Satakunnan ammattikorkeakoulu
OPINNÄYTETYÖ

Ville-Veikko Luomanen

Ville-Veikko Luomanen

RYHMÄKÄYTÄNNÖT SATAKUNNAN AMMATTIKORKEAKOULUN LIIKETOIMINNAN JA KULTTUURIN PORIN YKSIKÖSSÄ

Tietojenkäsittelyn koulutusohjelma
2009

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

RYHMÄKÄYTÄNNÖT SATAKUNNAN AMMATTIKORKEAKOULUN LIIKETOIMINNAN JA KULTTUURIN PORIN YKSIKÖSSÄ

Luomanen, Ville-Veikko
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Huhtikuu 2009
Nieminen, Hans
UDK: 004.451, 004.455.2
Sivumäärä: 67

Asiasanat: Windows, palvelimet, profiilit, työasemat

Tämän opinnäytetyön aiheena oli tutustua Satakunnan ammattikorkeakoulun liiketoiminnan ja kulttuuri Porin yksikössä olevien ryhmäkäytäntöjen toimintaan ja samalla dokumentoida nykyinen ryhmäkäytännöistä koostuva ympäristö. Myös mahdollisten parannusten kartoitus oli yksi tavoite. Työ toteutettiin pääasiassa palvelimilla, jotka tällä hetkellä käytössä aktiivihakemiston ja ryhmäkäytäntöjen osalta.

Opinnäytetyön lähtökohtana oli oma kiinnostukseni aiheeseen sekä osaamiseni kehittäminen palvelinympäristössä. Ryhmäkäytäntöjen hallinta on niin laaja kokonaisuus, että perusasioiden oppiminen ja niiden soveltaminen käyttöön muodostui kaikkein tärkeimmäksi osa-alueeksi.

Aluksi kerättiin paljon teoriaa liittyen ryhmäkäytöntöihin. Tietolähteinä toimivat pääasiassa painettu alan kirjallisuus sekä Internet. Sen jälkeen tutustuttiin nykyiseen ympäristöön ja muodostettiin selkeä kuva sen toimivuudesta sekä eri ryhmäkäytäntöobjektien vaikutuksesta eri organisaatioyksiköihin.

Opiskelijat ja henkilökunta olivat suurimmat käyttäjäryhmät, joihin ryhmäkäytännöt vaikuttivat. Tarkoitus oli kartoittaa, miten ryhmäkäytännöt vaikuttivat heidän normaaliin työpöytäkäyttöön ja mitä rajoituksia oli käytössä.

Ryhmäkäytäntöjen kautta saatava hyöty tietoturva-asetuksiin oli myös yksi oleellinen osa opinnäytetyötä. Koska työasemia käyttää sadat eri opiskelijat, tietoturva korostuu entisestään. Hyvän strategian ja toimivan ympäristön luonne korostuu myös tällöin entisestään.

Lopputulos antoi hyvän kuvan liiketoiminta ja kulttuuri Porin yksikön ryhmäkäytäntöjen toiminnasta. Ympäristö oli nykyiselläänkin jo toimiva kokonaisuus, mutta myös kehitysmahdollisuuksia tuotiin esille.

GROUP POLICIES IN SATAKUNTA UNIVERSITY OF APPLIED SCIENCES – FACULTY OF BUSINESS AND CULTURE PORI

Luomanen, Ville-Veikko
Satakunta University of Applied Sciences
Degree in Business Information Technology
April 2009
Nieminen, Hans
UDC: 004.451, 004.455.2
Number of pages: 67

Key words: Windows, servers, profiles, workstations

The purpose of this thesis was to explore and to document the group policies that are used in Satakunta University of Applied Sciences – Faculty of Business and Culture Pori. Also the possibility to improve the current system was one of the tasks. Most of the work was implemented basically with the servers that are maintaining the active directory and group policies.

Starting point of this thesis was my own interests to the subject and a chance to improve my skills in server environment. To administrate the group policies is so extensive project that learning the basics and to adapt them came the primary part of this thesis.

At first a lot theory was gathered concerning the group policies. Sources were mainly the books and the Internet. Next task was to explore the current settings and create a clear picture of their functionality and how they effect to the organizational units.

Students and staff were the biggest user groups affected by the group policies. The purpose was to find out, how the group policies affect to their normal desktop usage and what limitations were applied.

One benefit of this thesis was getting to know the security settings that were made by group policies. There are hundreds of students using the workstations, so it's very important to have good security settings. To have a good strategy and working environment is a key feature.

As a result, this thesis gives a good picture about the group policies used in Faculty of Business and Culture Pori. The settings were well designed and they were working like they should be. There also were a couple of improvements to think about.

SISÄLLYS

SYMBOLI- JA TERMILUETTELO

Aktiivihakemisto	Active Directory. Aktiivihakemisto toimii käyttäjien ja muiden toimialueresurssien keskitettynä hallintapisteenä.
GPMC	Group Policy Management Console. Ryhmäkäytäntöjen ylläpitoon suunniteltu hallintakonsoli.
GPOE	Group Policy Object Editor. GPO:n luontiin tarkoitettu editori.
Hallintamallit	Administrative templates (ADM). Ryhmäkäytäntöobjektien luontiin käytettävät asetukset, jotka tekevät muutoksia tietokoneen rekisteritietoihin.
Loopback processing	Ryhmäkäytäntöobjektien käyttöönotto tietokoneen sijainnin perusteella.
MSI (Windows Installer Package)	Ohjelmistojen asentamiseen käytettävä tiedostomalli.
Ohjauspalvelin (Domain Controller)	Ylläpitää tietokantaa toimialueen resursseista ja tunnistaa toimialueelle kirjautuvat käyttäjät.
Organisaatioyksikkö (OU)	Aktiivihakemiston säiliö, joka voi pitää sisällään käyttäjä- tai tietokoneobjekteja.
Palvelin	Palvelinohjelmistoa suorittava tietokone.
RSoP	Resultant Set of Policy. Ryhmäkäytäntöjen suunnittelu- ja diagnostiikkatila.
Ryhmäkäytäntö (GP)	Ryhmäkäytäntö on infrastruktuuritekniikka, jonka avulla määrityksiä tai käytäntöasetuksia voidaan tehdä valituille käyttäjille ja valituissa tietokoneissa.
Ryhmäkäytäntöobjekti (GPO)	Ryhmäkäytännöillä tehdyt määrittelyt tallentuvat ryhmäkäytäntöobjekteiksi.

Service Pack	Tietokoneohjelmiston täydennysosa, ns. huoltopäivitys, jolla korjataan ohjelmistossa olevia virheitä ja mahdollisesti lisätään uusia ominaisuuksia.
Toimialue (Domain)	joukko Microsoft Windows -käyttöjärjestelmän sisältäviä tietokoneita, joita voidaan hallita keskitetysti yhdeltä tai useammalta Windows-palvelimelta.
Toimipaikka (Site)	Fyysinen rakenne, johon aktiivihakemisto perustuu.
WMI	Windows Management Instrumentation. Ryhmäkäytäntöobjektien yhteydessä käytettävä suodatin, jolla voidaan tutkia tietokoneen ominaisuuksia.

1 JOHDANTO

Nykypäivän oppilaitosympäristö on hyvin tietotekninen kokonaisuus. Monet opiskeluun liittyvät asiat hoidetaan sähköisesti käyttämällä joko työasemia tai kannettavia tietokoneita. Myös muut tietoverkon laitteet, kuten tulostimet ovat jatkuvassa päivittäisessä käytössä. Koska oppilaitoksissa käyttäjiä on parhaassa tapauksessa satoja tai jopa tuhansia, on hyvin tärkeää, että laitteiden käyttöä rajoitetaan tietyin käyttöoikeuksien sekä määrittelyjen avulla. Kun laitekanta kasvaa satoihin, niiden hallinta hankaloituu ilman yhtenäistä ja loogista toimintamallia.

Tämän opinnäytetyön tarkoitus on havainnollistaa ryhmäkäytäntöobjektien ominaisuuksia ja kertoa, mihin tarkoituksiin niitä voidaan hyödyntää. Ryhmäkäytäntöobjektit antavat järjestelmänvalvojille sekä muille tietoverkkoa hallitseville henkilöille mahdollisuuden luoda sääntöjä, joilla pakotetaan työasemat sekä niiden käyttäjät toimimaan tiettyjen rajoitusten puitteissa. Ryhmäkäytännöt tuovat myös paljon hyötyä keskitettyyn hallintaan.

Tutkimani ympäristö on Satakunnan ammattikorkeakoulun liiketoiminnan ja kulttuurin Porin yksikkö, missä ryhmäkäytäntöobjektit ovat käytössä rajoittamassa työasemien sekä käyttäjien käyttöoikeuksia sekä helpottamassa tietoverkon hallintaa. Tarkoitukseni on selvittää, mitä asetuksia tällä hetkellä on käytössä ja millä tavalla ryhmäkäytäntöobjektien käyttöä voisi jatkossa vielä tehostaa.

Opinnäytetyöni koostuu teoriaosuudesta, missä kerron ryhmäkäytäntöjen käyttömahdollisuuksista, käyttöönotosta sekä niiden hallinnasta. Toisena osuutena dokumentoin nykyisen ympäristön ja sen pohjalta aion tutkia mahdollisuutta ottaa käyttöön uusia säännöksiä, jotka parantavat keskitettyä työasemien sekä käyttäjien hallintaa.

Idea opinnäytetyöhön syntyi järjestelmäasiantuntija Petri Nuutisen ehdotuksesta, joka aihetta suositteli. Itse olen tällä hetkellä Satakunnan ammattikorkeakoulun Liiketoiminnan ja kulttuurin Porin yksikössä töissä, ja aihe-ehdotus vaikutti erittäin mielenkiintoiselle. Samalla opin yhden tärkeän hallintakäytännön nykypäivän tietoverkon ylläpitoa ajatellen.

Olen rajannut opinnäytetyöni käsittelemään ryhmäkäytäntöobjekteja Windows XP, Windows Vista sekä Windows Server 2003-ympäristössä. En ota kantaa uuteen, Windows Server 2008:n mukana tuomaan, Group Policy Preferences-työkaluun. Tämä johtuu siitä, että kyseinen työkalu on vielä uusi ja tuo mukanaan niin paljon ominaisuuksia, että siitä saisi oman opinnäytetyöaiheen. Liiketoiminta ja kulttuuri Porin yksikössä ei myöskään ole kyseistä Group Policy Preferences-työkalua käytössä, joten sen ominaisuuksien tutkiminen ei olisi tässä opinnäytetyössä järkevää.

2 RYHMÄKÄYTÄNTÖJEN YLEISKUVA

2.1 Tarve keskitettyyn hallintaan

Microsoft julkisti 90-luvun lopulla termin ”zav–Zero administration windows.” Sen tarkoituksena oli pienentää Windows 9x:n ja silloisen NT:n ylläpitotyötä ja laskea niiden käyttökustannuksia. Työasemien asetusten keskitetty hallinta tapahtui policy editor -ohjelmalla laadittavilla pol-rajoitustiedostoilla. (Rousku 2005, 40.)

Menetelmän ongelma oli rajoitettavien asetusten vähäisyys, laajemmissa verkkoympäristöissä hankala pol-tiedostojen ylläpito sekä se, että asetukset tulivat voimaan vain työasemien tai käyttäjien kirjautuessa verkkoon. Pol-tiedostoja oli mahdollista ohjelmoida itse, mutta se ei ollut mitenkään helppoa. (Rousku 2005, 40.)

Microsoft kehitti Windows 2000-käyttöjärjestelmään ja aktiivihakemistoon uudet hallintakeinot. Näin tulivat ryhmäkäytännöt eli group policyt, jatkossa GP. GP kattaa lähes kaikki Windows 2000- ja etenkin Windows XP-käyttöjärjestelmien muutettavissa olevat asetukset. XP Service Pack 2 toi mukanaan yli 500 uutta GP-asetusta, joten tällaisessa työasemassa on kaikkiaan 1 378 ryhmäkäytäntöasetusta. (Rousku 2005, 40.)

2.2 Ryhmäkäytännön toimintaperiaate

Ryhmäkäytäntö eli GP on aktiivihakemiston kautta käytettävä työkalu. GP:lla pystytään keskitetysti hallitsemaan käyttäjiä sekä konfiguroimaan tietokoneita, joiden käyttöjärjestelmänä toimii Microsoft Windows Server 2008, Microsoft Windows Server 2003, Microsoft Windows 2000, Microsoft Windows XP tai Microsoft Windows Vista. (Ivens 2003, 738.)

Ryhmäkäytännöillä tehtävät asetukset jaetaan viiteen eri kategoriaan:

- **Rekisteripohjaiset käytännöt**. Näihin kuuluu ryhmäkäytäntö Windows XP -käyttöjärjestelmälle ja sen osille sekä ohjelmille.
- **Suojausasetukset.** Näitä ovat paikallisen tietokoneen, toimialueen ja verkon suojausasetukset.
- **Ohjelmiston asentamisen ja ylläpidon asetukset.** Näitä käytetään ohjelmien asennuksen, päivityksen ja poistamisen keskitettyyn hallintaan.
- **Komentosarja-asetukset**. Näitä ovat komentosarjat tietokoneen käynnistämiseen ja sammuttamiseen sekä käyttäjän kirjaamiseen sisään ja ulos.
- **Kansion uudelleenohjauksen asetukset**. Näiden avulla järjestelmänvalvojat voivat ohjata käyttäjien erityiskansiot uudelleen verkkoon.

GP:n avulla voidaan määritellä automaattisia konfiguraatioita, jotka voidaan kohdistaa tiettyyn toimipaikkaan (site), toimialueeseen (domain) tai organisaatioyksikköön (OU). Organisaatioyksikkö voi sisältää joko yksittäisiä käyttäjiä, käyttäjäryhmiä sekä työasemia ja palvelimia. Yleinen käytäntö kuitenkin on, että laitteisto, kuten työasemat, sijaitsevat omissa organisaatioyksiköissä ja käyttäjät omissaan. Tämä johtuu siitä, että GP:t täytyy aina kohdistaa joko tietokoneisiin tai käyttäjiin. Kuitenkin, jos päällekkäisyyksiä esiintyy, tietokoneeseen tehdyt asetukset ohittavat aina käyttäjäkohtaiset asetukset.

Otettaessa GP käyttöön OU:ssa, täytyy kuitenkin huomioida se, että oletuksena käyttäjä, käyttäjäryhmä tai tietokone perii kaikki ylemmillä tasoilla sijaitsevien ryhmien asetukset, kuten esimerkiksi toimipaikan tai toimialueen päätasolle rakennetut De-

fault Domain Policyn määrittelyt. Tällainen periytyminen on kuitenkin mahdollista myös estää. Näistä asioista tulen kertomaan tarkemmin myöhemmin opinnäytetyössäni.

GP:lla tehdyt muutokset tulevat voimaan työasemaan sen käynnistymisen (computer configuration) tai käyttäjän sisäänkirjautumisen (user configuration) yhteydessä sekä halutuin aikavälein automaattisesti. Oletusaikaväli on 90 minuuttia + 30 minuutin satunnainen viive. Jos tietokone on päällä 24 tuntia vuorokaudessa, se hakee uusimmat GP-asetukset vähintään kahden tunnin välein. (Rousku 2005, 40.)

2.3 Ryhmäkäytäntöobjektit (Group Policy Object)

GP:lla tehdyt asetukset tallentuvat ryhmäkäytäntöobjekteiksi (GPO=Group Policy Object). GPO:t linkitetään aktiivihakemiston kautta haluttuun paikkaan, joita voivat olla toimipaikka, toimialue tai organisaatioyksikkö, kuten jo aikaisemmin on mainittu. GPO voi pitää sisällään useita eri määrittelyjä, jotka vaikuttavat välittömästi sen jälkeen, kun linkitys esimerkiksi OU:hun on tehty.

GPO:t tallentuvat palvelimelta löytyvään SYSVOL-nimiseen kansioon. Jokainen GPO saa oman tunnisteensa, GUID:n (Globally Unique Identifier), jonka avulla se voidaan tunnistaa vikatilanteissa. Esimerkiksi Default Domain Policylla sekä Default Domain Controllers Policylla on aina samat GUID:t jokaisessa aktiivihakemiston käyttämässä ympäristössä. Ryhmäkäytäntöjä tulisi aina hallita niitä varten suunnitelluilla työkaluilla. SYSVOL-kansion manipulointi aiheuttaa vikatilanteita ennemmin tai myöhemmin. (Kouti & Seitsonen 2005, 669.)

2.3.1 Lokaalit ryhmäkäytäntöobjektit

Toinen GPO-tyyppi on Local Group Policy Object (LGPO), joka löytyy jokaisesta tietokoneesta, on sitä käsin määritelty tai ei. LGPO:t eivät ole linkitetty aktiivihakemiston kautta, joten niitä ei voi sen kautta hallita. LGPO:n avulla pystytään konfigu-

roimaan lokaalisti tietokone toimimaan halutulla tavalla. LGPO-määrittelyt myös ajavat kaikkien aktiivihakemiston kautta tulevien GPO-määrittelyjen edelle. Jos käytössä on toimialue, on tällaisten yksittäisten tietokoneiden määrittely kuitenkin hyvin harvinaista ja hankalaa. LGPO:t mahdollistavat myös huomattavasti vähemmän määrittelyvaihtoehtoja, kuin aktiivihakemiston kautta määriteltävät GPO:t.

2.3.2 Oletuksena mukana tulevat ryhmäkäytäntöobjektit

Toimialueeseen (Domain) on oletuksena linkitetty kaksi GPO:a; Default Domain Policy sekä Default Domain Controller Policy. Näistä Default Domain Policy pitää sisällään asetuksia, jotka vaikuttavat esimerkiksi salasanakäytäntöön, sisäänkirjautumiseen sekä käyttäjätileihin. Default Domain Policyssä on määritelty salasanan minimipituus, kuinka monta kertaa käyttäjä voi yrittää syöttää salasanansa ennen käyttäjätilin lukkiutumista sekä salasanan uusimisvälin, mikä voi olla esimerkiksi 30 päivää. Default Domain Controllers Policy puolestaan pitää sisällään pääasiassa käyttäjäoikeuksia, kuten määrittelyt ryhmille, jotka voivat kirjautua lokaalisti ohjauspalvelimille (Domain Controllers). (Kouti & Seitsonen 2005, 632.)

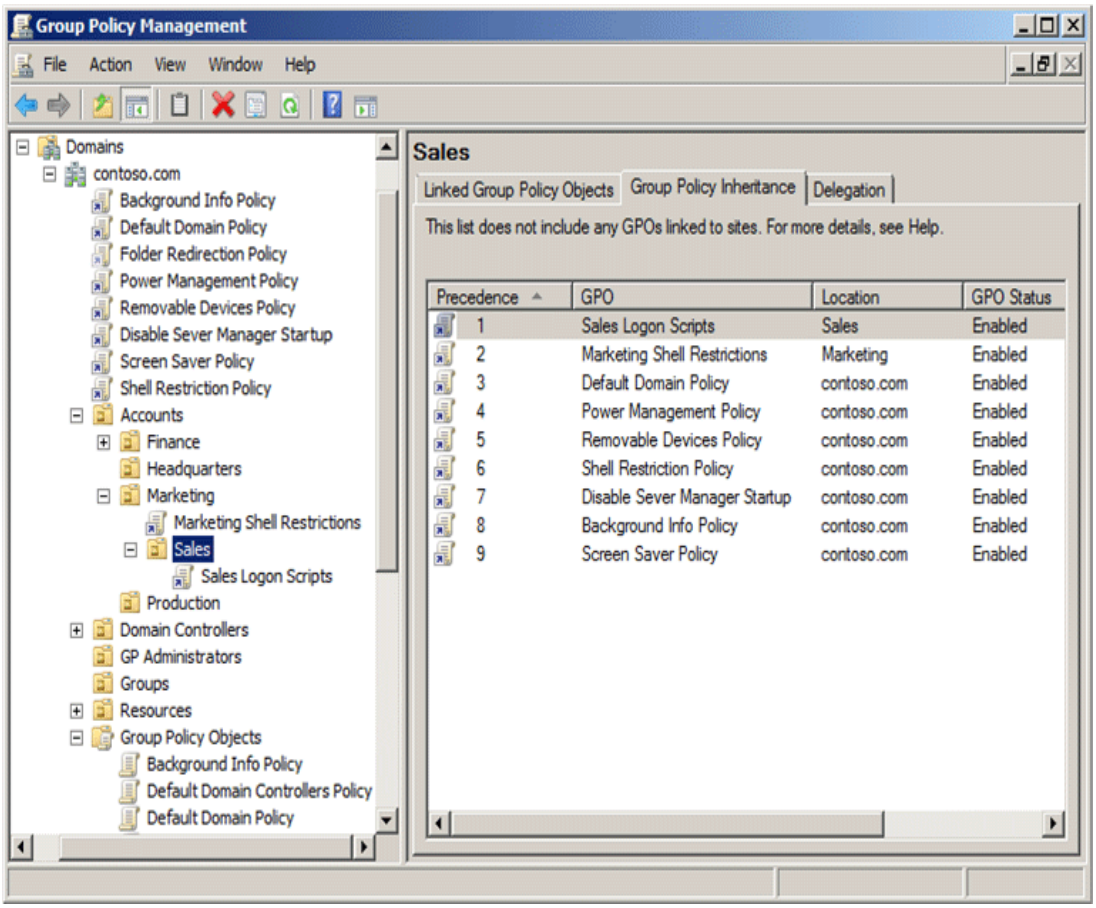
Näiden asetuksien lisäksi sieltä löytyy monta muuta asetusta, joiden muuttaminen vaikuttaa radikaalisti koko toimialueeseen. Nämä kaikki toimenpiteet on tehty parantamaan tietoteknisen ympäristön tietoturvaa ja asetukset ovat tarpeen vaatiessa muokattavissa.

Vaikka Default Domain Policy GPO on muokattavissa, niin siihen täytyy suhtautua suurella varovaisuudella. Yleisesti on kahta eri koulukuntaa, joilla on eri toimintamallit ajatellen Default Domain Policyn muokkausta:

- Käyttäjätileihin vaikuttavia asetuksia muokataan Default Domain Policy GPO:ssa. Tämän jälkeen varmistetaan, että sen asetukset tulevat toimialueella voimaan, riippumatta muista GPO:sta. Tämä tehdään määrittelemällä se arvojärjestyksessä korkeimmalle. Näin ollen tilanne on se, että jos toimialueelle

luodaan ja linkitetään muita GPO:ta, Default Domain Policy GPO ”voittaa” aina.

- Jätetään Default Domain Policy GPO muokkaamatta. Tehdään uusi GPO, joiden muutoksien on tarkoitus ajaa Default Domain Policy GPO:n muutoksien yli. Tämän jälkeen linkitetään uusi GPO toimialueelle ja määritellään arvojärjestyksessä Default Domain Policy GPO:ta korkeammalle. Tämä tilanne on havainnollistettu kuvassa 1.



Kuva 1. Uusi GPO on linkitetty Default Domain Policy GPO:n yläpuolelle.

2.4 Ryhmäkäytäntöjen määrät

Oletuksena ryhmäkäytännöillä voidaan konfiguroida vähintään 115 tietoturvaasetusta, 97 rekisteripohjaista tietokoneasetusta ja 359 rekisteripohjaista käyttäjäasetusta. Nämä luvut ovat Windows 2000 Service Pack 4 asennuksesta. (Kouti & Seitsonen 2005, 637.)

Alla olevassa kuvassa on listattu eri asetuksien määrät Windows 2000 Service Pack P4, Windows XP Service Pack 1 sekä Windows Server 2003 asennuksissa.

Asetuksen tyyppi	Windows 2000 SP4	Windows XP SP1	Windows Server 2003
Tietoturva-asetukset	115	136	145
Rekisteripohjaiset tietokoneasetukset	97	316	340
Rekisteripohjaiset käyttäjäasetukset	359	467	468

Kuva 2. GPO-asetusten määrät eri käyttöjärjestelmissä

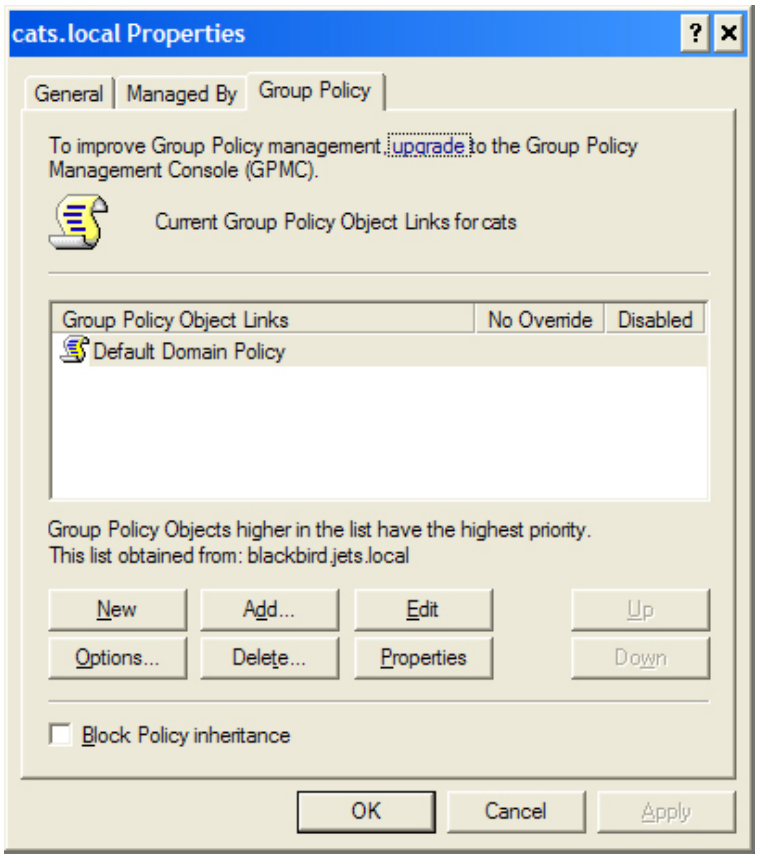
3 RYHMÄKÄYTÄNTÖJEN HALLINTATYÖKALUT

GP:n keskitettyä hallintaa varten tarvitaan aktiivihakemisto. Toki määrittelyt voidaan tehdä aikaisemmin läpikäydyllä Local Group Policy-objekteilla (LGPO), mutta tämä on aikaakuluttavaa ja konekohtaista määrittelyä. Koska GP on luotu tehostamaan keskitettyä hallintaa, on tärkeää tutustua niihin työkaluihin, joilla määrittelyt voidaan tehdä yhdeltä tietokoneelta vaikuttamaan toimialueen muihin tietokoneisiin ja tietokoneita käyttäviin käyttäjäryhmiin.

3.1 Aktiivihakemiston ryhmäkäytännöt

Windows 2000/Server 2003:n aktiivihakemistot pitävät sisällään valmiin työkalun GP:n ylläpitoon. Ohjelma on nimeltään Group Policy Object Editor (GPOE). Tämä työkalu löytyy aktiivihakemiston Users And Computers-työkalun ominaisuuksista. Tätä käytetään silloin, kun halutaan linkittää GPO toimialueeseen (domain) tai organisaatioyksikköön (OU). (Kouti & Seitsonen 2005, 632.)

Sama GP-editori aukeaa tarvittaessa myös aktiivihakemiston Sites and Services-työkalun kautta. Tätä käytetään silloin, kun halutaan linkittää GPO toimipaikkaan (site). (Kouti & Seitsonen 2005, 632.)



Kuva 3. Ryhmäkäytäntöjen hallintakonsoli aktiivihakemiston Users and Computers-työkalusta. (Huomaa myös “upgrade-valinta” jonka kautta on mahdollista ottaa GPMC-työkalu käyttöön).

GPOE on Microsoft Management Consolen (MMC) kautta käytettävä hallintakonsoli. Se on kuitenkin hyvin pelkistetty ja tietyiltä osilta puutteellinen työkalu GP:n hallintaan. Siitä puuttuu aktiivihakemiston tyylinen hierarkkinen näkymä, jonka avulla voisi erottaa toimialueen ja organisaatioyksiköiden muodostaman rakenteen.

Microsoft julkaisi jatkossa Group Policy Management Console-nimisen ohjelman (GPMC), joka pitää sisällään erillisen käyttöliittymän GP:n hallintaa varten, tuoden samalla mahdollisuuden mm. varmuuskopiointiin ja raportointiin. Näitä ominaisuuksia ei aktiivihakemiston GPOE:sta löydy.

Nykypäivänä suurin osa verkon ylläpitäjistä käyttää GP:n hallintaan nimenomaan GPMC:a, joten tarkoitukseni on tässä opinnäytetyössä keskittyä enemmän sen ominaisuuksiin.

3.2 Group Policy Management Console (GPMC)

Windows Server 2003 toi mukanaan tervetulleen parannuksen GP:n hallintaan. Ohjelman nimi on Group Policy Management Console (GPMC). GPMC voidaan käynnistää Käynnistä-valikosta (Start), valitsemalla Hallintatyökalut (Administrative Tools) | Group Policy Management.

GPMC pitää sisällään kaikki tarpeelliset työkalut ryhmäkäytäntöjen hallintaan liittyen, pois lukien henkilökohtaiset käyttäjien asetukset. GPMC mukana tuli myös uusia toiminnallisuuksia, kuten raportointi, varmuuskopiointi ja yksittäisten GPO-määritysten palauttaminen. (Kouti & Seitsonen 2005, 631.)

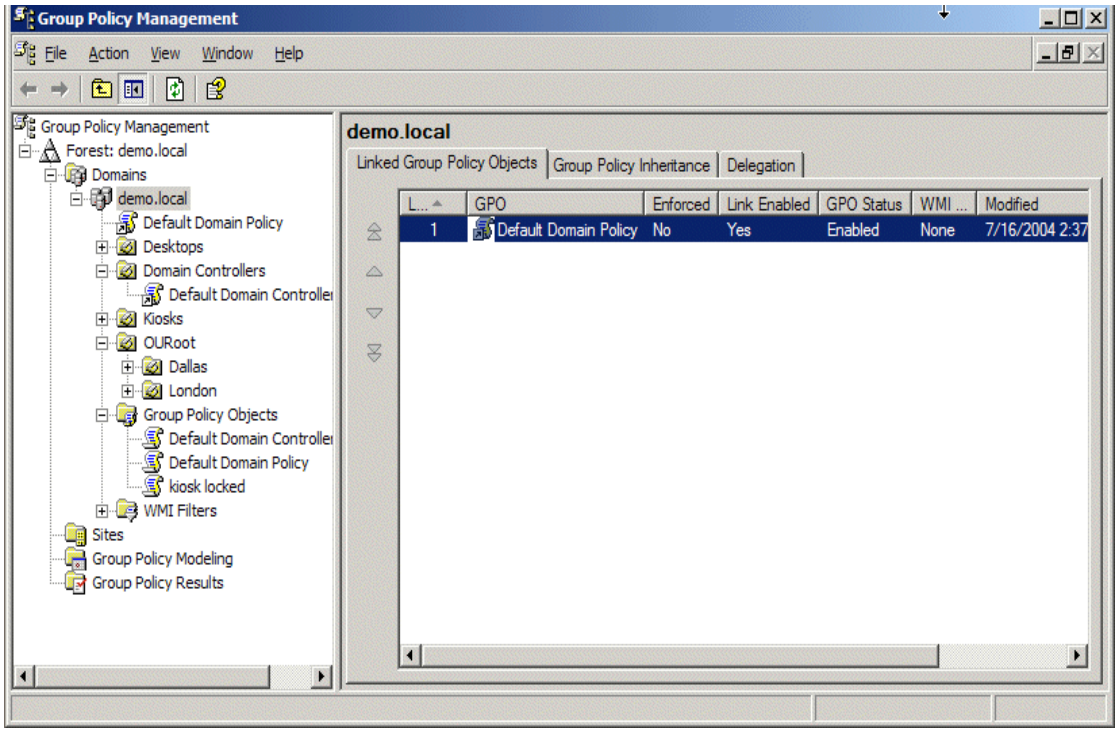
GPMC:n käyttöä varten tarvitaan Windows Server 2003 tai Windows XP (vähintään Service Pack 1 sekä .NET Framework asennettuna) käyttöjärjestelmällä varustettu tietokone. Windows 2000 ohjauspalvelimet pitää olla päivitetty Service Pack 2 tasolle, vaikkakin Service Pack 3 taso on suositeltavaa. (Kouti & Seitsonen 2005, 631.)

Microsoft julkaisi myöhemmin GPMC:lle Service Packin, joka nykyään on poikkeuksetta käytössä. Usein törmää nimeen GPMC SP1, joka on siis tuo päivitetty versio. SP1 toi mukanaan seuraavat päivitykset:

Ongelmien korjaukset. Käyttäjien ilmoittamat ongelmat mallikomentosarjoissa, raportointityökalussa sekä Migration Table Editorissa (MTE), jota käytetään GPO:en kopiointiin toimialueiden välillä.
Uudet käyttökielet. SP1 jälkeen GPMC:a pystyy käyttämään englannin lisäksi ranskaksi, saksaksi, japaniksi, kiinaksi sekä espanjaksi.

Päivitetty EULA-lisenssi. SP1 pitää sisällään päivitetyn EULA:n (end-user license agreement), jonka perusteella GPMC:n käyttö on sallittua niin kauan, kun omistaa voimassaolevan Windows Server 2003 tai Windows 2000 Server lisenssin.
Päivitetty MSXML4. MSXML4 on päivitetty MSXML4 Service Pack 1:sta MSXML4 Service Pack 2:een.

GPMC:n avulla GPO:en määrittely, hallinta sekä vianselvitys ovat helpompaa, kuin aikaisemmalla aktiivihakemistoon linkitetyn työkalun kautta. Tämä perustuu siihen, että GPMC tuo mukanaan uuden käyttöliittymän.

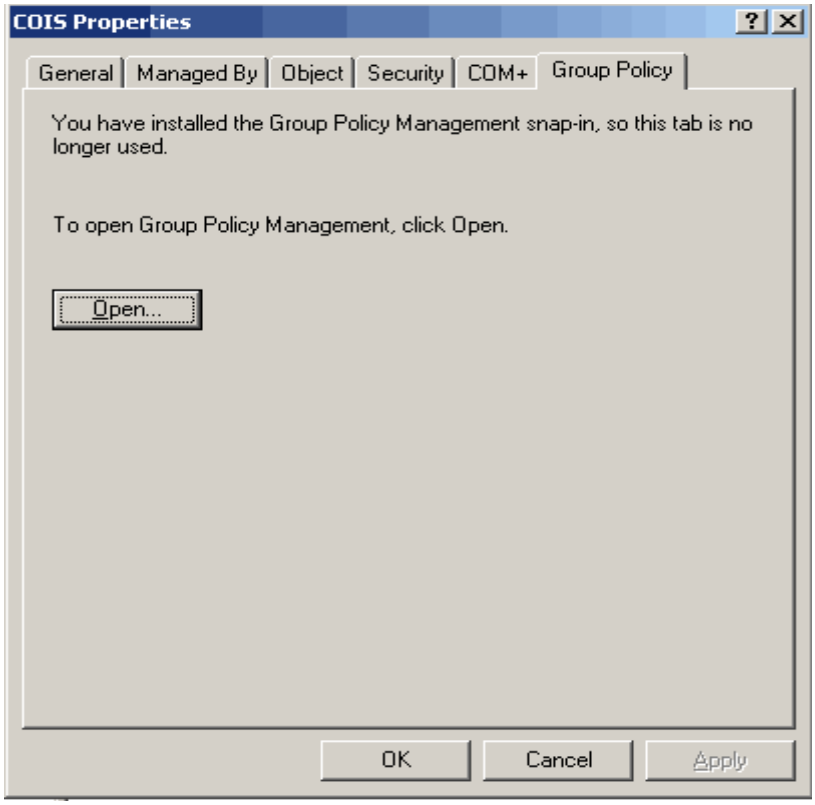


Kuva 4. Group Policy Management Consolen käyttöliittymä

Kuvassa 4 olevasta puuhierarkiasta näkee helposti, mihin paikkoihin GPO on linkitetty ja minkä niminen se on. Lisäksi puuhierarkia sisältää Group Policy Objects -haaran, minne listautuvat automaattisesti kaikki olemassa olevat GPO:t.

GPMC pitää sisällään myös ikkunan, josta pystyy tarkastelemaan luotua GPO:a helposti ja nopeasti, kuten kuvassa 4 on esitetty. Oikeanpuoleisen ominaisuusikkunan kautta pystytään mm. nopeasti toteamaan, onko luotu GPO käytössä (GPO Status), onko se linkitettynä (Link Enabled) ja koska GPO on luotu (Modified).

Kun GPMC on asennettuna, se korvaa aktiivihakemiston Users and Computers sekä Sites and Services työkalujen “Properties” – valinnoista löytyvän GP hallinnan. GPMC:n asennuksen jälkeen sieltä on mahdollista valita ainoastaan Open-toiminto, joka ohjaa käyttäjän GPMC:n käyttöön. Kuvassa 5 on tilannetta selventävä kuva.



Kuva 5. GPMC asennuksen jälkeen Properties-ikkunasta löytyvä Group Policy toiminto korvataan GPMC:n Open-toiminnolla.

4 RYHMÄKÄYTÄNTÖJEN HALLINTA GROUP POLICY MANAGEMENT CONSOLELLA

Ryhmäkäytäntöjen tärkeimpiä ominaisuuksia on linkittäminen ja periytyminen. Näitä molempia voidaan hallita GPMC:n kautta. Linkittämisellä tarkoitetaan sitä, kun luo-

daan uusi GPO, muokkaamalla joko käyttäjään tai tietokoneeseen vaikuttavaa asetusta, ja tämän jälkeen määritellään joko toimialue tai OU, missä halutaan GPO:n tulevan voimaan. Linkittämisen toinen ominaisuus on se, että jos halutaan jonkun OU:n GPO:n asetusten tulevan voimaan myös toisessa OU:ssa, voidaan tämä jo kerran luotu GPO linkittää toiseenkin OU:hun, eikä näin ollen tarvitse luoda uutta GPO:ta. GPO:ta ei voi kuitenkaan linkittää oletuksena aktiivihakemiston mukana tuleviin säilöihin, joita ovat Builtin, Computers ja Users, koska nämä eivät ole OU:tä. (Kouti & Seitsonen 2005, 673).

GPMC:ssa uuden GPO:n luonti ja linkittäminen voidaan tehdä kahdella tavalla:

- Luodaan GPO suoraan Group Policy Objects-säilöön. Tämän jälkeen voidaan valita haluttu toimialue tai OU ja linkitetään GPO manuaalisesti sinne.
- Voidaan valita halutun toimialueen tai OU:n päällä optio, jolla luodaan ja linkitetään uusi GPO. Tämän jälkeen luotu GPO tulee automaattisesti näkyviin myös Group Policy Object-säilöön. (Moskowitz 2004, 27.)

4.1 GPO:n tai sen linkityksen poistaminen

Jos GPMC on asennettuna, on GPO:n poistaminen yksinkertainen operaatio. Haluttu GPO etsitään Group Policy Objects-haarasta, valitaan poistettava GPO hiiren oikealla klikkauksella ja otetaan Delete-toiminto. Käyttäjää pyydetään varmistamaan poisto, ennen kuin se lopullisesti poistetaan. (Kouti & Seitsonen 2005, 714.)

Linkityksen poistaminen tapahtuu hyvin samalla tavalla. Ensin etsitään haara, minne GPO on linkitetty, tämän jälkeen valitaan GPO hiiren oikealla klikkauksella ja poistetaan Link Enabled käytöstä. Käyttäjältä pyydetään vielä varmistus poistosta. Linkityksen poisto ei vaikuta itse GPO:in, eikä myöskään poista linkityksiä toiseen toimipaikkaan. (Kouti & Seitsonen 2005, 714.)

GPO:n linkitys on hyvä myös jättää tekemättä silloin, kun on tarkoitus luoda uusi GPO, johon halutaan lisätä useita eri asetuksia. Jos linkitys olisi käytössä samalla,

kun asetuksia muokataan, hakisivat GPO:n vaikutuksenalaiset käyttäjät tai tietokoneet myös nuo puutteelliset asetukset. Olettaen, että määrittelyyn menee tarpeeksi aikaa. Näin ollen linkitys kannattaa kytkeä päälle vasta, kun GPO on käyttövalmis. (Moskowitz 2004, 61.)

4.2 Periytyminen

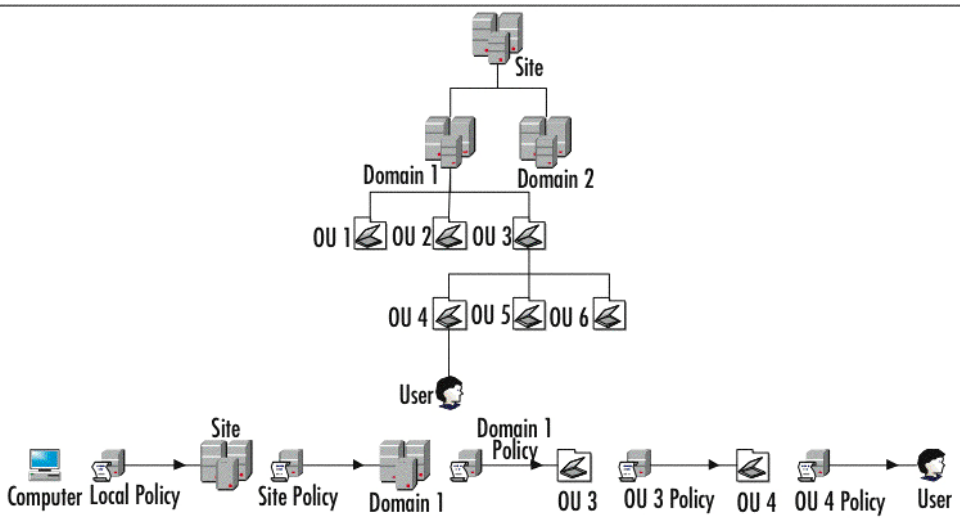
Ennen kuin GPO:en luonti ja niiden linkitys aloitetaan, on hyvä hahmottaa niiden vaikutus oman aktiivihakemiston rakenteeseen. Miten GPO:t prosessoidaan ja miten periytymisen hierarkkinen rakenne vaikuttaa siihen, mitkä asetukset tulevat käyttäjille ja tietokoneille voimaan. Näiden asetusten tunteminen antaa paljon enemmän mahdollisuuksia hyödyntää GP:n ominaisuuksia. (Ivens 2003, 743.)

GP voidaan määritellä vaikuttamaan käyttäjiin ja tietokoneisiin niille tasoille, jotka noudattavat aktiivihakemiston rakennetta. Näitä ovat toimipaikka, toimialue ja organisaatioyksikkö. Ylemmille tasoille määritellyt GPO:t periytyvät automaattisesti alemmille tasoille. Jos samassa tasossa on määriteltynä kaksi GPO:a, joiden asetukset ovat ristiriidassa, sovelletaan korkeamman prioriteetin omaavan GPO:n asetuksia. (Group Policy Inheritance 2003.)

GPO:a sovelletaan käyttöön samalla tavalla tasomäärittelyjen perusteella, kuitenkin tärkeysjärjestys menee alhaalta ylöspäin. Eli OU:hun määritelty GPO kumoaa esimerkiksi toimialueelle määritellyn GPO:n vaikutuksen. Windows 2000, Windows XP Professional sekä Windows 2003 Server käyttöjärjestelmissä GPO:t prosessoidaan seuraavalla tavalla:

1. Lokaalit GPO:t (jos niitä on tietokoneelle määritelty)
2. Toimipaikan GPO:t
3. Toimialueen GPO:t
4. Organisaation GPO:t
5. *isäntä* OU:n GPO:t
6. *lapsi* OU:n GPO:t

Kuvassa 6 on selvitetty, miten prosessointi tapahtuu, kun käyttäjä kirjautuu sisään tietokoneelle.



Kuva 6. GPO:n prosessointikaavio sisäänkirjautumisen yhteydessä.

Kuvasta 6 voidaan todeta, että toimipaikan, toimialueen ja organisaatioyksiköiden säännöt tulevat käyttäjälle voimaan sisäänkirjautumisen yhteydessä. Kaikki määrittelyt, jotka tulevat OU 3 tasolta, tulevat voimaan ennen OU 4:n määrittelyjä. Periytymissäännön mukaisesti OU 3:n määrittelyt tulevat voimaan kaikille OU 3, OU 4, OU 5 ja OU 6 tasoilla oleville objekteille, vaikka OU 4, OU 5 tai OU 6 tasoille ei olisikaan tehty yhtään määrittelyä. (Shinder ym. 2003, 566.)

Jos OU 3:ssa on määritelty käyttöönotettavaksi sääntö, jota ei ole määritelty OU 4:ssa, OU 3:en säännöt tulevat voimaan myös OU 4:ssa. Jos sääntö on pois käytöstä OU 3:ssa, mutta on käytössä OU 4:ssa, tulee se tällöin voimaan OU 4:ssa. Tämä on periytymissäännön mukainen prosessi, jossa lähimpänä oleva GPO jää voimaan. (Shinder ym. 2003, 566.)

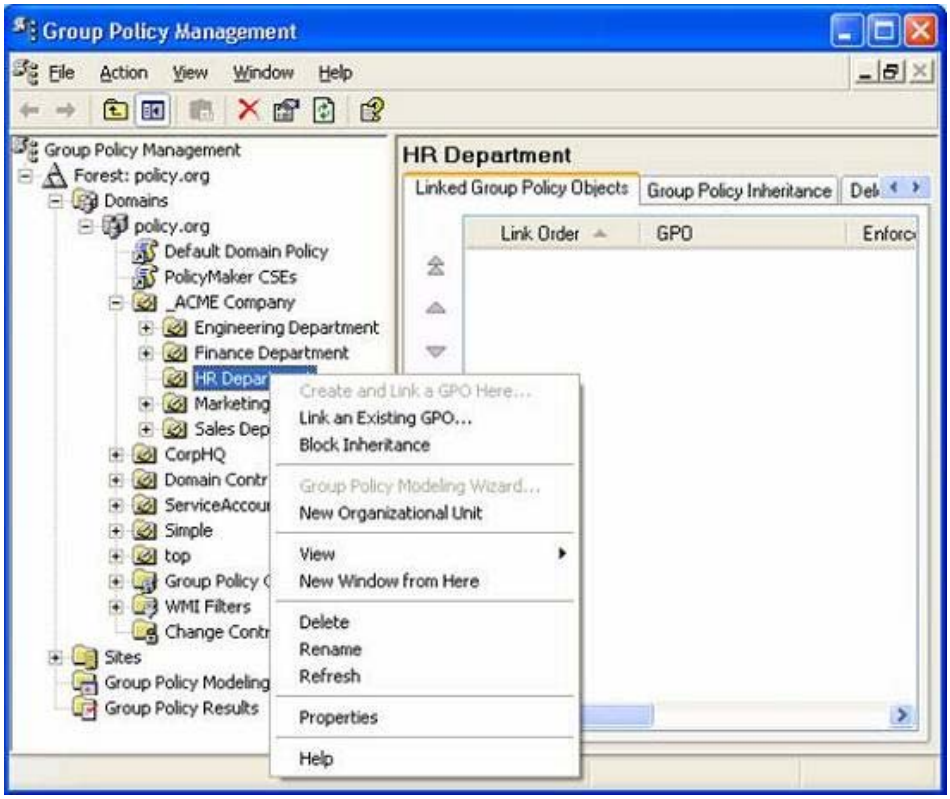
4.2.1 Periytymisen estäminen

Periytyminen voidaan tarpeen vaatiessa myös estää. Tällöin puhutaan periytymisenestosta (Block Inheritance). Jos periytyminen estetään esimerkiksi OU-tasolla, kaikki toimipaikalta ja toimialueelta sekä ylemmiltä OU-tasoilta tulevat GPO:t eivät tule voimaan. Periytymisenesto ei kuitenkaan vaikuta tietokoneiden lokaalisti tehtyi-

hin sääntöihin, vaan ainoastaan aktiivihakemiston kautta tuleviin sääntöihin. (Shinder ym. 2003, 566.)

Poikkeuksen periytymisen estoon tekevät GPO:t, jotka on merkitty pakotetuiksi (Enforced). Tämä toiminto tunnetaan myös nimellä *no-override*. No-override nimeä käytetään aktiivihakemiston omassa Group Policy editorissa, eli silloin, kun käytössä ei ole GPMC:a). Tällöin kaikki ylemmällä tasolla olevat GPO:t, jotka on merkitty pakotetuiksi, tulevat voimaan myös alemmilla tasoilla. Siitäkin huolimatta, vaikka alemmilla tasoilla olisi käytössä periytymisen esto (Block Inheritance). Se on kuitenkin erittäin voimakas määrittelytapa, jonka vaikutukset täytyy olla hyvin tiedossa.

Periytymisen esto tehdään GPMC:n kautta valitsemalla OU, jolta halutaan periytyminen estää. Tämä toiminto on esitelty kuvassa 7.



Kuva 7. GPO:n periytyminen voidaan estää Block Inheritance – toiminnolla.

Kun periytymisenesto on käytössä, on hyvä muistaa, että se vaikuttaa silloin kaikkiin OU:hun linkitettyihin GPO:hin, eikä vain yhteen, jonka periytyminen halutaan estää.

4.3 Käyttäjäprofiilien hallinta toimialueella

Ryhmäkäytäntöjen yksi käyttömahdollisuuksista on, rajoitusten tekemisen lisäksi, mahdollisuus hallita käyttäjien profiileja ja käyttäytymistä verkossa. Käyttäjäprofiilit on mahdollista säilyttää palvelimella, jolloin ne liikkuvat käyttäjien mukana työasemista riippumatta. Tällöin hyödynnetään mm. kansioiden uudelleenohjausta sekä levyresurssien käyttöä suoraan palvelimelta.

4.3.1 Kansion uudelleenohjaus (Folder Redirection)

Kun käyttäjä kirjautuu ensimmäistä kertaa työasemalle, Windows-käyttöjärjestelmä automaattisesti luo tälle käyttäjälle profiilin. Profiilit tallennetaan Documents and Settings-kansioon, joka pitää sisällään alikansioita käyttäjien nimien perusteella.

Käyttäjän profiili pitää sisällään tiettyjä alikansioita ja tiedostoja, jotka olisi parempi säilyttää palvelimella lokaalin työaseman asemasta. Käyttäjän profiilitiedostot sijaitsevat kansiossa %SystemDrive%\Documents and Settings\User sisäänkirjautumiseen käytettävän tunnuksen mukaisesti. Profiilissa säilytettäviä tiedostoja ovat mm. Internet-selaimen suosikit ja työpöytä pikakuvakkeineen. Kun näiden kansioiden sisältämät tiedostot ovat fyysisesti palvelimella, ne voidaan keskitetysti varmuuskopioida. (Kouti & Seitsonen 2005, 662.)

Yleensä verkon ylläpitäjät neuvovat käyttäjiä tallentamaan kaiken oleellisen tiedon verkkolevyille. Näin ollen tärkeät tiedostot pysyvät automaattisesti palvelimella. Mutta väistämättä jossain vaiheessa tulee vastaan tilanne, missä käyttäjä tallentaakin jotain työaseman kiintolevylle. Jos kiintolevy sattuu rikkoutumaan, myös kaikki siellä sijaitseva tieto on mennyttä.

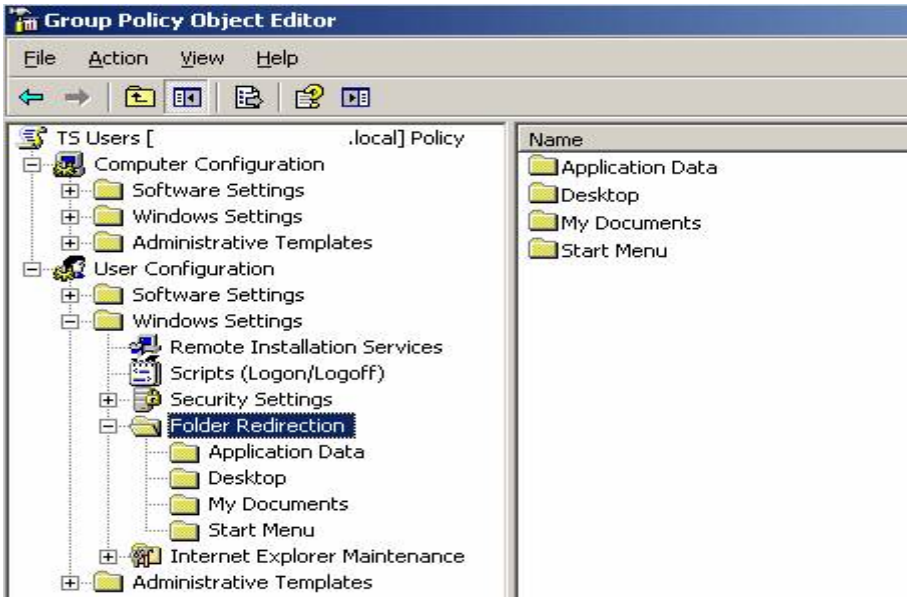
Kun kansion uudelleenohjaus on käytössä, myös järjestelmänvalvojat saavat mahdollisuuden keskitettyyn hallintaan, samalla kuin käyttäjät voivat käyttää työasemaa aivan kuin ennenkin. Perusidea on siinä, että luodaan GPO, joka pitää sisällään asetukset yhden, tai useamman, kansion uudelleenohjaamisen palvelimelle. Yleensä

GPO määritellään OU-tasolle, jolloin sen vaikutus tulee voimaan kaikille OU:n sisällä oleville käyttäjille. (Moskowitz 2004, 372.)

Windows 2000/Server 2003 Aktiivihakemiston sisältämä kansion uudelleenohjaus antaa mahdollisuuden ohjata tietyt käyttäjän profiilissa sijaitsevat kansiot tiedostopalvelimelle. Kansion uudelleenohjauksen käyttöön ottavan GPO:n asetuksiin pääsee Group Policy Object Editorin haarasta User Settings | Windows Settings | Folder Redirection. Sen kautta seuraavat kansiot ovat mahdollista uudelleenohjata:

- Application Data
- Desktop
- My Documents
- My Pictures
- Start Menu

(Kouti & Seitsonen 2005, 662.)

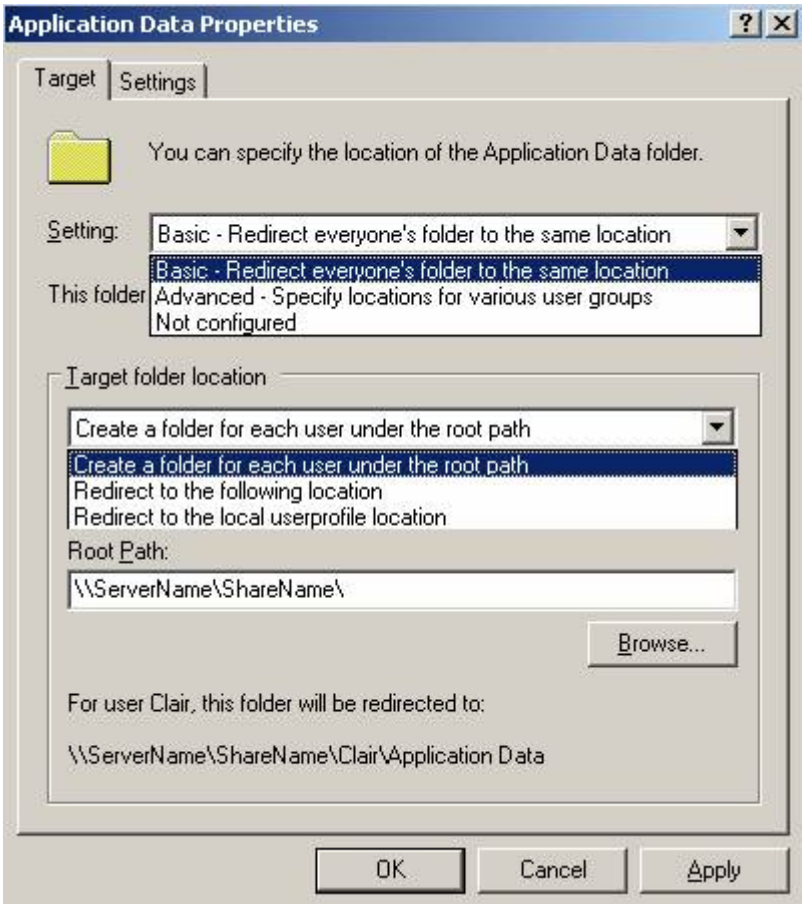


Kuva 8. Kansion uudelleenohjaus tapahtuu GPO:n määrittelyllä

Kansioiden uudelleenohjaukseen voidaan käyttää kahta eri tapaa; Perus (Basic) tai Edistynyt (Advanced.) Perus pitää sisällään määrittelyt, joiden avulla jokaisen käyttäjän, johon GPO vaikuttaa, kansiot uudelleenohjataan samaan jakokansioon palvelimella. Tämän yhteisen jakokansion sisälle voidaan automaattisesti luoda henkilö-

kohtaiset, tietoturvalliset kansiot jokaista yksittäistä käyttäjää varten. (Moskowitz 2004, 372.)

Edistynyt vaihtoehdon avulla voidaan käyttää hyväksi aktiivihakemiston ryhmiä ja niiden jäsenyyksiä. Näiden avulla voidaan määritellä, minne jakokansioon kunkin käyttäjän tiedot uudelleenohjataan. Esimerkiksi voidaan määritellä, että kaikkien käyttäjien, jotka kuuluvat Testi-ryhmään, kansiot uudelleenohjataan palvelimelle X ja sieltä Työpöydät nimiseen kansioon. (Moskowitz 2004, 372.)



Kuva 9. Application Datan ominaisuuksista voidaan valita Perus tai Edistynyt sekä muut tarvittavat optiot.

Kun kansion uudelleenohjaus on käytössä, on hyvä muistaa tarkistaa vielä jakokansioiden käyttöoikeudet. Käyttäjällä täytyy loogisesti olla täysi käyttöoikeus omaan palvelimella sijaitsevaan kansioon, joka pitää sisällään hänen profiilinsa tiedostot.

4.3.2 Käyttäjälle määritelty levykiintiö (Disk quota)

Levykiintiö rajoittaa käyttäjän käyttämän levytilan määrää joko lokaalisti työasemalla tai palvelimella. Levykiintiö on hyvin tärkeä työkalu, koska ilman sitä, pelkästään yksi käyttäjä voisi täyttää koko palvelimen salliman levytilan. (Moskowitz 2004, 421.)

Kiintiötä voidaan myös käyttää toisellakin tavalla, kuin tallennuskapasiteetin rajoittamisena. Toinen tapa on rajoittaa tiedostojen sekä kansioiden määrää, joita käyttäjä pystyy tekemään. (Disk quota – Wikipedia.)

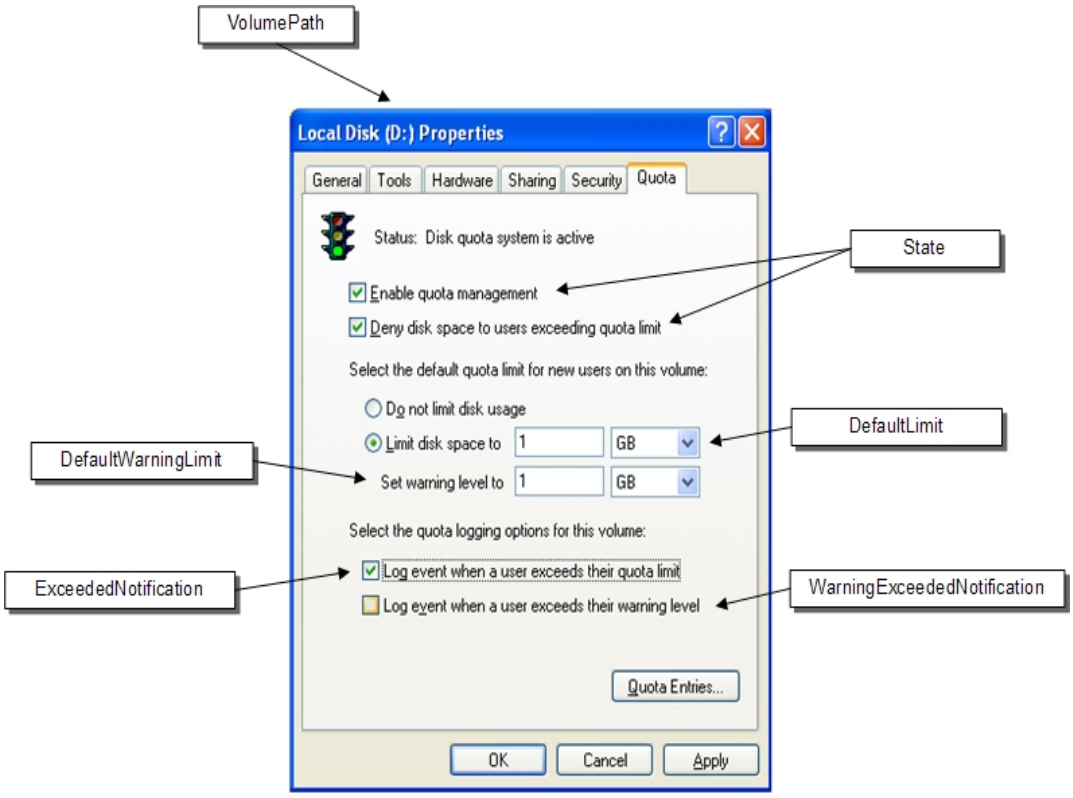
Levykiintiötä ei voida määritellä tietokonepohjaisesti. Sen sijaan se noudattaa NTFS-pohjaista levyosiomäärittelyä. Esimerkiksi kiintolevy voidaan jakaa eri osioihin; C, D ja E. Jokaisella levyosiolla on oma kiintiö. C- ja D-osioille voidaan määritellä kiintiö, mutta E-osiosta se voidaan jättää pois. Myös määrä voidaan määritellä levyosion mukaan. C-osiolle voidaan laittaa 50 Mt tilaa käyttäjää kohti, kun taas D-osiolla se voi olla 100 Mt.

Levykiintiö voidaan määritellä käyttäjälle käyttäjä/levyresurssi-periaatteella. Eli käyttäjällä on käytössään oma verkkolevy-kansio, jolle voidaan antaa tietty määrä tallennuskapasiteettia. Harmillisesti levykiintiö ei kuitenkaan sisällä ominaisuutta, jolla voitaisiin määritellä tietyn palvelimella sijaitsevan jaon yhteiskapasiteetti. Esimerkiksi niin, että ”kotikansio” niminen jakokansio ei saa kasvaa yli 500 Mt:n. Vaan kaikki käyttäjät saavat käyttöönsä heille määritellyn kiintiön ja riskinä on koko levytilan täyttyminen.

Levykiintiö voidaan määritellä kolmella eri tavalla:

- Kaikilla käyttäjillä, joilla on tiedostoja verkkolevyllä, on sama kiintiö.
- Tietyille käyttäjille, joilla on tiedostoja verkkolevyllä, määritellään tietty kiintiö.
- Kaikilla käyttäjillä, joilla on tiedostoja verkkolevyllä, on sama kiintiö ja sen lisäksi tietyille käyttäjille määritellään eri kiintiö.

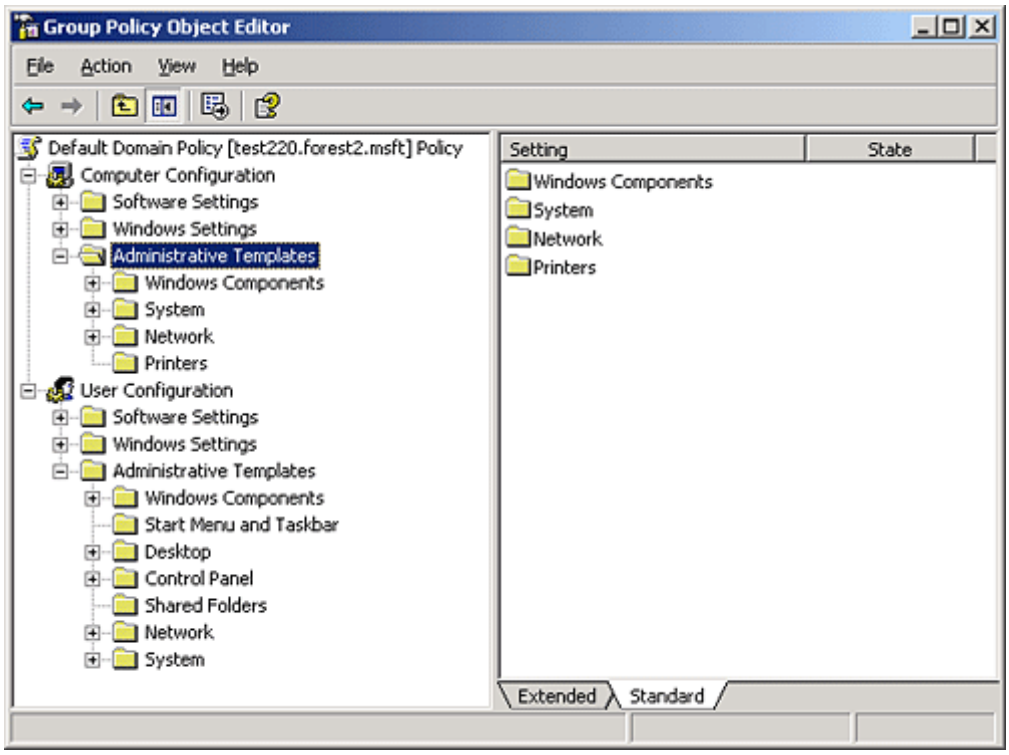
Yllä olevien määrittelyiden lisäksi verkon ylläpitäjä yleensä ottaa käyttöön myös varoitusilmoituksen. Varoitusilmoitus määritellään halutulle tasolle, jonka jälkeen käyttäjille tulee ilmoitus siitä, kun tallennuskapasiteetti alkaa täyttyä. Verkon ylläpitäjä voi myös kerätä näistä tapahtumista lokitietoja. (Disk quota – Wikipedia.) Varoitustason lisäksi voidaan myös määritellä optio, joka vaatii käyttäjää vapauttamaan tilaa verkkolevyltään, ennen kuin hän pystyy tallentamaan sinne lisää tietoa.



Kuva 10. Levykiintiön käyttöönotto levyosiolla sekä siihen sisältyvät määrittelyt.

4.4 Hallintamallit – Administrative templates

Hallintamallien avulla hallitaan rekisteriin perustuvia asetuksia, jotka vaikuttavat mm. sovelluksiin, työpöydän ulkoasuun ja järjestelmän palvelujen käyttäytymiseen. Hallintamallit ovat Unicode-merkistöä käyttäviä tekstitiedostoja, joiden pääte on .adm. Näiden avulla muodostuu käyttöliittymä GP:n muokkausta varten, jolloin pystytään tekemään tarvittavia muutoksia verkossa oleviin tietokoneisiin tai rajoittaa tietokoneita käyttävien käyttäjäryhmien oikeuksia.



Kuva 11. Hallintamallit käytettävissä GP-hallintakonsolin kautta.

Hallintamalleilla saadaan parhaiten työasemat ja käyttäjät toimimaan halutulla tavalla, koska niiden tarjoamat muokkausvaihtoehdot ovat lähes rajattomat. Niiden avulla tehdään suurin osa GPO:sta, koska siellä sijaitsevat asetukset vaikuttavat suoraan rekisteritietoihin, joka tekee asetuksista pysyviä.

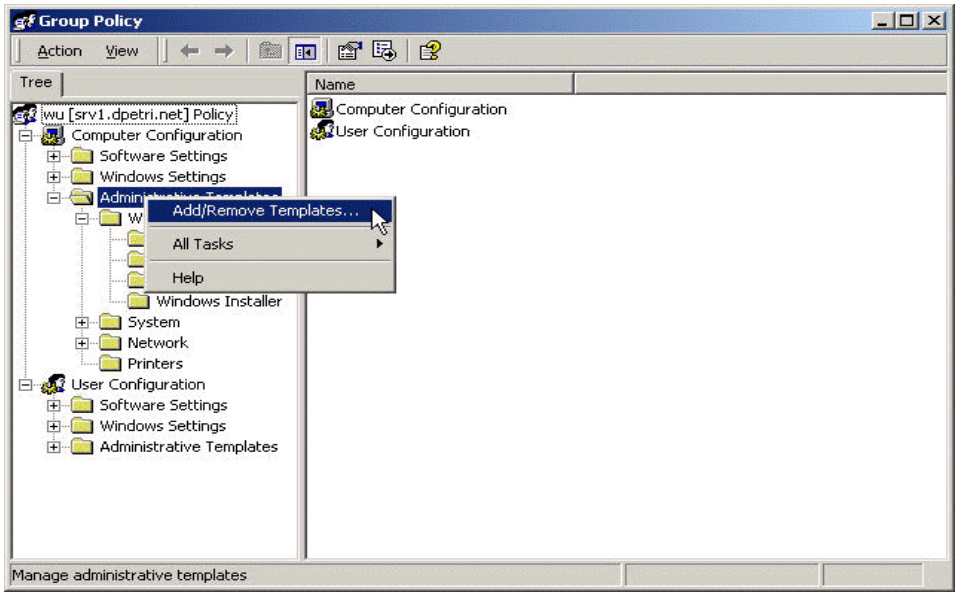
Hallintamallien muokkausvaihtoehtoja on käytössä kaksi. Niiden avulla voidaan tehdään muutoksia joko tietokoneisiin (Computer Configuration) tai käyttäjiin (User Configuration). Tietokoneisiin tehtävät muutokset muokkaavat rekisteristä HKLM-haaraa (HKEY_LOCAL_MACHINE) ja käyttäjämuutokset muokkaavat HKCU-haaraa (HKEY_CURRENT_USER).

Oletuksena Windows 2000-järjestelmässä on käytössä kolme hallintamallia (conf.adm, inetres.adm ja system.adm). Windows Server 2003-järjestelmässä näitä on viisi (conf.adm, inetres.adm, system.adm, wmplayer.adm ja wuau.adm). Hallintamalleja säilytetään palvelimella %systemroot%/inf-kansiossa. (Kouti & Seitsonen 2005, 652.)

Tiedosto	Asetukset	Huomio
AER_1003.adm	Vikaraportin lähetys	Vain Windows 2000 SP3 ja SP4
common.adm	Windows NT:n asetukset	Ei voida määritellä GP:lla. Ei Windows XP:ssa.
conf.adm	NetMeetingin asetukset	---
inetcorp.adm	IEAK asetukset aikaisempiin Internet Explorer-versioihin	Ei voida määritellä GP:lla
inetres.adm	Internet Explorerin asetukset	---
inetset.adm	IEAK asetukset aikaisempiin Internet Explorer-versioihin	Ei voida määritellä GP:lla
system.adm	Kaikki muut asetukset paitsi IE ja NetMeeting	Suurin hallintamalli, sisältää eniten asetuksia
windows.adm	Windows 9x: asetukset	Ei voida määritellä GP:lla. Ei Windows XP:ssa.
winnt.adm	Windows NT:n asetukset	Ei voida määritellä GP:lla. Ei Windows XP:ssa.
wmp.adm (wmplayer Windows XP:ssa ja Windows Server 2003:ssa	Windows Media Playerin asetukset	---
wuau.adm	Windows Update Automatic Update clientin asetukset	Windows 2000 SP3 (tai uudempi) XP SP1 (tai uudempi) ja Windows Server 2003 (tai uudempi)

Kuva 12. Oletuksena Windows Server 2003 mukana tulevat hallintamallit ja niiden käyttötarkoitukset.

Jos valmiiden hallintamallien käyttämien 800 rekisterimuokkauksen joukosta ei löydy haluttua määrittelyä, on mahdollista luoda oma malli. Lisää malleja pystyy lisäämään valitsemalla Administrative Templates-kohdan vikavalikosta toiminto Add/Remove Templates joko Computer Configuration -haarassa, tai User Configuration -haarassa. Omien mallien tekemisestä kerron myöhemmin tässä opinnäytetyössä.



Kuva 13. Lisää uusi hallintamalli.

4.4.1 Rekisterimuutoksien sijainti

Windows NT 4.0 – järjestelmässä oli käytössä järjestelmäkäytännöt (System Policy template), jolla tehdyt määrittelyt muokkasivat rekisteriä useista eri paikoista. Tehtyjen muutoksien poistaminen oli ongelmallista, koska sitä varten piti tehdä toinen määrittely, joka poistaa aiemmin tehdyn määrittelyn, tai sitten piti käyttää tietokoneen omaa rekisterieditoria. Tästä johtuen, Windows 2000-käyttöjärjestelmästä lähtien, kaikki rekisterimuutokset, jotka tehdään GP:lla, tapahtuvat neljässä rekisteriavaimessa. (Kouti & Seitsonen 2005, 658.) Nämä rekisteriavaimet ovat:

HKEY_LOCAL_MACHINE\Software\Policies (tietokonemäärittelyt, oletussijainti)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies (tietokonemäärittelyt, vaihtoehtoinen sijainti)
HKEY_CURRENT_USER\Software\Policies (käyttäjämäärittelyt, oletussijainti)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies (käyttäjämäärittelyt, vaihtoehtoinen sijainti)

Nämä sijainnit ovat suositeltuja sen takia, koska niiden pääsyä on oletuksena rajoitettu käyttöoikeuksin, jolloin tavallinen käyttäjä ei pääse muokkaamaan avaimia. Kun näihin haaroihin vaikuttava GPO kytketään käyttöön, rekisteriavainta muokataan. Kun GPO kytketään pois käytöstä, myös rekisterissä oleva muutos poistuu. (Moskowitz 2004, 208.)

4.4.2 Ohjelmistovalmistajien hallintamallit

Hallintamallit, jotka tulevat Windowsin mukana, ovat vain pieni osa mahdollisuuksista, joita niiden avulla voidaan hallita. Hallintamallien idea on, että järjestelmänvalvoja tai kolmannen osapuolen toimittaman ohjelmiston valmistaja voi tehdä omia

malleja. Itse tehdyillä malleilla pystytään rajoittamaan tai muokkaamaan käyttöjärjestelmää tai ohjelmistoa halutulla tavalla. (Moskowitz 2004, 211.)

Esimerkiksi Microsoft Office tarjoaa omia malleja, joilla pystyy tekemään käyttörajoituksia sen mukana tuleviin ohjelmistoihin. Näiden käyttöönottoa varten voi Internetistä ladata tarvittavat työkalut.

- Office 2000 Resource Kit tools: www.microsoft.com/office/ork/2000/appndx/toolbox.htm
- Office XP Resource Kit tools: www.microsoft.com/office/ork/xp/appndx/appa18.htm
- Office 2003 templates, Office 2003 Resource Kit: www.microsoft.com/office

Ohjelma, jolla asennetaan mallit käyttöön, on Office 2000 ja Office XP – ympäristöissä nimeltään Orktools.exe. Office 2003 – ympäristössä ohjelma on nimeltään Ork.exe. Kun haluttu Resource Kit on asennettu ohjauspalvelimelle, sen sisältämät hallintamallit tulevat näkyviin %systemroot%/inf – kansioon. Nyt mallit voidaan tuoda Group Policy Object Editoriin muokattavaksi.

Office2000 mallit	OfficeXP mallit	Office2003 mallit	Kuvaus
Access9.adm	Access10.adm	Access11.adm	Accessin asetukset
Clipga15.adm	Gal10.adm	GAal11.adm	mediatiedostojen esto
Excel9.adm	Excel10.adm	Excel11.adm	Excelin asetukset
Frontpg4.adm	Fp10.adm	Fp11.adm	Frontpagen asetukset
Instlr1.adm	Instalr11.adm	Instalr11.adm	Windows Installerin asetukset
Office9.adm	Office10.adm	Office11.adm	Yhteiset Office-ohjelmistojen asetukset
Outlk9.adm	Outlk10.adm	Outlk11.adm	Outlook 2000:n asetukset
Ppoint9.adm	Ppt10.adm	Ppt11.adm	PowerPointin asetukset
Pub9.adm	Pub10.adm	Pub11.adm	Publisherin asetukset
Word9.adm	Word10.adm	Word11.adm	Wordin asetukset
N/A	N/A	Aer.adm	Windowsin vikaraportin lähettäminen
N/A	N/A	Rm11.adm	Microsoft Relationship Managerin sijainti
N/A	N/A	Scrib11.adm	Microsoft OneNote 2003:n asetukset

Kuva 14. Lista Office 2000, Office XP ja Office 2003 käytössä olevista hallintamalleista.

Hallintamallien käyttöönoton jälkeen on mahdollista tuoda esimerkiksi Word9.adm tiedosto GPMC:n kautta editoitavaksi. Jos organisaatiossa on kyseinen Word-versio käytössä, voitaisiin mallin kautta kytkeä esimerkiksi oikoluku pois päältä ja puolestaan kytkeä tavutus päälle. Sen jälkeen voitaisiin linkittää muutokset sisältävä GPO haluttuun OU:hun.

4.4.3 Oman hallintamallin tekeminen

Omien hallintamallien tekeminen on myös mahdollista, ja suositeltavaa, jos halutaan tehdä jotain sellaisia muutoksia, mitä ei oletuksena mukana tulevien hallintamallien avulla voida tehdä. Omien mallien tekemiseen on kolme vaihtoehtoa:

- Olemassaolevan hallintamallin muokkaaminen. Tämä on hankalaa, koska määrittelyt täytyy tehdä oikeaan paikkaan ja valmiin koodin tulkitseminen voi viedä aikaa.
- Uuden hallintamallin luominen, joka pitää sisällään kaikki halutut muutokset.
- Uusi hallintamalli jokaiselle halutulle muutokselle. (Moskowitz 2004, 219.)

Hallintamallien tekeminen on suhteellisen helppoa, koska niitä voidaan luoda tekstieditorilla, esimerkiksi Notepad-ohjelmalla. Malli koostuu kuvauksesta, rekisteritiedosta (rekisteritiedoista) ja niihin liitetyistä arvoista. Mallin rakenne on seuraavanlainen:

CLASS MACHINE tai USER (määrittelee sen, vaikuttaako sääntö HKEY_USER vai HKEY_LOCAL_MACHINE -haaraan)
CATEGORY (säännön kategorian nimi)
SUB-CATEGORY (säännön ala-kategorian nimi on valinnainen, käytetään tarpeen vaatiessa)
POLICY (säännön nimi)
KEYNAME (rekisteriavaimen nimi.) Pois lukien ensimmäinen taso, esimerkiksi HKEY_USER)
VALUENAME (rekisteriarvon nimi) VALUEON ”1” VALUEOFF ”0”

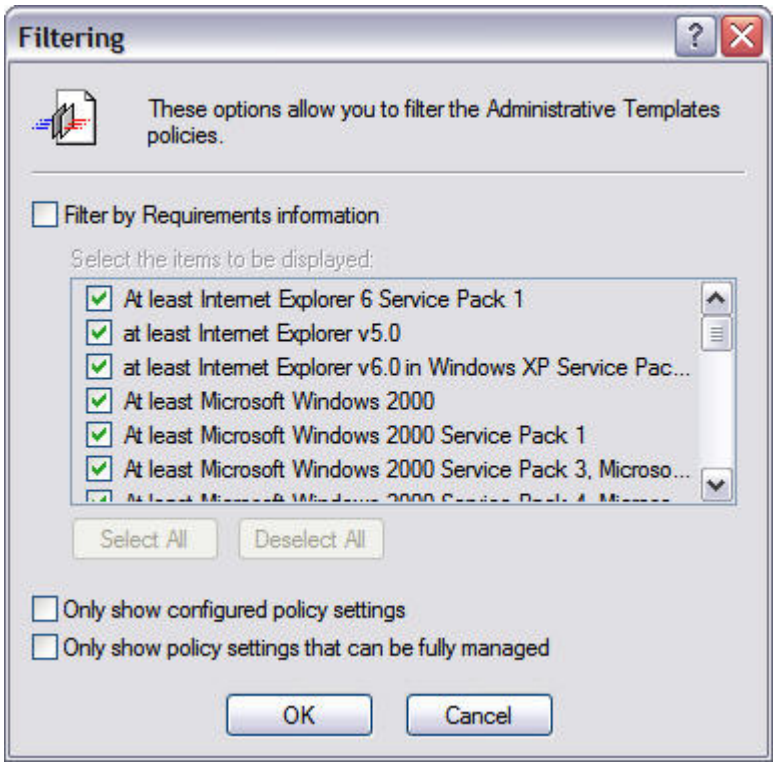
END POLICY
END CATEGORY;
(Buike 2005.)

Tässä esimerkki tekstitiedostosta, joka on tehty käyttämällä yllä olevaa rakennetta:

CLASS MACHINE
CATEGORY *"Removable Storage Write Access"*
POLICY *"USB Write Access"*
KEYNAME *"SYSTEM\CurrentControlSet\Control\StorageDevicePolicies"*
VALUENAME *"WriteProtect"*
VALUEON NUMERIC 1
VALUEOFF NUMERIC 0
END POLICY
END CATEGORY;
(Buike 2005.)

Tämä tekstitiedosto voidaan nyt nimetä ja tallentaa esimerkiksi *Removable Devices.adm* nimellä. Tämän jälkeen tiedosto kopioidaan %systemroot%\inf-hakemistoon. Nyt valmis malli voidaan avata käyttöön Group Policy Object Editorin kautta, *Add/Remove-template*-toiminnolla. Esimerkissä luodun hallintamallin avulla voidaan muokata usb-laitteiden sekä optisten asemien käyttöoikeutta halutuissa työasemissa.

Itse tehtyjen hallintamallien määrittelyt eivät kuitenkaan tule oletuksena näkyviin. Tätä varten on tehtävä yksi muutos. Valitsemalla Group Policy Object Editorista View | Filtering, päästään käsiksi suodatukseen liittyviin määrittelyihin. Sieltä tulee poistaa merkintä kohdasta ”Only show policy settings that can be fully managed.” Kuten kuvasta 15 voidaan huomata.



Kuva 15. Suodatukseen liittyvät määrittelyt.

4.5 Varmuuskopiointi

GPO:n varmuuskopioinnissa sen sisältämä data tallennetaan tietojärjestelmään. Varmuuskopiointi toimii myös Vie-toimintona, jolloin se voidaan palauttaa tai siirtää toiseen tietojärjestelmään. (Backup using GPMC: Group Policy 2005.)

Varmuuskopioinnin yhteydessä tallentuu seuraavat tiedot:

- GPO:n GUID (Globally Unique Identifier) sekä toimialue (domain).
- GPO:n sisältämät asetukset
- Discretionary Access Control List (DACL), joka määrittelee, ketkä pääsevät muokkaamaan GPO:a.
- WMI-suodattimen linkitys, jos sellainen on. Mutta ei itse WMI-suodatinta.
- Linkit IPSec (IP Security) asetuksiin, jos sellaisia on määritelty.
- XML-raportti GPO-asetuksista, joita voidaan tarkastella GPMC:n kautta HTML-muodossa.
- Aikaleima siitä, milloin varmuuskopio on otettu.

- Varmuuskopiolle annettu kuvaus.

Varmuuskopioinnissa ei tallenneta seuraavia tietoja:
GPO:n varmuuskopioinnissa tallentuu ainoastaan data, joka on GPO:n sisällä. Data, joka jää GPO:n ulkopuolelle, koostuu seuraavista tiedoista:

- Linkit toimipaikkaan, toimialueelle tai organisaatioyksikköön.
- WMI-suodatin.
- IPSec-asetus (IP Security)

Nämä tiedot eivät ole enää saatavilla, kun GPO palautetaan alkuperäiseen tai uuteen paikkaan. Yhdestä tai useammasta GPO:sta voidaan tehdä tarpeen vaatiessa useita eri varmuuskopioita samaan tietojärjestelmään. Tällöin jokainen varmuuskopio saa oman tunnisteen. (Backup using GPMC: Group Policy 2005.)

4.5.1 Varmuuskopioiden turvaaminen

Väärinkäytöksien sekä luvattoman käytön ehkäisemiseksi on hyvä tallentaa GPO:en varmuuskopiot turvalliseen paikkaan suojattuna rajoitetuin käyttäjäoikeuksin, jolloin ainoastaan hyväksytyillä käyttäjillä on mahdollisuus käyttää varmuuskopioita. Tehostetun suojan hyödyntämiseksi on hyvä käyttää Windows 2000 tai uudempaa käyttöjärjestelmää. Tämä estää datan ”peukaloinnin” siirrettäessä tietoa verkon yli. Tämä johtuu siitä, että kaikki SMB-liikenne on oletuksena digitaalisesti suojattua kyseisissä käyttöjärjestelmissä. (Backup using GPMC: Group Policy 2005.)

Varmuuskopion ottaminen GPMC:lla:

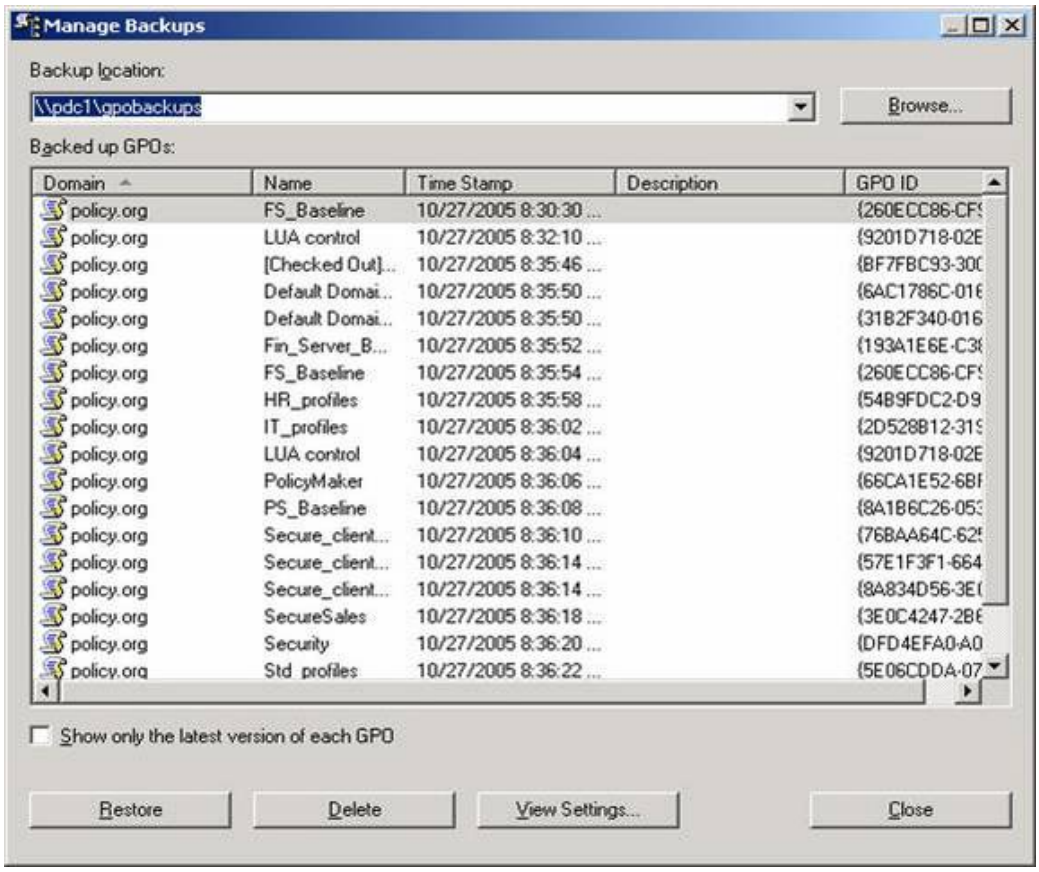
- Avataan GPMC
- Valitaan Group Policy Objects-haara ja sieltä GPO, joka halutaan varmuuskopioida.
- Jos halutaan varmuuskopioida yksi GPO, valitaan se hiiren oikealla klikkauksella ja otetaan Back Up. Jos halutaan varmuuskopioida kaikki toimipaikan GPO:t, valitaan hiiren oikealla klikkauksella Group Policy Objects ja otetaan Back Up All.

- Backup Group Policy Object-dialogissa syötetään Location-kohtaan polku, jonne halutaan GPO varmuuskopioida. Tai valitaan Browse ja etsitään haluttu kansio varmuuskopiota varten.
- Description-kohtaan kirjoitetaan kuvaus varmuuskopioitavalle GPO:lle ja valitaan Backup. Jos varmuuskopioidaan useampia GPO:a, kuvaus tulee näkyviin kaikille valituille GPO:lle.
- Lopuksi valitaan OK.

On tärkeää varmistaa, että ainoastaan halutuilla käyttäjillä on oikeudet käyttää kansiota, minne GPO:t varmuuskopioidaan. Lisäksi käyttäjällä täytyy olla luku- ja kirjoitusoikeudet kansioon, minne varmuuskopiota ollaan ottamassa.

4.5.2 Varmuuskopion palauttaminen

Varmuuskopion palauttaminen on itsessään yhtä helppo toimenpide, kuin varmuuskopion ottaminenkin. Varmuuskopioiden palauttamista voidaan hallita GPMC:n kautta *Manage Backups*-toiminnolla. Manage Backups-toiminnon voi käynnistää hiiren oikean napin klikkauksella toimialue-haaran päällä tai Group Policy Objects-haaran päällä. Jos Manage Backups avataan Group Policy Objects-haarasta, tietojärjestelmä näyttää ainoastaan kyseisen toimipaikan GPO:en varmuuskopiot. Avattaessa toimialue-haarasta, näkyy kaikki varmuuskopioidut GPO:t, riippumatta siitä, mistä toimipaikasta ne on otettu. Olettaen, että käytössä on useampi, kuin yksi toimipaikka.



Kuva 16. Manage Backups-toiminnolla voidaan hallita varmuuskopioita ja niiden palauttamista.

Varmuuskopio palautetaan valitsemalla haluttu GPO listasta ja otetaan *Restore*-toiminto. Jos halutaan varmistaa, että kyseessä on haluttu GPO, voidaan tilanne varmistaa *View Settings*-toiminnolla, joka näyttää GPO:n sisältämät asetukset HTML-raporttina.

4.6 Loopback-prosessointi

Yleisesti ryhmäkäytännöt vaikuttavat käyttäjään tai tietokoneeseen sen mukaan, miten ne löytyvät aktiivihakemistosta. Kuitenkin tietyissä tapauksissa on hyvä, jos asetukset tulevat voimaan sen perusteella, mihin työasema on sijoitettu. Tällöin käyttäjälle määritetään sääntöjä OU:hun, joka pitää sisällään tietokoneobjekteja. Tätä määrittelytapaa kutsutaan nimellä *Loopback Processing*. Kun Loopback-prosessointi on

käytössä, tietokone käytännössä unohtaa olevansa tietokone ja aloittaa GPO:n prosessoinnin aivan kuten olisi käyttäjä.

Loopback-ominaisuutta voidaan käyttää ottamaan GPO voimaan sen perusteella, mille tietokoneelle käyttäjä kirjautuu sisään. Loopback-ominaisuudesta riippumatta käyttäjälle tulee kuitenkin tarvittaessa voimaan myös häneen vaikuttavat käyttäjätason GPO:t. (Loopback processing of Group Policy 2007.)

Ominaisuus voidaan ottaa käyttöön seuraavalla tavalla:

- Avataan (GPMC), GPO:a editoitaessa valitaan Computer Configuration
- Valitaan Administrative templates | System | Group Policy | "User Group Policy Loopback processing mode"

Tämän jälkeen GPO:t, jotka on määritelty tietokoneelle, tulevat voimaan käyttäjälle, joka kirjautuu sisään. Tämä on tehokas tapa ottaa käyttöön haluttuja ominaisuuksia esim. julkisilla paikoilla tai luokkahuoneissa sijaitseville koneille. Esimerkkinä voidaan ajatella esimerkiksi tulostinta, joka tulisi käyttöön aina, kun käyttäjä kirjautuu tietokoneelle tietyssä luokkahuoneessa.

Loopback-prosessointi on käytössä ainoastaan aktiivihakemistossa. Näin ollen molempien, käyttäjä- ja tietokonetilin, tulee löytyä aktiivihakemistosta. Sen lisäksi tietokoneessa täytyy olla joku seuraavista käyttöjärjestelmistä:

- Windows XP Professional
- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2003 Server

(Loopback processing of Group Policy 2007.)

Loopback-prosessointi voidaan määritellä toimimaan kahdella eri tavalla:

- Korvaus (Replace mode)
- Lomitus (Merge mode)

Lomituksessa tietokone käynnistyessään hakee ensin sille määritellyt tietokone-OU:n GPO:t ja tämän jälkeen käyttäjän kirjautuessa sisään, käyttöön tulevat häneen linkitetyt GPO:t. Seurauksena tietokone luulee olevansa käyttäjä ja kaikki käyttäjän OU:sta tulevat GPO:t vaikuttavat myös tietokoneeseen. Kuitenkin ristiriitatilanteen sattuessa tietokone-OU:n GPO:t omaavat korkeamman prioriteetin. (Moskowitz 2004, 131.)

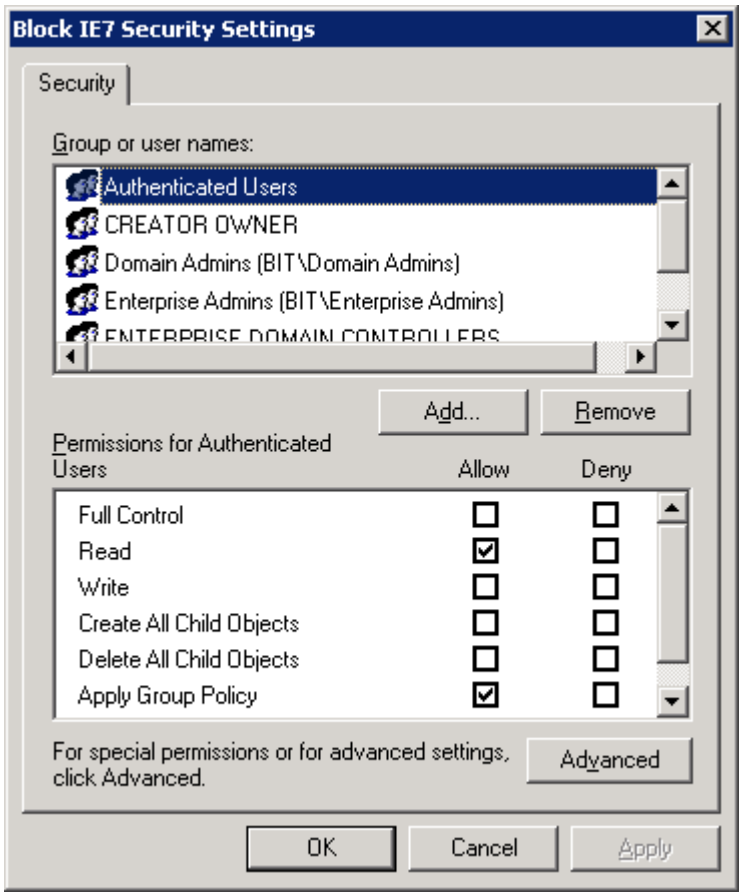
Korvauksessa tietokone prosessoi normaalisti sille voimaan tulevat GPO:t toimialue-, toimipaikka- sekä organisaatioyksikkötasolla. Käyttäjän kirjautuessa sisään, häneen vaikuttavat käyttäjätason GPO:t eivät tule voimaan. Sen sijaan tietokone luulee olevansa käyttäjä, ja voimaan tulevat kaikki käyttäjiin vaikuttavat GPO:t aktiivihakemiston linkityksen mukaisesti. (Moskowitz 2004, 135.)

Loopback-prosessoinnissa korvaus-vaihtoehtoa kannattaa käyttää kuitenkin vain erikoistapauksissa, koska se varaa itselleen jonkin verran prosessorin laskentatehoa sekä palvelimilta että työasemilta. Myös vikatilanteiden selvittäminen saattaa olla hankalaa. (Moskowitz 2004, 135.)

4.7 Käyttäjäryhmien suodatus

Useasti oletetaan, että GPO:t voidaan laittaa vaikuttamaan ainoastaan tietokoneisiin, toimipaikkaan (site), toimialueeseen (domain) tai organisaatioyksikköön (OU), mutta ei ollenkaan ryhmiin tai käyttäjiin. Vaikka monet edellä mainituista kohteista pitävätkin sisällään parhaimmillaan useita ryhmiä, niin välillä tulee tarve, että tietyt GPO:t vaikuttavat ainoastaan OU:n sisällä oleviin haluttuihin käyttäjiin.

Oletuksena tilanne Group Policy Management Consolessa (GPMC) on se, että esimerkiksi OU:hun linkitetyt uudet GPO:t vaikuttavat aina kaikkiin käyttäjiin, jotka pystyvät kirjautumaan sisään tietokoneisiin. Tätä käyttäjäryhmää kutsutaan nimellä *Authenticated Users*. Jotta GPO:t vaikuttaisivat käyttäjäryhmiin, tulee niillä olla sekä *read* että *Apply Group Policy* oikeudet linkitettyyn GPO:in (Kouti & Seitsonen 2005, 680). Tämä tilanne näkyy kuvassa 17.



Kuva 17. Oletuksena tulevat käyttöoikeudet uudelle GPO:lle

Domain Admins, Enterprise Admins ja System ryhmillä on luotuihin GPO:in kaikki oikeudet, paitsi All Extended Rights ja Apply Group Policy. Enterprise Domain Controllers ryhmällä on lukuoikeudet kaikkiin luotuihin GPO:in. Koska yllämainitut ryhmät ovat myös osa Authenticated Users-ryhmää, GPO:t vaikuttavat myös näihin ryhmiin. (Kouti & Seitsonen 2005, 681).

Tapa, jolla saadaan haluttu GPO vaikuttamaan tiettyihin käyttäjiin, on poistaa Authenticated Users-ryhmältä *Apply Group Policy*-merkintä ja luoda uusi ryhmä, mihin kuuluu vain halutut käyttäjät. Tälle ryhmälle annetaan *Read* ja *Apply Group Policy*-oikeudet.

5 SOVELLUSTEN HALLINTA

Aikaisemmat Windows-versiot (NT, 9x ja Millenium Edition) eivät mahdollistaneet keskitettyä ohjelmistojen hallintaa. Aktiivihakemisto yhdessä ryhmäkäytäntöjen kanssa mahdollistavat keskitetyn hallinnan sille, mitkä ohjelmistot ovat saatavilla tai asennettuina halutuille tietokoneille. Myös ohjelmistojen päivitykset, korjaukset sekä poistaminen on mahdollista suorittaa GP:n kautta. (Kouti & Seitsonen 2005, 639.)

Ohjelmistoja voidaan määritellä GP:n avulla vaikuttamaan joko käyttäjään tai tietokoneeseen. Käyttäjään vaikuttavat ohjelmistot asennetaan, kun käyttäjä itse käynnistää asennuksen tai vaihtoehtoisesti asennuksen käynnistyminen on automatisoitu, jolloin asennus tapahtuu käyttäjän kirjautuessa sisään. Tietokoneeseen vaikuttavat ohjelmistot asennetaan automaattisesti, kun tietokone käynnistetään, jolloin se hakee sille määritetyt GPO:t.

Kun ohjelmistoja on tarkoitus alkaa jakamaan, on hyvä tehdä strategia, minkä perusteella jakelu tapahtuu. Tällöin säästyy aikaa ja pystytään määrittelemään tarkasti käyttäjät, joille haluttu ohjelmisto tulee käytettäväksi. (MCSE Guide, s.643.) Seuraavassa muutama huomioitava asia:

- Ohjelmistojakelu voidaan tehdä hierarkkisesti eri aktiivihakemiston tasoille. Taso voi olla toimipaikka, toimialue tai organisaatioyksikkö. Microsoft suosittelee, että määrittelyt tehtäisiin ohjelmistojakelun osalta mahdollisimman korkealle tasolle, koska tämä estää useiden GPO:n syntymisen, jotka saattaisivat jakaa samaa sovellusta.
- Sen sijaan, että olisi useita GPO:a jakamassa eri ohjelmistoja, on helpompaa hallita GPO:a, joka pitää itsessään sisällään useita ohjelmistojakelumäärittelyjä. Tämä nopeuttaa sisäänkirjautumista, koska GPO:en määrällinen prosessointi on pienempi.
- Jos määriteltynä on useampi GPO, jotka vaikuttavat samaan käyttäjäryhmää, tulee pitää mielessä, missä järjestyksessä GPO:t vaikuttavat; ensin on toimi-

paikka, sitten toimialue ja sen jälkeen organisaatioyksikkö. (Chellis 2006, 686.)

5.1 MSI-paketit

2000-luvun alussa tuli mahdolliseksi käyttää uutta Windows Installer-teknologiaa. Tämän kautta tuli työkaluja, joilla voi pakata ja jakaa ohjelmistoja Windows-käyttöjärjestelmissä. Samalla GP toi mukanaan ominaisuuden ohjelmistojakeluun, jolloin maksullisten tuotteiden käyttö ei ollut enää pakollista. (Shinder ym. 2003, 606.)

Installer-teknologia koostuu seuraavista komponenteista:

- Installer-palvelu, jonka avulla käyttöjärjestelmä, joka käyttää Windows Installer-paketteja, suorittaa ohjelmistoasennuksia, ohjelmistojen muokkauksia sekä niiden poistoja.
- .msi tiedosto, joka pitää sisällään yhteen pakattuja tiedostoja sekä niille luodut komentosarjat ohjelmiston asennusta ja muokkausta varten. Se on relationaalinen tietokanta, joka pitää sisällään tietoa ohjelmistosta. Tiedostoa voidaan käyttää sekä uusiin asennuksiin, että olemassa olevan asennuksen päivitykseen.
- Ohjelman ohjelmointirajapinta (API = Application Programming Interface), jonka avulla ohjelma neuvottelee Installer-palvelun kanssa.

Windows Installerin suuri hyöty on siinä, että se pitää sisällään ns. ”roll back” toiminnon, jonka avulla voidaan palata ennen asennusta olevaan tilaan, jos asennuksessa esiintyy ongelmia. Installer-palvelu toimii myös itsensä korjaavana asennuksena. Se pystyy tarkistamaan, puuttuuko ohjelmasta tiedostoja tai ovatko ne mahdollisesti korruptoituneet. Tällöin palvelu pystyy automaattisesti palauttamaan vioittuneet tai puuttuvat tiedostot ja komponentit, jolloin ohjelma saadaan taas toimimaan normaalisti. (Shinder ym. 2003, 606.)

Windows Installer–paketteja voi luoda niille suunnitelluilla pakkaustyökaluilla, mutta useilla ohjelmistotoimittajilla on omat .msi-päätteiset paketit, jotka ovat vapaasti ladattavissa Internetistä. Tällöin kannattaa kuitenkin huolehtia testauksesta ennen varsinaista ohjelmistojakelua.

Uudemmat Microsoftin ohjelmistot pitävät yleensä mukanaan .msi – paketin, jolla asennuksen voi suorittaa. Office 2000 oli ensimmäinen ohjelmisto, jossa .msi – paketti oli jo valmiiksi mukana. Tämän jälkeen useat muut ohjelmistotoimittajat ovat seuranneet Microsoftin esimerkkiä ja lisänneet omiin ohjelmiinsa .msi – asennuspaketit. (Chellis 2006, 693.)

Huomioitavaa on myös se, että Windows Installer-palvelun täytyy olla käynnissä niillä tietokoneilla, joille ohjelmistoja on tarkoitus jakaa. Tämä palvelu kuitenkin on käyttöjärjestelmän toimesta oletuksena käynnissä.

Kun .msi – paketit yleistyivät, ohjelmistovalmistajat alkoivat toimittamaan asennuspaketteja, joiden kautta ohjelmisto on valmiina asennettavaksi. Tämä kuitenkin tarkoittaa sitä, että muutoksien tekeminen ohjelmistoihin on hankalaa, jos esimerkiksi halutaan eri määritykset työpaikan eri osastoille. Tätä varten on kehitetty *Transformit*. (Chellis 2006, 693.)

Windows Installer Transform (.mst) on MSI-paketin kaltainen tiedosto, jossa on määritelty mitä muutoksia alkuperäiseen MSI-pakettiin halutaan asennettaessa tehdä. Transformissa määritellyt muutokset voidaan yhtä hyvin tehdä suoraan alkuperäiseen MSI-pakettiinkin, mutta useat eri transformit mahdollistavat helposti erilaiset asennukset. (Turun Yliopisto – playground.utu.fi 2007.)

Transformit ovat erityisen hyödyllisiä silloin, kun halutaan automatisoida asennuksia, eli käyttää niin sanottua ”silent-asennusta.” Silent-asennuksessa on ohjelmistoon tehty valmiiksi tarpeelliset merkinnät, joita ovat esimerkiksi asennuspolku, asennukseen sisältyvät komponentit, poisjätettävät komponentit ja lisenssiavain. Nämä asetusmäärittelyt piilotetaan loppukäyttäjältä ja ohjelmistoasennus käyttää niitä ennalta määriteltyinä tietoina.

Transformeja ei voida kuitenkaan jakaa sellaisenaan, vaan ne tulee olla liitettyinä siihen .msi-pakettiin, mistä transformi on tehty.

5.2 Sovellusten jakelu

Kun verkon ylläpitäjä on tehnyt valmiin asennuspaketin, voi sitä ruveta jakamaan toimialueen tietokoneille tai käyttäjille. Jakelu suoritetaan riippuen jakelutavasta. Ohjelmistoja voidaan GP:n avulla jakaa kahdella eri tavalla. Vaihtoehtoina ovat joko *Published* tai *Assigned.*

Published-vaihtoehdossa käyttäjän on mahdollista asentaa jaettava ohjelmisto Ohjauspaneelin Lisää/Poista ohjelmia-työkalulla. Käyttäjä ei kuitenkaan saa mitään ilmoitusta siitä, että kyseinen ohjelma olisi mahdollista asentaa. Tarpeen vaatiessa käyttäjä voi itse valita, asentaako ohjelman, vai ei. Tällä tavoin käyttäjät pääsevät käsiksi ohjelmiin, joita ei työasemissa normaalisti tarvita, mutta joiden käyttö halutaan mahdollistaa tarpeen vaatiessa. Tällaisia ovat esimerkiksi satunnaiset projektit. (Shinder 2004, 603.)

Published-vaihtoehdossa käyttäjällä on myös mahdollisuus poistaa ohjelma tietokoneelta, toisin kuin Assigned-vaihtoehdossa, missä ohjelma pysyy asennettuna, vaikka käyttäjä manuaalisesti poistaisi tiedostot ohjelman kansiosta.

Published-määritelty ohjelmisto määritellään asennettavaksi Group Policy Object Editorin (jos käytössä ei ole GPMC:a) tai GPMC:n kautta, josta löytyy Computer Configuration | Software Settings –haara, ja sen kautta Software Installation – optio. Assigned–vaihtoehtoa käytetään silloin, kun halutaan, että käyttäjät pääsevät ohjelmaan käsiksi, riippumatta siitä, mille tietokoneelle he ovat kirjautuneena sisään. toimialue-ympäristössä assigned-määritelty ohjelma ”seuraa” käyttäjää tietokoneelta toiselle. (Shinder 2004, 603.)

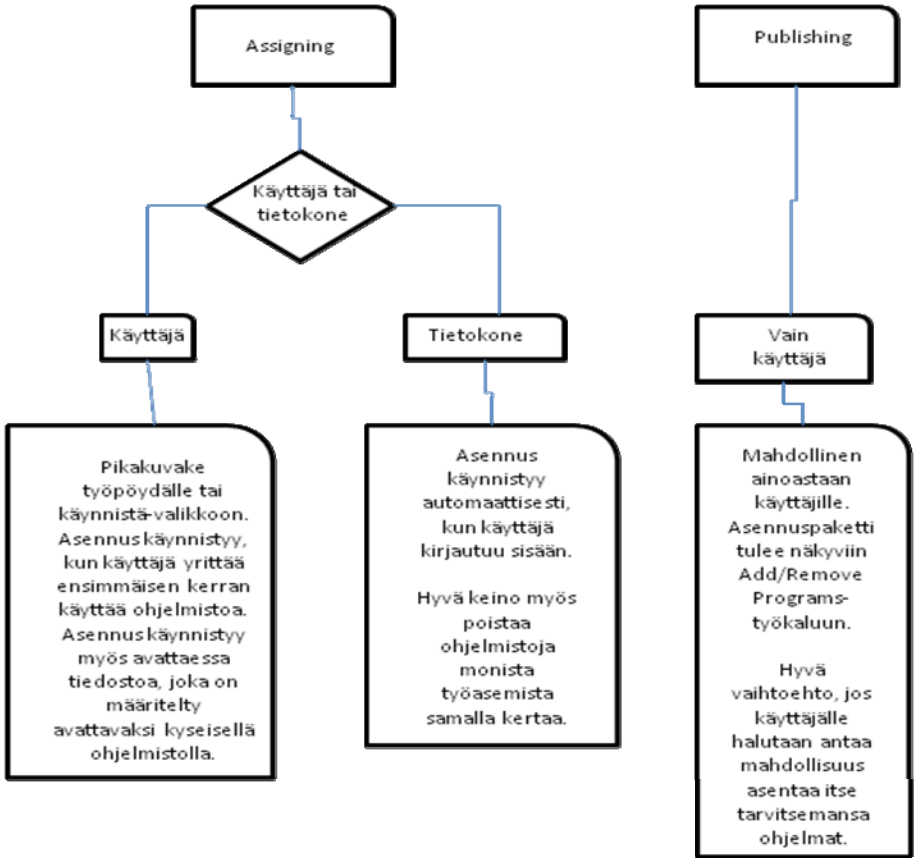
Assigned vaihtoehdossa haluttu ohjelmisto tekee itsestään pikakuvakkeen Käynnistävalikkoon tai työpöydälle, josta käyttäjä voi itse käynnistää asennuksen. Ohjelmisto

ei ole valmiiksi asennettuna, vaikka se tekeekin itsestään käynnistettävän pikakuvakkeen. Asennus lähtee käyntiin, kun käyttäjä yrittää ensimmäisen kerran käyttää ohjelmistoa tai yrittää avata tiedoston, joka on määritelty avattavaksi kyseisellä ohjelmistolla. (Shinder 2004, 603.) Tämä toiminto on käytössä myös Published-vaihtoehdossa.

Toinen vaihtoehto on automatisoida ohjelmiston asennus kirjautumisen yhteyteen, kuten aikaisemmin jo todettiin. Assigned-vaihtoehto on myös ainoa tapa, jota voidaan käyttää tietokonetta koskevissa määrityksissä. Silloin asennuksen käynnistyminen on pakko automatisoida, koska käyttäjä ei pääse vaikuttamaan asennukseen.

Assigned-ohjelmistoasennus suoritetaan GP:lla sen option perusteella, asentuuko ohjelmisto automaattisesti (Computer Configuration) vai käyttäjän toimenpiteiden seurauksena (User Configuration). Tietokonekohtaiset määrittelyt tehdään Group Policy Object Editorin tai GPMC:n kautta Computer Configuration | Software Settings -haarasta, mistä löytyy Software Installation-optio. Vastaavasti käyttäjäkohtaiset määrittelyt tehdään User Configuration | Software Settings-haarasta, mistä löytyy vastaava optio.

Alla on kuva, joka havainnollistaa tilanteet, miten Published- ja Assigned-jakelut toimivat.



Kuva 18. Published- ja Assigned-jakelu

Ohjelmistot, jotka tulevat ohjelmistojakelun kautta käyttäjille näkyviin, eivät oletuksena esiinny missään kategorioissa. Kun käyttäjä hakee tarvittavia ohjelmistoja Add/Remove Programs – työkalulla, voi halutun ohjelman löytäminen olla hankalaa. Tämän vuoksi on hyvä kategorisoida ohjelmat tietyllä kaavalla. Kategoriat voidaan muodostaa vaikka toimipisteen, työnkuvan tai muun loogisen perusteen mukaan. (MCSE s.691.) Esimerkiksi ”toimisto-ohjelmistot”, jonka alle tulee Office-ohjelmisto ja Adobe Reader sekä ”Internet-selaimet”, jonka alle voidaan laittaa Mozilla Firefox ja Opera.

5.3 WMI – Windows Management Instrumentation

WMI-suodattimia käytetään GPO:en hienosäätöön. Niiden avulla voidaan määritellä entistä tarkemmin, missä tilanteissa GPO:t tulevat voimaan. Yleensä WMI-suodatinta käytetään poikkeustapauksissa, eli kun tulee esimerkiksi uusi ohjelmisto,

joka vaatii toimiakseen tietyn määrän keskusmuistia, voidaan WMI-suodattimen avulla tehdä kysely, joka tarkistaa, onko työasemassa tarpeeksi keskusmuistia.
Kun WMI-suodatinta halutaan käyttää, luodaan GPMC-työkalulla uusi suodatin. Tähän käytetään WMI Query Language (WQL) -kyselyä, joka vastaa SQL-kieltä. Tämä kysely ohjataan GPO:n yhteydessä haluttuun kohteen, esimerkiksi organisaatioyksikköön, ja GPO tulee voimaan ainoastaan, jos WMI-suodattimen sisältämä kysely palauttaa ”true”-arvon.

WMI-suodattimet toimivat ainoastaan Windows Server 2003 sekä sitä uudemmissa palvelinkäyttöjärjestelmissä. Sekä Windows XP ja sitä uudemmissa käyttöjärjestelmissä. Jos käytössä on Windows 2000-käyttöjärjestelmä, GPO:n mukana oleva WMI-suodatin jätetään huomioimatta ja GPO tulee automaattisesti voimaan. WMI-suodattimet ovat käteviä monissa tilanteissa, mutta itse WQL:n tekeminen ei välttämättä ole kaikille luontaista (Group Policy Wiki 2006.)

Nykyään on saatavilla myös kolmannen osapuolen valmistamia työkaluja, joilla kyselyiden tekeminen on helpompaa. Myös uusi Windows Server 2008 tuo mukanaan Group Policy Preferences-työkalun, missä WMI-suodattimien teko on paljon helpompaa, kuin tällä hetkellä. Alla on esimerkki WMI-suodattimesta:

*Select * FROM Win32_OperatingSystem WHERE Caption="Microsoft Windows XP Professional" AND CSDVersion="Service Pack 2"*

Tämä suodatin tarkistaa työasemalta, onko sen käyttöjärjestelmä Microsoft Windows XP Professional ja onko siihen sen lisäksi asennettu Service Pack 2. Muuten GPO ei tule voimaan.

Kun on varmistuttu siitä, että GPO on tullut voimaan kaikissa halutuissa työasemissa suodattimen avulla, kannattaa se poistaa GPO:n yhteydestä. Tämä johtuu siitä, että muuten suodatinta ajettaisiin joka kerta, kun kyseinen GPO prosessoidaan työasemalla joko sisäänkirjautumisen yhteydessä tai tietokoneen käynnistyessä. Tämä tapahtuma voi aiheuttaa pidemmän päälle verkon kuormitusta.

Jokainen GPO voi sisältää vain yhden WMI-suodattimen. Mutta saman suodattimen voi laittaa useamman eri GPO:n yhteyteen.

6 RYHMÄKÄYTÄNTÖJEN VIKADIAGNOSTIIKKA

Ryhmäkäytäntöjen kanssa työskentely ei aina ole helppoa. Onnistuneiden asetuksien teko on tietysti palkitsevaa, kun näkee niiden toimivuuden suoraan käyttäjien työasemilla. On kuitenkin mahdollista, että odottamattomia virheitä tulee ja niiden selvittäminen voi viedä aikaa. Suurin ongelma on yleensä siinä, kun pitää päätellä, *mistä* asetus tulee ja *miten* se tulee käyttöön. Ja entäpä jos koko GPO ei toimi?

Jotta ongelmien ratkaiseminen olisi helpompaa, on ensin luotava itselle selkeä kuva siitä, miten GPO prosessoidaan asiakaskoneella. GPO:n prosessoinnissa on kaksi erillistä vaihetta: (Troubleshooting Group Policy Problems: Group Policy 2005.)

- *Core Group Policy processing*. Kun asiakaskone alkaa prosessoida GPO:a, sen täytyy ottaa selville, onko yhteys ohjauspalvelimeen saatavilla, ovatko GPO:t muuttuneet ja mitkä GPO:t tulee prosessoida.
- *Client side extension (CSE) processing*. Sääntömäärittelyt on jaettu eri kategorioihin, kuten Administrative Templates, Security Settings, Folder Redirection, Disk Quota ja Software Installation. Jokainen kategoria tarvitsee tietyn CSE:n näiden asetusten prosessointiin ja jokaisella CSE:lla on omat säännöt prosessointia varten. (Troubleshooting Group Policy Problems: Group Policy 2005.)

6.1 Vianetsinnän toimintatavat

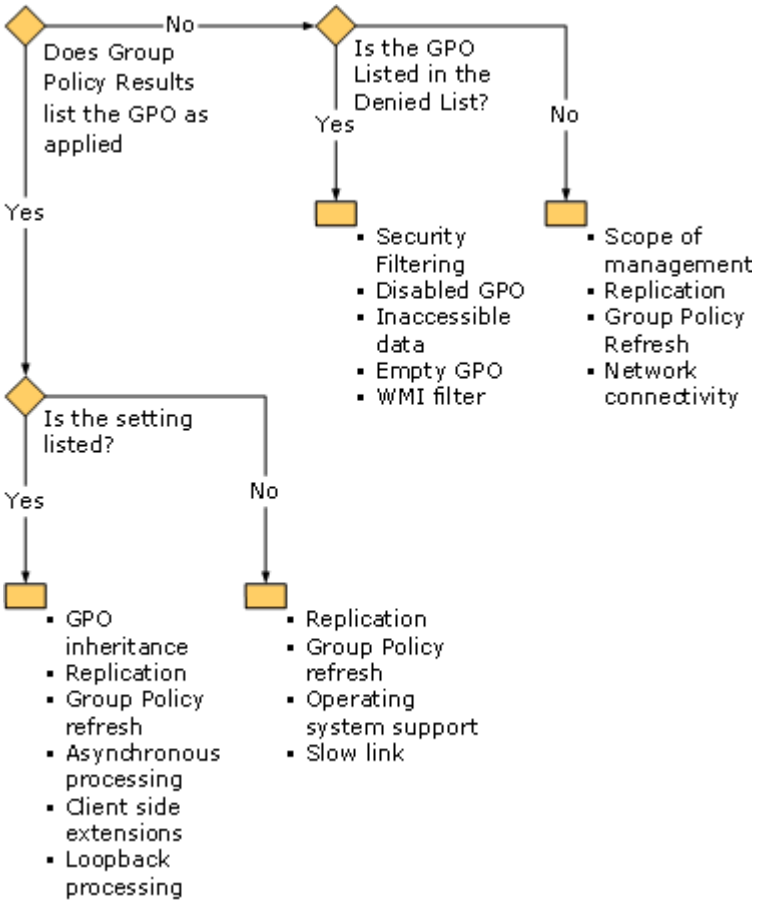
Tarvittavan infrastruktuurin selvittämiseksi on hyvä ensin varmistaa, että tarpeelliset palvelut ja komponentit ovat käytettävissä sekä määriteltynä oikein. Tietokoneen tulee olla verkkoyhteydessä, liitetty toimipaikkaan ja aikamäärittelyt annettuna oikein.

GP pitää sisällään ns. erikoismäärittelyjä, joita ovat mm. tietoturva-asetukset, WMI-suodattimet, periytymisenesto, pakotus, loopback processing ja hidas linkki-määrittelyt. Näiden toimivuus sekä vaikutus tulee myös selvittää.

GPO:en voimaantuloa voidaan tarkastella erinäisillä työkaluilla. Näitä ovat esimerkiksi GPResult.exe, GPOTool.exe ja GPMC. Työkalujen kautta saatuja tuloksia voidaan analysoida tapahtumalokien ja CSE-lokien avulla ratkaisun löytämiseksi.

Ongelman syyn löytämiseksi voidaan käyttää apuna seuraavaa toimintatapaa:

1 Luo Group Policy Results – raportti GPMC:lla.
2 Tutki tuloksia ja etsi vastaukset seuraaviin kysymyksiin:
3 Onko GPO listattu ”applied”-tilaan?
4 Näkyykö asetus listattuna Group Policy Results-raportissa?
5 Onko GPO listattu ”denied”-tilaan?
6 Vertaa raportista saatavia tuloksia, kuvassa 19 esitettyyn taulukkoon.



Kuva 19. GPO:n vianselvitystä helpottamaan suunniteltu vuokaavio.

6.2 Yleisimmät ongelmatilanteet

Käyttäjä saattaa varoittamatta soittaa ja ilmoittaa, että hänen työpöytänsä on muuttunut ja sieltä puuttuu oleellisia asioita. Tällaisissa tilanteissa on kuitenkin useita muuttujia, jotka pitää ottaa huomioon. Ensinnäkin, on neljä tasoa, joiden vaikutukset saattavat näkyä käyttäjälle; lokaalit GPO:t, toimipaikka, toimialue sekä organisaatioyksikkö. Seuraava riskitekijä voi olla se, että jollakin muullakin on oikeus tehdä muutoksia GP-asetuksiin. Ehkä käytössä on Windows 2003 metsä, jolla on luottosuhde toiseen Windows 2003 metsään, ja näin ollen käyttäjät voivat kirjautua mistä tahansa. (Moskowitz 2004, 149.)

Tässä muutamia yleisimpiä vikatilanteita, joita saattaa esiintyä Group Policyjen yhteydessä:

Poiskytketyt GPO:t. GPO:n paikallistaminen, jos se on kytketty pois käytöstä.
Periytymisongelmat. Kun on käytössä eri tasoja; toimipaikka, toimialue ja useat organisaatioyksiköt, on hankala löytää GPO, jonka periytyminen ei toimi halutulla tavalla.
GPO:en määrä linkitetyllä tasolla. Jos tietylle tasolle (esimerkiksi OU) on linkitetty useampia GPO:a, on vianselvitys hankalaa.
Käyttöoikeusongelmat. Jos GPO:n linkitys ja periytyminen on todettu oikeelliseksi, on GPO:n käyttöoikeudet vielä selvitettävänä.
Replikointi. GPO:n toimivuus itse ohjauspalvelimien suuntaan tulee varmistaa, kun vikaa etsimään.
Hitaat linkit. Joku työasemista on ns. hitaan linkin takana, miten se hakee GPO:t.
Jotta pystytään selvittämään vikatilanteita mahdollisimman hyvin, on tärkeää tietää, miten koko Group Policy – ympäristö toimii. Jos esimerkiksi käyttäjä kirjautuu lokaalisti työasemalle, avaa Local Group Policy Editorin ja tekee muutoksia, ne tulevat vaikuttamaan jokaiseen, joka koneelle jatkossa kirjautuu. Näitä lokaalisti tehtyjä muutoksia ei voida aktiivihakemiston kautta hallinnoida, kuten aikaisemmin tässä opinnäytetyössä on kerrottu.

6.3 RSOP – Resultant Set of Policy

Kuten aikaisemmin on jo todettu, GP:n vaikutus on kumulatiivinen, silloin kun se on oikein määritelty kaikille halutuille tasoille. Eli asetukset vaikuttavat portaittain aktiivihakemiston rakenteen mukaan. Tulos, joka syntyy siitä, miten määritellyt säännöt vaikuttavat käyttäjään tai tietokoneeseen, on nimeltään *RSop – Resultant Set of Policy*. RSoP on hyvin kätevä työkalu silloin, kun on syystä tai toisesta menetetty kontrolli GPO:en käyttäytymiseen tai halutaan selvittää, miksi tehty GPO ei periydy esimerkiksi halutulle OU-tasolle.

Microsoft esitteli RSoP:n Windows Server 2003:n mukana ja sitä voidaan käyttää Windows XP:ssä sekä sen jälkeen ilmestyneissä käyttöjärjestelmissä. Sen tarkoitus on helpottaa GP:n suunnittelussa sekä vianetsinnässä. RSoP:n yksi työkaluista on nimeltään ”planning mode.” Sillä on mahdollista ennalta katsoa, miten säännöt tule-

vat voimaan. Ja vasta sen jälkeen ottaa ne käyttöön tuotannossa. Tästä lisää myöhemmin.

The Resultant Set of Policy Wizard on kyselypohjainen ohjelma, joka käy läpi olemassa olevia Group Policyja. Keräämällä tietoa kaikista toimialueen, toimipaikan sekä organisaatioyksiköiden käyttäjistä ja tietokoneista, RSoP antaa selkeän kuvan siitä, mitkä GPO:t tulevat voimaan milläkin tasolla ja mitkä GPO:t ovat estettyjä. (Piltzecker 2003, 311.)

RSoP kerää tiedot Common Information Management Object Model (CIMOM) tietokannasta Windows Management Instrumentationin (WMI) avulla. CIMOM-tietokanta pitää sisällään tietoja siitä, kun tietokone kirjautuu verkkoon, tietokoneen komponenttien kokoonpanon, Group Policyn kautta asennetut ohjelmistot, Internet Explorerin asetukset, skriptit, kansioiden uudelleenohjauksen ja tietoturva-asetukset. (RSoP overview: Group Policy 2005.)

Kun sääntöjä on määritelty useille eri tasoille, ne voivat olla joissakin tapauksissa ristiriidassa keskenään. RSoP:n avulla voidaan selvittää, mistä ristiriidat johtuvat ja missä tärkeysjärjestyksessä säännöt tulevat voimaan. (RSoP overview: Group Policy 2005.)

RSoP:a voidaan käyttää eri tilanteissa. RSoP Snap-in on työkalu, joka pitää sisällään kaksi eri vaihtoehtoa: *logging mode* ja *planning mode.* Logging mode näyttää säännöt, jotka ovat voimassa verkkoon kirjautuneilla tietokoneilla ja käyttäjillä. Jos halutaan saada tiedot tietyltä käyttäjältä tai tietokoneelta, tulee toimia seuraavalla tavalla, jotta päästään käyttämään logging modea:

- Avataan Microsoft Management Console. (Avataan Start-valikko, valitaan Run, kirjoitetaan mmc, jonka jälkeen OK). Lisätään Resultant Set of Policy snap-in Microsoft Management Consoleen (MMC).
- valitaan konsolihakemistosta Resultant Set of Policy ja sen jälkeen ”Generate RSoP Data” – toiminto.
- Resultant Set of Policy Wizardissa valitaan “next.”

- Mode Selection-sivulla valitaan Logging mode ja sen jälkeen “next.”
- Computer Selection-sivulla määritellään tietokone, jolla halutaan ajaa RSoP ja sen jälkeen ”next. ”
- User Selection-sivulla määritellään käyttäjä, jolta halutaan kerätä RSoP-tiedot ja sen jälkeen ”next. ”
- Summary of Selections-sivustolla valitaan “next” ja sen jälkeen odotetaan, että RSoP on prosessoinut kaiken tiedon.
- Completing the Resultant Set of Policy Wizard-sivulla valitaan “finish.”
- Konsolihakemistosta valitaan äsken luotu RSoP-kysely.

(Access RSoP data for an existing computer and user (logging mode): Group Policy 2005.)

Logging modesta on eniten hyötyä seuraavissa tilanteissa:

- Halutaan saada selville, mitkä säännöt vaikuttavat tietokoneisiin tai käyttäjiin
- Halutaan löytää väärin toimivat säännöt.
- Halutaan nähdä tietoturvamäärittelyjen vaikutus sääntöihin.

Planning modessa voidaan simuloida tilannetta, jossa halutaan nähdä tietyn säännön vaikutus käyttäjään tai tietokoneeseen. Vaihtoehtoisesti voidaan myös tarkistaa säännön vaikutus tietokoneeseen, joka ei ole kyseisellä hetkellä käytössä tai käyttäjään, joka ei ole kirjautuneena verkkoon. Planning modea voidaan käyttää seuraavalla tavalla:

- Lisätään Resultant Set of Policy snap-in Microsoft Management Consoleen (MMC).
- Käynnistetään the Resultant Set of Policy Wizard planning modessa, jonka jälkeen valitaan “next.”
- User and Computer Selection-sivulla määritellään käyttäjä ja tietokone, jonka jälkeen valitaan ”next.”
- Advanced Simulation Options-sivulla määritellään halutut simulaatiovalinnat, jonka jälkeen valitaan ”next.”
- User Security Groups-sivulla varmistetaan syötetyt tiedot oikeiksi, jonka jälkeen valitaan ”next.”

- Computer Security Groups-sivulla varmistetaan, että tiedot ovat oikein ja valitaan ”next.”
- WMI Filters for Users-sivulla varmistetaan lista WMI-suodattimista ja valitaan ”next.”
- WMI Filters for Computers-sivulla varmistetaan lista WMI-suodattimista ja valitaan ”next.”
- Summary of Selections-sivulla varmistetaan tieto ohjauspalvelimista, jonka jälkeen valitaan “next.”
- Completing the Resultant Set of Policy Wizard-sivulla valitaan “finish.”

Planning modesta on eniten hyötyä seuraavissa tilanteissa:

- Halutaan simuloida, miten tietyt säännöt vaikuttavat tietokoneeseen tai käyttäjään, toimialueeseen, toimipaikkaan tai organisaatioyksikköön.
- Käyttäjä sijaitsee toistaiseksi vain aktiivihakemistossa (esimerkiksi uusi käyttäjätili).

Halutaan testata sääntöjen vaikutus seuraavissa tilanteissa:

- Käyttäjä ja tietokone kuuluvat eri tietoturvamäärittelyn piiriin.
- Käyttäjä ja tietokone ovat eri organisaatioyksiköissä.
- Käyttäjä tai tietokone on tarkoitus siirtää uuteen paikkaan.
- Halutaan simuloida yhteyttä ”hitaan linkin” kautta.
- Halutaan luoda loopback-simulaatio.

(RSoP planning mode: Group Policy 2005.)

7 OPINNÄYTETYÖPROJEKTIN TOTEUTUS

Työ toteutettiin Satakunnan ammattikorkeakoulun liiketoiminnan ja kulttuurin Porin toimipisteessä (myöhemmin LIKU). Tietoverkko oli rakennettu Windows Server 2003 pohjalle, joka piti sisällään aktiivihakemiston. Aktiivihakemisto on perusedel-

lytys siihen, että ryhmäkäytäntöjä (Group Policies) ja ryhmäkäytäntöobjekteja (GPO) pystytään hallitsemaan.

Jotta saatiin selkeä kuva siitä, mitä ryhmäkäytäntöobjekteja LIKU:ssa oli tällä hetkellä käytössä, tutkin palvelimella pääasiassa GPMC-työkalulla tehtyjä määrittelyjä. Tämän lisäksi tutustuin tällä hetkellä olemassa olevaan organisaatioyksikköjen jaotteluun ja niiden sisältämiin käyttäjä- ja tietokoneobjekteihin. Samalla sain paljon kokemusta itse GPMC-työkalusta ja sen toiminnallisuuksista, joka on erittäin tärkeää, jotta pystytään hallitsemaan ryhmäkäytäntöobjekteja mahdollisimman tehokkaasti.

Jotta tämän hetken käytössä olevista ryhmäkäytäntöobjekteista saatiin selkeyttävä kuva, oli tutkimus nyky-ympäristön toimivuudesta annettu opinnäytetyön yhdeksi osa-alueeksi. Tällä tavalla saatiin arvokasta tietoa ryhmäkäytäntöobjektien toimivuudesta ja tarpeellisuudesta sekä kartoitettiin parannusmahdollisuuksia. Opinnäytetyön tekijä puolestaan sai tutustua uuteen ja mielenkiintoiseen aiheeseen.

7.1 Nykytilan kuvaus

Nykytilan kuvaus pitää sisällään tämän hetkisen ryhmäkäytäntöihin vaikuttavan rakenteen. Eli pääasiassa kyse on aktiivihakemistosta, jonka perusteella ryhmäkäytännöt toimivat. LIKU:ssa aktiivihakemisto koostuu yhdestä toimialueesta, jonka alla on useita organisaatioyksiköitä. Organisaatioyksiköiden jaottelu on tehty niin, että tiettyjen käyttäjäryhmien hallinta olisi mahdollisimman loogista ja helppoa. Esimerkiksi opiskelijat ovat omassa OU:ssa, ja tämän alle on tehty omat lapsi-OU:t jokaiselle koulutusohjelmalle. Näitä ovat mm. liiketalous, matkailu, tietojenkäsittely ja viestintä. Lisäksi löytyy oma OU vierailijoita varten. Opiskelijoiden OU:n lisäksi myös henkilökunnalle on tehty oma OU, johon kuuluvat kaikki LIKU:ssa työskentelevät opettajat, hallinnollinen henkilöstö sekä muu henkilökunta.

Myös tietokoneet on jaettu omiin organisaatioyksiköihin niiden käyttötarpeiden mukaan. Palvelimille on tehty oma OU, kuten myös työasemille. Työasemat OU:n alle

on tehty lisäksi omat lapsi-OU:t jokaiselle luokkatilalle, jotta pystytään tarpeen vaatiessa hallinnoimaan GPO:lla tiettyä luokkatilaa. Näiden lisäksi DC:t ovat omassa OU:ssa, koska niiden hallinta ja ylläpito on erittäin tärkeää koko tietoverkon kannalta. Tällä pyritään varmistamaan, etteivät GPO:t vahingossa pääse vaikuttamaan näihin DC-palvelimiin.

7.2 Käyttäjien eroavaisuudet

Kuten jo aikaisemmin on mainittu, ryhmäkäytäntöobjekteja käytetään rajoittamaan sekä käyttäjien että tietokoneiden toimintaa toimialueella. LIKU:ssa on luotu ryhmäkäytäntöobjekteja vaikuttamaan sen mukaan, onko käyttäjä henkilökunnan jäsen vai opiskelija. Vaikka molemmille on luotu perus työpöytäkäyttöä rajoittavia GPO:a, on henkilökunnan jäsenille hieman enemmän vapauksia käyttää työasemia. Tämä johtuu siitä, että he tarvitsevat opetuskäytössä mm. mahdollisuuden asentaa ohjelmia, joita hyödynnetään opintojaksoilla. Henkilökunnan käyttö on usein myös työasemien suhteen rajoittuneempaa, koska he käyttävät opetusluokissa aina opettajille tarkoitettua työasemaa. Tämän lisäksi henkilökunnalla on käytössä henkilökohtaiset työasemat tai kannettavat tietokoneet.

Opiskelijoiden työasemien käyttöä on rajoitettu henkilökuntaa enemmän. LIKU:ssa on käytössä useita luokkatiloja, missä opiskelijat voivat kirjautua vapaasti mille tahansa työasemalle. Näin ollen täytyy varmistaa se, että työasemien käyttö on tietoturvallista ja toisaalta myös rajoittaa opiskelijoiden käyttöoikeuksia ylläpidon kannalta, jotta niille ei päästä asentamaan ylimääräisiä ohjelmia tai aiheuttamaan mitään tahallista tai tahatonta vahinkoa.

7.3 Käytössä olevat ryhmäkäytäntöobjektit

Halusin tarkistella käytössä olevia GPO-määrittelyjä *Group Policy Modeling* -ohjelmalla, joka löytyy suoraan GPMC:n sisältä. Sen käyttö oli helppoa ja työkalu käynnistyi hiiren painalluksella halutun OU:n päällä. Tämän jälkeen käynnistyi ”vel-

ho”, joka automaattisesti täyttää ohjelman tarvitsemat tiedot kyseisen OU:n tiedoilla. Tästä syntyi raportti, joka kertoo, mitkä GPO:t tulevat OU:ssa voimaan ja mitkä eivät. Samalla se kertoi myös syyn, miksi GPO ei tule voimaan. Group Policy Modeling antoi myös tarkan raportin siitä, mitä asetuksia voimaan tulevat GPO:t pitävät sisällään. Tällä tavalla saatiin nopeasti hyvä yhteiskuva siitä, miten nykyinen ympäristö toimii ryhmäkäytäntöjen osalta ja samalla saatiin kerättyä tietoja mahdollisiin vikatilanteisiin.

LIKU:ssa on sekä henkilökunnalla, että opiskelijoilla käytössä kansioiden uudelleenohjaus (Folder Redirection), jonka avulla voidaan käyttäjien profiilit pitää keskitetysä hallinnassa palvelimella. Samalla saadaan kansioista varmuuskopiot vikatilanteita varten. Kansiot, jotka ovat uudelleenohjauksessa, ovat Application Data, Desktop sekä My Documents. Jokaiselle käyttäjäryhmälle, tässä tapauksessa koulutusohjelmalle, on luotu palvelimelle jakokansiot, jonne kansiot uudelleenohjataan. Jos käyttäjä kuuluu esimerkiksi tietojenkäsittelijöihin, hänen kansionsa tallentuvat palvelimelle ”tietojenkäsittely” kansion alle hänen omalla nimellään olevan kansion sisälle.

Käyttäjien henkilökohtaisia tietoja varten jokaiselle käyttäjälle, sekä henkilökunnalle että opiskelijoille, on annettu käyttöön verkkolevy-resurssi, jonne voi tallentaa tiedostoja. Verkkolevy tulee näkyviin Windowsin resurssienhallintaan Z:-asemana. Hyötyä voidaan mitata kahdella tavalla; verkkolevy liikkuu käyttäjän profiilin yhteydessä työasemasta riippumatta, eli henkilökohtaiset tiedostot kulkevat aina mukana. Toinen hyöty saadaan varmuuskopioinnin yhteydessä. Koska verkkolevy sijaitsee palvelimella, se voidaan aina keskitetysti varmuuskopioida.

LIKU:ssa on verkkolevyn kokoa rajoitettu levykiintiöllä. Tällä tavalla pystytään valvomaan palvelimen kiintolevyn täyttöastetta. Käytössä on myös varoitus, joka ilmoittaa käyttäjälle verkkolevyn täyttymisestä. Jos verkkolevy tulee täyteen, on palvelimelle määritelty optio, joka estää levylle kirjoittamisen.

Opiskelijoihin vaikuttavat GPO:t rajoittavat paljon itse työaseman käyttöä. Esimerkiksi ohjelmien asentaminen tiettyjen tiedostopäätteiden osalta on kiellettyä. Tällä pyritään estämään mahdollisten haittaohjelmien asentaminen sekä työasemien vää-

rinkäyttö. Tällaisia väärinkäyttöön liittyviä tilanteita on mm. laittoman materiaalin, kuten pelin ja elokuvien, lataaminen Internetistä.

Ryhmäkäytännöt mahdollistavat komentosarjojen käytön, joita on otettu käyttöön myös LIKU:n ympäristössä. Jokaiselle opiskelijalle on sisäänkirjautumisen yhteydessä määritelty komentosarja, joka vaikuttaa tulostuskiintiöön. Tällä pyritään vähentämään turhien tulostuksien määrää, jolloin säästetään sekä tulostimien käyttökustannuksissa, että paperin kulutuksessa. Komentosarja toimii niin, että opiskelijalle lataantuu näkyviin hänelle määritetty tulostuskiintiö, joka sitten vähenee jokaisen tulostuksen yhteydessä tulostettavan sivumäärän verran.

Ylläpitäjän kannalta on erittäin tärkeää, että hallittava ympäristö olisi mahdollisimman homogeeninen, eli kaikki työasemat olisivat samanlaisia ja niiden hallintaa ei muuttuisi jatkuvasti. Tämän vuoksi itse työasemien muokkaamista on pyritty rajoittamaan eri keinoin. Esimerkiksi ohjauspaneelista on opiskelijoilta estetty kaikkien muiden ohjelmien käyttö, paitsi näyttöasetuksien muokkaaminen, mihin kuuluu mm. resoluution vaihtaminen. Muut kuvakkeet, kuten *järjestelmä* ja *lisää/poista sovelluksia*, antaisivat opiskelijoille mahdollisuuden muuttaa työaseman toimintaa, mitä ei haluta tapahtuvan.

7.4 Työasemien käyttö

LIKU:ssa on työasemien osalta ns. sekaympäristö, joka tarkoittaa sitä, että käytössä on eri käyttöjärjestelmillä toimivia työasemia. Tällä hetkellä käytössä on Windows XP- sekä Windows Vista-käyttöjärjestelmillä toimivia työasemia. Tulevaisuudessa käytössä saattaa olla myös Applen valmistamia Mac-tietokoneita ja Linux-käyttöjärjestelmällä toimivia tietokoneita. Mutta näihin eriäviin järjestelmiin en tässä opinnäytetyössä puutu.

Ryhmäkäytäntöjen osalta sekaympäristön hallinta ei kuitenkaan ole kovin hankalaa. Sekä XP että Vista noudattavat samoja ryhmäkäytäntöobjekteja, ja niitä voidaan hal-

lita GPMC:n kautta, joten niiden käyttöönotto tapahtuu molemmissa käyttöjärjestelmissä ihan samalla tavalla.

LIKU:ssa työasemiin ja palvelimiin on otettu käyttöön GPO -määrittelyjä, jotka parantavat paljon ennen kaikkea tietoturvaa. Tämä on tärkeää juuri sen takia, koska käyttäjiä on paljon ja he ovat atk-taidoiltaan eritasoisia. LIKU:ssa on GPO-määrittelyllä Windowsin oma palomuuri poistettu käytöstä kaikista luokkatilojen työasemista. Tämä johtuu siitä, että käytössä on F-Securen tarjoama Client Security palomuuri- ja virustorjuntaohjelmisto, joka ei suostu asentumaan, jos Windowsin oma palomuuri on aktiivisena.

Palvelimien tietoturvaa pyritään seuraamaan aktiivisesti ja sitä helpottamaan on otettu käyttöön GPO, joka määrittelee palvelimet keräämään lokitietoja kaikista onnistuneista sekä epäonnistuneista sisäänkirjautumisista. Hyöty on selkeästi mitattavissa niin, että jos palvelimille alkaa tulla lyhyellä aikavälillä useita epäonnistuneita sisäänkirjautumisyrityksiä, voidaan epäillä tietomurron yritystä ja asiaan pystytään reagoimaan nopeasti.

7.5 Tietoturva-asetukset

Kaikkien sekä käyttäjiä että tietokoneita rajoittavien ryhmäkäytäntöjen lisäksi LIKU:ssa on määritelty myös Default Domain Policy, jonka asetukset vaikuttavat automaattisesti kaikkiin toimialueen organisaatioyksikköihin, ellei sen periytymistä ole estetty. Tällä hetkellä periytyminen on estetty Domain Controllers -OU:lta sekä Servers -OU:lta. Muihin OU:hin Default Domain Policy-GPO tulee voimaan.

Kuten aikaisemmin tässä opinnäytetyössä kerroin, on Default Domain Policyn muokkaaminen erittäin vaarallista ja sen hallinta täytyy pitää käsissä. LIKU:ssa on tehty Default Domain Policyyn määrittelyjä, joten jatkoa ajattelen on tärkeää huomioida sen vaikutukset kaikkiin aktiivihakemiston organisaatioyksiköihin.

LIKU:ssa Default Domain Policyyn on määritelty pääasiassa salasanoihin sekä sisäänkirjautumiseen liittyviä asetuksia. GPO -määrittelyt on tehty Computer Configuration -haaraan, joten vaikutukset kohdistuvat työasemiin. Näin ollen käyttäjäryhmiä ei tarvitse valvoa, vaan kun pidetään huolta työasemista, niin samalla varmistetaan se, että GPO:n sisältämät määrittelyt tulevat voimaan.

Nyt olemassa oleva Default Domain Policy-GPO pitää sisällään määrittelyt salasanan minimipituudelle, eli kuinka monta merkkiä salasanan tulee vähintään sisältää. Lisäksi löytyy sisäänkirjautumisen yhteyteen liitetyt määrittelyt, joka valvoo kirjautumisen oikeellisuutta. Jos käyttäjä yrittää kirjautua väärillä tunnuksilla tarpeeksi monta kertaa, hänen käyttäjätilinsä menee lukkoon 30 minuutiksi. Tällä estetään sitä, että jos käyttäjätunnus joutuu vääriin käsiin ja työasemalle yritetään päästä esimerkiksi arvaamalla salasanaa, saadaan kyseisiä tilanteita rajoitettua. Samaan tietoturvaan pyritään myös GPO -asetuksella, joka ei näytä edellisen käyttäjän kirjautumistunnuksia, vaan käyttäjätunnus- ja salasanakentät ovat tyhjiä.

7.6 Varmuuskopiointi

LIKU:ssa ei ole käsin otettu varmuuskopiota ryhmäkäytäntöobjekteista, vaan ne kuuluvat samaan System State varmuuskopioon, joka otetaan päivittäin Symantec Backup Exec-ohjelmalla. GPO:a ei myöskään ole tällä hetkellä tarvetta siirtää muille palvelimille, joten tässä tapauksessa manuaalinen varmuuskopiointi GPMC:n kautta ei ole ollut tarpeellista. Toki jatkoa ajatellen, jos ympäristöön tulee muutoksia, niin GPO:sta voisi ottaa myös käsin varmuuskopiot jonnekin levyresurssille, jolloin ne olisi sieltä nopeasti palautettavissa Tuo-toiminnolla suoraan GPMC:lla.

7.7 Tulevaisuuden näkymät

Windows Vista –käyttöjärjestelmä tulee korvaamaan Windows XP –käyttöjärjestelmän muutaman vuoden sisällä kokonaan. Se tuo ryhmäkäytäntöjen hallintaan silloin uusia mahdollisuuksia Group Policy Preferences –hallintatyökalun

kautta. Se tarjoaa mm. nykyisen muokkausnäkymän sijasta graafisen näkymän, jonka avulla GPO -asetusten määrittely on paljon mielekkäämpää. Uskon, että Group Policy Preferences otetaan käyttöön myös LIKU:ssa. Ainakin se olisi erittäin suositeltavaa. Tietysti palvelinpuolella ryhmäkäytäntöjen hallintaa voitaisiin tehostaa uusimalla nykyisten palvelimien käyttöjärjestelmät Windows Server 2008 -käyttöjärjestelmillä, mutta tämä saattaa olla käyttöönottoprojektina jo aika iso muutos ja sitä ei voi vaan tehdä pelkästään ajatellen ryhmäkäytäntöjä.

Ohjelmien asentamiseen voitaisiin LIKU:ssa käyttää enemmän ryhmäkäytäntöjen kautta hallittavaa keskitettyä ohjelmistojen jakelua. Toistaiseksi ohjelmien päivitykset ja uudet asennukset on aina hoidettu lomasesonkeina, mutta tällöin mm. tietoturva-asetusten päivittyminen viivästyy. Samoin myös ohjelmistopäivitykset eivät asennu. Hyötyä saataisiin myös siinä, että oltaisiin aina selvillä eri ohjelmistojen versionumeroista kaikissa luokkahuoneissa. Ohjelmien asennuksen yhteydessä voidaan hyödyntää WMI-suodattimia, joilla pysytään tarkistamaan esimerkiksi aikaisempi ohjelmistoversio.

8 POHDINTAA

Ymmärsin tätä opinnäytetyötä tehdessäni, kuinka tärkeää, mutta samalla monitahoista on käyttäjien sekä tietokoneiden hallinta oppilaitosympäristössä. Kaikki asetukset, mitä ryhmäkäytännöillä voi tehdä, on mahdoton hallita. Sen vuoksi on erittäin hyvä tehdä suunnitelma, miten ryhmäkäytännöt rakentaa, jotta saataisiin selkeä kuva siitä, miten ne vaikuttavat jatkossa erinäisiin hallittaviin objekteihin. Jos ryhmäkäytäntöjä aletaan tehdä pelkästään yhtä asetusta varten, on taatusti ennemmin tai myöhemmin tiedossa ongelmia. Sen verran hankala on isoa käyttäjäympäristöä hallita.

Kaikkein tärkeintä on verkkoympäristön suojaus. Oli sitten kyse käyttäjästä tai tietokoneesta. Jos niiden toiminta saadaan pysymään kaikilla samankaltaisena, on ylläpitotehtävissä onnistuttu. Näin ollen säästyy myös aikaa muihin ylläpidollisiin tehtäviin. Oppilaitosympäristössä opiskelijoilla ei tarvitse olla juurikaan ylimääräisiä oikeuksia perus työpöytäkäyttöä varten, mihin työasemia pääasiassa käytetään. Yleensä ylläpidollisesti asiat menevätkin niin, että mitä helpompi hallittava, sitä enemmän täytyy tehdä töitä. Tämä ajattelen siis alkuasetelmaa. Siihen pisteeseen päästäkseen on ensin tehtävä todella paljon testausta ja tarkistettava toiminnallisuuksia.

Liiketoiminta ja kulttuuri Porin ryhmäkäytäntöjä oli mielekästä tutkia, koska minusta ne olivat hyvin suunniteltu. Organisaatioyksiköt olivat loogisesti jaoteltu, pitäen sisällään eri koulutusohjelmien käyttäjäryhmät sekä luokkatilojen tietokoneet.

Nykymaailman tietotekniikka kehittyy edelleen hurjaa vauhtia ja se tuo tietysti omat haasteensa myös hallittavuuteen. Uusia tekniikoita kehitetään jatkuvasti, esimerkkinä virtualisointi. Näiden asioiden huomioonottaminen ryhmäkäytäntöjä ajatellen on taas yksi huomioitava asia.

Uskon, että tämän opinnäytetyön avulla järjestelmänvalvojat saavat hyvän kuvan ryhmäkäytäntöjen mahdollisuuksista sekä löytävät apua toimivan ympäristön suunnitteluun. Jatkoa ajatellen olisikin hienoa päästä hyödyntämään tämän opinnäytetyön kautta saatua kokemusta työelämässä. Ryhmäkäytännöt mahdollistavat niin paljon

erilaisia määrittelyjä ja rajoituksia, joilla voisi tehokkaasti ylläpitää kuinka isoa ympäristöä tahansa.

LÄHTEET

Itsenäiset teokset

Chellis, J. 2006. MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance, Exam 70-294 (2nd Edition). Indianapolis. Wiley Publishing.

Ivens, K. 2003. Windows Server 2003: The Complete Reference. New York. McGraw-Hill/Osborne.

Kouti, S, Seitsonen, M. 2005. Inside Active Directory Second Edition. Boston. Addison-Wesley.

Moskowitz, J. 2004. Group Policy, Profiles, and IntelliMirror: For Windows 2003, Windows XP, and Windows 2000. San Francisco. Sybex Inc.

Piltzecker, A, Hunter, L, E, Craft, M. 2003. MCSE Exam 70-296 Study Guide: Planning, Implementing and Maintaining a Windows Server 2003 Environment for an MCSE Certified on Windows 2000. Rockland. Syngress Publishing.

Shinder, T, W, Shinder, D, L, Martin, J, A. 2003. MCSE Exam Study Guide: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure. Rockland. Syngress Publishing.

Shinder, T, W, Shinder, D, L. 2004. The Best Damn Windows Server 2003 Book Period. Rockland. Syngress Publishing.

Artikkelit

Rousku, K. 2005. Työasemat ruotuun ryhmäkäytännöillä. MikroPC 2005(3), 40-43.

Elektroniset lähteet

Buike, R. 2005. Creating Custom ADM Templates [verkkodokumentti]. [Viitattu 20.1.2009] Saatavissa: http://thelazyadmin.com/blogs/thelazyadmin/archive/2005/07/05/Creating-Custom-ADM-Templates.aspx

Group Policy Wiki. 2006. Group policy – WMI Filters [verkkodokumentti]. [Viitattu 20.3.2009] Saatavissa: http://grouppolicy.editme.com/WMIFilters

Microsoft Knowledge Base, Article ID: 231287. 2007. Loopback processing of Group Policy [verkkodokumentti]. [Viitattu 2.2.2009] Saatavissa: http://support.microsoft.com/kb/231287

Microsoft TechNet. 2005. Troubleshooting Group Policy Problems: Group Policy [verkkodokumentti]. [Viitattu 3.3.2009] Saatavissa: http://technet.microsoft.com/en-us/library/cc787386.aspx

Microsoft TechNet. 2005. RSoP overview: Group Policy [verkkodokumentti]. [Viitattu 17.2.2009] Saatavissa: http://technet.microsoft.com/en-us/library/cc778752.aspx

Microsoft Technet. 2005. Access RSoP data for an existing computer and user (logging mode): Group Policy [verkkodokumentti]. [Viitattu 17.2.2009] Saatavissa: http://technet.microsoft.com/en-us/library/cc785715.aspx

Microsoft TechNet. 2005. RSoP planning mode: Group Policy [verkkodokumentti]. [Viitattu 17.2.2009] Saatavissa: http://technet.microsoft.com/en-us/library/cc737327.aspx

Microsoft TechNet. 2003. Group Policy Inheritance [verkkodokumentti]. [Viitattu 10.2.2009] Saatavissa: http://technet.microsoft.com/en-us/library/cc739343.aspx

Microsoft TechNet. 2005. Backup using GPMC: Group Policy [verkkodokumentti]. [Viitattu 23.1.2009] Saatavissa: http://technet.microsoft.com/en-us/library/cc784474.aspx

Turun Yliopisto – playground.utu.fi. 2007. Ohjeet:windowsinstaller [verkkodokumentti]. [Viitattu 30.1.2009] Saatavissa: http://playground.utu.fi/tympea/doku.php?id=ohjeet:windowsinstaller

Wikipedia. 2009. Disk quota – Wikipedia [verkkodokumentti]. [Viitattu 18.1.2009] Saatavissa: http://en.wikipedia.org/wiki/Disk_quota