin läpi. (Microsoft 2013.)

Kuten aiemmin mainittiin, AGPM sisältää ryhmäkäytäntöarkiston. Arkistokansio sisältää oman kansion jokaista AGPM:n hallinnoimaa ryhmäkäytäntöä kohti. Arkiston tarvitsema levytila voidaan arvioida ennen asennus-

ta. Tarvittava tila riippuu hallittavien ryhmäkäytäntöjen määrästä, säilytettävistä ryhmäkäytäntöversioiden määrästä sekä ryhmäkäytäntöjen tiedostokoosta. Tiedostokoon keskiarvokokona voidaan käyttää 64 kilotavua. AGPM-palvelin säilyttää oletusarvoisesti kaikki ryhmäkäytäntöversiot, mutta tarvittaessa määrää voidaan muuttaa. Nykyisissä levytilakokoluokissa arkiston tarvitsema tila on kaiken kaikkiaan melkoisen vähäinen. Arkisto voidaan sijoittaa joko AGPM-palvelimelle, erilliselle koneelle tai jaetulle verkkolevylle. Oletussijainti arkistolle on AGPM-pavlelimen polku %ProgramData%\Microsoft\AGPM. (Microsoft 2013.)

AGPM:n asennuksessa on valittavissa kaksi eri konfiguraatiomallia, joita ovat keskitetty ja hajautettu malli. Keskitetyssä konfiguraatiossa asennetaan yksi AGPM- palvelin sekä yksi tai useampi AGPM-asiakasohjelma. Sitä käytetään yhden AD DS -metsän ympäristöissä, jolloin yksi AGPM-palvelin palvelee kaikkia metsään kuuluvia toimialueita. AGPM-palvelin voi käsitellä suurta työkuormaa, joten mikäli halutaan käsitellä vain yhden metsän ryhmäkäytäntöjä, yksi AGPM-palvelin yleensä riittää. Jos kuitenkin on tarpeen rakentaa skaalautuva ja saatavuudeltaan varmempi ympäristö, täytyy valita hajautettu konfiguraatiomalli. Hajautetussa konfiguraatiossa asennetaan vähintään kaksi AGPM-palvelinta. On huomioitava, että yksi AGPM-palvelin voi hallita vain yhden metsän ryhmäkäytäntöjä. Tämän vuoksi hajautetussa ympäristössä asennetaan erilliset AGPM-palvelimet jokaista metsää kohti sekä myös jokaiselle toimipaikalle, joka verkon tai organisaation rakenteen vuoksi sitä vaatii. AGPM-palvelin voi kuitenkin hallita yhden tai useamman toimialueen ryhmäkäytäntöjä, mutta yhden toimialueen ryhmäkäytäntöjä voi hallita vain yksi AGPM-palvelin. Kuva 10 esittää usean AGPM-palvelimen hajautetun konfiguraatiomallin. (Microsoft 2013.)



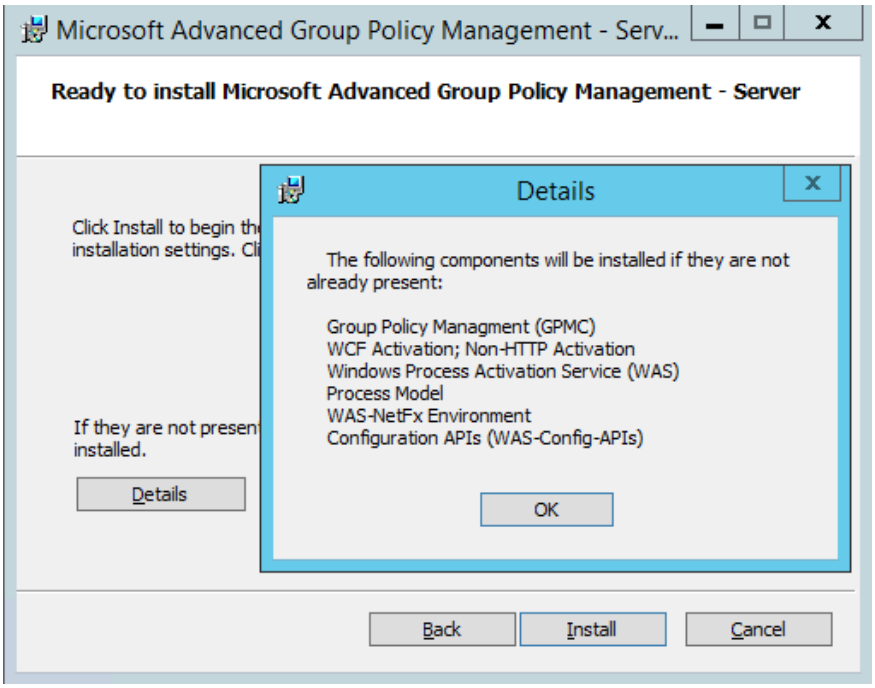
Kuva 10. Esimerkki hajautetusta konfiguraatiosta. (Mukaillen Microsoft 2013.)

Sekä AGPM-palvelin että AGPM-asiakasohjelma vaativat GPMC:n pohjalleen. Microsoftin mukaan AGPM-koneissa täytyy olla asennettuna .NET Framework versio 3.5 tai uudempi ja sen sisältämät komponentit Windows Communication Foundation (WCF) non-http activation sekä Windows Process Activation Service (WAS). Palvelimen asennusohjelma lisää kaikki vaaditut komponentit automaattisesti, mikäli ne puuttuvat, kun puolestaan asiakasohjelmakoneelle ne täytyy asentaa itse. AGPM-asiakasohjelma voidaan asentaa myös samalle koneelle AGPM-palvelimen kanssa. (Microsoft 2013.)

6.1 Palvelimen asennus

Ennen asennusta luotiin AGPM-palvelutunnus. Tietoturvasyistä sitä ei lisätty toimialueen Domain Admins -ryhmään, vaan oikeudet määritettiin kappaleessa 6 mainitulla vaihtoehtoisella tavalla. AGPM ei tee muutoksia toimialueen kaavaan, joten se asennettiin suoraan tuotantotoimialueelle. Oulun Tietotekniikan tapauksessa päädyttiin asentamaan oma palvelin pelkästään AGPM:ia varten. Koska tarkoituksena on hallita ainoastaan yhden toimialueen ryhmäkäytäntöjä, valittiin keskitetty konfiguraatiomalli. Palvelimen käyttöjärjestelmäksi valittiin Windows Server 2012 R2 Standard ja AGPM-versioksi 4.0 SP2. Asennusta varten noudettiin .iso-tiedostomuotoa oleva MDOP 2014 -paketti Microsoftin voluumilisenssiasiakkaiden sivustolta. Palvelimelle kirjauduttiin Domain Admins -ryhmään kuuluvalla toimialuetunnuksella ja paketista AGPM-kansion alta kopioitiin agpm_402_server_adm64.exe tiedosto palvelimelle.

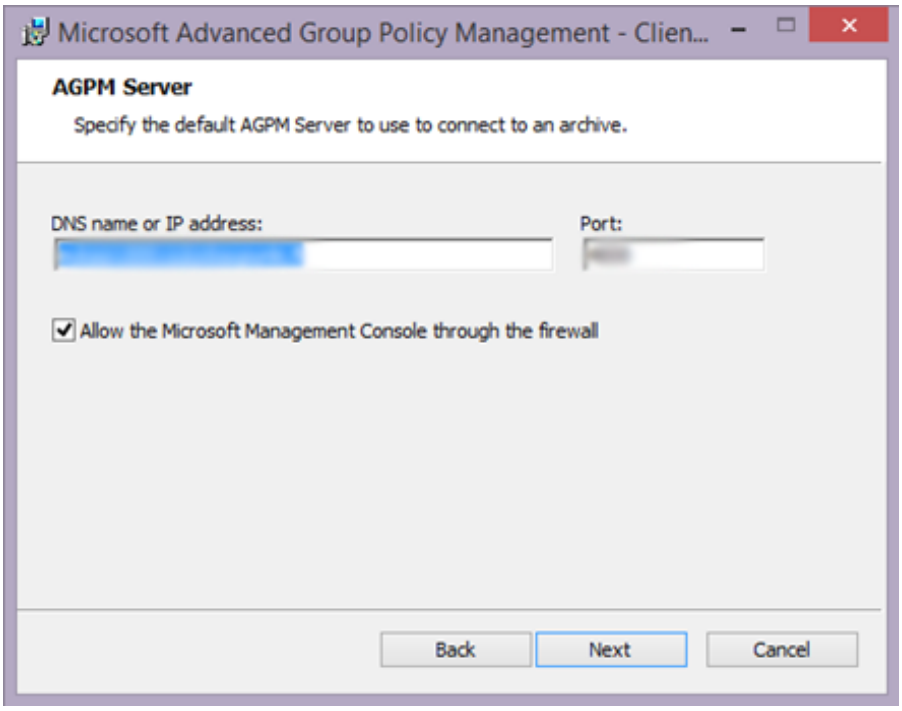
Asennuksen esitietojen määrittely käynnistyi tervetuloa-ikkunalla, jota seurasivat lisenssiehdot ja niiden hyväksyminen. Asennus eteni AGPM-palvelinohjelman asennuspolun päättämisellä sekä AGPM-arkiston lokaation valintana, joka vaihdettiin asennettavaksi AGPM-palvelimelle omalle levyosiolleen. Tämän jälkeen ilmoitettiin aiemmin luodun AGPM-palvelutunnuksen ja arkiston omistajan tiedot. Seuraavassa vaiheessa kerrottiin palomuuriportti, jonka kautta AGPM-palvelu kommunikoi AGPM-palvelimen ja -asiakasohjelmien välillä. Asennusohjelma lisää portin, joka oletusarvoisesti on 4600, Windowsin palomuurin sallittuun liikenteeseen, mikäli asentaja niin haluaa. Viimeisessä vaiheessa ennen varsinaisen asennuksen käynnistämistä valittiin asennettava kieli ja tarkistettiin, mitä komponentteja palvelinohjelmiston lisäksi asentuu, mikäli ne puuttuvat. Kyseinen ikkuna nähdään kuvassa 11. Asennus ei vaatinut käyttöjärjestelmän uudelleen käynnistämistä.



Kuva 11. Palvelinohjelmiston lisäksi tarvittavat komponentit.

6.2 Asiakasohjelman asennus

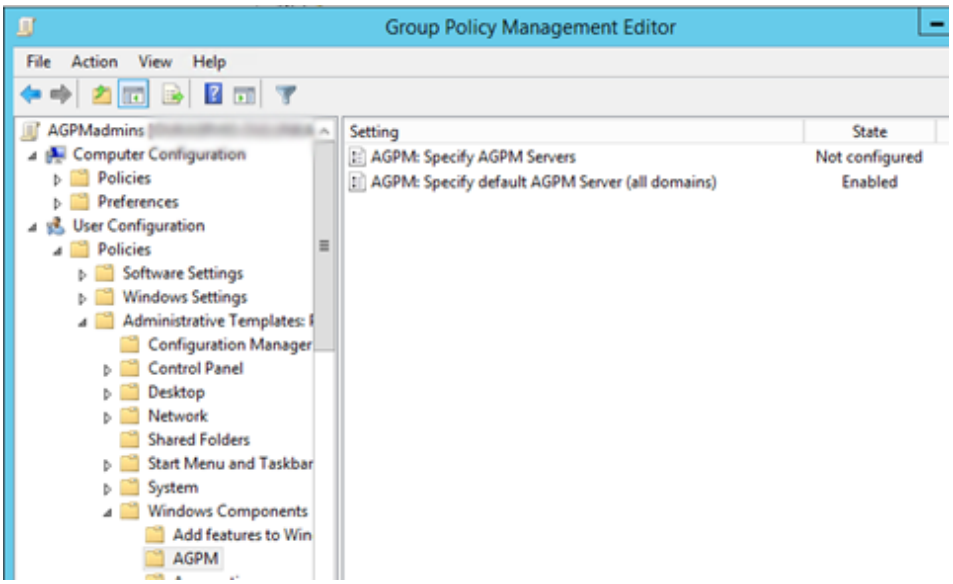
Asiakasohjelma asennettiin koneelle, jonka käyttöjärjestelmänä on Windows 8.1. Koneelle kirjauduttiin sillä tunnuksella, joka palvelimen asennuksen aikana lisättiin kohtaan Archive Owner. Asennusohjelma ei salli asennuksen jatkuvan, mikäli jokin esivaatimuksissa vaadittu komponentti puuttuu. Tästä syystä koneelle asennettiin RSAT-paketti sekä .NET Frameworkin versio 4.5. Vaikka Microsoft (n.d.e.) kertoo AGPM:n asennusohjeessa .NET Frameworkin versioksi kelpaavan 3.5, tai uudemman, AGPM-asiakasohjelman asennus ei asennettua versiota hyväksynyt. Sen vuoksi päädyttiin asentamaan myös .NET Framework 3.5. Varsinaiset asiakasohjelman asennusvaiheet etenivät pitkälti samaan tapaan, joskin hieman yksinkertaisemmin, kuin palvelinohjelman käyttöönotossa. Asennus ei tarvinnut AGPM:n hallintaan käytettävien tunnusten tietoja, palomuuriportin määritystä tai arkistoon liittyviä tietoja. Jotta asiakasohjelma osaa yhdistää AGPM-palvelimeen, asennuksen aikana pyydettiin palvelimen nimi- ja porttitiedon, kuten nähdään kuvassa 12. Asiakasohjelma asennettiin myös palvelinkoneelle.



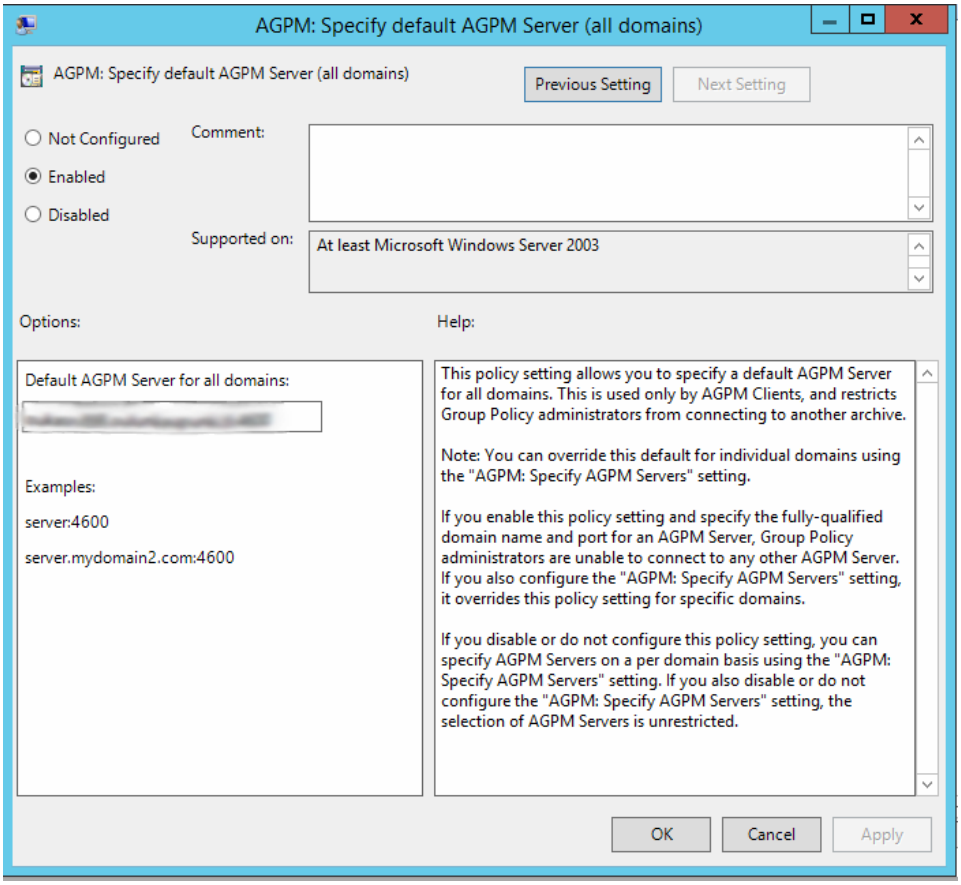
Kuva 12. AGPM-palvelintietojen syöttäminen AGPM-asiakasohjelman asennuksessa.

6.3 Palvelinyhteyden määrittäminen käyttäjille

AGPM-palvelimen nimi- ja porttitieto voidaan jakaa ryhmäkäytäntöjen ylläpitäjille myös ryhmäkäytännön avulla. Uusi ryhmäkäytäntö luodaan tai olemassa olevaa muokataan sillä koneella, johon AGPM-asiakasohjelma on asennettu, sillä muokattava ominaisuus tulee AGPM-asennuksen mukana. Ryhmäkäytäntö pitää kohdistaa sellaiseen organisaatioyksikköön, johon ylläpitäjien tunnukset kuuluvat. Koneelle kirjaudutaan Archive Owner -tunnuksella ja avataan GPMC, johon AGPM on integroitunut. Muokattavaan tai luotavaan ryhmäkäytäntöön otetaan käyttöön polusta User Configuration → Policies → Administrative Templates: Policy defenitions (ADMX files) retrieved from the local computer. → Windows Components → AGPM löytyvä AGPM: Specify default AGPM Server (all domains) ominaisuus joka nähdään kuvassa 13. Kun ominaisuus otetaan muokattavaksi, voidaan se asettaa enabled-tilaan sekä lisätä tarvittava palvelintieto portteineen. Kuvassa 14 nähdään muokattavaksi otettu ominaisuus.



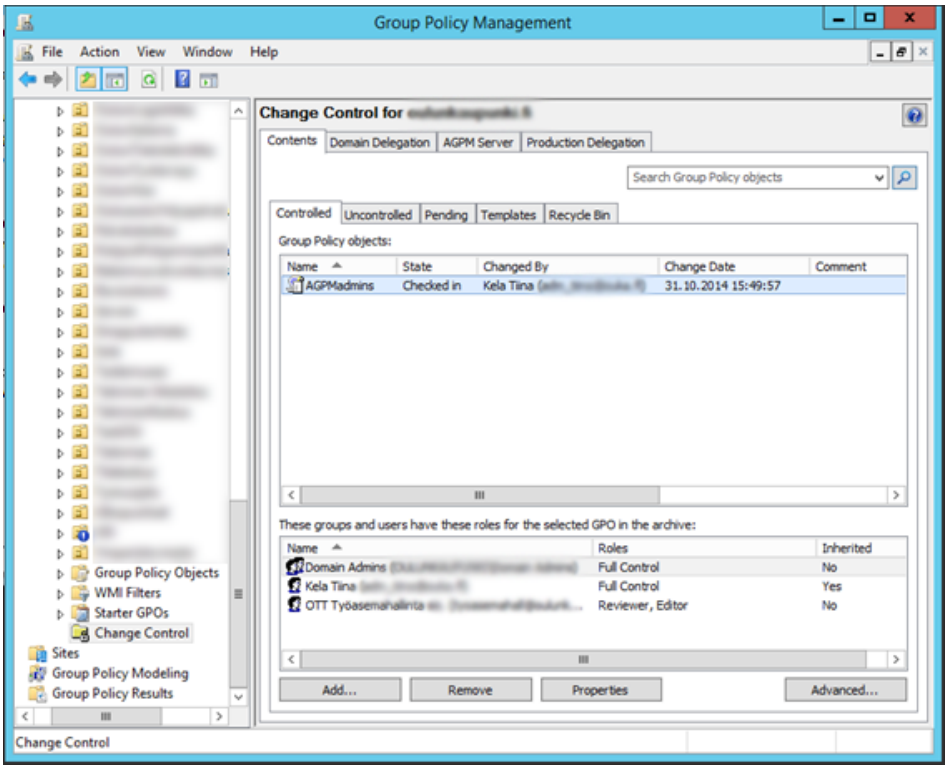
Kuva 13. Ominaisuus, jolla AGPM-palvelintiedot voidaan jakaa ylläpitäjille.



Kuva 14. Muokkaustilassa oleva ryhmäkäytännön ominaisuus AGPM: Specify default AGPM Server (all domains).

6.4 Asiakasohjelman käyttöliittymä ja toiminnot

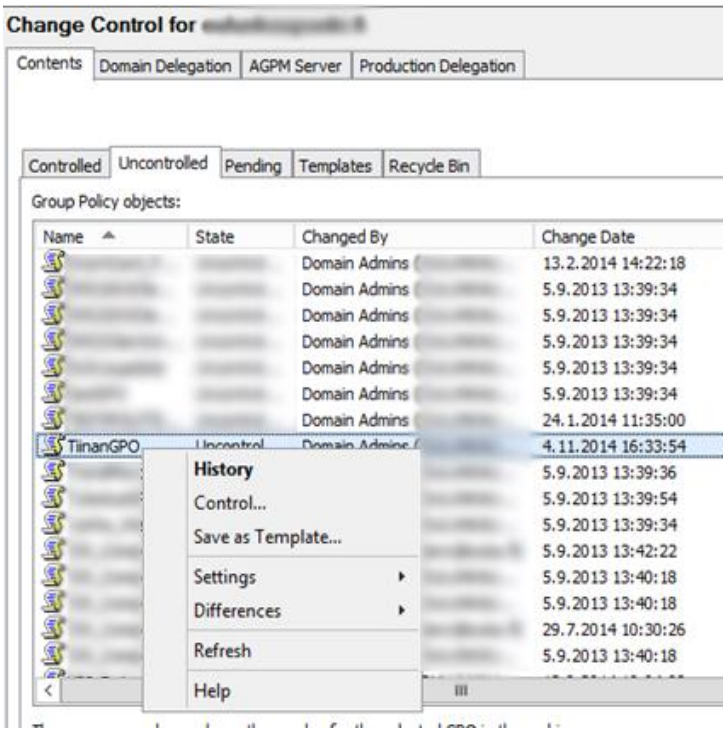
Kuten aiemmin on mainittu, AGPM on GPMC:n liitännäinen. AGPM:n asennus luo GPCM:in vasempaan valikoon toimialueen alle Change Control -kansion. Sen valitessaan käyttäjälle avautuu ohjelman oikeaan ruutuun näkymä, jonka välilehdiltä löytyvät kaikki AGPM:n tuomat lisäominaisuudet ryhmäkäytäntöjen hallintaan. Kuvassa 15 nähdään AGPM:n ominaisuuksien näkymä. AGPM:n yhteydessä puhuttaessa tuotantopuolesta, tarkoitetaan sillä GPMC-puolen näkymää. Ryhmäkäytäntöjen linkitys AD DS objekteihin tapahtuu edelleen GPMC:n kautta.



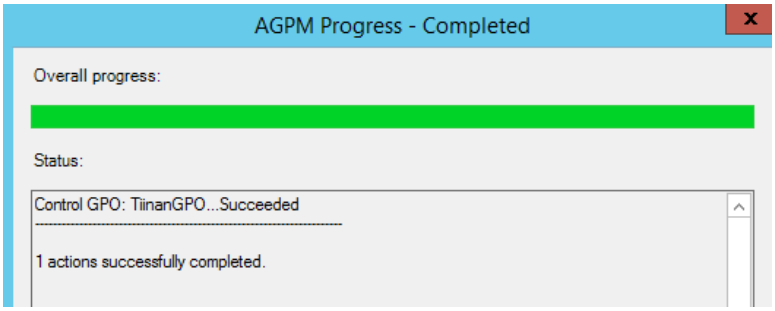
Kuva 15. AGPM-asiakasohjelman yleisnäkymä.

Ennen kuin olemassa olevat ryhmäkäytännöt saadaan AGPM:n tarjoamien ominaisuuksien piiriin, täytyy ne tuoda AGPM:n arkistoon. Tämä tapahtuu AGPM:n ominaisuuksista välilehdeltä Contents löytyvältä Uncontrolled-sivulta, jossa listataan kaikki AGPM:n hallinnan ulkopuolella olevat toimialueen ryhmäkäytännöt. Ryhmäkäytäntöjä voidaan tuoda joko yksittäin tai useita kerralla. Usean ryhmäkäytännön valinta tapahtuu joko ctrl- tai shift-näppäimen painamisella sekä hiiren vasemman painikkeen klikkauksella, riippuen siitä halutaanko valita listalta peräkkäisiä vai erillään olevia käytäntöjä. Kun valittujen ryhmäkäytäntöjen päällä klikataan hiiren oikeaa painiketta, ilmestyy valikko, josta löytyy toiminto Control. Uncontrolled-välilehden sisältö ja kyseinen valikko nähdään kuvassa 16. Kun toiminto valitaan, voidaan avautuvaan ikkunaan kirjoittaa halutessa kommentti ryhmäkäytännön tai -käytäntöjen siirrosta, jonka jälkeen tehtävä suoritetaan. Tällöin avautuu ikkuna, joka kertoo tuonnin etenemisestä ja ilmoittaa onnistuiko vai epäonnistuko siirto. Siirron onnistumiseksi täytyy AGPM-palvelutunnuksella olla ryhmäkäytäntöön täydet oikeudet. Kuvassa 17 on näytetty onnistuneesta siirrosta ilmoittava ikkuna. Lähes kaikissa AGPM:n

toiminnoissa ilmestyy vastaava onnistuneesta tai epäonnistuneesta toiminnosta kertova ikkuna.



Kuva 16. Valikko, jonka kautta ryhmäkäytännön hallinta siirretään.

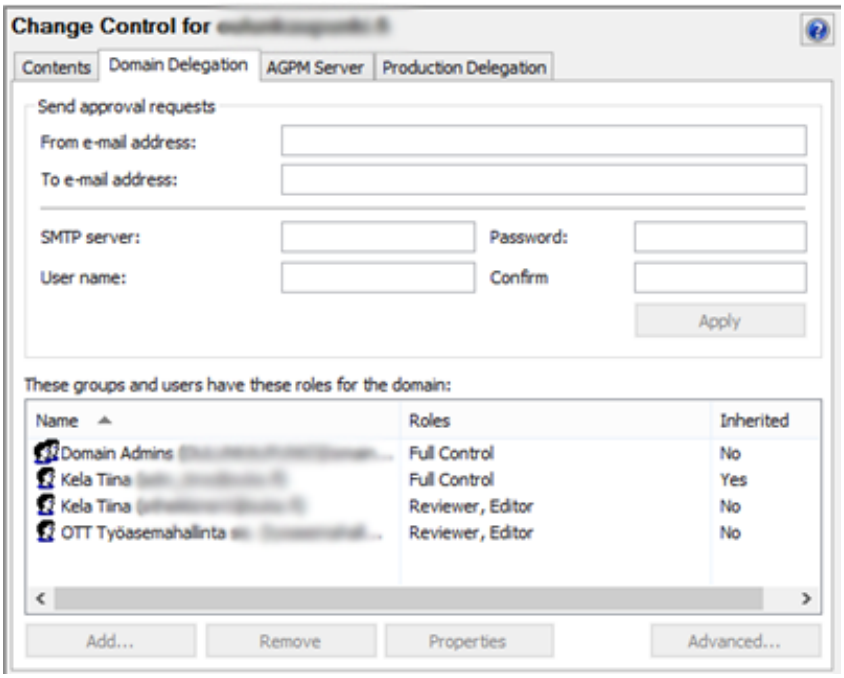


Kuva 17. Ilmoitus onnistuneesta siirrosta.

Kappaleessa 5.2 käsiteltiin hallintaoikeusryhmiä. Jotta ryhmäkäytännöistä, joille hallintaryhmään Editor kuuluvat jäsenet pyytävät tarkastuksia, lähtee sähköposti-ilmoitus, täytyy välilehdelle Domain Delegation määrittää tarvittavat sähköpostiasetukset. Niitä ovat ilmoitukset lähettävä ja vastaanottava osoite, lähtevän postin palvelimen nimi sekä mahdollisesti sen autentikointitiedot. Samalla välilehdellä voidaan lisätä ja poistaa käyttäjiä tai ryhmiä ryhmäkäytäntöjen hallintaryhmistä. Hallintaoikeudet periytyvät kaikkiin AGPM:n hallintaan tuotuihin ryhmäkäytäntöihin.

Oulun Tietotekniikan organisaatiorakenteessa on omat tiiminsä työasema- sekä palvelinhallinnalle. Palvelinhallintatiimi vastaa myös AD DS -toimialueen ylläpidosta. Työasematiimille myönnettiin AGPM:iin ryhmän Editor oikeudet ja palvelinhallintatiimin AD DS -ryhmä lisättiin AGPM ryhmään Approvers. Osa palvelinhallintatiimin jäsenistä kuuluu AD DS -

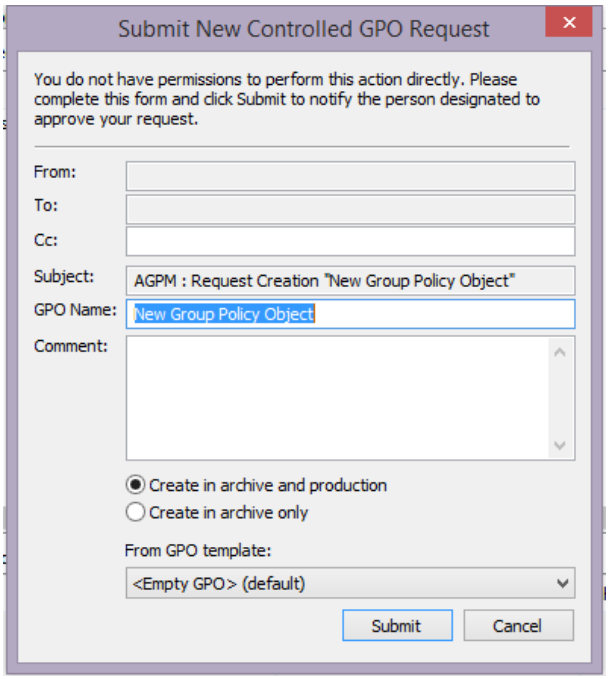
ryhmään Domain Admins, jolloin heillä on täydet oikeudet AGPM:n hallinnassa. Koska ylläpito-oikeudet lisätää AD DS -ryhmien perusteella, ei AGPM:n puolella oikeuksiin tarvi juurikaan puuttua sen jälkeen, kun ne on asetettu. Tunnusten lisäykset ja poistot kohdistetaan suoraa tarvittaviin AD DS -ryhmiin. Kuva 18 esittää AGPM:n ikkunaa, jossa määritellään hallintaryhmäoikeudet sekä sähköpostiasetukset.



Kuva 18. Domain Delegation -välilehti, johon määritellään hallintaryhmäoikeudet sekä sähköpostiasetukset.

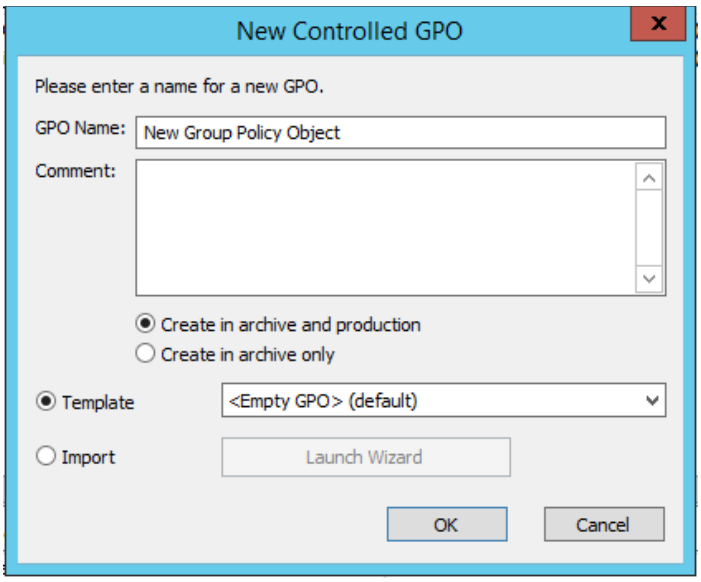
Välilehdeltä AGPM Server voidaan vaihtaa asiakasohjelman käyttämä AGPM-palvelimen nimi ja portti. Yhden AGPM-palvelimen ympäristöissä tätä asetusta ei ole tarpeen muuttaa, ellei AGPM-palvelinta ole vaihdettu. Samalta välilehdeltä voidaan määrittää kuinka monta versiota ryhmäkäytännöistä arkistossa säilytetään. Välilehdeltä Production Delegation löytyy hallintaoikeudet, mitkä ryhmäkäytännöillä on voimassa AGPM:n ulkopuolella, eli tuotantopuolella.

Kuten aiemmin mainittiin, ryhmän Editor jäsen ei voi itse luoda uutta ryhmäkäytäntöä, vaan hän voi pyytää ryhmään Approver tai Full Control kuuluvalta jäseneltä käytännön luomisen. Kun ryhmän Editor jäsen klikkaa Controlled-välilehdellä hiiren oikeaa painiketta, avautuu valikko, josta löytyy vaihtoehto New Controlled GPO. Kyseisen vaihtoehdon valittaessa avautuu kuvan 19 mukainen ikkuna, joka on esitäytetty aiemmin määritetyillä sähköpostiasetuksilla. Cc-kenttään voidaan lisätä tarvittaessa toinen vastaanottava sähköpostiosoite automaattisesti lisätyn To-kentästä löytyvän vastaanottajan lisäksi. Kenttään GPO Name määritetään uudelle ryhmäkäytännölle haluttu nimi sekä Comment-kenttään voidaan kirjoittaa perustelu pyynnölle.



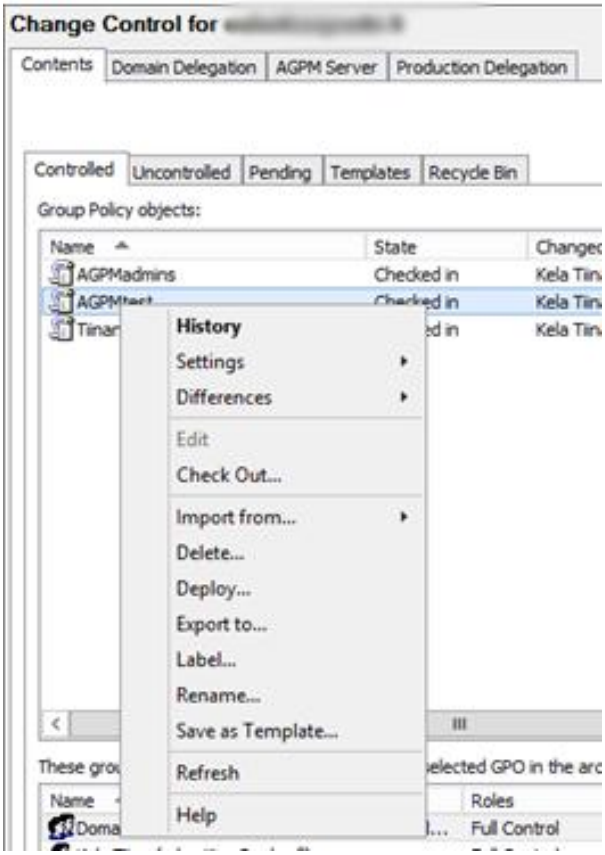
Kuva 19. Editor-ryhmän jäsenen pyyntö uuden ryhmäkäytännön luomiseksi.

Ryhmiin Approver ja Full Control kuuluvat ylläpitäjät voivat luoda uusia ryhmäkäytäntöjä itse. Kun he valitsevat aiemmin mainitun kohdan New Controlled GPO, avautuu kuvan 20 mukainen näkymä. Uusi ryhmäkäytäntö voidaan luoda arkistoon ja tuotantoon (production) tai pelkästään arkistoon. Jos ryhmäkäytäntö luodaan myös tuotantoon, se voidaan löytää GPMC:n alta polusta Group Policy Management → Forest: metsän nimi → Domains → Toimialueen nimi → Group Policy Objects. Ryhmäkäytäntö voidaan luoda myös mallia (template) käyttämällä. Malleja voi luoda olemassa olevista ryhmäkäytännöistä ja niitä hallitaan AGPM-näkymän Templates-välilehden kautta.



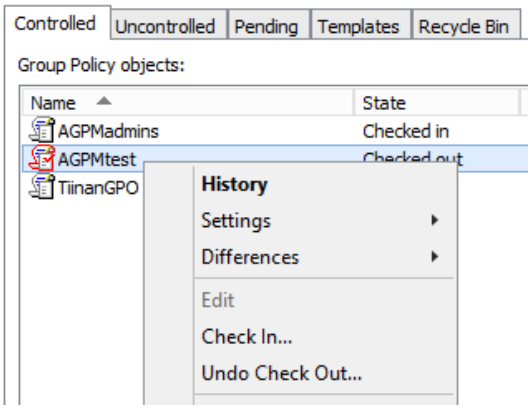
Kuva 20. Uuden ryhmäkäytännön luonti AGPM:lla.

Ryhmäkäytännön uloskuittaus tapahtuu klikkaamalla Controlled-välilehdellä ryhmäkäytännön päällä hiiren oikeaa painiketta ja valitsemalla kohta Check Out. Valikkonäkymä on esitetty kuvassa 21. Ennen kuin ryhmäkäytäntö on kuitattu ulos muokkausta varten, ei kohta Edit ole valittavissa. Mikäli ryhmäkäytäntöä on jostain syystä muokattu GPMC:n puolella, voidaan muutokset tuoda AGPM:n arkistossa olevaan ryhmäkäytäntöön valitsemalla kohta Import from.



Kuva 21. AGPM:n hallinnassa olevan ryhmäkäytännön toimintovalikko.

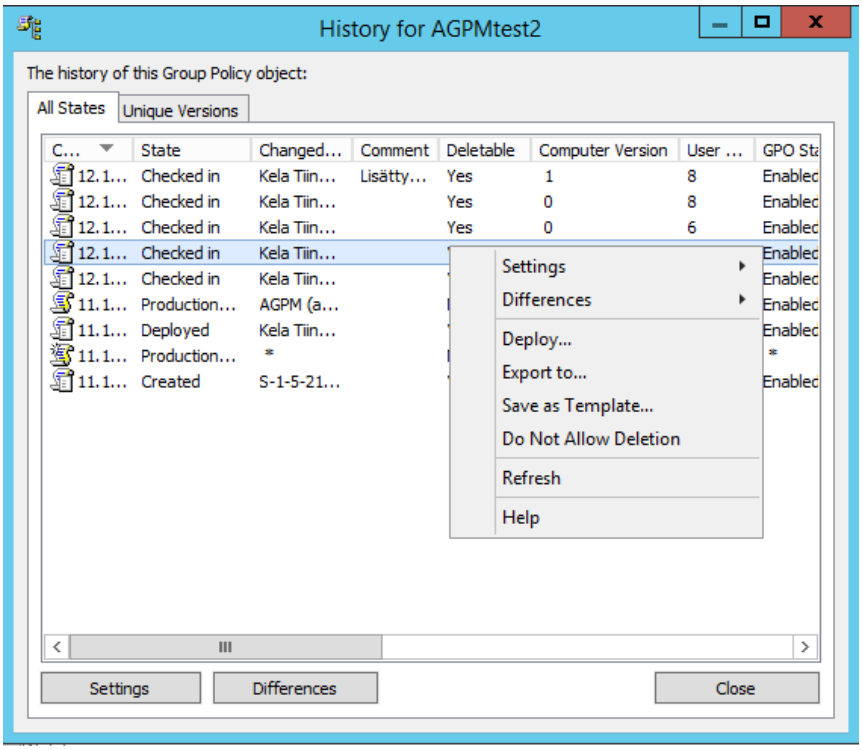
Kun ryhmäkäytäntö on kuitattu ulos arkistosta muokkausta varten, sen ulkoasu Controlled-näkymässä muuttuu. Kuvassa 22 nähdään, kuinka ryhmäkäytäntö AGPMtest on kuitattu muokattavaksi. Kun joku muu, kuin uloskuittauksen tehnyt käyttäjä avaa uloskuitatun ryhmäkäytännön toimintavalikon, ei Edit-valinta ole käytettävissä. Tämä voidaan todeta kuvan 22 näkymässä. Koska kuvassa näkyvä valikko on avattu ryhmään Full Control kuuluvalla jäsenellä, ovat valinnat Check In ja Undo Check Out mahdollisia. Editor-ryhmään kuuluvalla jäsenellä kyseiset valinnat eivät olisi valittavissa.



Kuva 22. Ryhmäkäytäntö AGPMtest on kuitattu ulos AGPM-arkistosta.

Kun ryhmäkäytännölle on tehty halutut muutokset, se kuitataan takaisin siään Check In -valintaa käyttämällä. Mikäli ryhmäkäytäntö halutaan tuotantoon, valikosta valitaan kohta Deploy. Editor-ryhmän jäsenelle avautuu samankaltainen näkymä, kuin uuden ryhmäkäytännön luontia pyydettäessä. Ryhmien Approver ja Full Control jäsenet saavat lisättyä ryhmäkäytännön tuotantoon itse.

Ryhmäkäytännön toimintovalikosta valittaessa kohta History, avautuu ryhmäkäytännön historiatietoikkuna. Sen välilehdillä nähdään ryhmäkäytännön eri versiot jotka arkistoon on talletettu. Ryhmäkäytännön version päällä hiiren oikeaan painiketta klikattaessa saadaan esille valikko, josta valittaessa Deploy versio voidaan ylläpitäjän oikeuksista riippuen julkaista tuotantoon tai sille voidaan pyytää julkaisu. Valikko ja historiatiedot nähdään kuvassa 23. Valikon kautta voidaan myös esimerkiksi tallentaa ryhmäkäytäntö malliksi, viedä ryhmäkäytännön tiedot HTML- tai XML-raporttiin sekä tutkia, mihin ryhmäkäytäntö on linkitetty. Kaksi ryhmäkäytäntöä valittaessa ctrl-näppäimen avustuksella, voidaan valitsemalla Differences valikosta tai painikkeella luoda raportti, josta nähdään ryhmäkäytäntöversioiden eroavaisuudet, kuten kuvasta 24. voidaan todeta.



Kuva 23. Ryhmäkäytännön historiasivu.

Kuva 24. Ryhmäkäytännön kahden eri version vertailu.

Mikäli ryhmäkäytäntö halutaan poistaa, klikataan AGPM:n päänäkymässä Controlled-välilehdellä poistettavan ryhmäkäytännön päällä hiiren oikeaa painiketta ja valitaan vaihtoehto Delete. Poistovaihtoehtoina on pelkkä arkisto tai sekä arkisto että tuotanto. Poistettu ryhmäkäytäntö löytyy Recycle Bin -välilehdeltä ja se voidaan tarvittaessa palauttaa takaisin arkistoon. Se tapahtuu klikkaamalla Recycle Bin -välilehdellä ryhmäkäytännön päällä hiiren oikeaa painiketta ja valitsemalla vaihtoehto Restore. Jos ryhmäkäytäntö halutaan poistaa lopullisesti, valitaan puolestaan vaihtoehto Destroy.

6.5 Käyttöönotto

AGPM:n käyttöönotto täytyy suunnitella ja aikatauluttaa huolellisesti. Sen jälkeen, kun olemassa olevat ryhmäkäytännöt on tuotu AGPM:iin, ei ole toivottua, että GPMC:a käytetään ryhmäkäytäntöjen hallintaan enää lainkaan niiltä osin joilta AGPM tarjoaa vaihtoehtoisen tavan. Tästä syystä henkilölle, joita muutos koskee, täytyy tarjota uuden työkalun käyttöohjeistus, asiakasohjelman asennus ja tarkka tiedotus ennen lopullista muutosta. On tarpeen sopia käyttökatko, jonka aikana ryhmäkäytäntöihin ei tehdä lainkaan muutoksia tai uusia käytäntöjä luoda. Ennen käyttökatkoa voidaan hallintaoikeusryhmämäärittelyt tehdä jo valmiiksi. Käyttökatkon aikana tuodaan kaikki ryhmäkäytännöt AGPM:n piiriin ja katkon jälkeen kaikki ryhmäkäytäntöylläpitäjät siirtyvät käsittelemään ryhmäkäytäntöjä AGPM:n kautta.

7 YHTEENVETO

Keskitetty hallinta on yksi ydinosa toimivassa ja helposti ylläpidettävässä IT-infrastruktuurissa. Kasvavan tietomäärän käsittely turvallisesti ja inhimilliset virheet minimoiden on haaste varsinkin suurille ja keskisuurille organisaatioille. Active Directory -ympäristöissä ryhmäkäytännöt ovat tärkeä osa keskitettyä hallintaa, jonka avulla ylläpitäjien työkuormaa vähennetään ja työskentelyä nopeutetaan. Group Policy Management Console ei sisällä kaikkia toimintoja, joita ylläpitäjät kaipaavat. Versionhallinta ja selkeät käyttöoikeusryhmät ryhmäkäytäntöjen käsittelyyn ovat Advanced Group Policy Managementin tuoma helpotus lukuisia ryhmäkäytäntöjä ja ylläpitäjiä sisältäville organisaatioille.

Opinnäytetyön teoriaosuudessa paneuduttiin siihen, mitkä tekniikat mahdollistavat ryhmäkäytäntöjen käyttämisen. Active Directory ja nimenomaan sen Domain Services -palvelu luovat pohjan ryhmäkäytännöille. Hyvin toteutettu ja looginen toimialuerakenne organisaatioyksikköineen edesauttavat suunnitelmallista ryhmäkäytäntöjen jakelua.

Työn tarkoituksena oli Advanced Group Policy Managemen -työkalun testaus, asennus ja käyttöönotto toimeksiantajan ympäristössä. Toimeksiantajan aikataulullisten haasteiden vuoksi varsinaista käyttöönottoa päätettiin lykätä lähitulevaisuuteen. Työ toteutui kuitenkin muilta osin. Verrattaessa Advanced Group Management Consolea ja Group Management Consolea, voitiin Advanced Group Management Consolen nähdä todellakin olevan vain liitännäinen Group Management Consoleen. Tästä huolimatta Advanced Group Policy Managementin voitiin todeta olevan tervetullut apuväline tukemaan ryhmäkäytäntöjen hallintaa.

Aikataulullisten vaikeuksien lisäksi oman haasteensa toi lähdemateriaalin keräys. Osa löytyneestä tiedosta oli vanhentunutta teknologioiden kehittymisen ja uusien versioiden vuoksi, jonka takia vertailua eri lähteiden välillä piti tehdä runsaasti. Itse asennetusta työkalusta ei juurikaan löytynyt käyttökokemuksia kertovaa materiaalia, joten opinnäytetyön kirjoittajan omille havainnoille ja kokemuksille ei löytynyt vertailukohteita. Tämän vuoksi opinnäytetyön tuloksia voivat hyödyntää ne yritykset ja organisaatiot, jotka ovat pohtineet Advanced Group Policy Managementin käyttöönottoa.

LÄHTEET

AgileIT n.d.a. Single Sign-On (SSO) for Office 365 and other Cloud Services. Viitattu 30.10.2014.
http://www.agileit.com/single-sign-on-sso-for-office-365-and-other-cloud-services/

Holme, D. Ruest, D. Ruest, N. 2008. Configuring Windows Server 2008 Active Directory.

Honeycutt, J. 2007. An Owerview of Group Policy Preferences. Viitattu 15.11.2014.
http://www.microsoft.com/en-us/download/details.aspx?id=24449

Honeycutt, J. 2009. Overview of Microsoft Advanced Group Policy Management. Viitattu 23.10.2014.
http://www.microsoft.com/en-us/download/details.aspx?id=13975

Mar-Elia, D. Melber, D. Stanek W. & Microsoft Group Policy Team 2005. Microsoft Windows Group Policy Guide.

Microsoft 2009. Group Policy Planning and Deployment Guide. Viitattu 3.11.2014.
http://technet.microsoft.com/en-us/library/cc754948(v=ws.10).aspx

Microsoft 2010. Windows Server 2003/2008: Group Policy Administration and Troubleshooting.

Microsoft 2012. Active Directory Lightweight Directory Services Overview. Viitattu 7.10.2014.
http://technet.microsoft.com/en-us/library/6a3bedf7-9c5b-4ada-9a51-6b794adc9ab8

Microsoft 2013. Planning Guide for Advanced Group Policy Management 4.0 SP1. Viitattu 29.10.
http://www.microsoft.com/en-us/download/confirmation.aspx?id=38401

Microsoft 2013a. Choosing Which Version of AGPM to Install. Viitattu 23.10.2014.
http://technet.microsoft.com/en-us/library/dd553090.aspx

Microsoft n.d.a. So What Is Active Directory? Viitattu 10.9.2014.
http://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx

Microsoft n.d.b. Active Directory Logical Structure Background Information. Viitattu 10.11.2014.
http://technet.microsoft.com/en-us/library/cc756901(v=ws.10).aspx

Microsoft n.d.c. Directory Partitions. Viitattu 14.10.2014.
http://technet.microsoft.com/en-us/library/cc961591.aspx

Microsoft n.d.d. Software Assurance Overview. Viitattu 21.10.2014. http://www.microsoft.com/licensing/software-assurance/default.aspx#tab=2

Microsoft n.d.e. Step-by-Step Guide for Microsoft Advanced Group Policy Management 4.0. Viitattu 31.10.2014. http://technet.microsoft.com/en-us/library/ee378482.aspx

Microsoft n.d.f. Active Directory Collection. Viitattu 10.11.2014. http://technet.microsoft.com/en-us/library/cc780036(v=ws.10).aspx

Microsoft n.d.g. What is the Global Catalog? Viitattu 10.11.2014. http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx

Microsoft n.d.h. Use Windows PowerShell to Manage Group Policy. Viitattu 10.11.2014. http://technet.microsoft.com/en-us/library/dd759177.aspx

Kivimäki, J. 2005. Active Directory – Tehokas hallinta.

Oulun Tietotekniikka 2014. Toimintakertomus 2013. Viitattu 28.8.2014. http://www.ouluntietotekniikka.fi/c/document_library/get_file?uuid=a7facfd2-6377-448b-ab80-0b4487d14db2&groupId=4568021

Oulun Tietotekniikka n.d. Organisaatio. Viitattu 29.10.2014. http://www.ouluntietotekniikka.fi/organisaatio

Oulun Tietotekniikka n.d.a. Oulun Tietotekniikka. Viitattu 17.11.2014. http://www.ouluntietotekniikka.fi/etusivu

Seitsonen, M. 2014. Mihin matka, Active Directory? Viitattu 30.9.2014. http://kilta.sovelto.fi/core/infra/mihin-matka-active-directory/

Wright, S. 2011. AGPM Operations (under the hood part 3: check in). Viitattu 11.11.2014. http://blogs.technet.com/b/askds/archive/2011/04/11/agpm-operations-under-the-hood-part-3-check-in.aspx