ACTIVE DIRECTORYN GROUP POLICYJEN PARHAAT KÄYTÄNNÖT

Case Palmia

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, syksy 2013

Teppo Salminen

Teppo Salminen

HAMK
HÄMEEN AMMATTIKORKEAKOULU

HÄMEENLINNA, VISAMÄKI
Tietojenkäsittelyn koulutusohjelma

Tekijä Teppo Salminen **Vuosi** 2013

Työn nimi Active Directoryn Group Policyjen parhaat käytännöt, case Palmia

TIIVISTELMÄ

Opinnäytetyön toimeksiantajana oli Helsingin kaupungin Palmia liikelaitos. Tämä opinnäytetyö tehtiin, koska Palmialla otettiin käyttöön Windows 8 -käyttöjärjestelmä tablet-tietokoneissa ja uusi käyttöjärjestelmä tarvitsi myös ryhmäkäytäntöasetusten määrittämisen. Ryhmäkäytännöt oli määritelty myös sekavasti.

Työssä selvitetään aluksi ryhmäkäytäntöjen toimintaperiaatetta ja esitetään yleisiä parhaita käytäntöjä, joiden mukaan ryhmäkäytäntöjä tulisi määritellä. Tietolähteenä on käytetty pääasiallisesti Microsoft-ympäristöihin perehtyneiden asiantuntijoiden Internet-sivuja ja blogeja.

Työn aluksi tehtiin nykytilan kartoitus, josta saatiin yleiskäsitys, mitä on tehty hyvin ja mitkä osa-alueet vaativat muutoksia. Tämän kartoituksen pohjalta laadittiin kehitysehdotuksia, joista osa päätettiin toteuttaa. Windows 8 -käyttöjärjestelmän asetuksiin ja optimointiin määriteltiin asetukset linjassa olemassa olevan ympäristön asetusten kanssa.

Opinnäytetyön tuloksena syntyi Palmialle yksinkertainen ryhmäkäytäntöjen ympäristö, jota on helppo ylläpitää. Ryhmäkäytäntöobjektit on suunniteltu niin, että ne painottavat vähäistä vaikutusta loppukäyttäjään. Lisäksi havaittiin, että ryhmäkäytäntöjä ei tule jättää määrittelyn jälkeen vaille huomiota, koska tietokoneissa oleva käyttöjärjestelmä ja käytetyt sovellukset päivittyvät jatkuvasti ja ympäristön asetuksien tulee olla koko ajan ajantasaiset.

Avainsanat Aktiivihakemisto, ryhmäkäytännöt, parhaat käytännöt

Sivut 33 s. + liitteet 2 s.

HÄMEENLINNA, VISAMÄKI
Degree Programme in Business Information Technology

Author Teppo Salminen **Year** 2013

Subject of Bachelor's thesis Best Practices of Active Directory Group Policies, case Palmia

ABSTRACT

This thesis was commissioned by the City of Helsinki Public Utility Palmia as they introduced the Windows 8 operating system in their tablet computers. The purpose of the thesis was to define a proper Group Policy configuration as Group Policies were poorly defined.

First, the principle of Group Policies is described and what the general best practices are on how Group Policies should be set. The data source is mainly Internet sites and blogs of experts specialized in Microsoft environments.

The thesis was started by studying the current state of Group Policies, which gave an overview of what has been done well and what areas require changes. On the basis of this survey development proposals were drawn up and some of those were decided to implement.

As a result of this study Palmia got a simple Group Policy environment that is easy to maintain. Group Policies were designed so that the impact on the end user is minimized. In addition, it was found out that the Group Policies should not be left ignored after they have once been defined and set. That is because the operating systems and applications of computers are continuously updated and the environment settings must be constantly up-to-date.

Keywords Active Directory, Group Policies, best practices.

Pages 33 p. + appendices 2 p.

AD
Active Directory (aktiivihakemisto), hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista.

AGPM
Advanced Group Policy Management. Edistyksellisempi versio GPMC-työkalusta, joka hallitsee mm. versionhallinnan.

CSE
Client-side Extension on ryhmäkäytäntölaajennus, jolla voidaan määrittää kohdetietokoneen ryhmäkäytäntöjä. Ryhmäkäytäntölaajennukset jakaantuvat usealle eri osa-alueelle.

DC
Domain Controller, toimialueen ohjauskone on aktiivihakemiston säiliö, joka voi pitää sisällään käyttäjä- tai tietokoneobjekteja.

DFS-R
Tiedostojärjestelmä replikointi

Domain
Toimialue, joukko Microsoft Windows -käyttöjärjestelmän sisältäviä tietokoneita, joita voidaan hallita keskitetysti yhdeltä tai useammalta Windows-palvelimelta.

GINA
Graphical Identification and Authentication, Graafinen tunnistaminen ja todentaminen, eli kirjautumisikkuna.

GP
Group Policy (ryhmäkäytäntö), keskitetysti AD:n kautta käytettävä hallintatyökalu.

GPC
Group Policy Container, ryhmäkäytäntöjen säilö.

GPMC
Group Policy Management Console. Ryhmäkäytäntöjen ylläpitoon suunniteltu hallintakonsoli.

GPO
Group Policy Object, ryhmäkäytännöillä tehdyt määrittelyt tallentuvat ryhmäkäytäntöobjekteiksi.

GPP
Group Policy Preference, GPO:n osa-alue, jolla voidaan määrittää oletusasetuksia tietokoneeseen.

GPT
Group Policy Template, ryhmäkäytäntömalli.

Item-Level Targeting
Group Policy Preferenssissä käytetty osiotason kohdistaminen, jolla voidaan kohdistaa asetuksia erilaisten suodattimien mukaan.

LDAP
Lightweight Directory Access Protocol on hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla. LDAP:in yleisin käyttötarkoitus on käyttäjäntunnistus ja käyttöoikeuksien tarkistaminen.

MDOP
Microsoft Desktop Optimization Pack on Software Assurance -asiakkaille suunnattu kokoelma erilaisia tekniikoita, joilla voidaan tehostaa Microsoft Windows -ympäristön hallintaa.

MSI
Windows Installer Package on ohjelmistojen asentamiseen käytettävä tiedostomalli.

OU
Organisaatioyksikkö, aktiivihakemiston säiliö, joka voi pitää sisällään käyttäjä- tai tietokoneobjekteja.

RSAT
Remote Server Administration Tools, työkalupaketti palvelimen etähallintaan.

RSoP
Resultant Set of Policy, Ryhmäkäytäntöjen suunnittelu- ja diagnostiikkatila.

Site
Toimipaikka. Fyysinen rakenne, johon aktiivihakemisto perustuu.

SCCM
Microsoftin System Center Configuration Manager on päivitysten ja sovellusten keskitettyyn hallintaan tarkoitettu maksullinen ohjelmisto.

WMI
Windows Management Instrumentation. Ryhmäkäytäntöobjektien yhteydessä käytettävä suodatin, jolla voidaan tutkia tietokoneen ominaisuuksia.

SISÄLLYS

Liite 1 WMI-suodattimia
Liite 2 Ryhmäkäytäntöobjektin muutosprosessi

1 JOHDANTO

Yrityksen toimivan IT-infrastruktuurin taustalla ovat lähes poikkeuksetta Windows-käyttöjärjestelmät ja aktiivihakemisto (AD, Active Directory). Jotta IT-infrastruktuuri saadaan toimimaan halutusti ja tietoturvallisesti, tarvitaan siihen keskitetty hallintajärjestelmä. AD on hakemisto, johon tallennetaan tieto työasemista, käyttäjistä ja käyttäjäryhmistä. Ryhmäkäytännöt mahdollistavat työasemien asetusten keskitetyn hallinnan.

Opinnäytetyön tarkoitus on kartoittaa Palmian ryhmäkäytäntöjen nykytila ja optimoida asetuksia parhaiden käytäntöjen mukaisesti. Työssä käsitellään teoreettisella tasolla, mitkä ovat parhaat käytännöt ryhmäkäytäntöjen määrityksessä, miten ryhmäkäytäntöjä optimoidaan Windows 8:lle ja mitä hallintatyökaluja ryhmäkäytäntöjen hallintaan on käytettävissä. Lisäksi konkreettisella tasolla selvitetään, mitä parhaita käytäntöjä Palmia jo noudattaa ryhmäkäytännöissä. Työn tavoitteena on saada Palmialle toimiva ja helposti ylläpidettävä sekä optimoitu ryhmäkäytäntöjen ympäristö toimivalla muutosprosessilla.

Opinnäytetyön aihe syntyi omasta kiinnostuksesta ryhmäkäytäntöjä kohtaan ja Palmialla käynnissä olleesta Windows 8 -käyttöönottoprojektista. Uutta Windows 8 -käyttöjärjestelmää ei voida ottaa käyttöön ilman kunnollisia ryhmäkäytäntöjä. Palmia on kolmen käyttöjärjestelmän (Windows XP/7/8) sekaympäristö ja ympäristön hallintaan käytetyt ryhmäkäytännöt suunnittelemattoman ylläpidon tuloksena sekavat.

Vaikka ryhmäkäytännöt ovat hyvä ja helppo keino hallita ympäristöä keskitetysti, piilee niissä kuitenkin käyttäjäkokemukseen liittyvä suorituskykymiina. Jos asetuksia tehdään ymmärtämättä ryhmäkäytäntöjen yleistä toimintalogiikkaa, voidaan pahimmillaan hidastaa käyttäjän työasemaan kirjautumista useilla minuuteilla.

Aihe rajataan käsittelemään ryhmäkäytäntöjen parhaita käytäntöjä tietokoneille ja käyttäjille, käytettäviä työkaluja ja ryhmäkäytäntöjen toimintaperiaatetta. Hallintatyökalujen osalta keskitytään Microsoftin omien työkalujen käyttöön. Lisäksi käydään läpi hyödylliseksi havaittuja kolmannen osapuolen ilmaisia työkaluja, mutta maksullisia työkaluja ei käsitellä.

2 TOIMEKSIANTAJANA PALMIA

Palmia on Helsingin kaupungin omistama liikelaitos, jonka pääasiallinen toimiala on toimitila- ja hyvinvointipalvelut. Palmia tuottaa catering-, siivous-, kiinteistö-, turva-, puhelin- ja hyvinvointipalveluja pääasiassa Helsingin kaupungin virastoille ja liikelaitoksille. Työntekijöitä Palmialla on lähes 3000 yli 1000 palvelukohteessa. Toimintansa Palmia aloitti vuonna 2003.

Palmian tietotekninen ympäristö koostuu n. 1115 työasemasta, 96 kassakoneesta ja n. 2100 aktiivihakemiston käyttäjästä. Kassakoneissa on Windows

XP -käyttöjärjestelmä. Työasemissa ja kannettavissa tietokoneissa on Windows 7 -käyttöjärjestelmä, tablet-tietokoneissa on Windows 8 -käyttöjärjestelmä. Tavoitetila on ylläpitää sekaympäristöä Windows 7 ja Windows 8 -käyttöjärjestelmillä. Windows XP tullaan korvaamaan vuoden 2013–2014 aikana uudemmalla käyttöjärjestelmäversiolla.

Palmialla ei ole omaa AD:ta vaan ainoastaan oma organisaatioyksikkö (OU) Helsingin kaupungin yhteisessä AD:ssa. Palmia hallinnoi vain omaa OU-haaraa, sen rakennetta ja ryhmäkäytäntöjä. OU-rakenne on kaupungin keskushallinnon ohjeistuksen mukainen ja osa ryhmäkäytännöistä tulee pakotettuna (Enforced) ylätasolta. Ryhmäkäytäntöobjekteja ennen työn aloittamista oli 53, joista käyttäjiin kohdistuvia objekteja oli 32 ja tietokoneisiin kohdistuvia 21.

3 RYHMÄKÄYTÄNTÖJEN TOIMINTAPERIAATE

Jotta ryhmäkäytäntöjä voi ylipäänsä ryhtyä optimoimaan parhaiden käytäntöjen mukaan, pitää ymmärtää, kuinka niitä käsitellään työasemassa. Tärkeää on ymmärtää milloin mitäkin asetuksia prosessoidaan tietokoneessa ja mitkä asetukset ovat kalliita, eli vievät paljon aikaa prosessointiin ja mitkä asetukset ovat nopeita prosessoida.

3.1 Client-side Extensions

Asiakkaan ryhmäkäytäntölaajennukset eli CSE:t, joista myöhemmin käytetään nimitystä ryhmäkäytäntölaajennukset, määrittävät ryhmäkäytäntöjä kohdetietokoneella. Jokainen ryhmäkäytäntöjen asetus kuuluu määriteltyyn ryhmäkäytäntölaajennukseen. Esimerkiksi kansioiden uudelleen ohjaus on oma ryhmäkäytäntölaajennus ja rekisteriasetukset omansa. Ryhmittelemällä ryhmäkäytäntölaajennukset ryhmäkäytäntöobjekteihin järkevästi voidaan säästää aikaa ryhmäkäytäntöjen prosessoinnissa, mikä näkyy käyttäjälle nopeampana kirjautumisena. Ryhmäkäytäntöjen suunnittelussa on tärkeää miettiä monoliittisten ja funktionaalisten ryhmäkäytäntöjen suhde (ks. luku 5.1.1).

Microsoft (n.d.) on kuvannut ryhmäkäytäntölaajennukset, joita on 38 kappaletta, joskaan lista ei ole täydellinen, koska Empson (2010) on listannut 83 kappaletta ryhmäkäytäntölaajennuksia. Huolimatta ryhmäkäytäntölaajennusten määrästä, näiden listojen avulla voidaan helpommin nähdä miten asetukset jakaantuu ryhmäkäytäntölaajennuksiin ja tehdä päätelmiä monoliittisten ja funktionaalisten ryhmäkäytäntöobjektien suhteen.

3.2 Suorituskykyä hidastavat ryhmäkäytäntölaajennukset

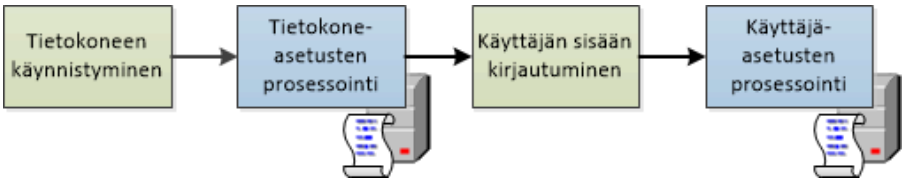
Suorituskykyä hidastavat tai kalliit ryhmäkäytäntölaajennukset ovat ensimmäisenä suurennuslasin alla, kun pitää selvittää tietokoneen käynnistystä ja sisäänkirjautumista hidastavia tekijöitä. Ryhmäkäytännöillä voi helposti asentaa työasemiin vaikka sovelluksia, sovellusasennus (Software Installa-

tion) on kuitenkin yksi hitaimmista prosessoitavista ryhmäkäytäntölaajennuksista. Isoissa ympäristöissä on järkevämpää käyttää sovellusjakeluihin tarkoitettuja työkaluja, kuten Microsoftin System Center Configuration Manager (SCCM). (Mar-Elia 2008.)

Suorituskykyä hidastavaa on myös kansion uudelleenohjaus (Folder Redirection), joka ensimmäisellä prosessointikerralla kopioi käyttäjäprofiilin tiedostoja verkkolevyille ja on tästä syystä hidasta prosessoida. Tämän lisäksi hitautta aiheuttavat suurien määrien käyttöoikeusmäärittelyt tiedosto- tai rekisterihaaraan. Myös suuri määrä rekisteriasetuksia voi aiheuttaa paljon prosessointia, joka hidastaa esim. kirjautumista. (Mar-Elia 2008, 2012a.)

3.3 Tausta- ja edustaprosessointi

Tietokoneessa ryhmäkäytäntöjä prosessoidaan tausta- ja edustaprosessoinnissa. Edustaprosessointi tapahtuu tietokoneessa käynnistyksen yhteydessä ja käyttäjille sisäänkirjautumisen yhteydessä (Kuva 1). Taustaprosessointi suoritetaan nimensä mukaisesti taustalla. Oletuksena prosessointi tapahtuu 90 minuutin välein, johon lisätään satunnaisesti arvottu 0–30 minuutin aika. Taustaprosessointi tapahtuu siis 90–120 minuutin välein. Oletusaikaa voidaan muuttaa ryhmäkäytäntöasetuksella. (Mar-Elia 2012a; Holme, Ruest & Ruest 2008, 235.)



Kuva 1. Edustaprosessoinnin vaiheet

Windows Vistassa ja sitä uudemmissa käyttöjärjestelmissä taustaprosessointiin on lisätty niin sanottu NLA-prosessointi (Network Location Awareness). Jos toimialueen ohjauskone (DC) ei ole tavoitettavissa, kun taustaprosessointi tulisi suorittaa, suoritetaan se seuraavan kerran heti, kun toimialueen ohjauskone on jälleen tavoitettavissa. (Mar-Elia 2012a.) Windows 8 -käyttöjärjestelmässä tätä prosessointia on paranneltu entisestään vieläkin nopeammaksi (Mar-Elia 2012b).

Suojausasetusten ryhmäkäytäntölaajennus suoritetaan taustaprosessina oletuksen 16 tunnin välein, huolimatta siitä, onko ympäristössä tapahtunut muutoksia. Asetusta voi muuttaa ryhmäkäytännöillä, mutta kokonaan sitä ei voi ottaa pois. (Mar-Elia 2012b; Holme ym. 2008, 236.)

3.4 Synkroninen ja asynkroninen prosessointi

Tärkeä osa prosessia on synkronisen ja asynkronisen prosessoinnin ymmärtäminen. Näihin liittyvillä määrityksillä on mahdollista saada suuria suorituskykyyn liittyviä parannuksia aikaan, jos niin halutaan. Tietokonepohjainen ryhmäkäytäntöprosessointi käynnistyy, kun tietokone käynnistyessä ottaa yhteyttä verkkoon. Jos tämä prosessointi on määritelty synkroniseksi, käyttäjä ei näe kirjautumisikkunaa (GINA) ennen kuin prosessointi on suoritettu loppuun. Kun käyttäjä kirjautuu tietokoneelle, alkaa käyttäjäpohjainen ryhmäkäytäntöprosessointi – käyttäjä ei näe työpöytää ennen kuin prosessointi on valmis. Synkroninen prosessointi siis hidastaa käynnistystä ja sisäänkirjautumista.

Microsoft muutti edustaprosessoinnin Windows XP:n julkaisun yhteydessä oletuksena asynkroniseksi. Asynkroninen prosessointi tunnetaan paremmin nopean kirjautumisen optimointina (Fast Logon Optimization). Asynkronisessa prosessoinnissa tietokone jatkaa sisäänkirjautumista, vaikka ryhmäkäytäntöjen prosessointi on vielä käynnissä. Käyttäjälle tämä näkyy nopeana kirjautumisena, mutta saattaa aiheuttaa ylimääräisiä tietokoneen uudelleen käynnistyksiä ja uudelleen kirjautumisia, jotta kaikki määritellyt asetukset tulevat voimaan. Ryhmäkäytännöillä määritellyt sovellukset saattavat jäädä asentumatta ensimmäisillä kirjautumiskerroilla. (Mar-Elia 2012a.)

Mar-Elia (2012b) ei itse enää suosittele synkronista prosessointia pakotettuna. Jos on valmis kestämään muutaman tietokoneen uudelleen käynnistyksen tai käyttäjän sisäänkirjautumisen, voi saada suurenkin ajallisen hyödyn käyttäjän sisään kirjautumisen yhteydessä määrittämällä prosessoinnin asynkroniseksi. Holme ym. (2008, 236) ovat kuitenkin sitä mieltä, että synkronoidun prosessoinnin pakotettu käyttöönottaminen on erittäin suositeltavaa.

Ryhmäkäytäntöjä suunniteltaessa on hyvä huomioida seuraavat poikkeukset synkronisessa ja asynkronisessa prosessoinnissa. Valtaosa ryhmäkäytäntölaajennuksista suoritetaan taustaprosesseissa, mutta Software Installation, Folder Redirection, Microsoft Disk Quota ja Group Policy Preferences Drive Mappings suoritetaan kuitenkin aina synkronisessa edustaprosessissa. Taustaprosessointi suoritetaan aina asynkronisesti ja palvelimien ryhmäkäytäntöjen prosessointi suoritetaan aina synkronisesti. (Mar-Elia 2012b.)

Synkronisen prosessoinnin voi käyttöönottaa pakotetusti määrittelemällä `Computer Configuration\Policies\Administrative Templates\System\Logon\Always Wait for the network at computer startup` - ryhmäkäytäntöasetus enabled-tilaan. (Microsoft 2003a; Mar-Elia 2012a).

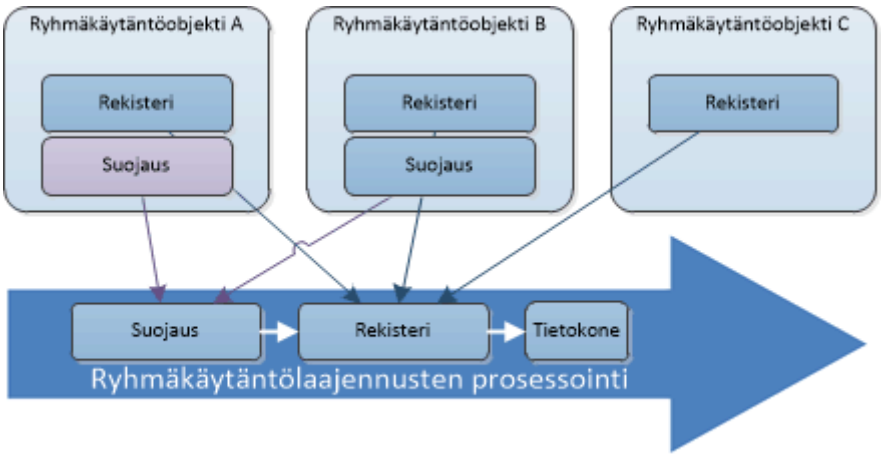
3.5 Ryhmäkäytäntöjen prosessointi

Ryhmäkäytäntöjen prosessointi on monimutkainen tapahtumien ketju. Korkealla tasolla on kaksi osaa ryhmäkäytäntöjen prosessointia. Ensimmäinen

on niin sanottu ydin- tai ryhmäkäytäntöjen infrastruktuurin prosessointi. Tässä vaiheessa Windows-ryhmäkäytäntöasiakas tekee kyselyn lähimpänä olevalle toimialueen ohjauskoneelle selvittääkseen, mikä on yhteyden nopeus toimialueen ohjauskoneelle, missä tietokone sijaitsee aktiivihakemiston hierarkiassa (toimipaikka, toimialue, OU eli organisaatioyksikkö) ja mitkä ryhmäkäytäntöobjektit koskettavat tietokonetta tai käyttäjää. (Mar-Elia 2008.)

Kun lista ryhmäkäytäntöobjekteista on saatu luotua, suoritetaan toisessa vaiheessa ryhmäkäytäntölaajennusten prosessointi. Jokainen rekisteröity ryhmäkäytäntölaajennus prosessoi kaikki ryhmäkäytäntöobjektit, joissa on määritelty asetuksia tälle ryhmäkäytäntölaajennusten alueelle. Rekisteri tai hallintamallien ryhmäkäytäntölaajennukset suoritetaan esimerkiksi aina ensin kaikissa tapauksissa ja ne prosessoidaan kaikissa ryhmäkäytäntöobjekteissa joissa näitä asetuksia on määritelty. (Mar-Elia 2008.)

Näiden seikkojen takia usein päivittyvät ryhmäkäytännöt kannattaakin määritellä omaan funktionaaliseen ryhmäkäytäntöobjektiin. Kuva 2 osoittaa, kuinka ryhmäkäytännössä A muutettu suojausasetus aiheuttaa kaikkien kolmen ryhmäkäytännön prosessoinnin. Tämä johtuu siitä, että ryhmäkäytäntöjen prosessointi tietää ryhmäkäytäntöobjektin A muuttuneen, mutta ei tiedä, mitä sen sisällä on muutettu. Tästä syystä koko ryhmäkäytäntöobjekti pitää prosessoida. Koska ryhmäkäytäntöobjektissa on määritelty myös rekisteriasetuksia, pitää myös ryhmäkäytäntöobjektit B ja C prosessoida, jotta tietokone saa kaikki hierarkian mukaiset asetukset ja voi päätellä, mitkä koskettavat sitä. (Mar-Elia 2012a.)



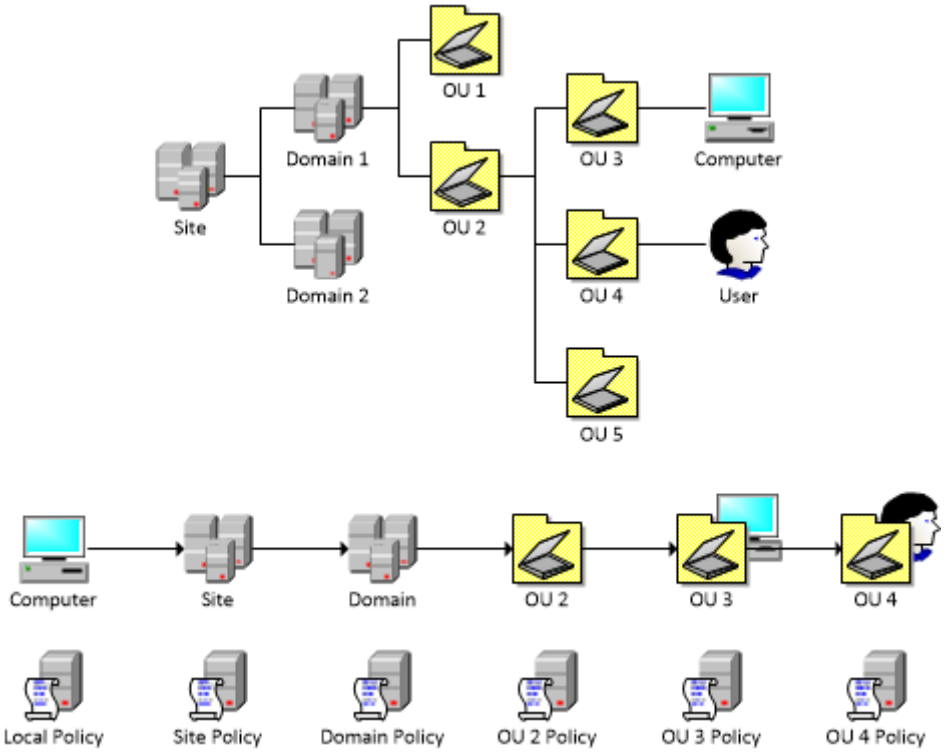
Kuva 2. Ryhmäkäytäntölaajennusten ryhmittämisen vaikutus suorituskykyyn (Mar-Elia 2012a.)

3.6 Milloin prosessointi tapahtuu?

Ryhmäkäytäntöjä prosessoidaan tietokoneessa tasojen mukaan. Tärkeysjärjestys on kuitenkin käänteinen. Toisin sanoen OU:hun määritelty ryhmäkäytäntöobjekti on vahvempi kuin toimialueelle määritellyn ryhmäkäytäntöobjekti (Kuva 3). Ryhmäkäytännöt prosessoidaan seuraavasti:

1. Lokaalit ryhmäkäytäntöobjektit (jos niitä on tietokoneelle määritelty)
2. Toimipaikan ryhmäkäytäntöobjektit
3. Toimialueen ryhmäkäytäntöobjektit
4. Organisaation ryhmäkäytäntöobjektit
5. *Isäntä* OU:n ryhmäkäytäntöobjektit
6. *Lapsi* OU:n ryhmäkäytäntöobjektit

(It Free Training, n.d.)



Kuva 3. Ryhmäkäytäntöjen prosessointikaavio sisäänkirjautumisen yhteydessä

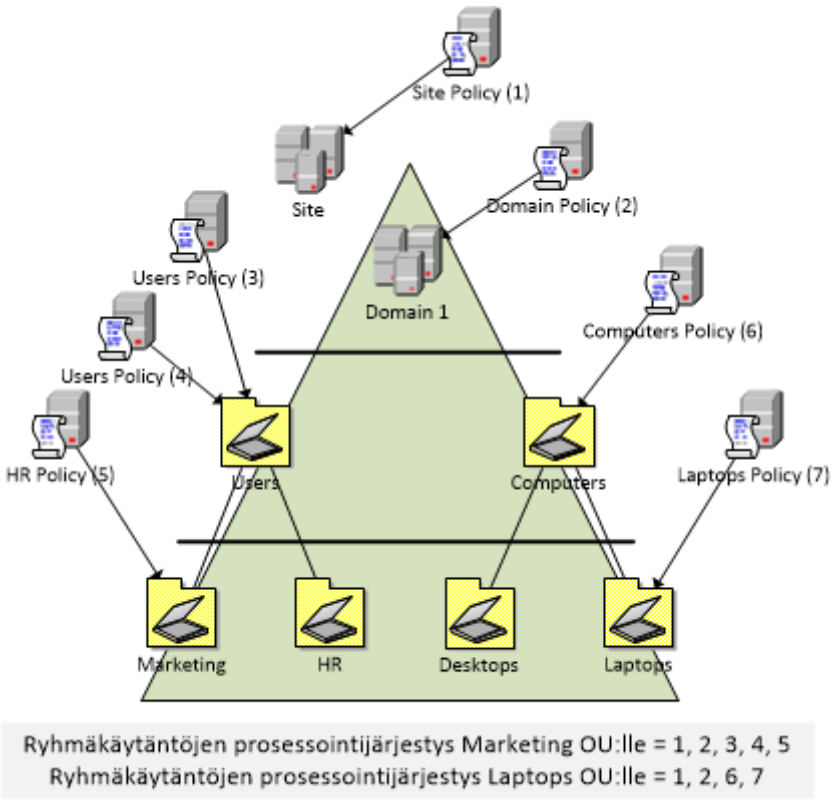
Microsoft on rakentanut ryhmäkäytäntöjen prosessointiin sisäänrakennetun optimoinnin. Jos mitään asetuksia ympäristössä ei ole muuttunut, kun viimeksi ryhmäkäytännöt prosessoitiin, ei tietokoneella tai käyttäjällä myöskään suoriteta ryhmäkäytäntöjen prosessointia. Ryhmäkäytäntöjen uudelleenprosessointi tapahtuu, jos ryhmäkäytäntöjen lista on muuttunut, käyttäjän tai tietokoneen ryhmäjäsenyys on muuttunut, WMI-suodatus on muuttunut tai ryhmäkäytännön versionumero on eri kuin tietokoneen paikallisessa rekisterissä. (Mar-Elia 2008.)

Prosessointia tarkasteltaessa on huomioitava, että ryhmäkäytäntöpreferenssin osiotason kohdistaminen (Item-Level Targeting) ei vaikuta tähän muutospäätelmään. Preferenssien osiotason kohdistaminen suoritetaan aina viimeisenä. (Mar-Elia 2012b.)

3.7 Ryhmäkäytäntöobjektien periytyminen ja arvojärjestys

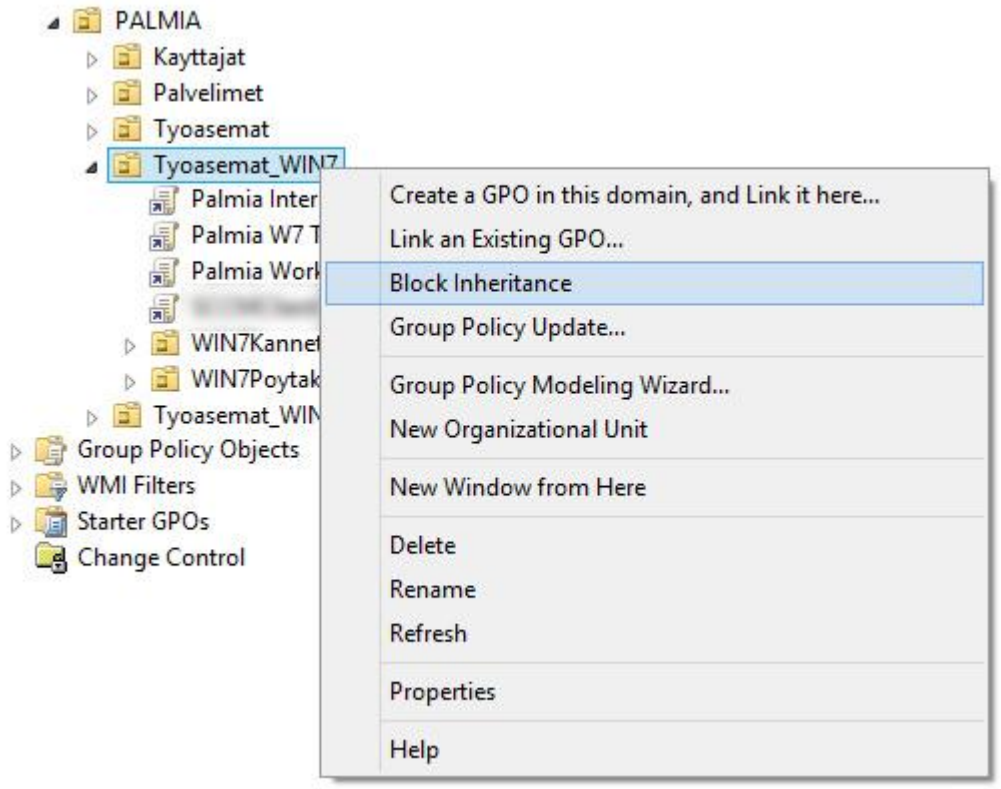
Ryhmäkäytäntöasetuksia voidaan määritellä useassa ryhmäkäytäntöobjektissa ja ne voivat olla toisiinsa nähden ristiriidassa. Yhdessä ryhmäkäytäntöobjektissa voidaan sallia jokin asetus, kun taas toisessa se voidaan kieltää ja kolmannessa siihen ei oteta kantaa lainkaan. Näissä tapauksissa ryhmäkäytäntöjen arvojärjestys vaikuttaa siihen, mikä asetuksista jää voimaan. (Holme, ym. 2008, 257–262.)

Arvojärjestyksen voi tarkistaa GPMC-työkalulla toimialueen tai OU:n Group Policy Inheritance -välilehdeltä – mitä pienempi numero sitä arvokkaampi ryhmäkäytäntöobjeki on. Toimipaikalla, toimialueella tai OU:ssa voi olla useita linkitettyjä ryhmäkäytäntöobjekteja. Niiden arvojärjestys määräytyy sen mukaan, kuinka korkealle ryhmäkäytäntöobjekti on määritetty listalla. Ryhmäkäytäntöobjektien arvojärjestystä voi myös käsin muuttaa OU:n sisällä. Kuva 4 osoittaa kuinka ryhmäkäytäntöobjektien periytyminen tapahtuu oletuksena. (Holme, ym. 2008, 257–262.)



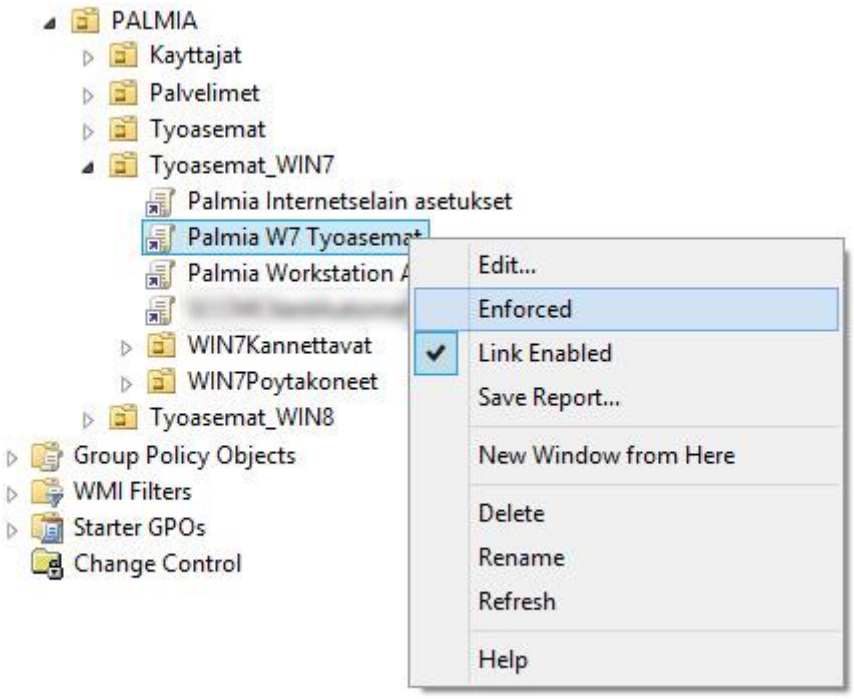
Kuva 4. Ryhmäkäytäntöjen oletusprosessointijärjestys (Holme, ym. 2008, 257–262.)

Joskus aktiivihakemiston suunnittelussa joudutaan tekemään kompromisseja ja tulee vastaan tilanteita, joissa ylhäällä hierarkiassa määritellyt ryhmäkäytäntöobjektit tulisi estää alemmalla tasolla. Tätä varten voidaan käyttää Block Inheritance -määritystä (Kuva 5) toimialue- tai OU-tasolla. Määritys estää kaikkien ylhäältä tulevien ryhmäkäytäntöasetuksien voimaan tulon alemmalla tasolla. Vaikka Block Inheritance -määritys on helposti määriteltävissä, tulisi aktiivihakemiston suunnittelussa pyrkiä siihen, että sitä tulisi käyttää harvoin, jos ollenkaan. (Holme, ym. 2008, 257–262.)

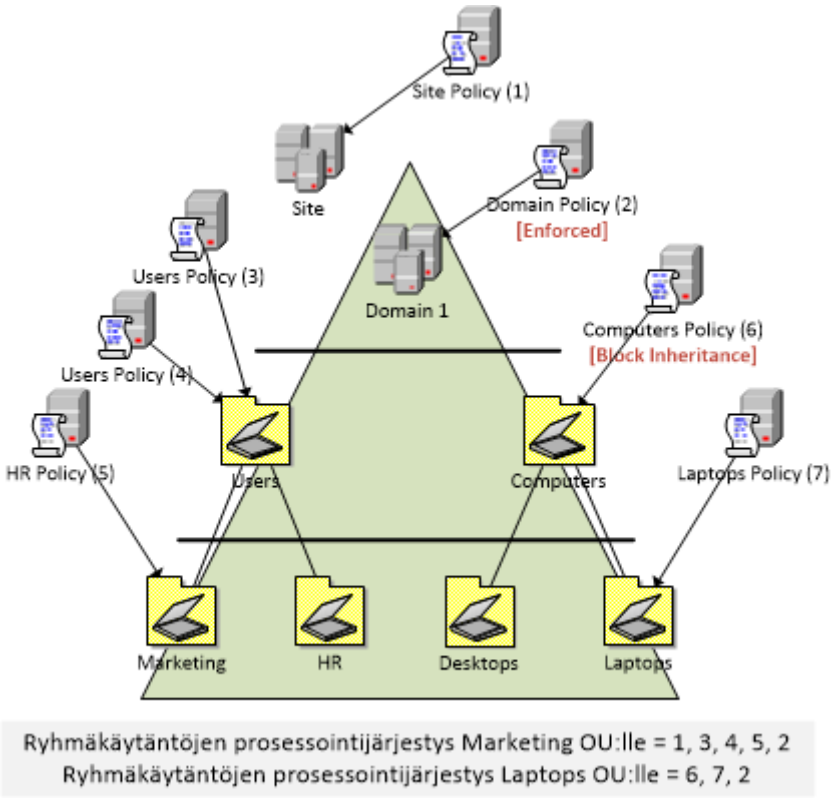


Kuva 5. Block Inheritance -tilan määrittäminen

Ryhmäkäytäntöasetuksia voidaan myös pakottaa päälle Enforced-määrityksellä (Kuva 6). Pakottaminen ohittaa kaikki Block Inheritance -määritykset ja lisää ryhmäkäytäntöobjektin arvojärjestyksessä listan ensimmäiseksi. Kuva 7 kuvataan kuinka Enforced- ja Block Inheritance -määritykset vaikuttavat ryhmäkäytäntöobjektien prosessointiin ja arvojärjestykseen. (Holme, ym. 2008, 257–262.)



Kuva 6. Enforced-tilan määrittäminen



Kuva 7. Ryhmäkäytäntöjen prosessointi, kun käytössä on Enforced- ja Block Inheritance -määritykset (Holme, ym. 2008, 257–262.)

Vaikka Enfroced-määritys ohittaa kaikki Block Inheritance -määritykset, sillä voidaan myös pakottaa jokin asetus toimialuetasolta kaikkiin työasemiin ja varmistua sen käyttöönotosta, vaikka alemmalla tasolla olisikin määritelty sama asetus toisin. (Holme, ym. 2008, 261.)

4 HALLINTATYÖKALUT

Hallintatyökaluja tarvitaan ryhmäkäytäntöjen määrittämiseen ja raportointiin. Raportoinnin avulla voidaan todentaa, mitä asetuksia tietokoneelle on mennyt läpi ja mitä ei. Raportointi on erittäin tärkeää, kun suoritetaan vianselvitystä. Työkaluilla on myös mahdollista mallintaa ryhmäkäytäntöasetuksien vaikutuksia käyttäjässä tai tietokoneessa ilman ryhmäkäytäntöasetuksen käyttöönottoa.

4.1 Group Policy Management Console

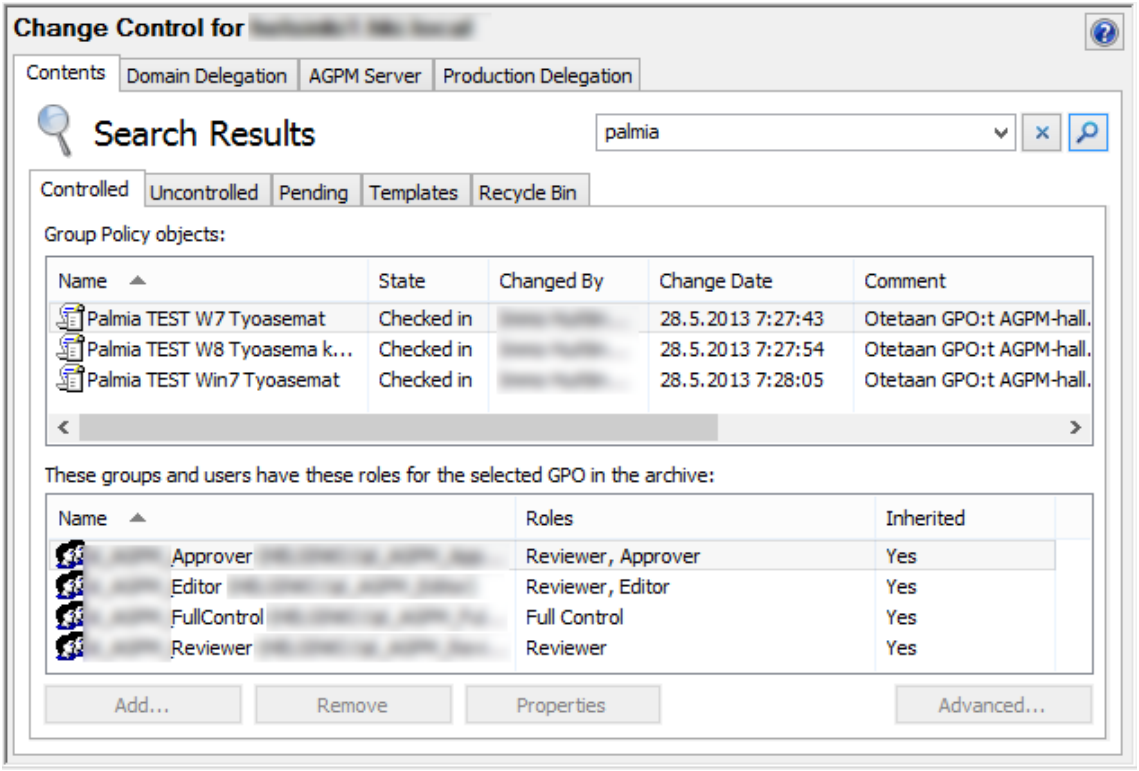
Group Policy Management Console, eli GPMC, on Microsoftin julkaisema standardityökalu yrityksen kaikkien ryhmäkäytäntöobjektien hallintaan. Työkalulla voidaan hallita, varmuuskopioida, palauttaa, tuoda ja viedä ryhmäkäytäntöobjekteja. Lisäksi työkalulla voidaan raportoida ja mallintaa ryhmäkäytäntöobjektien asetuksia. GPMC vaatii toimiakseen vähintään Windows XP:n SP1:llä tai uudemman version. Lisäksi Microsoft .NET Framework 1.1 pitää olla asennettuna tietokoneella. GPMC on ilmainen ja käyttäjällä tulee olla vain lisensoitu versio Windows Server käyttöjärjestelmästä. (Microsoft 2012.)

Melber (2008) kertoo, että Windows Server 2008 R2 julkaisun jälkeen on ollut mahdollista asentaa tietokoneelle RSAT, eli Remote Server Administration Toolkit. RSAT sisältää joukon Windows-palvelimien hallintaan tarkoitettuja työkaluja ja Group Policy Management Tools on yksi näistä työkaluista. Rux (2007) toteaa kuitenkin, että GPMC:stä puuttuu tärkeitä ominaisuuksia isojen ja monimutkaisten AD-ympäristöjen hallintaan, kuten version- ja muutoshallinta sekä offline-säilö.

4.2 Advanced Group Policy Management

Advanced Group Policy Management, eli AGPM, on Microsoftin Software Assurance -asiakkaille tehty työkalu parempaan ryhmäkäytäntöobjektien hallintaan. Varsinkin laajemmissa ympäristöissä, joissa ryhmäkäytäntöjen parissa työskentelee useampia henkilöitä, tämä on suositeltava työkalu. AGPM:llä voit kuitata ryhmäkäytäntöobjekteja sisään ja ulos sekä hallita versioita. Työkalun avulla on helppoa palauttaa asetukset ennalleen, jos jokin meni pieleen. Suurissa ympäristöissä, joissa on useita ylläpitäjiä, on kahden ylläpitäjän mahdollista muokata samaan aikaan samaa ryhmäkäytäntöobjektia toisistaan tietämättä. AGPM:n avulla tällaista tilannetta ei pääse muodostumaan, koska muokatakseen ryhmäkäytäntöobjektia, se on pakko kuitata ulos, jolloin toinen käyttäjä ei saa sitä muokkauksen alle, ennen kuin se on kuitattu takaisin sisään. AGPM:llä voidaan myös rauhassa

muokata asetuksia offline-tilassa ja myöhemmin ottaa ne käyttöön. (Burchill 2010.)

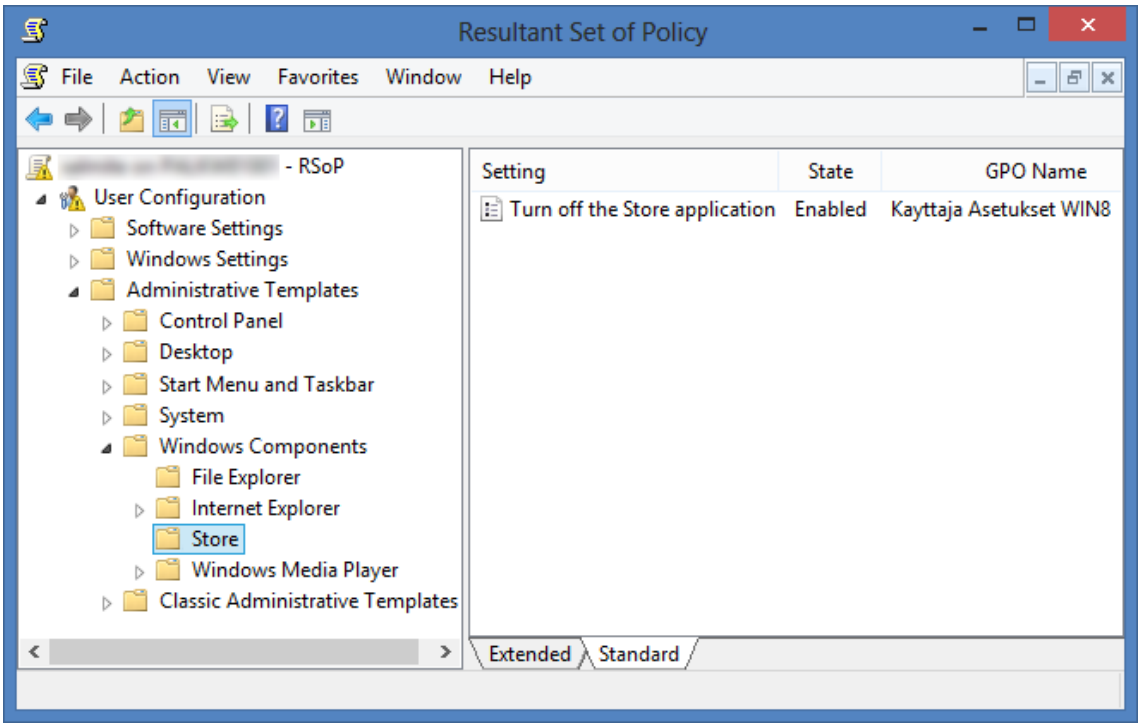


Kuva 8. AGPM Change Control -näkymä

4.3 Resultant Set of Policy

Eräs ryhmäkäytäntöobjektien hallinnan haasteista on todentaa mitkä asetukset tietokoneeseen tai käyttäjään loppujen lopuksi kohdentuvat. Tämä ongelma esiintyy varsinkin suurissa ympäristöissä, joissa määritellään paljon ryhmäkäytäntöobjekteja. Resultant Set of Policy, eli RSoP, ratkaisee tämän ongelman. RSoP-työkalulla voidaan tarkastaa yksittäisellä tietokoneella mitä asetuksia määritellään ryhmäkäytäntöobjekteilla ja mikä ryhmäkäytäntöobjekti jää viimeisenä voimaan, eli on niin sanottu voittava asetus. (Microsoft 2003b.)

RSoP:n raportoinnissa on kaksi erilaista tilaa, suunnittelu- ja diagnostiikkatilat. Suunnittelutilassa voidaan simuloida mitä jos -skenaario sijoittamalla kuvitteellinen käyttäjä valitun OU:n alle ja tietokone toisen OU:n alle ja tarkastelemalla, mitä ryhmäkäytäntöobjekteja niihin kohdistuu ja mitkä asetukset jäävät voimaan. Diagnostiikkatilassa voidaan raportoida tietokoneelta, mitkä asetukset siihen jo vaikuttavat. (Microsoft 2003b.)



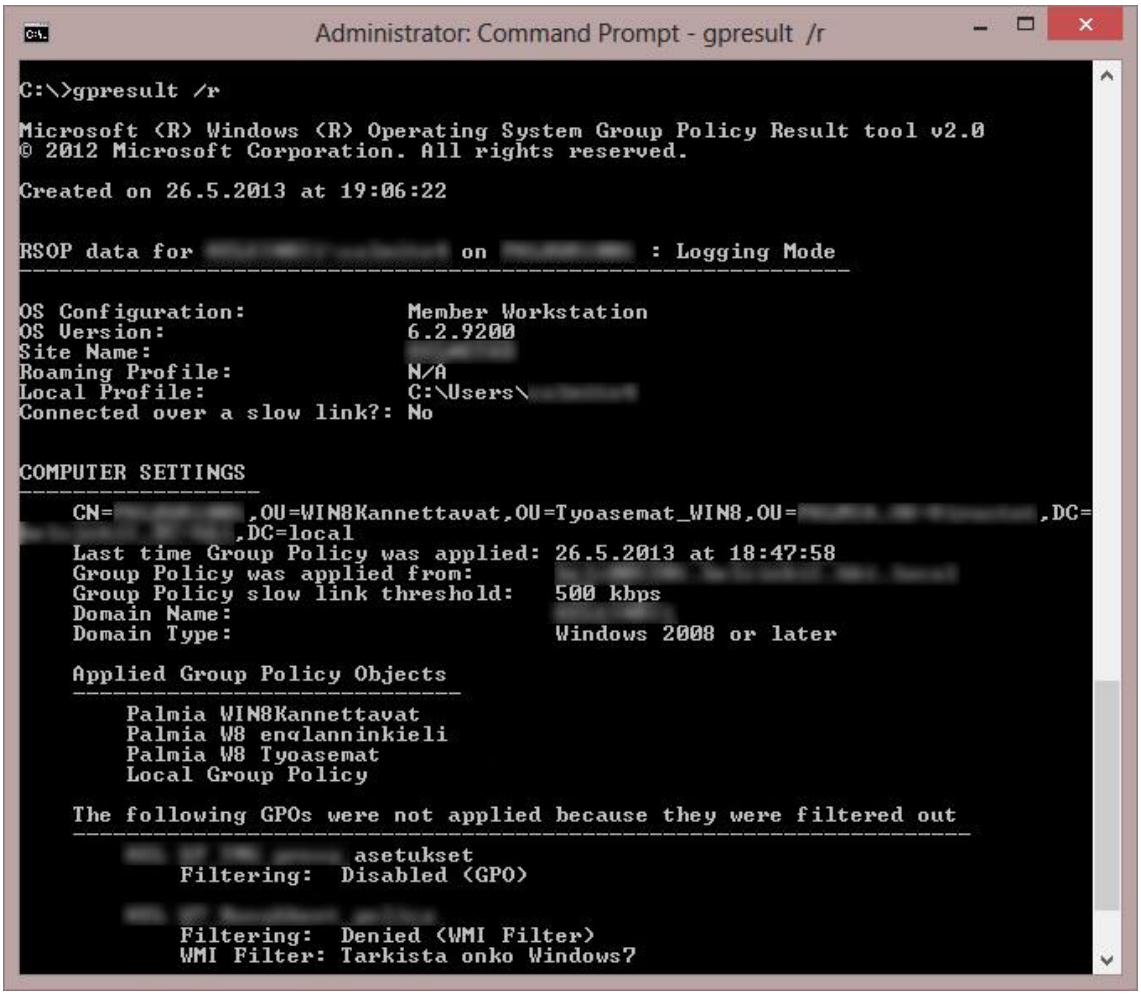
Kuva 9. RSoP-raportti käyttäjäasetuksista

4.4 Gpupdate ja Gpresult

Gpupdate on komentorivipohjainen komento. Gpupdate korvasi aikaisemmin Windows 2000 -käyttöjärjestelmässä käytetyn SECEDIT /refreshpolicy -komennon (Microsoft n.d.). Gpupdate-komennolla voit pakottaa tietokoneen prosessoimaan ryhmäkäytännöt, jolloin ei esimerkiksi tarvitse odottaa seuraavaa taustaprosessointia. (Microsoft n.d.; Holme ym. 2008, 235.)

Gpupdate-komento simuloi normaalia taustaprosessointia, kun taas gpupdate /force pakottaa prosessoimaan kaikki ryhmäkäytännöt huolimatta siitä milloin ne on viimeksi prosessoitu tai onko niissä muuttunut mitään asetuksia (ks. luku 3.6). (Mar-Elia 2012a; Burchill 2010; Holme ym. 2008, 235.)

Gpresult on myös komentorivipohjainen komento, jolla voidaan todentaa mihin ryhmiin tietokone ja käyttäjä kuuluvat, mitä ryhmäkäytäntöjä niiden OU- hierarkiassa on sekä mitä ryhmäkäytäntöjä otetaan käyttöön ja mitä on suodatettu pois. Gpresult on nopea ja helppo työkalu tietokoneeseen ja käyttäjiin kohdistuvien ryhmäkäytäntöjen todentamiseen. (Microsoft 2001.)



Kuva 10. Gpresult-työkalun tulokset Windows 8 -tietokoneessa, joka on toimialueen jäsen.

4.5 Kolmannen osapuolen ilmaiset työkalut

Mar-Elia (2012b) viittaa esityksessään WMI Filter Validation Utility -työkaluun, jolla pystytään hakemaan kaikki AD:ssa olevat WMI-suodattimet ja tarkastelemaan niitä mitä tahansa AD:ssa olevaa tietokonetta vasten. WMI Filter Validation Utility kertoo läpäiseekö tarkastelussa oleva tietokone WMI-suodatuksen ja kuinka kauan sen prosessointiin kuluu aikaa. Työkalua pitää käyttää palvelimelta, koska paikalliselta tietokoneelta suoritettuna prosessointiaika on virheellisesti 0 ms. GPTime on myös Mar-Elian (2012b) suosittelema sovellus, jolla pystytään tarkistamaan yleisen ryhmäkäytäntöjen prosessointiaika tietokoneessa.

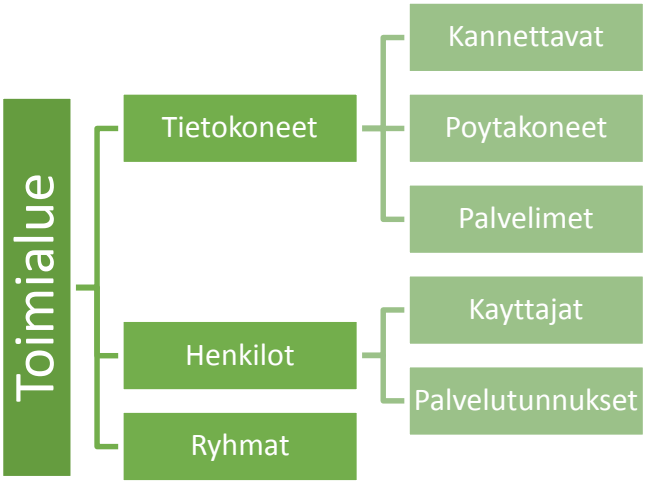
5 PARHAAT KÄYTÄNNÖT

Parhaita käytäntöjä käyttöönotettaessa on ensin määriteltävä tavoitetila mihin pyritään. Parhaat käytännöt saattavat olla ristiriidassa keskenään ja se johtuu vain siitä, että toiset painottavat esimerkiksi ylläpidon helppoutta kun toiset taas turvallisuutta. Sellaista ratkaisua on vaikea löytää, missä voidaan soveltaa täysin kaikkia parhaita käytäntöjä, yleensä vaaditaan siis kompromisseja jonkin verran. Mar-Elia (2012a) esittää, että tavoitetilaksi

kannattaa valita joko vähäinen vaikutus loppukäyttäjälle, turvallisuuden ja työaseman koventamisen tasapaino tai vähäinen hallittavuus ja monimutkaisuus.

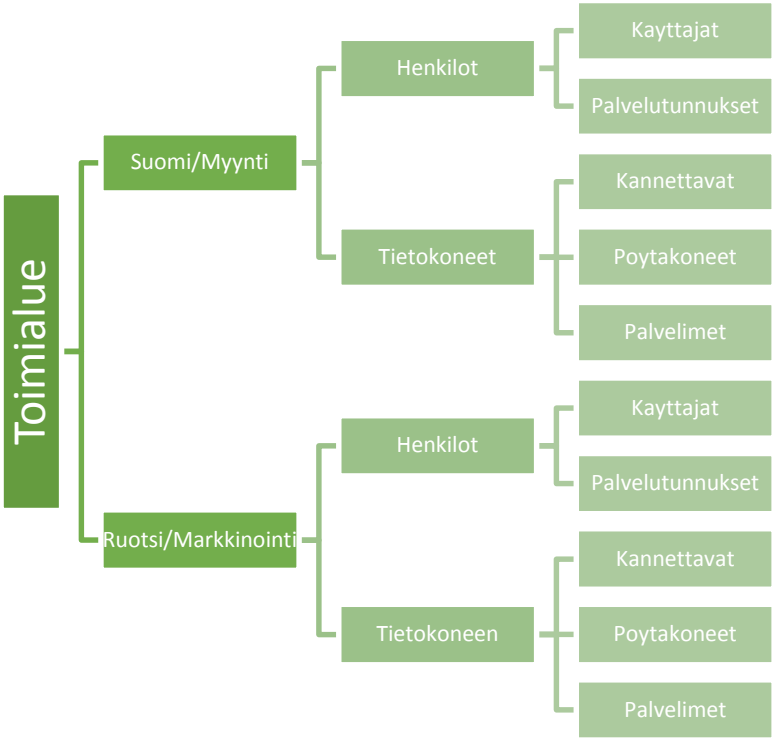
5.1 Suuren vaikutuksen käytännöt

Aktiivihakemiston rakenne on aktiivihakemistoa käyttöönotettaessa ensimmäinen suuri päätös. Käytännössä on kaksi vaihtoehtoa, joilla kummallakin on eri tavoitteet. Voidaan rakentaa aktiivihakemiston rakenne, jossa painotetaan OU-rakennetta turvallisuuden, ylläpidon ja sovellusten näkökannasta. Toinen vaihtoehto on lähestyä asiaa ryhmäkäytäntöjen kannalta. Tällöin keskitytään ryhmäkäytäntöjen kohdistamisen helppouteen, käyttöjärjestelmien (palvelimet ja työasemat) erilaisuuteen. (Mar-Elia 2012b.)



Kuva 11. Aktiivihakemiston rakenne, joka suosii turvallisuutta ja ylläpitoa (Mar-Elia 2012b).

Kuva 11 esittämä rakenne on yksinkertainen, koska kaikki tietokoneet ovat selkeästi yhdessä OU-haarassa ja kaikkiin voidaan kohdistaa helposti ryhmäkäytäntöasetuksia Tietokoneet-haarasta. Huonoa on kuitenkin juuri se, että kaikki käyttäjät ja tietokoneet ovat samassa OU:ssa. Aktiivihakemiston rakenteen suunnittelussa tulisi välttää liian matalaa OU-rakennetta. Esimerkiksi, jos kaikki käyttäjät ovat samassa OU:ssa, on myöhemmin hankala kohdistaa asetuksia tietylle käyttäjäryhmälle.



Kuva 12. Aktiivihakemiston rakenne, joka rakentuu maantieteellisen tai organisaation mukaisesti ryhmäkäytäntöjen hallinnan kautta (Mar-Elia 2012b).

Kuva 12 esittämässä mallissa hyvänä voi pitää sitä, että eri maantieteelliset sijainnit tai organisaatiot ovat selkeästi omissa OU-haaroissaan, jolloin niiden hallinnointi tapahtuu erillään niin, että ryhmäkäytäntöobjektit voidaan linkittää mahdollisimman lähelle. Huonoa on taas se, että organisaatioilla on tapana muuttua koko ajan, mikä saattaa aiheuttaa suuria aktiivihakemiston rakennemuutoksia. (Mar-Elia 2012b.)

5.1.1 Monoliittinen vai funktionaalinen ryhmäkäytäntöobjekti

Aktiivihakemiston rakenteen jälkeen ehkä toiseksi tärkein asia on määrittää miten ryhmäkäytäntöobjekteja luodaan. Kuten aktiivihakemiston rakenteessa, tässäkin kaksi vaihtoehtoa, joissa kummassakin on hyvät ja huonot puolensa. Monoliittisessa ryhmäkäytäntöobjektissa, jota voisi kutsua lähes kaiken kattavaksi ryhmäkäytäntöobjektiksi, on suuri määrä asetuksia eri ryhmäkäytäntölaajennusten alueelta. Monoliittisen ryhmäkäytäntöobjektin tarkoitus on kattaa valtaosa asetuksista ja kohdistaa ne pääsääntöisesti kaikkiin tietokoneisiin tai käyttäjiin. (Mar-Elia 2012a.)

Monoliittinen ryhmäkäytäntöobjekti on hyvä myös siinä tapauksessa, jos halutaan luovuttaa hallinta ryhmäkäytäntöobjektin ylläpitoon toiselle taholle. Kuva 12 esimerkiksi voitaisiin luoda monoliittinen ryhmäkäytäntöobjekti markkinointiosastolle ja delegoida hallintaoikeudet markkinoinnin IT-tukeen, jolla olisi oikeus muokata tätä ryhmäkäytäntöobjektia, mutta ei oikeutta luoda uusia ryhmäkäytäntöobjekteja markkinoinnin OU-haaraan. (Mar-Elia 2012b.)

Toinen vaihtoehto on luoda funktionaalinen ryhmäkäytäntöobjekti. Funktionaalisella ryhmäkäytäntöobjektilla on tarkoitus hallita vain pientä osaa asetuksista ja yleensä yhden ryhmäkäytäntölaajennuksen alueelta. Microsoft Office 2010 tai Internet Explorer ovat hyviä esimerkkejä funktionaalisesta ryhmäkäytäntöobjektista. Funktionaalista ryhmäkäytäntöobjektia on hyvä hyödyntää esimerkiksi tietokoneen paikallisen järjestelmänvalvojan salasanan vaihtamisessa, varsinkin jos sitä vaihdetaan usein. Kuten luvussa 3.5 on esitetty, yksi muutos monoliittisessa ryhmäkäytäntöobjektissa aiheuttaa koko ryhmäkäytäntöobjektin prosessoinnin ja yleensä samalla kaikkien ympäristön ryhmäkäytäntöobjektien prosessoinnin.

Taulukko 1. Monoliittisen ja funktionaalisen ryhmäkäytäntöobjektin vertailu (Mar-Elia 2008.)

Asia	Monoliittinen GPO	Funktionaalinen GPO
Delegointi/ eristäminen	Hankalaa, koska jokainen ryhmäkäytäntöobjekti voi sisältää asetuksia useilta alueilta ja voit tehdä delegointia ryhmäkäytäntöobjektitasolla, et asetustasolla	Helppoa, koska jokainen ryhmäkäytäntöobjekti sisältää yhden alueen asetuksia. Esim. sovellusasennus ryhmäkäytäntöobjektin voi delegoida sovellusasennuksista vastaavalle taholle jne.
Hallinta ja Monimutkaisuus	Mahdollisesti yksinkertaisempi ja helpompi hallita, koska jokainen ryhmäkäytäntöobjekti sisältää kaikki asetukset yhdessä paikassa.	Mahdollisesti vaikeampaa, koska suurempi määrä ryhmäkäytäntöobjekteja tarkoittaa enemmän paikkoja, joista etsiä ongelmia.
Suorituskyky	Mahdollisesti hitaampi. Riippuu siitä, mitä ryhmäkäytäntölaajennusta käytetään. Jos yksi ryhmäkäytäntöobjekti muuttuu, kaikki ryhmäkäytäntölaajennukset pitää ajaa läpi vasten kaikkia käytettävissä olevia ryhmäkäytäntöobjekteja.	Riippuu siitä, kuinka monta ryhmäkäytäntöobjektia on käytössä ja kuinka usein ne muuttuvat. Suorituskyky voi olla parempi dynaamisissa ympäristöissä verrattuna monoliittisiin ryhmäkäytäntöobjekteihin

5.1.2 80/20 -sääntö

Säännön tai suosituksen idea on määrittää valtaosa asetuksista samaan ryhmäkäytäntöobjektiin, jotka vaikuttavat kaikkiin tietokoneisiin tai käyttäjiin. OU-rakenne tulisi suunnitella niin, että 80 % asetuksista voidaan määritellä linkittämällä ryhmäkäytäntöobjekti niin lähelle kuin mahdollista. Loppujen 20 % asetuksien määrittäminen vaatii jonkinasteisen kompromissin, eivätkä niinkään aktiivihakemiston rakenteen muutoksia. (Mar-Elia 2012b.) Suositusta voi tulkita myös niin, että 80 % asetuksista määritellään monoliittiseen ryhmäkäytäntöobjektiin (Burchill 2010).

5.1.3 Käytä ensisijaisesti olemassa olevia ryhmäkäytäntöobjekteja

Olemassa olevien ryhmäkäytäntöobjektien uudelleen käyttäminen on erittäin suositeltavaa kahdestakin syystä. Pienempi määrä ryhmäkäytäntöobjekteja on ylläpidon kannalta aina helpompi vaihtoehto, mutta ryhmäkäytäntöobjektien määrää ei kannata kasvattaa turhaan myöskään sen takia, että jokainen niistä vie tilaa noin 5 mb aktiivihakemiston SYSVOL-kansiossa. Jokainen ryhmäkäytäntöobjekti pitää muuttuessaan replikoida, eli kopioida kaikille aktiivihakemistopalvelimille. Tällöin satojen, jopa tuhansien ryhmäkäytäntöobjektien ympäristöissä tästä voi kehittyä suorituskykyongelma. (Burchill 2010.)

Phillips (2008) kertoo, että hajautettu tiedostojärjestelmäreplikointi (DFS-R), jota pystytään hyödyntämään Windows Server 2008 -käyttöjärjestelmästä lähtien, poistaa suureksi kasvaneen SYSVOL-kansion käsittelyn ongelman. Muuttunutta ryhmäkäytäntöobjektia ei tarvitse replikoida kokonaisuudessaan – riittää kun muuttuneet bitit replikoidaan. On silti hyvä käytäntö pitää ryhmäkäytäntöobjektien lukumäärä mahdollisimman vähäisenä ja tehdä uusi ryhmäkäytäntöobjekti vain jos käyttäjä- tai tietokoneryhmä on eri kuin olemassa olevissa ryhmäkäytäntöobjekteissa (Burchill 2010).

Kuva 3 esimerkissä OU 2:n alla on kolme OU:ta. Jos OU 4:ään ja OU 5:een haluttaisiin määritellä samat asetukset, mutta OU 3:een ei haluttaisi näitä asetuksia, ei ryhmäkäytäntöobjektia voitaisi linkittää OU 2:n alle, koska ne periytyisivät kaikkiin alemmalla tasolla oleviin objekteihin. OU 3:n voisi määrittää Block Inheritance -määrityksellä, mutta se estäisi kaikkien asetusten läpi pääsyn. OU 4:ään ja OU 5:een voitaisiin tehdä omat ryhmäkäytäntöobjektit, mutta identtisten asetusten tekeminen ei ole järkevää. Paras käytäntö onkin linkittää molempiin OU 4:ään ja OU 5:een sama ryhmäkäytäntöobjekti ja nimetä se kuvaavasti. (Burchill 2010.)

5.2 Ylläpitoa helpottavat käytännöt

Ryhmäkäytäntöobjektien järkevä nimeäminen on ensimmäinen käyttöä helpottava ja helposti käyttöönotettava käytäntö. Vaikka nimeäminen ei vaikuta millään tavalla ryhmäkäytäntöjen prosessointiin, on sillä suuri vaikutus ylläpitoon ja hallittavuuteen – huonosti nimetyillä ryhmäkäytäntöobjekteilla ympäristön saa erittäin sekavaksi. Nimeämisessä on syytä käyttää yhteneväistä tapaa. Hyvä käytäntö on välttää sanoja Policy tai GPO ryhmäkäytäntöobjektin nimessä, koska on selvää, että kyseessä on Group Policy Object. (Burchill 2010.)

Toinen suositeltava sääntö on käyttää ryhmäkäytäntöobjektin nimessä samaa nimeämiskaavaa kuin OU-rakenteessa. Tällä käytännöllä on helppo ymmärtää mihin kyseinen ryhmäkäytäntöobjekti vaikuttaa. Ryhmäkäytäntöobjektien nimet voidaan vaihtaa olemassa olevaan ympäristöön ilman riskiä, että ympäristöön tulee ongelmia. Nimen muutoksen jälkeen kohde-tietokoneet prosessoivat ryhmäkäytännöt uudestaan. (Burchill 2010.)

Huolimatta siitä, että nimeämiset eivät vaikuta suorituskykyyn lainkaan, ovat ne kuitenkin pieni asia, jolla ylläpidosta saadaan helpompaa kaikille

ylläpitäjille. Tämä korostuu varsinkin isoissa ympäristöissä, joissa on useita ryhmäkäytäntöjen ylläpitäjiä ja paljon ryhmäkäytäntöobjekteja. Nimeämisen lisäksi tilatiedon näyttäminen tietokoneen käynnistämisen ja sammuttamisen sekä kirjautumisen ja uloskirjautumisen yhteydessä voi olla hyödyllistä ylläpitäjille. Tietokonepuolen asetuksista pitää määrittää `Computer Configuration\Policies\Administrative Templates\System\Verbose vs. Normal Status Messages` -asetus päälle. Jos asetus ei ole päällä, asetus näyttää normaalit viestit, kuten Applying your personal settings, mutta kun asetuksen määrittää päälle, nähdään tarkemmat tiedot kuten Mapping Drives ja Applying Power Settings. Lisätiedon hyödyt ovat ylläpitäjille selkeät, koska sillä näkee mitä GP-prosessointia kone tekee parhaillaan ja tätä tietoa voi hyödyntää vianselvityksessä. Käyttäjille tästä asetuksesta voi myös olla hyötyä, ja näytössä näkyvästä lisätiedosta saattaa käyttäjälle tulla tunne, että tietokone toimii nopeammin. (Burchill 2009.)

5.2.1 Muutosprosessi ja testiympäristö

Yrityksen koosta huolimatta erittäin tärkeää ylläpidon kannalta on luoda perusperiaatteet muutoksenhallintaan. Muutoksenhallinta käsittää ohjeistuksen, kuinka siirtyä nykytilasta uuteen tavoitetilaan. Muutoshallinnan sydämessä on prosessi, ilman kunnollista prosessia ei muutosta hallita. Hyvällä prosessilla kaikki ylläpitäjät pystyvät luomaan, muokkaamaan ja poistamaan ryhmäkäytäntöobjekteja hallitusti. Prosessissa pitää vähintään määritellä, kuka saa tehdä mitä. Vähimmäisvaatimuksena voi pitää suunnittelija- ja hyväksyjäroolien määrittämistä. Hyväksyjä on rooli, joka arvioi ryhmäkäytäntöobjektin muutokset ennen niiden viemistä tuotantoon. Erityisen suositeltava paras käytäntö onkin käyttää prosessia, jossa tehdään muutettavien asioiden tarkastusta ja hyväksyntää. (Shields 2012.)

Suuren ympäristön hallinnassa on tärkeää testata kaikki muutokset ryhmäkäytännöissä ennen niiden viemistä tuotantoon. Paras vaihtoehto on luoda täysin identtinen AD, jossa asetuksia voidaan testata täysin tuotantoympäristöä vastaavassa ympäristössä. Käytännössä identtisen AD:n rakentaminen voi olla yritykselle kallista ja sen ylläpito vaatii paljon resursseja. Kevyempänä ratkaisuna on luoda olemassa olevaan tuotantoympäristöön OU-rakenne testausta varten. Tällöin OU-rakenne voi olla edelleen identtinen tuotantoympäristöstä ja testi-OU:ssa voi olla kopiot jokaisesta ryhmäkäytäntöobjektista. Tässä vaihtoehdossa ei ole vaaraa, että testauksessa olevia asetuksia päätyy vahingossa tuotantoympäristöön, koska asetukset kohdistetaan OU-tasolla. (Burchill 2010.)

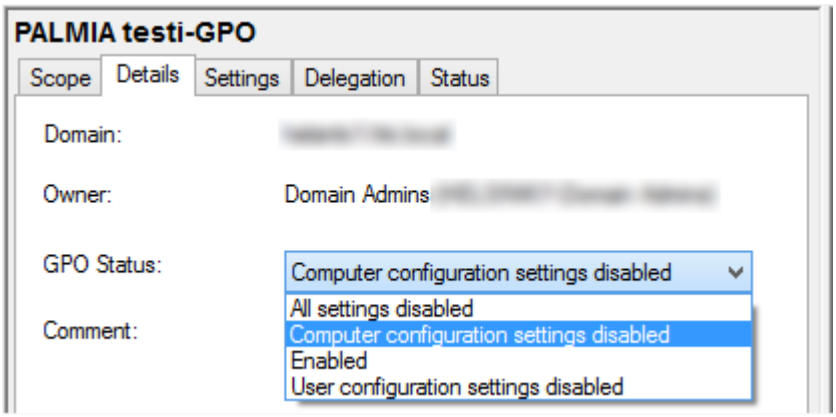
Kevyimpänä vaihtoehtona on luoda tuotantoympäristöön sisälle testiryhmäkäytännöt. Tällöin kohde tietokoneet ja käyttäjät suodatetaan testiryhmän avulla. Tämän vaihtoehdon etu on erittäin vähän ylläpitoa vaativa testiympäristö, mutta kääntöpuolena on suuri riski sekoittaa testauksessa olevia ryhmäkäytäntöjä tuotantoympäristöön inhimillisen virheen seurauksena. (Burchill 2010.) Oli ratkaisu näistä vaihtoehdoista mikä tahansa, on erittäin tärkeää, että ryhmäkäytäntöihin tehtäviä muutoksia testataan ennen niiden viemistä tuotantoympäristöön.

5.2.2 Ryhmäkäytäntöjen kohderyhmät

Ryhmäkäytäntöjä voidaan määrittää linkittämällä ne OU:hun tai suodattamalla niitä ryhmillä tai WMI-suodattimilla. Suositeltavaa on linkittää ryhmäkäytäntöobjekti niin lähelle kuin mahdollista kohdetietokoneita tai käyttäjiä, koska prosessoinnissa ei tarvitse päätellä erikseen mihin ryhmäkäytäntöobjekti vaikuttaa. Ryhmäkäytäntöobjektin linkittäminen ylemmäs OU-rakenteessa ja sen suodattaminen, joko ryhmillä tai WMI-suodattimilla voi olla myös hyvä tapa. Suodattamisessa joudutaan kuitenkin aina erikseen prosessoimaan sen vaikutus OU-rakenteen sisällä joko ryhmän jäseniin tai prosessoimalla WMI-suodattimella esimerkiksi tietokoneen käyttöjärjestelmä ja määrittämään sen perusteella, tulevatko ryhmäkäytännöt voimaan vai ei. Valinta linkittämisen tai suodattamisen välillä pitää aina tehdä kyseessä olevan AD-rakenteen mukaisesti. Tietynlaisessa AD-rakenteessa voi olla mahdotonta käyttöönottaa ryhmäkäytäntöobjektia linkittämällä, jolloin suodattamista on pakko käyttää. Lisähaastetta suodattamiseen tuo ryhmäkäytäntöpreferenssit, joissa on mahdollista suodattaa jokainen asetus erikseen. Tällöin ryhmäkäytännön prosessointi muodostuu sitä hitaammaksi mitä enemmän suodatuksia on käytetty ryhmäkäytäntöpreferensseissä. (Mar-Elia 2012b.)

WMI-suodattimia kannattaa käyttää tilanteissa, joissa suodattamiseen kuluva aika on nopea, kuten käyttöjärjestelmän tunnistamiseen (liite 1). Kaikissa tilanteissa ei ole järkevää tai edes mahdollista tehdä omaa OU:ta käyttöjärjestelmäversion mukaisille työasemille, tällöin WMI-suodatus on hyvä vaihtoehto. (Mar-Elia 2012b.)

Yleisesti ryhmäkäytäntöobjektiin tehdään asetuksia vain joko käyttäjä- tai tietokoneasetuksiin, jolloin toinen osa-alue jää käyttämättömäksi. Jos tätä käyttämätöntä osa-aluetta ei poisteta käytöstä, myös se käsitellään prosessoinnin aikana, vaikka siinä ei ole asetuksia. Hyvä käytäntö on tällaisissa tapauksissa estää käyttämättömät tietokone- tai käyttäjäasetukset. Ensinnäkin tämä selventää asetuksien määrittämistä, estää virhetilanteita ja tuo pienen suorituskyvyn parantumisen ryhmäkäytäntöobjekteja prosessoidessa. (Burchill 2010.)



Kuva 13. Ryhmäkäytäntöobjektin käyttäjä- tai tietokoneasetuksien estäminen

Tilanteissa, joissa on tarvetta sallia jollekin käyttäjäryhmälle erikoisvapauksia tai estää jotkin asetukset tietokoneella, on syytä käyttää GPO-

estoryhmää. Tällä ryhmällä voidaan estää asetukset tietyltä käyttäjä- tai tietokoneryhmältä helposti luomatta erikseen ryhmäkäytäntöä, joka toisi niille erivapauksia. Tässä tapauksessa on järkevää nimetä estoryhmä kuvaavasti, jos ryhmäkäytäntöobjektin nimi on Computers, on hyvä ja kuvaava nimi estoryhmälle Computers GPO Deny. (Burchill 2010.)

5.3 Vältettävät käytännöt

Ryhmäkäytäntöobjekteja on mahdollista säilyttää OU-rakenteessa käyttämättöminä, joko poistamalla niistä ryhmäkohdistus, määrittämällä GPO status tilaan All settings disabled tai poistaa ryhmäkäytäntöobjektin enabled-tila. Ryhmäkäytäntöobjekteja ei tule linkittää turhan takia OU-rakenteisiin, koska kaikki OU:ssa olevat ryhmäkäytäntöobjektin linkit tallennetaan ryhmäkäytäntösäilön gpLink-attribuuttiin ja siten ne pitää aina prosessoida läpi. Vaikutus ei ole kovin suuri, mutta se hidastaa prosessointia ja lisäksi vaikeuttaa ylläpitoa. (Mar-Elia 2012b.)

Ryhmäkäytännöillä on mahdollista määrittää asetuksia, jotka selvästi hidastavat ryhmäkäytäntöjen prosessointia. Voidaan esimerkiksi määrittää asetus, että jokainen ryhmäkäytäntölaajennus prosessoidaan, vaikka siinä ei ole tapahtunut muutoksia. Tämän kaltaiset asetukset ovat omiaan hidastamaan ryhmäkäytäntöjen prosessointia ja niitä tulisi ehdottomasti välttää. (Mar-Elia 2008.)

Mar-Elia (2012b) myös väittää, että useiden ryhmien käyttäminen ryhmäkäytäntöobjektin suodattamisessa hidastaa sen käsittelyä, joten useiden ryhmien käyttämistä tulisi välttää. Suositeltavaa olisikin kohdistaa asetukset OU-tasolla käyttäen Authenticated Users -ryhmää tai sitten yhtä ryhmää, joka sisältää kaikki tarvittavat käyttäjät tai tietokoneet.

Vaikka WMI-suodattimet on osoitettu hyväksi havaituiksi, kun ne ovat tarpeeksi yksinkertaisia ja nopeita prosessoida, voidaan niillä tehdä myös monimutkaisia ja hitaita suodattimia. WMI-suodattimien kanssa kannattaa olla tarkkana ja käyttää ainakin WMI Filter Test Utilityä nähdäkseen, kuinka kauan sen prosessointi kestää. Monimutkaisten tai liian monen WMI-suodattimen käyttöä tulisi välttää, koska niiden prosessointi voi kestää kauan. (Mar-Elia 2012b.)

Useat ryhmäkäytäntöjen asiantuntijat ovat sitä mieltä, että aktiivihakemisto tulisi suunnitella siten, että Enforced- tai Block Inheritance -määrityksiä tulisi välttää mahdollisimman paljon - niitä ei oikeastaan tulisi käyttää lainkaan. Tilanteissa, joissa on harkittava edellä mainittujen asetuksien määrittämistä, tulisi tarkemmin miettiä aktiivihakemiston rakennetta ja sitä, voitaisiinko siihen tehdä muutoksia. Mikäli kyseessä on hallinnollinen asia, jossa pyritään sulkemaan pois, etteivät alemman tason ylläpitäjät muuta asetuksia, kannattaisi tätä ongelmaa lähestyä ennemmin henkilöstöhallinnollisin keinoin, kuten ohjeistamalla. Ryhmäkäytäntöjen estämistä ja pakottamista ei suositella käytettäväksi lainkaan, koska se tekee ympäristön vianselvityksestä erittäin hankalaa. (Burchill 2010; Holme, ym. 2008, 260–262; Microsoft, n.d.)

Sovellusasennusten tekemistä ryhmäkäytännöillä tulisi välttää. Burchill (2010) kertoo, että ryhmäkäytännöillä on mahdollista asentaa MSI-sovelluspaketteja tietokoneille. Tämä on helppo tapa asentaa tavallisia sovelluksia tietokoneille, mutta jos verrataan sovellusjakeluihin varta vasten tehtyjä järjestelmiä, kuten SCCM:ää tai muita Microsoftin tai kolmansien osapuolien sovellusjakeluohjelmia, on ryhmäkäytännöillä tehdyt sovellusasennukset huomattavasti huonompi tapa. Yksi yleinen tapa on käyttää ryhmäkäytäntöasetusta uninstall this application when it falls out of the scope of management, joka siis poistaa sovelluksen tietokoneelta, kun se ei enää ole ryhmäkäytännön kohderyhmässä. Tällaisia tilanteita tulee vastaan, kun tietokonetili siirretään AD:ssa toiseen OU:hun tai kokonaan toiselle toimialueelle. Kun näin toimitaan, seuraavalla tietokoneen käynnistyksellä kaikki sovellukset poistetaan koneelta, jos niissä on ollut yllä mainittu asetus päällä, ja tämä saattaa kestää kauan aikaa. Pahimmillaan uudessa kohde-OU:ssa on määriteltynä samat sovellukset ja ne joudutaan sitten asentamaan uudelleen. Vaikka tätä asetusta ei olisikaan määritelty, niin tietokoneen tulee silti käsitellä sovellukset uudelleen repair- tai check toiminnolla.

Jos uninstall this application when it falls out of the scope of management -asetusta ei määritetä, johtaa se tilanteeseen, että käyttäjien tietokoneille kertyy paljon sovelluksia, jotka vaikuttavat tietokoneen suorituskykyyn ja vakauteen sekä jatkuvasti kasvaviin lisenssikustannuksiin. Ryhmäkäytännöillä voi ainoastaan asentaa MSI-sovelluspaketteja, siinä missä SCCM:llä ja muilla sovellusjakeluohjelmistoilla voi tehdä paljon laajemmin sovellusjakeluun liittyviä hallintatehtäviä. (Burchill 2010.)

6 PARHAIDEN KÄYTÄNTÖJEN TOTEUTUS

Tärkeä seikka ennen työn aloittamista oli määritellä, mikä on Palmian kannalta tavoiteltava tila, jotta pystyimme käyttöönottamaan siihen kohdistuvat parhaat käytännöt. Palmian tietohallinnon asiantuntijoiden kesken päädyimme siihen, että helppo ylläpidettävyys ja pieni vaikutus loppukäyttäjiin olivat ne tärkeimmät tekijät, joita muutoksella haluttiin saada aikaan. Toisin sanoen asetuksia pyrittiin optimoimaan siten, että ne olisivat nopeampia prosessoida tietokoneilla ja niin, että muutoksia olisi helppo hallita.

Työ aloitettiin nykytilan kartoituksella ja muutosehdotusten laatimisella. Muutosehdotusten laatimisen aikaan saimme Helsingin kaupungin keskushallinnolta tiedotteen, jossa ilmoitettiin AGPM-ryhmäkäytäntöjen muutoshallintalaajennuksen käyttöönotosta. Tämä tieto vaikutti olennaisesti tuleviin muutoksiin ja varsinkin käyttöönotettavaan muutoshallinnan prosessiin.

6.1 Nykytilan kuvaus

Parhaiden käytäntöjen käyttöönottoa varten piti ensin saada käsitys nykytilasta tekemällä analyysia yleisesti aktiivihakemiston rakenteesta ja nykyisistä ryhmäkäytännöistä ja niiden vaikutuksista työasemiin ja käyttäjiin. Analyysia tehtiin pääasiassa tutkimalla GPMC-työkalulla ryhmäkäytäntöjä

ja niissä määriteltyjä asetuksia. Tästä analyysista pystyttiin tekemään johtopäätöksiä mitkä asiat olivat hyvin ja mitkä olivat niitä osa-alueita, joihin haluttiin keskittyä ja mahdollisesti tehdä muutoksia.

Palmialla oli vain yksi hallittava OU Helsingin kaupungin AD:ssa. Palmian OU:n alla olivat omat OU:t käyttäjille ja työasemille sekä muille hallittaville kokonaisuuksille. Kaikki käyttäjät, joita oli noin 2100, olivat yhdessä OU:ssa, joten tässä suhteessa jokainen käyttäjä oli samanarvoinen ja niihin kohdistettiin linkittämällä samat asetukset. Poikkeukset ryhmäkäytäntöobjekteissa oli tehty joko WMI-suodatuksella tai ryhmäjäsenyyksillä. Poikkeuksia oli yhteensä viisi, joista vain yksi olisi voitu tehdä myös rakentamalla käyttäjäryhmälle oma OU. Loput poikkeuksista koskettivat käyttöjärjestelmän tunnistamista tai Office-version tunnistamista eikä näitä määrityksiä voitu korvata lajittelemalla käyttäjiä esimerkiksi organisaation mukaiseen OU-rakenteeseen.

Työasemien kohdalla tilanne oli toinen. Palmian OU on perustettu kaupungin AD:hen aikana, jolloin Palmialla oli käytössä vain Windows XP -käyttöjärjestelmällä varustettuja tietokoneita. Tuolloin oli järkevää perustaa työasemat-OU, jonka alle tehtiin erikseen OU:t kannettavia ja pöytäkoneita varten. Sittemmin vastaavat rakenteet on perustettu Windows 7- ja Windows 8 -käyttöjärjestelmiä varten.

Lähtötilanteessa Palmialla oli yhteensä 53 omaa ryhmäkäytäntöobjektia, joiden lisäksi oli keskushallinnon määrittelemiä ryhmäkäytäntöobjekteja 23 kappaletta. Näistä viisi oli määritelty Enforced-tilaan, jotta keskushallinto pystyy varmistumaan asetusten voimaan tulosta. Keskushallinnon määrittelemiin ryhmäkäytäntöobjektien asetuksiin ei Palmialla ollut mahdollisuutta vaikuttaa. Palmian omista ryhmäkäytäntöobjekteista pystytiin heti toteamaan, että osa oli täysin käyttämättömiä. Joko niiden WMI-suodatus ei enää koskettanut yhtään käyttäjää tai tietokonetta, niiden kohdistus ryhmän mukaan oli määritelty väärin tai sitten ryhmäkäytäntöobjekti oli linkittämätön tai linkitetty ryhmäkäytäntöobjekti ei ollut aktiivisena. Näitä ryhmäkäytäntöobjekteja oli yhteensä 11 kappaletta.

Pidemmän analyysin tuloksena todettiin, että eri käyttöjärjestelmäversioille oli kullekin tehty oma ryhmäkäytäntöobjekti tietokoneen ja käyttäjän asetuksia määrittämään. Windows 8 -käyttöjärjestelmän testissä olevista ryhmäkäytäntöobjekteista pystyttiin heti havaitsemaan, ettei tällaisen ympäristön ylläpito ole helppoa, kun samoja asetuksia pitää määritellä useaan paikkaan. Esimerkiksi Windows 7 ja Windows 8 -tietokoneiden asetuksissa oli ainoastaan kolmen asetuksen ero. Yhden asetuksen muuttaminen pitäisi siis aina tehdä vähintään kahteen ryhmäkäytäntöobjektiin.

Palmialla ryhmäkäytäntöjen hallinnalle ja ylläpidolle oli nimetty yksi henkilö, mutta käytännössä ylläpitoa kuitenkin suoritti neljä asiantuntijaa eri projekteissa ja sijaistustilanteissa. Palmian sisäisesti käyttöoikeuksia ei ollut rajattu mitenkään, vaan kaikilla ylläpitäjillä oli samanlaiset oikeudet tehdä muutoksia ryhmäkäytäntöihin. Tämä oli havaittu hankalaksi käytännöksi, koska mitään muutoshallintaprosessia ei ollut käytössä ja muutoksia

pystyi tekemään kuka tahansa neljästä ylläpitäjästä ilman velvollisuutta edes tiedottamiseen.

6.2 Yleiset periaatteet

Yleiset periaatteet oli hyvä määrittää, jotta ryhmäkäytäntöjä ylläpidettäessä on olemassa punainen lanka, kuinka asioita tehdään. Yhdessä asiantuntijoiden kesken päätimme määritellä yleiset periaatteet WMI-suodattimista, monoliittisista ja funktionaalisista ryhmäkäytäntöobjekteista, niiden nimeämisistä ja kommentoinnista.

Parhaissa käytännöissä oli otettu myös kantaa asynkronisen ja synkronisen prosessoinnin valinnassa sekä puolesta että vastaan. Palmialla tätä asiaa pohdittiin ja päädyttiin yksimielisesti käyttämään pakotetusti synkronista prosessointia, jotta varmistutaan määriteltyjen asetuksien voimaan astumisesta tietokoneessa.

6.2.1 WMI-suodattimien käyttäminen

Luvussa 4.5 esitelty WMI Filter Validation Utility oli hyvä työkalu päätettäessä WMI-suodattimien käyttämisestä. Palmialla käytiin kaikki käytössä olevat WMI-suodattimet läpi yksitellen ja tuloksilla saatiin perusteltua WMI-suodattimien hyödyllisyys.

Taulukko 2. WMI-suodattimien prosessointiaikavertailu millisekunneissa

		Prosessointiaika (ms)			
WMI-suodatin		WIN8 etäyhteys	WIN8 tablet	WIN7 pöytäkone	WIN7 kannettava
Tarkista onko IE9 tai IE10	1.	968	250	93	93
	2.	312	62	15	15
	3.	578	46	31	15
Keskiarvo		**619**	**119**	**46**	**41**
Tarkista onko Office 2010	1.	656	234	62	46
	2.	625	78	31	31
	3.	437	78	15	15
Keskiarvo		**573**	**130**	**36**	**31**
Tarkista onko Windows 8	1.	562	156	62	62
	2.	281	46	31	31
	3.	234	46	15	31
Keskiarvo		**359**	**83**	**36**	**41**

Taulukko 2 osoittaa kuinka käyttöön jääneet WMI-suodattimet vaikuttavat ryhmäkäytäntöasetusten prosessointiin. Huomionarvoista on se, että etäyhteyden päässä oleva Windows 8 -kannettava tietokone on selvästi hitain kaikista testatuista tietokoneista ja Windows 8 tablet-tietokone on toiseksi hitain. Tablet-tietokoneen hitaus selittyi sillä, että se oli liitetty langattomaan sisäverkkoon, mikä jää nopeudessa kiinteästä lankaverkosta. Kun tablet-tietokone liitettiin verkkokaapelilla kiinteästi verkkoon, sen WMI-suodattimien prosessointiajat olivat samaa luokkaa kuin testin nopeimmalla

Windows 7 -kannettavalla. Prosessoinnin nopeuteen näytti vaikuttavan enemmän verkon nopeus kuin koneen suorituskyky.

Testaus suoritettiin ajamalla Palmian tiedostopalvelimella WMIFTest.exe, valitsemalla validoitava WMI-suodatin ja tarkasteltava tietokone. Itse työkalun käytössä huomasin, että ensimmäinen validointi kesti aina kauimman aikaa, kun sen jälkeen tehdyt usein paljon vähemmän. Työkalua ei voi pitää täysin luotettavana, mutta se antaa hyvän yleiskäsityksen, kuinka kauan prosessointi kestää. Tästä syystä tein testit kolmeen kertaan ja laskin näistä tuloksista keskiarvon, jota voi pitää riittävän luotettavana tuloksena.

Kaikki käytössä olevat WMI-suodattimet olivat hyvin nopeita prosessoida, jos käytössä on nopea verkko. WMI-suodattimien käyttö oli tämän testin perusteella edelleen suositeltavaa Palmian ympäristössä. Jos WMI-suodattimista luovuttaisiin, tulisi AD:n rakennetta muuttaa tai tehdä samat ryhmittelyt AD:n ryhmäjäsenyyksien avulla.

6.2.2 Monoliittiset ja funktionaaliset ryhmäkäytäntöobjektit

Monoliittisten ja funktionaalisten ryhmäkäytäntöjen valinnassa päätöstä pohjattiin hyvin paljon asiantuntijoiden kokemukseen ympäristön hallinnassa. Palmialla oli käytössä entuudestaan molempia ryhmäkäytäntöobjektityyppejä, jotka tunnistettiin aikaisemmin käytetyn hyvin järkevän nimeämisen ansiosta. Monoliittisten ryhmäkäytäntöobjektien joukosta löytyi kuitenkin useita sellaisia ryhmäkäytäntöobjekteja, joissa oli asetuksia määritelty osittain päällekkäin tai ne olivat identtisiä kahdessa eri OU:ssa.

Asiantuntijat päätyivät sekaympäristöön monoliittisissa ja funktionaalisissa ryhmäkäytäntöobjekteissa. Ryhmäkäytäntöobjekteja kuitenkin järkeistettiin siten, että käyttäjille jätettiin yksi yhteinen monoliittinen ryhmäkäytäntöobjekti ja tietokoneille vastaavasti vain yksi ryhmäkäytäntöobjekti. Jos tietokoneen käyttöjärjestelmä asetti poikkeuksia niin käyttäjän kun tietokoneenkin asetuksiin, tehtiin nämä asetukset erillisessä ryhmäkäytäntöobjektissa, joka nimettiin kuvaavasti kuten Palmia Kayttaja Asetukset WIN8.

6.2.3 Ryhmäkäytäntöobjektien nimeäminen

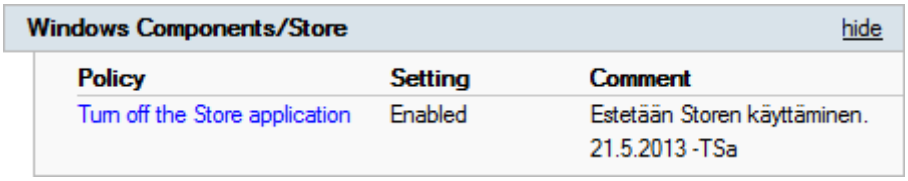
Helsingin kaupungin keskushallinto on linjannut, että hallintokuntien ryhmäkäytäntöobjektit pitää nimetä kuvaavasti ja ryhmäkäytäntöobjektin nimi tulee alkaa hallintokuntakohtaisella lyhenteellä. Palmian ryhmäkäytäntöobjektit alkavat kaikki Palmia-nimellä. Näin eri hallintokuntien ryhmäkäytäntöobjektit on helppo erottaa toisistaan, koska ne sijaitsevat samassa ryhmäkäytäntöobjektisäilössä. Palmialla on lisäksi käytetty yleisenä ohjenuorana, että AD:n OU:ssa tai ryhmäkäytäntöobjekteissa ei ole lainkaan skandinaavisia erikoismerkkejä, kuten ä- tai ö-kirjaimia. Tästä johtuen työasemat-OU kirjoitetaan ilman ö-kirjainta. Palmian ryhmäkäytäntöobjektien nimeämisessä hyödynnettiin OU-rakenteen mukaista nimeämistä. Funktionaalisten ryhmäkäytäntöobjektien nimeäminen pidettiin erittäin kuvaavana.

Palmia Internet-selain -ryhmäkäytäntöobjekti on funktionaalinen ja sen nimi kertoo helposti, mitä asetuksia siinä käsitellään. Palmia\Tyoasemat_WIN8\WIN8Kannettavat OU:ssa sijaitseva Windows 8 kannettaville tietokoneille suunnattu monoliittinen ryhmäkäytäntöobjekti on nimetty Palmia WIN8Kannettavat -nimiseksi OU:n mukaisesti.

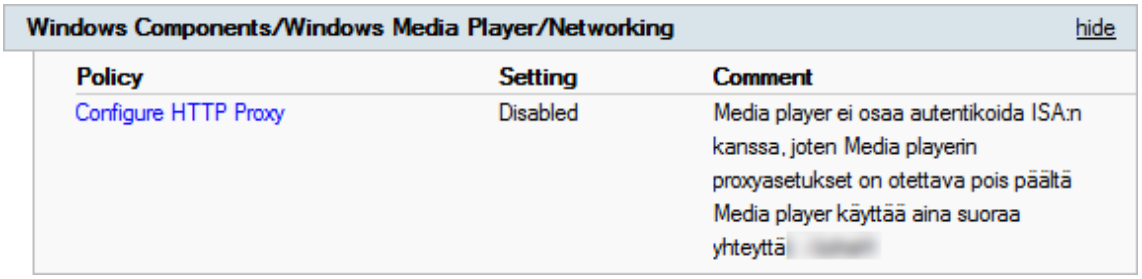
Windows 7 -tietokoneille oli määritelty erikseen asetukset-ryhmäkäytäntöobjekti, joka on monoliittinen ryhmäkäytäntöobjekti. Tämän lisäksi oli määritelty rajoitukset-ryhmäkäytäntöobjekti. Nimeämisen mukaan näiden ryhmäkäytäntöjen sisältöä tulkittiin niin, että toisessa ryhmäkäytäntöobjektissa oli sallivia asetuksia ja toisessa rajoittavia asetuksia. Näin ei kuitenkaan ollut. Ryhmäkäytäntöobjekteja on tyypillisesti kahdenlaisia, salli minut tai estä minut -tyylisiä. Kummankin tyyliset asetukset voidaan määrittää joko enabled- tai disabled-tilaan. Kun salli minut -asetus määritellään disabled-tilaan se itse asiassa estää asetuksen eikä salli sitä. Rajoitukset-ryhmäkäytäntöobjektissa oli asetuksia määritelty väärin, eivätkä ne olleet rajoittavia. Koska nimeäminen oli harhaanjohtava näissä kahdessa ryhmäkäytäntöobjektissa, ne päätettiin yhdistää ja nimetä kuvaavasti vain Palmia Kayttaja asetukset.

6.2.4 Kommentointi

Ryhmäkäytäntöobjektissa on mahdollisuus kommentoida jokaista asetusta huolimatta siitä, onko sitä määritelty. Tämä on käytäntö, jota olen itse ryhtynyt käyttämään ennen tätä projektia. Kommenttien käyttämisestä ei tutkimustyössä löytynyt yhtään viittausta, mutta pidän sitä itse erittäin hyvänä käytäntönä. Joskus määritellyt asetukset ovat vaikeaselkoisia, eikä niistä pysty päättelemään, minkä takia kyseessä oleva asetus on määritelty. Tällaisissa tapauksissa kommentit kertovat, miksi asetus on määritelty ja avustavat uusien asetuksien määrittelyssä sekä vianselvityksessä. Kommenteista (kuva 14 ja kuva 15) on hyötyä varsinkin niissä tilanteissa, kun ympäristö muuttuu ja ryhmäkäytäntöobjektien tarvetta ja asetuksia tarkastellaan uudelleen.



Kuva 14. Esimerkki kommentista, jolla ei suoranaista lisäarvoa



Kuva 15. Esimerkki kommentista, jolla on huomattavasti lisäarvoa

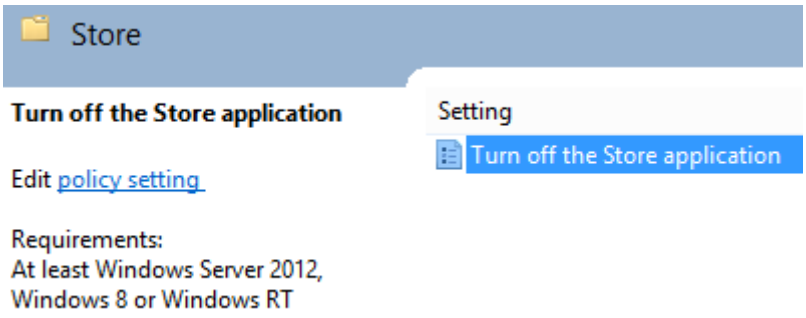
Vaikka kaikista kommenteista ei olekaan suoranaista lisäarvoa, päätettiin niitä käyttää kuitenkin systemaattisesti. Palmian luoman käytännön mukaan kommentista selviää asetuksen määrittelypäivä ja kuka asetuksen on tehnyt.

6.3 Windows 8 -käyttöjärjestelmän asetukset

Windows 8 - ja Windows Server 2012 -julkaisun yhteydessä julkaistiin myös uudet ryhmäkäytäntöasetukset, joista 169 asetusta vaativat Windows 8 tai Server 2012 -käyttöjärjestelmän (Carpenter 2013). Yhteensä uusia ryhmäkäytäntöjen asetuksia on julkaistu 357, ja niistä osa vaikuttaa myös vanhoihin käyttöjärjestelmäversioihin. Kaiken kaikkiaan ryhmäkäytäntöasetuksia on 3486 kpl. (Microsoft n.d.)

Windows 8 -käyttöjärjestelmä otettiin Palmialla käyttöön vain tablet-tietokoneissa. Käyttöön otettavia asetuksia määriteltiin siltä pohjalta, että Windows 8 -käyttöjärjestelmälle tehdään yhteiset asetukset yhdessä Windows 7 -käyttöjärjestelmän kanssa ja erikseen luodaan sitten poikkeavat asetukset omiin käyttöjärjestelmäkohtaisiin ryhmäkäytäntöobjekteihin, jos tarvetta niille esiintyy. Tietokoneille luotiin lisäksi laitemallikohtaiset ryhmäkäytännöt, joilla voidaan määritellä kannettavien laitteiden synkronointi-, virransäästö- tai kryptaus-asetuksia käyttöjärjestelmästä riippumatta. Lopputuloksena tietokoneille käyttöön jäi kolme kappaletta monoliittisia ryhmäkäytäntöobjekteja, joilla määritellään yleisiä työasemien asetuksia. Näiden lisäksi on kymmenen funktionaalisia ryhmäkäytäntöobjekteja.

Windows 8 -käyttöjärjestelmässä on mahdollisuus kirjautua PIN-koodilla, Microsoft-tilillä tai kuvakirjautumisella perinteisen kirjautumisen lisäksi. Tämän lisäksi Storen käyttö oli tullut uutena ominaisuutena verrattuna Windows 7 -käyttöjärjestelmään. Kirjautumiseen liittyvät asetukset ovat tavalliselle kuluttajalle hyviä ominaisuuksia, mutta yrityskäyttöön katsottiin niiden olevan tietoturvan kannalta huonoja sellaisenaan, joten ne estettiin. Windows Storen käyttö estettiin siitä syystä, että Windows 8 -käyttäjien yritystarpeet huomioiden ei koettu Windows 8 Storen kautta ladattavien sovellusten tuovan lisäarvoa Palmian käyttäjille. Nämä asetukset eivät vaikuta Windows 7 -käyttöjärjestelmään, koska niiden vähimmäisvaatimuksena on Windows 8 -, Windows RT - tai Windows Server 2012 -käyttöjärjestelmä, mutta tästä huolimatta asetukset määritettiin omaan käyttöjärjestelmäkohtaiseen ryhmäkäytäntöobjektiin, jotta ryhmäkäytäntöobjektien rakenne pysyy selkeänä. Myöhemmin myös muita Windows 8 -käyttöjärjestelmään vaikuttavia asetuksia määriteltiin, jolloin linjaus omasta ryhmäkäytäntöobjektista osoittautui hyväksi.



Kuva 16. Asetuksen vähimmäisvaatimukset

Internet Explorerin uusien versioiden yhteydessä julkaistaan aina uusia ryhmäkäytäntöasetuksia, jolla selaimen uusia ominaisuuksia voidaan hallita. Windows 8 -käyttöjärjestelmän ja Internet Explorer 10 -version yhteydessä lakkautettiin tuki vanhoille Internet Explorer asetuksille, joita määriteltiin ryhmäkäytäntöobjektissa Internet Explorer Maintenance -osiossa. Tämä puute havaittiin RSOP-työkalulla, joka ei enää Windows 8 -tietokoneella näyttänyt kyseisiä ominaisuuksia, vaan ilmoitti ongelmasta kyseisten asetuksien suhteen. Lisäksi GPMC-työkalussa näitä asetuksia ei enää päässyt määrittelemään. Jouduimme käymään kaikki Internet Exploreriin vaikuttavat asetukset läpi ja määrittämään ne uudelleen Group Policy Preferenssiellä.

Palmialla oli päätetty ottaa käyttöön tiukemmat salasanakäytännöt tietokoneen paikallisille järjestelmänvalvoja-tunnuksen salasanoille. Tähän oli aiemmin hyödynnetty Group Policy Preferenssin Local Users and Groups -määrityksiä osana yhtä monoliittista ryhmäkäytäntöä. Koska monoliittisen ryhmäkäytännön jatkuva muuttaminen aiheutti käytännössä lähes kaikkien ympäristön ryhmäkäytäntöjen prosessoinnin, päätettiin luoda tätä tarvetta varten oma funktionaalinen ryhmäkäytäntöobjekti.

Ryhmäkäytäntöobjektin nimeksi määriteltiin Workstation Admin Password, mikä kuvaa hyvin ryhmäkäytäntöobjektin sisältämiä asetuksia. Tähän ryhmäkäytäntöobjektiin oli tarkoitus keskittää kaikki saman ryhmäkäytäntölaajennuksen asetukset, jotta kun asetuksia muutetaan, tapahtuu prosessointi vain tässä ryhmäkäytäntöobjektissa.

Pian ryhmäkäytäntöobjektin käyttöönoton jälkeen Helsingin kaupungin keskushallinto ilmoitti koko kaupungin ympäristöön vaikuttavasta keskitetystä salasanojen hallinasta. Tämä kaupunkitasoinen muutos teki juuri tekemämme muutoksen käytännössä tarpeettomaksi, joten asetukset palautettiin ennalleen ja kolmatta osapuolta pyydettiin poistamaan Workstation Admin Password -ryhmäkäytäntöobjekti.

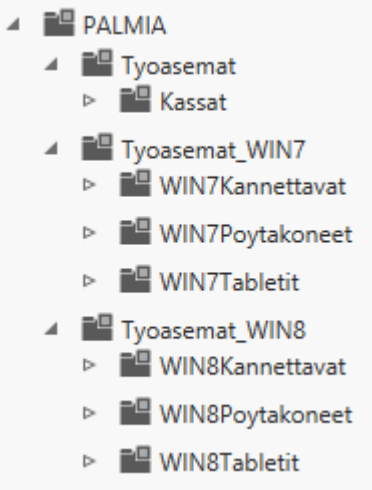
6.4 Tavoitetilan rakentaminen

Nykytilakuvauksessa esiin nousseet parhaiden käytäntöjen vastaiset toteutukset olivat sellaisia asioita, joihin haluttiin puuttua. Ympäristö oli pitkään

ollut huonossa ylläpidossa ja se osoittautui käyttämättöminä ryhmäkäytäntöobjekteina ja huonosti määriteltyinä asetuksina. Näistä havaituista ongelmakohdista, kuten AD-rakenteesta, on kerrottu seuraavissa kappaleissa.

6.4.1 AD-rakenteen muutokset

Nykytilan kuvauksen ja asetusten optimoinnin aikana havaittiin työasema-OU -rakenteen olevan huonosti soveltuva nykyiseen tilanteeseen, koska työasemilla ei ole yhtä yhteistä OU:ta, johon voitaisiin määritellä kaikkia työasemia koskevat perusasetukset ja käyttöjärjestelmäkohtaisesti poikkeavat asetukset niiden päälle. Asetukset olisi pitänyt tehdä Palmia-tason OU:ssa, jossa ne teknisesti olisi ollut määriteltävissä, mutta Palmia OU:ta ei ole tarkoitettu tämän kaltaisten asetusten määritykseen. Helsingin kaupungin AD-rakenteen takia Palmia OU:ta voi verrata Kuva 4 esitettyyn Domain 1 -tasoon.



Kuva 17. Palmian työasemien OU-rakenne

Koska työasemien rakenne on keskushallinnon määrittelemä, emme voineet vaikuttaa sen rakenteeseen, vaan asetuksien määrittäminen piti tehdä saman ryhmäkäytäntöobjektin linkittämisellä useampaan OU:hun. Menetelmä on hyväksi havaittu kompromissi AD-rakenteen suunnittelun ja ryhmäkäytäntöjen linkittämisen välillä.

6.4.2 Muutokset ryhmäkäytäntöjen rakenteeseen

Lähtötilanteessa ryhmäkäytäntöobjekteja oli 76 kappaletta, joista Palmian itse määrittelemiä oli 53 kappaletta. Turhien ryhmäkäytäntöobjektien poistaminen ja ryhmäkäytäntöobjektien harmonisointi monoliittisiin ryhmäkäytäntöobjekteihin vähensi ryhmäkäytäntöobjektien määrää. Kaupunkitasoiset Enforced-tilassa olevat ryhmäkäytäntöobjektit jäivät edelleen voimaan, koska emme itse voineet vaikuttaa niihin. Tässä suhteessa oli mietittävä kompromisseja asetuksien määrittämisen kanssa. Ideaalitilanteessa olisimme poistaneet Enforced-tilalla määritellyt ryhmäkäytäntöobjektit käytöstä ja määritelleet asetukset jo olemassa oleviin ryhmäkäytäntöobjekteihin.

Työasemille tarkoitettuja asetuksia oli määritelty käyttöjärjestelmän mukaisiin ryhmäkäytäntöobjekteihin. Windows XP:lle, -7:lle ja -8:lle oli kullekin omat ryhmäkäytäntöobjektinsa. Windows XP -tietokoneisiin vaikuttaneet ryhmäkäytäntöobjektit voitiin poistaa, koska Windows XP -kassakoneisiin oli omat ja poikkeavat asetuksensa ja Palmialla ei enää ollut lainkaan normaalissa työasemakäytössä olevia Windows XP -tietokoneita. Jäljelle jääneet Windows 7:n ja -8:n asetukset yhdistettiin samaan Palmia Tyoasemat -nimiseen ryhmäkäytäntöobjektiin, koska niissä oli käytännössä vain kolmen asetuksen ero ja nämä kolme asetusta eivät vaikuttaneet lainkaan Windows 8:aa vanhempiin käyttöjärjestelmiin.

Kaikkiaan Palmian määrittelemiä ryhmäkäytäntöobjekteja jäi käyttöön 26 kappaletta, joka oli hieman alle puolet lähtötilanteesta. Keskushallinnon määrittelemiä ryhmäkäytäntöobjekteja saatiin vähennettyä kahdeksan kappaletta, joten vain 15 ryhmäkäytäntöobjektia jäi ympäristöömme käyttöön, joista edelleen viisi olivat enforced-tilassa.

6.4.3 Muutosprosessin luominen

Nykytilankuvauksessa havaittiin, että ryhmäkäytäntöjen muutoksiin ei ollut lainkaan prosessia. Palmialla neljä eri ylläpitäjää pystyi tekemään muutoksia ryhmäkäytäntöobjekteihin, eikä sovittua tiedotuskanavaa tai hyväksymisketjua ollut määritelty. Tältä pohjalta prosessia lähdettiin luomaan niin, että siihen lisättiin hyväksymispiste. Kesken prosessin suunnittelun saimme yllättäen tietää, että keskushallinto ottaa käyttöön AGPM-palvelun, joka käytännössä tulisi muuttamaan prosessia Palmiasta riippumattomista syistä.

Helsingin kaupungin AD:ssa käyttöönotettiin kaupunginlaajuisesti AGPM 28.5.2013, joka muutti aikaisemmin määriteltyjä tavoitteita. AGPM-käyttöönotto myös määritteli, miten muutosprosessi jatkossa tultaisiin tekemään. AGPM muutti prosessia (liite 2) paremmaksi tuoden siihen uutena elementtinä kolmannen osapuolen hyväksynnän prosessin loppuvaiheessa ennen asetusten käyttöönottoa.

Vaikka AGPM lisäsi prosessiin hyväksyntäpisteen, haluttiin Palmialla edelleen pitää oma hyväksymispiste ennen muutoksen viemistä AGPM:n mukaiseen hyväksyntäpisteeseen. Tällä haluttiin varmistaa, että tehtävät muutokset ovat linjassa Palmian ryhmäkäytäntöjen rakenteen kanssa, koska kolmas osapuoli ei muutoksen hyväksyjänä osaa ottaa kantaa siihen, missä ryhmäkäytäntöobjektissa asetus tulisi määritellä, vaan ainoastaan siihen onko asetus ja sen vaikutus yleisessä linjassa keskushallinnon määrittelyjen kanssa.

Palmian vastuulle jäi testata muutokset yhdessä testi-ryhmäkäytäntöobjektissa, joka ei kuulunut AGPM:n piiriin ja siinä pystyttiin testaamaan asetuksia vapaasti kahdelle testitunnukselle ja kahdelle työasemalle. Kun muutokset oli testattu toimiviksi, ne hyväksytettiin Palmian ryhmäkäytäntövastaavalla, jonka jälkeen ne voitiin siirtää tuotantoympäristöön AGPM:n prosessia noudattaen. Muutettu tuotantoympäristön ryhmäkäytäntöobjekti lähetet-

tiin kolmannelle osapuolelle hyväksyttäväksi määrittämällä se deploy-tilaan. Kolmannen osapuolen kanssa sovittujen palvelun vasteaikojen mukaisesti se käsitellään ja siirretään tuotantoon.

Uutta muutosprosessia haluttiin testata, jotta varmistuttiin kolmannen osapuolen toiminnasta rutiinimuutoksessa sekä häiriötilanteessa. Ensimmäiset muutokset menivät AGPM:n prosessin läpi erittäin hyvin. AGPM:n kautta ei kuitenkaan pystytty tekemään useita muutoksia ajastettuna, kuten ryhmäkäytäntöobjektin uudelleen nimeämistä, vaikutusalueen muutosta (Security Filtering) tai ryhmäkäytäntöobjektin luomista tai poistamista. Myöhemmin tehdyssä muutosten sarjassa osa muutoksista tehtiin AGPM:n kautta ja osa piti selvittää kirjallisesti sähköpostin välityksellä ja ajastaa tapahtumaan haluttuna ajankohtana. Tässä muutosvaiheessa tapahtui väärinkäsityksestä ympäristömme toimintaan vakavasti vaikuttava virhe ja jouduimme pikaisesti palauttamaan asetukset ennalleen. Tapauksesta opittiin, että kaikki muutokset tulee selostaa erittäin tarkkaan, jottei kolmannelle osapuolelle jää tulkinnanvaraa. Lisäksi muutoksien testaaminen tulee suorittaa erittäin huolellisesti.

7 YHTEENVETO

Tämän opinnäytetyön tarkoituksena oli harmonisoida Palmian ryhmäkäytäntöobjekteja ja luoda helposti ylläpidettävä ryhmäkäytäntöjen ympäristö. Työn tavoitteisiin päästiin kartoittamalla ryhmäkäytäntöobjektien nykytila ja optimoimalla ryhmäkäytäntöasetuksia parhaiden käytäntöjen mukaisesti. Lisäksi luotiin muutosprosessi ryhmäkäytäntöjen ylläpitoa varten. Ympäristössä oli paljon huonosti määriteltyjä asioita, joita tämän työn tuloksena saatiin karsittua pois. Työn tuloksia voi pitää erittäin hyvin onnistuneena, koska yli puolet ryhmäkäytäntöobjekteista saatiin karsittua pois ja jäljelle jäänyt ympäristö on yksinkertainen ja selkeä.

Opinnäytetyön tekijä havaitsi työtä tehdessään, kuinka tärkeää on, että organisaatiossa on vastuuhenkilö, joka ymmärtää ryhmäkäytäntöjen toimintaa hieman pintaa syvemmältä. Yrityksessä, jossa vastuu on hajautettu ja usein ainakin osittain ellei kokonaan ulkoistettu, saatetaan ajautua tilanteeseen, että ryhmäkäytäntöasetuksia määritellään sekavasti ja uusia ryhmäkäytäntöobjekteja luodaan liian kevyin perustein. Tämä johtaa väistämättä tilanteeseen, jossa kunnollista kokonaiskäsitystä ei ole kenelläkään ja vastuu ympäristön hallinnasta saattaa olla epäselvä. Projektissa kohdattiin useita haasteita - ne vaikuttivat projektin etenemiseen, mutta eivät estäneet sen toteuttamista.

Yleisenä havaintona voidaan todeta, että ryhmäkäytäntöobjekteja ei niinkään optimoida käyttöjärjestelmän mukaan vaan yleisesti koko ympäristön mukaisesti. Ryhmäkäytäntöjä ei saisi jättää määrittelyn jälkeen vaan niille sijoilleen vaan niitä tulisi jatkuvasti ylläpitää. Näin pitäisi toimia ainakin silloin kun ympäristössä otetaan käyttöön uusia versioita perusohjelmista, kuten Internet Explorerista, Microsoft Officesta tai kokonaan uusi käyttöjärjestelmäversio. Myös perusohjelmien, kuten Adobe Readerin tai Javan toimintaa ohjataan usein ryhmäkäytännöillä. Moni ryhmäkäytäntöasetus on

määritelty vain tiettyä versiota vasten, jolloin niiden toivottu ominaisuus saattaa lakata vaikuttamasta kun versio päivitetään.

Tämän opinnäytetyön tulokset ovat lähes poikkeuksetta kaikkien yritysten käytettävissä, koska Windows-käyttöjärjestelmät ja AD ovat keskeisiä asioita tietoteknisessä ympäristössä. Monelle yrityksen AD:sta ja ryhmäkäytäntöistä vastaavalle ylläpitäjälle työn tulokset saattavat olla uutta tietoa, koska ryhmäkäytäntöjen parhaita käytäntöjä ei ole tutkittu niin laajasti, mikä näkyy myös käyttämissäni lähteissä.

LÄHTEET

Burchill, A 2009. Group Policy Setting of the Week 2 - Verbose vs normal status messages. Viitattu 17.8.2013. http://www.grouppolicy.biz/page/64/

Burchill, A 2010. Best Practice: Group Policy Design Guidelines – Part 2. Viitattu 3.5.2013. http://www.grouppolicy.biz/2010/07/best-practice-group-policy-design-guidelines-part-2/

Carpenter, T. 2013. New Group Policy Settings in Windows 8 and Windows Server 2012. Viitattu 15.5.2013. http://www.tomcarpenter.net/2013/01/17/new-group-policy-settings-in-windows-8-and-windows-server-2012/

Empson, M. 2010. Group POlicy Client Side Extension List. Viitattu 19.5.2013. http://blogs.technet.com/b/mempson/archive/2010/12/01/group-policy-client-side-extension-list.aspx

Holme, D. Ruest, N. & Ruest, D. 2008. Microsoft MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server 2008 Active Directory.

It Free Training, n.d. Group Policy Processing Order. Viitattu 1.9.2013. http://itfreetraining.com/70-640/gpprocessingorder/

Mar-Elia, D. 2008. Optimizing Group Policy Performance. Viitattu 3.5.2013. http://technet.microsoft.com/en-us/magazine/2008.01.gpperf.aspx

Mar-Elia, D. 2012a. Group Policy Design Best Practices. Viitattu 5.5.2013. http://windowsitpro.com/group-policy/group-policy-design-best-practices

Mar-Elia, D. 2012b. Best Practices for Designing and Consolidating Group Policy for Performance and Security, video. Viitattu 10.5.2013. *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2012/WSV206*

Melber D. 2008. Installing and Using the Remote Server Administration Tools (RSAT) for Vista. Viitattu 27.6.2013. http://www.windowsecurity.com/articles-tutorials/windows_os_security/Installing-Using-Remote-Server-Administration-Tools-RSAT-Vista.html

Microsoft 2001. How to Use the Group Policy Results (GPResult.exe) Command Line Tool. Viitattu 19.5.2013. http://technet.microsoft.com/en-us/library/bb456989.aspx

Microsoft 2003a. Group Policy Processing. Viitattu 14.5.2013. http://technet.microsoft.com/en-us/library/cc758898%28v=ws.10%29.aspx

Microsoft 2003b. What Is Resultant Set of Policy?. Viitattu 26.6.2013. http://technet.microsoft.com/en-us/library/cc758010%28v=ws.10%29.aspx

Microsoft 2012. Group Policy Management Console. Viitattu 25.6.2013. http://msdn.microsoft.com/en-us/library/windows/desktop/aa814316%28v=vs.85%29.aspx

Microsoft n.d. 3.1.3.1 Group Policy Client-Side Extension List. Viitattu 19.5.2013. http://msdn.microsoft.com/en-us/library/hh150157.aspx

Microsoft n.d. Gpupdate. Viitattu 19.5.2013. http://technet.microsoft.com/en-us/library/bb490983.aspx

Microsoft n.d. Group Policy Settings Reference for Windows and Windows Server Viitattu 15.5.2013. http://www.microsoft.com/en-us/download/details.aspx?id=25250

Microsoft n.d. Tip: Five Command Line Tools for Managing Group Policy. Viitattu 19.5.2013. http://technet.microsoft.com/en-us/magazine/gg277500.aspx

Microsoft n.d. Workaround not to use "enforced policy" for an OU. Viitattu 2.6.2013. http://social.technet.microsoft.com/Forums/en-US/winserverGP/thread/a30dcac9-02a9-4ef0-a1e4-780a15e4c0d1

Phillips, J. D. 2008. Upgrading Your SYSVOL to DFS-R Replication. Viitattu 2.6.2013. http://blogs.technet.com/b/notesfromthefield/archive/2008/04/27/upgrading-your-sysvol-to-dfs-r-replication.aspx

Rux, E. B. 2007. 3 Tools to Manage Group Policy. Viitattu 3.5.2013. http://windowsitpro.com/systems-management/3-tools-manage-group-policy

Shields, G. 2012. 6 Best Practices in Setting Up & Managing GPO Changes. Viitattu 19.8.2013. http://communities.quest.com/community/quest-itexpert/blog/2012/11/08/6-best-practices-in-setting-up-amp-managing-gpo-changes

Liite 1

WMI-suodattimia

Seuraava WMI-suodatin tarkistaa onko käyttöjärjestelmän versio Windows 8, Windows 7, Windows Vista, Windows Server 2012, Windows Server 2008 R2 ja Windows Server 2008.

```
select * from Win32_OperatingSystem where Version like "6.%"
```

Määritelläksesi suodattimen vain Windows 8 ja Windows Server 2012:sta käytä seuraavaa:

```
Version like "6.2%"
```

Yhdistääksesi useita versioita käytä seuraavaa:

```
Version like "6.1%" or Version like "6.2%"
```

Suodattaaksesi vain asiakaskäyttöjärjestelmiä käytä ProductType-määritystä. Seuraava suodatin määrittää Windows 8 käyttöjärjestelmän:

```
select * from Win32_OperatingSystem where Version like "6.2%"
and ProductType="1"
```

Liite 2

Ryhmäkäytäntöobjektin muutosprosessi