Tampereen
ammattikorkeakoulu

Opinnäytetyö

Pienyrityksen käyttäjäympäristön kehittäminen AD:n ja skriptien avulla

Tuomas Huumonen

Tietojenkäsittelyn koulutusohjelma
Toukokuu 2008
Työn ohjaaja: Harri Hakonen

Helsinki 2008

Tekijä(t) Tuomas Huumonen
Koulutusohjelma(t) Tietojenkäsittely

Tutkintotyön nimi Pienyrityksen käyttäjäympäristön kehittäminen AD:n ja skriptien avulla

Työn valmistumis-kuukausi ja -vuosi Toukokuu 2008

Työn ohjaaja Harri Hakonen **Sivumäärä:** 44

TIIVISTELMÄ

Tässä opinnäytetyössä käsitellään käyttäjäympäristön suunnittelua ja kehittämistä pienyrityksen tietoteknisen järjestelmän näkökulmasta. Työssä tuodaan esille palvelimen yleiset käyttäjäympäristöön liittyvät asiat ja perehdytään yksityiskohtaisemmin käyttäjiin kohdistuvaan Active Directory-hallintakonsoliin ja sen käyttömahdollisuuksiin. Lopuksi työssä toteutetaan pienyrityksen käyttäjäympäristö tämän hallintakonsolin ja sitä tukevien skriptien avulla. Toteutuksen pohjana on Microsoftin VirtualPC-sovellus, jonka avulla virtuaaliseen työasemaan asennetaan Windows Server 2003-käyttöjärjestelmä.

Opinnäytetyön lähtökohtana on oman tietämykseni ja osaamiseni kehittäminen Windows Server 2003- ympäristössä. Tämä ympäristö on niin laaja, että sen tarkastelu kokonaisuudessaan jäisi tässä työssä vain pintaraapaisuksi, joten perehdyn tarkemmin palvelimen käyttäjätileihin ja niihin kohdistuviin ratkaisuihin.

Työn toteutusosuus kohdistuu kuvitteelliseen pienyritykseen nimeltään Eriväri. Yritys on 20 henkilön pienyritys, joka toimii mainosalalla. Idea kohteeksi kehitellystä mainosalan yrityksestä tuli työharjoittelussa tehdyistä pienyrityksien palvelinasennuksista. Tiukasti rajatut aikataulut ja enimmäkseen vain oppipoikana oleminen jättivät asioiden ymmärrykselle paljon toivomisen varaa. Opinnäytetyöni on siis oiva tilaisuus paikata näitä tietämyksen aukkoja.

Työn aineiston pohjana ovat asiantuntijoiden kirjoittamat Microsoftin palvelimiin liittyvä peruskirjallisuus, sekä Microsoftin omat palvelimia käsittelevät julkaisut. Näistä julkaisuista kerättyä aineistoa on sovellettu työhöni käyttäen kvalitatiivisen tapaustutkimuksen menetelmiä. Yrityksen käyttäjäympäristön toteuttamiseen liittyviin komentojonoihin on haettu tietoutta Internetistä löytyvien aihetta käsitteleviltä sivustoilta.

Opinnäytetyön tavoitteena on kehittää pienyritykselle toimiva käyttäjäympäristö, lähtien suunnittelusta ja päätyen toteuttamiseen erilaisia esimerkkejä käyttäen. Nykyisessä työtehtävässäni joudutaan päivittäin tarkastelemaan yritysten käyttäjätiliongelmia, uskon, että tämän työn tuloksista on hyötyä näiden ongelmien ymmärtämisessä.

Avainsanat Active Directory Käyttäjätilit Komentojono Palvelin

Author's Tuomas Huumonen
Degree Programme(s) Business Information Systems

Title Development of user environment to small enterprise with the AD and Scripts

Month and year May 2008

Supervisor Harri Hakonen **pages:** 44

ABSTRACT

This thesis covers the planning and development of a user environment of a small enterprise, focusing on the ICT system. It presents the universal issues concerning the user environment of a server and focuses more on the users' side of the Active Directory- maintenance console and the possibilities of using it. Finally, the user environment of a small enterprise is created with the Active Directory console and its supporting scripts. It is based on a Microsoft Virtual PC, which enables a Windows Server 2003 operating system being installed in the virtual server.

Basically in this thesis I wanted to develop my knowledge of the Windows Server 2003 environment. Because this environment is so expansive I will concentrate on the solutions of user accounts on the server.

The execution part of my thesis focuses on a fictional small enterprise called Eriväri. It's a 20 person company that operates on the advertising business. I got this idea from the company where I carried out my practical training. There we installed some servers in small enterprises. I didn't learn much from these cases because the schedules were tight and I was a little bit of a rookie. So this thesis is a good opportunity to improve my skills on that area.

The source material of this thesis is based on some basic literature of Microsoft servers written by experts of the matter, and some other articles and books published by Microsoft. I collected this material using the methods of qualitative case studies. On the internet I also found some information of scripts that helped me create the user environment to this fictional small enterprise.

The purpose of this thesis is to create a functional user environment to a small enterprise, starting with planning and ending to the execution, with many different observation examples. In my current job I face the problems of user accounts every day so I believe that what I will benefit from the results of this thesis will help me to understand more of these problems.

Keywords Active Directory User account Scripts Server

Sisällysluettelo

1. Johdanto

Opinnäytetyöni lähtökohtana on oman tietämykseni ja osaamiseni kehittäminen Windows Server 2003 ympäristössä. Kyseinen ympäristö on niin laaja, että sen tarkastelu kokonaisuudessaan jäisi tässä työssä vain pintaraapaisuksi. Tämän seikan takia perehdyn tarkemmin palvelimen käyttäjätileihin kohdistuviin ratkaisuihin. Opintosuuntautumiseeni kuuluvien palvelinkurssien myötä sain paljon tietoa perusasioista, jotka loivat perustan serveritietämykselleni. Syynä tähän päämäärääni syventää käyttäjätileihin kohdistuvaa serveritietämystäni on ollut lähinnä työpaikkojani, joissa serveriosaamista on hyödynnetty vain hieman, eikä itseopiskelulle ole jäänyt paljoakaan aikaa. Nyt opinnäytetyöni kautta haluan perehtyä paremmin muutamiin keskeisiin osa-alueisiin, jotka liittyvät palvelimen käyttäjätileihin ja niihin liittyviin käyttöoikeusratkaisuihin pienyritysympäristössä. Uskon, että käyttäjäympäristön paremmasta ymmärryksestä yritysmaailmassa on hyötyä nykyisessä työpaikassani, jossa päivittäin eteeni tulee ongelmaratkaisuja, jotka liittyvät käyttäjätilien luontiin ja niiden muokkauksiin sekä ryhmäoikeuksien tarkasteluun ja käyttäjiin kohdistuvien ryhmäkäytäntöjen selvittämiseen.

Alun perin kipinä käyttäjiin kohdistuvan palvelinosaamiseni kehittämiseen lähti työharjoittelupaikassani suorittamistani muutamista pienyrityksen serveriasennuksista. Yrityksien kiireellisten aikataulujen takia emme juuri kerinneet perehtyä niiden järjestelmää käyttävien käyttäjätilien suunnitteluun. Osasyynä tähän suunnittelun vähäisyyteen voidaan pitää Microsoftin tarjoamaa Small Business Serveriä, joka tarjosi paljon valmiita ratkaisuja käyttäjien hallintaan, joten oman näkemyksen ja kehittämisen osuus jäi aika minimiin. Myös yritysten alati vaihtuva vaatimustaso vaikeutti käyttäjätilien suunnittelua ja toteuttamista entisestään.

Nykyisessä työpaikassani yrityksen järjestelmiin liittyvien käyttäjäympäristöjen toiminnan ymmärrys on tärkeää. Tämä edellyttää myös, että AD-hallintakonsolin käyttö on hyvin hanskassa. Kohtaan haasteellisia ongelmaratkaisuja päivittäin, eikä asioiden itseopiskelulle ja koulun kursseilla opittujen asioiden soveltamiselle jää juurikaan aikaa. Uskon, että tämän opinnäytetyön johdosta minulla mahdollisuus paneutua serverin käyttäjäympäristön teoriaan ja käytäntöön parantaen taitojani tulevaisuuden varalle.

Opinnäytetyöni rakenne lähtee yleiseltä tasolta. Sen alkupuoli käsittelee käyttäjäympäristöä teoreettisesti, millainen on palvelimen käyttäjäympäristö, mistä osa-alueista se koostuu. Mikä on käyttäjien, ryhmien ja organisaatioyksiköiden vaikutus toisiinsa. Seuraavaksi käsittelen opinnäytetyössäni käyttämääni työkalua Windows server 2003:n

käyttäjiin kohdistuvaa hallintakonsolia Active Directory Users and Computers. Käyn läpi myös erilaisia metodeja, joiden avulla yrityksen käyttäjäympäristön suunnittelu ja kehittäminen voidaan mahdollistaa. Opinnäytetyöni toteutusvaiheessa suunnittelen ja toteutan pienyrityksen palvelimen käyttäjäympäristön.

Yksittäistasolla työni lähtee käyttäjistä, jotka kuuluvat ryhmiin, joita ohjaavat ryhmäkäytännöt. Käyttäjät ja ryhmät jäsennellään organisaatiotasolla, perustuen osastokohtaiseen organisaatioyksikkömalliin. Työkaluna käytän lähinnä edellä mainittua Windows Server 2003-järjestelmästä löytyvää Active Directory Users and Computer-hallintakonsolia ja sitä tukevia komentojonoja, skriptejä. Näitä apuna käyttäen suunnittelen ja perustan yritykselle toimivan käyttäjäympäristön, joka toivottavasti selkeille ja yksinkertaisilla ratkaisuilla helpottaa yrityksen käyttäjäympäristön hallintaa ja valvontaa. Otan myös esiin asioita, joita yrityksen käyttäjäympäristön toteuttajan tulisi ottaa huomioon suunnittelussa ja toteutuksessa.

Esimerkkiyrityksenä toimii pienyritys Eriväri, joka on 20 henkilön mainosfirma (kuviteltu yritys). Yritykseen halutaan toimiva ja selkeä käyttäjäympäristö, jota olisi helppo hallita, ja tulevaisuudessa laajentaa järkevällä tavalla yrityksen mahdollisesti kasvaessa. Toteutukseen liittyvään lukuun on lisätty paljon kuvallisia esimerkkejä, jotka havainnoivat yrityksen käyttäjäympäristön luomiseen kuuluvia vaiheita.

Työn lähteet koostuvat asiantuntijoiden kirjoittamasta Windows palvelimiin liittyvästä kirjallisuudesta, sekä Microsoftin omista palvelimiin kohdistuvista julkaisuista. Internetistä hyödynnän muutamaa komentojonoihin liittyvää nettiportaalia, joista saa hyviä perusesimerkkejä oman toteutukseni pohjaksi.

2. Käyttäjätilien suunnittelu

2.1 Yleistä

Käyttäjätilien suunnittelu kannattaa tehdä hyvin, jotta toimialueen palvelut, objektien käyttö ja kirjautumiset sujuisivat ongelmitta ja turvallisesti. Vaikka kyseessä olisi pienyritys pienine käyttäjämäärineen, niin kannattaa silti käyttäjätilien suunnittelun perusta kohdistaa osastoihin tai jonkinlaisiin organisaatioyksiköihin, jotta käyttäjätilien hallinta pysyisi selkeänä ja helposti käsiteltävinä. Tileille, joita organisaatioyksiköihin kohdistuvat ryhmäkäytännöt ohjaavat voidaan suunnitella erilaisia suojauksia ja käyttöoikeuksia ym. asetuksia toimialueen eri objekteihin sekä muihin resursseihin (jaetut kansiot, kirjoittimet jne.)

Yleisesti käyttäjätilejä voidaan hallita muuttamalla niiden asetuksia, määrittämällä käyttäjien kotikansioita ja luomalle heille tarpeittensa mukaisia käyttäjäprofiileja, jotka kuvastavat yrityksen työntekijää ja hänen työtehtäviään yrityksessä. Kirjautuessaan toimialueelle käyttäjä saa käyttöönsä käyttäjätiliinsä sidotut asetukset ja säilöt (työpöytä, suosikit, omat tiedostot) ja toimialueen tai keskitetysti ryhmien mukana tulevat ohjelmat. Profiilin perusteella siis määräytyvät työpöydän ja ohjauspaneelin asetukset, käytettävissä olevat valikkokomennot ja sovellukset sekä useita muita asetuksia. (Kivimäki 2005: 420)

2.2 Käyttäjätilien suunnitteluun ja luomiseen liittyvät tekijät

Et voi vain kopioida asiakkaalta saamiasi yrityksen työntekijöiden henkilötietoja järjestelmään, vaan käyttäjätilien suunnittelussa on otettava huomioon monta tärkeätä seikkaa. Niiden ominaisuudet ja asetukset vaikuttavat tulevan käyttäjäympäristön toimintaan ja sen ylläpitämiseen. Käyttäjätilien suunnittelussa tulisi paneutua nimeämiskäytäntöihin, käyttäjätilien voimassaoloaikoihin, salasanavaatimuksiin ja tilikäytäntöihin. Niiden kanssa kannattaa noudattaa johdonmukaisuutta, koska se edesauttaa erilaisten käytäntöjen käsittelyä ja muistamista. Näihin käyttäjätilejä ohjaaviin asetuksiin perehdytään lähemmin seuraavissa kappaleissa. (Kivimäki 2004: 434-435)

Nimeämiskäytännöt tulee suunnitella huolella, jotta vältyttäisiin nimeämiskonflikteilta. Käyttäjätilien nimet tulisivat olla joko työntekijän oikeita tai häntä kuvaavia nimiä. Ryhmäkäyttötunnuksien nimet muodostuvat yleensä ryhmän osastosta tai työtehtävästä. Käyttäjätileillä luodaan näyttönimet ja kirjautumistunnukset, jotka helpottavat käyttäjien erottelua toisistaan. Samannimisiä käyttäjiä voidaan erotel-

la esimerkiksi numerolla käyttäjätunnuksen jäljessä. Käyttäjätilin voimassaoloaikaa voidaan käyttää vaikkapa tapauksissa, joissa työntekijän työsuhde on määräaikainen, näin myös kirjautumisoikeuden on oltava määräaikainen. Palatakseni vielä nimeämiskäytäntöihin, määräaikainen työntekijä voidaan ottaa huomioon laittamalla kirjautumistunnuksen eteen kirjainsarja EXT-, näin tulevaisuudessa ehkä poistuvat tai disabloituvat tunnukset voidaan erotella kätevästi.

Tilikäytäntöjen avulla voidaan yhdenmukaistaa toimialueen käyttäjätiliasetukset. Niitä ovat salasanakäytännöt (Password Policy) esim. kuinka pitkä on salasananvaihtumisväli, tilien lukitsemiskäytännöt) Account Lockout Policy esim. kuinka kauan tili kannattaa pitää lukossa tarpeen vaatiessa ja Kerberos-käytännöt (Kerberos Policy) esim. vahvistaa Kerberos V5 -avaintenjakelukeskus käyttäjien oikeuskäytännöt. Tilikäytäntöjä voidaan ohjata Group Policyjen avulla. Niille luodaan turvaa käyttäjätasolle ja täten koko toimialueelle.
(Kivimäki 2004: 434-453, MSPress 3-40-42)

Käyttäjätilin luomisen yhteydessä käyttäjä saa SID-suojatunnuksen, joka koostuu toimialueen suojaustunnuksen etuliitteestä ja yksilöllisestä suhteellisesta tunnuksesta, jonka suhteellisten tunnisteiden palvelin on muodostunut. Toimialuetason käyttäjätilin avulla käyttäjä pääsee kirjautumaan toimialueelle, jolloin hänelle avautuvat verkon resurssit ja toimialueen asetukset. Kun yksilöllinen suojaustunnus SID on saatu käsiteltyä ja tunnistettua, sekä käyttäjätiedot replikoitua ohjauspalvelimen kanssa, voi käyttäjä alkaa käyttää hänelle tarkoitettuja resursseja. SID pysyy voimassa niin kauan kuin käyttäjän istunto kestää. (Stanek 2003:180)

2.3 Käyttäjätilien profiilit

Yleisesti ottaen toimialueen käyttäjä on objekti, jota voidaan hallita muuttamalla sen asetuksia. Käyttäjälle voidaan antaa omaa tilaa järjestelmässä, jakamalla hänelle omia resursseja, kuten kotikansio ja oma profiili. Kirjautuessaan toimialueelle käyttäjä saa käyttöönsä käyttäjätiliinsä omat vapaat resurssinsa, mutta myös tietyt toimialueeseen sidotut rajoitukset, jotka jäsentyvät käyttäjälle laajemmalla tasolla organisaatioyksikön tai lähemmin ryhmänjäsenyyden kautta. Palaamme näihin rajoituksiin tulevissa kappaleissa.
(Kivimäki 2005: 420)

Käyttäjän profiili voi olla paikallinen tai palvelimella sijaitseva (Roaming profile). Paikallinen profiili tallentuu paikallisesti työase-

maan, jolloin käyttäjän profiili muuttuu työaseman vaihtuessa, ja sen hallinta keskitetysti on näin mahdotonta. Käytettäessä palvelimella sijaitsevaa profiilia käytettävällä työasemalla ei ole merkitystä. Käyttäjän profiili latautuu palvelimelta ja tallennetut tiedot ja profiilin muutokset tallentuvat palvelimelle. Edellä mainittu ratkaisu voi olla hyvä pienissä tai keskisuurissa yrityksissä, koska uusien työasemien tai ongelmatilanteissa varakoneiden käyttöönotto helpottuu ja työntekijöiden tärkeät profiilitiedot pysyvät varmemmin tallessa palvelimella ja palvelimien varmistuksilla. Profiilit vaativat tallennustilaa, joten yksilöllisten profiilien teko suurten yritysten järjestelmiin ei ole ehkä kannattavaa. (Kivimäki 2005: 429 - 431)

Useimmille käyttäjille kuten tietyille organisaatioyksikön jäsenille voidaan suunnitella tietynlainen yhteinen, mukautettu profiili. Kun järjestelmään tulee lisää käyttäjiä, voidaan tällainen yhteinen profiili kopioida myös heille, jolloin he saavat käyttöönsä kaikki yksiköl-le/osastolle kuuluvat yhteydet, asetukset ja samanlaiset työpöydän mallit. Näitä mukautettuja profiileja voidaan tarvittaessa ohjata ja hallinnoida ryhmäkäytäntöjen avulla. Käyttäjäprofiilien suunnitteluvaiheessa on hyvä miettiä, millaisia vapauksia käyttäjälle annetaan oman profiilinsa suhteen. Pienemmissä yrityksissä, joissa järjestelmänvalvojalla on vielä mahdollisuus hallita ja tarkkailla pientä käyttäjäryhmää, voidaan antaa käyttäjälle tiettyjä vapauksia hallita omaa käyttäjäprofiiliaan helpottaen yrityksen käyttöympäristöön liittyviä ongelmia ja yleisesti ohjata toimintaa käyttäjäystävällisempään suuntaan. Mutta monissa yrityksissä on syytäkin estää käyttäjiä tekemästä omiaan, jotka voisivat jatkossa aiheuttaa ongelmia järjestelmään ja yrityksen muuhun toimitaan. (Kivimäki 2005: 420-421, MSpress 2004: 3-15, 3-16)

Järjestelmänvalvoja voi siis tarvittaessa määrittää tietyt käyttäjäprofiilit pakollisiksi (mandatory user profile), jolloin käyttäjä ei voi tehdä pysyviä muutoksia profiiliinsa. Tämän avulla käyttäjän työpöytä pikakuvakkeineen pysyy järjestyksessä ja vain oleelliset asiat ovat esillä. Ryhmäkäytännöillä voidaan määrittää profiilin kokoon liittyviä asetuksia sekä määritellä siihen kuuluvien kansioiden sijainti. Ryhmäkäytäntöihin palataan lähemmin tulevissa kappaleissa. Seuraavaksi käsitellään tarkemmin käyttäjäprofiilin toimintaa. (Stanek 2003: 236-237).

2.4 Käyttäjäprofiilien toiminta

Käyttäjäprofiilia luotaessa tulee miettiä käyttävätkö työntekijät vain yhtä henkilökohtaista konetta vai työskenteleekö hän useilla eri koneilla. Tämä seikka kertoo sen luodaanko käyttäjän profiili paikallisesti tietokoneelle vai sijaitseeko se palvelimella riippumatta siitä, mitä konetta käyttäjä tulee käyttämään. Käyttäjän kirjautuessaan ensimmäistä kertaa käyttöjärjestelmään, hänen profiilinsa tallentuu tietokoneeseensa paikallisesti. Tämä tapahtuu niin, että järjestelmä kopioi paikallisen Default User-kansion %systemdrive%:\documents and settings\(käyttäjän kirjautumisnimi) kansioon C:\documents and settings\ (käytäjän kirjautumisnimi). Kirjautumisnimi kansion sisällä sijaitsee joitakin tärkeitä tiedostoja ja kansioita, joissa on käyttäjään liittyvää informaatiota. Tärkeitä kansioita käyttäjään nähden ovat esim. My Documents, jossa sijaitsevat käyttäjän tallentamat tiedostot, Desktop, mihin on sijoitettu työpöydän kuvakkeet ja tiedostot, Favorites, käyttäjän nettisuosikit ja Local Settings, josta löytyvät paikalliset sovellusasetukset ja muut tiedot, joita ei kopioida profiilin mukana. Tiedoista voidaan mainita vaikkapa Ntuser.dat, johon tallentuvat käyttäjäkohtaiset ohjauspaneeliasetukset, esim. hiiren vasenkätisyys. (Kivimäki 2005: 422-423, MSPress 2003: 3-28; 3-29)

Muutokset käyttäjäprofiiliin tapahtuvat yrityksen käyttäjän kirjautuessa ulos järjestelmästä. Jos hän on tehnyt muutoksiaan työpöydän kuvakkeisiin tai vaikkapa tallentanut tekemänsä dokumentin, niin muutetut asiat synkronoituvat palvelimen kanssa ja muutokset tallentuvat profiiliin uloskirjautumisen yhteydessä. Seuraavan sisäänkirjautumisen yhteydessä voidaan huomioida, että muutokset ja tallennukset ovat pysyneet profiilin päivityksen myötä. Järjestelmävalvojan kannattaa ohjata työntekijöitä tallentamaan tiedostonsa oikeisiin paikkoihin (oletuksena voidaan pitää My documents-kansiota tai omia kotikansioita). Tämä toimenpide helpottaa ongelmatilanteiden selvitystä ja pitää käyttäjäprofiiliin liittyvät tiedot järjestyksessä. Käyttäjien omia/muita tallennuskansioita voidaan uudelleen ohjata ryhmäkäytäntöjen avulla ja sijoittaa niitä verkkoasemille, jolla kansioiden käytettävyyttä voidaan helpottaa, ryhmistä ja ryhmäkäytännöistä enemmän tulevissa luvuissa. Käyttäjän profiilista saadaan tietoa komentorivin set-komennolla, esimerkiksi käyttäjän tunnuksen, toimialueen, kotikansion ja profiilin sijainnin. (Kivimäki 2005: 422 - 425)

Järjestelmän käyttäjän kirjautuessa ensimmäistä kertaa toimialueelle hänelle tarkoitettu käyttäjäprofiili kopioidaan palvelimelta käyttäjän tietokoneeseen. Toimenpide tuo hänelle omat asetuksensa, kuten esim. työpöytäasetukset ja nettisuosikit. Käyttäjän kirjautuessa ulos järjestelmä aina vertaa paikallista profiilia palvelimella sijaitsevaan ja vain muokatut tiedot päivitetään. Yrityksen tietyille käyttäjille voidaan luoda mukautettu, keskitetty profiili osastoittain. Tietyn osaston

käyttäjälle luodaan mukautettu profiili tietynnäköisellä työpöydällä, jotta esim. myyjät saisivat yhtenäisen työympäristön, tehdään mukautetusta profiilista myös keskitetty. Näin myyjät saavat kaikki tarvittavat työkalunsa, eikä mitään epäolennaisia erityissovelluksia sallita. Keskitetystä profiilista kannattaa tehdä myös pakollinen (mandatory), koska siihen tehdyt muutokset vaikuttavat kaikkiin profiilia käyttäviin myyjiin. (Stanek 2003: 236-237, MSPress 2003: 3-28; 3-29)

Isoissa yrityksissä omien eri palvelimien tapauksessa monet palvelinprosessit kannattaa hajauttaa eri palvelimille ajan, turvallisuuden ja resurssien takia. Myös käyttäjäprofiilitapauksissa profiilien olisi hyvä sijaita muualla kuin toimialueen ohjauspalvelimelle. Ne voidaan tallentaa vaikka tiedostopalvelimelle tai muille jäsenpalvelimille. Tiedostot kuten myös käyttäjäprofiilit päivittyvät yleensä tiuhaan tahtiin, joten tiedostopalvelimen varmuuskopiointi kannattaa tehdä useammin kuin muiden palvelimien. (Kivimäki 2005: 422 - 423)

3 Organisaatioyksiköiden vaikutus käyttäjätileihin

3.1 Yleistä

Organisaatioyksiköitä voidaan sanoa toimialueen lokeroiksi. Niiden rakenne ilmentää yleensä yrityksen toiminnallista, organisatorista rakennetta. Organisaatioyksikkö on siis tietynlainen säilö, joka sisältää käyttäjäympäristön kannalta tärkeitä objekteja, joita ovat esimerkiksi käyttäjätilit, ryhmät tai aliorganisaatioyksikkö. Näiden yksiköiden avulla voidaan delegoida käyttäjäryhmiä, käyttäjiä ja resursseja koskevia järjestelmähallinnallisia oikeuksia. Organisaatioyksikön ominaisuuksiin kuuluvat käyttöoikeusluettelointi, delegointi ja ryhmäkäytäntöobjektien linkittäminen. Niiden käyttö ei ole kumminkaan pakollista, mutta se helpottaa järjestelmän hallintaa pienessäkin yrityksessä. Organisaatioyksiköt näkyvät kansiomaisessa muodossa AD:n Users and Computers-konsolissa. (ks. luku 6) (Stanek 2003: 137-138, Kivimäki 2005: 368-367)

Organisaatioyksikkö ei näy loppukäyttäjälle, vaan se toimii toimialueella, johon käyttäjä kirjautuu. Sen asetukset ja käytännöt alkavat vaikuttaa käyttäjän sisäänkirjautumisen yhteydessä. Organisaatioyksikön sisällä olevia objekteja voidaan hallinnoida ryhmäkäytäntöjen avulla (ks. enemmän luvusta 5). Organisaatioyksikkö on itsekin objekti, joten siihen liittyy myös käsite periminen, joka tapahtuu pääorganisaatioyksiköstä alaspäin aliorganisaatioyksikköön. Käyttöoikeudet ja asetukset valuvat siis ylhäältä alas. Organisaatioyksiköiden avulla voidaan mennä hyvin yksityiskohtaiselle hallinnoinnin tasolla, mutta se saattaa hankaloittaa ja syödä tehokkuutta järjestelmän valvonnalta. Turhien tai liian monien organisaatioyksiköiden sisäkkäisten tasojen määrää tulisi siis rajoittaa. Pienyrityksen toiminnallisen rakenteen jäsentämiseen riittää varmasti kolmen sisäkkäisen organisaatioyksikön malli. (Kivimäki 2004: 337-339)

3.2 Organisaatioyksikköjen suunnittelun ja toteuttamisen näkökulmia

Organisaatioyksiköiden suunnittelussa ja luomisessa kannattaa ottaa huomioon tiettyjä seikkoja. Yksiköille kannattaa antaa niitä kuvaavat selkeät nimet ja ne tulisi tehdä ja järjestää järkevästi, ihan tietoturvasyidenkin takia. Yrityksen toiminnalliset osastot voidaan erotella toisistaan, jolloin niihin voidaan asettaa erilliset ryhmäkäytännöt ja käyttöoikeudet. Tähän näkökulmaan vedoten työasemat ja käyttäjätilit kannattaa myös erotella omiksi organisaatioyksiköikseen. Ryhmäkäytännöt periytyvät (oletuksena) ylemmältä tasolta alemmalle ja niiden käsittelyjärjestys noudattaa samaa linjaa, joten organisaatioyksiköiden

sisäkkäinen sijoitus vaikuttaa sen jäsenten toimintaan. Organisaatio-yksikkörakenteella luodaan siis perusta toimialueen objektien hallinnointiin. Sitä voidaan käyttää laajasta ja tarvittaessa rajoitetusta näkökulmasta lähtien. (Kivimäki 2004: 340-341)

4. Ryhmät

4.1 Yleisesti ryhmistä

Windows Server 2003:ssa voidaan luoda käyttäjien lisäksi myös ryhmiä, mikä helpottaa isompien joukkojen ja kokonaisuuksien hallintaa. Ryhmä voi koostua käyttäjistä, tietokoneista, kontakteista tai vaikkapa muista ryhmistä. Ryhmien hyötynäkökulma ilmenee mahdollisuudessa asettaa erilaisia asetuksia isommalle joukolle objekteja, eikä vain vaikkapa sallia tai kieltää jokaista yksittäistä objektia erikseen. Oletuksena ryhmän jäsen perii siis ryhmän ominaisuudet, mm. käyttöoikeudet. Tämän takia kannattaa käyttää sisäisiä ryhmiä, joiden avulla vähennetään käyttölupien määrittämistyötä. Toimialueen käyttäjät ovat aina jonkin ryhmän jäseniä, jo oletuksena he ovat Domain Users-ryhmän jäseniä, joilla on hyvin rajoitetut oikeudet, mutta pikkuhiljaa uusien ryhmän jäsenyyksien myötä käyttöoikeudet kasvavat tarpeitten mukaan. (Shimonski, Chellis, Desai 2006: 260-261)

4.2 Ryhmien tyypit ja vaikutusalueet

Windows Server-järjestelmässä on mahdollisuus muodostaa kahden tyyppisiä ryhmiä, joko suojausryhmiä (Security) tai jakeluryhmiä (Distribution). Suojausryhmät edesauttavat ryhmäkohtaisten käyttöoikeuksien luontia, ja helpottavat täten järjestelmänvalvontaa. Jakeluryhmillä taas voidaan keskittää sähköpostien tai tiedotteiden lähetys suurellekin yhteisölle. Liittämällä niitä vaikkapa organisaatioyksiköihin, saadaan helposti luotua suuriakin jakelulistoja. (Shimonski, Chellis, Desai 2006: 260-261)

Ryhmiä tehtäessä tulee miettiä myös niiden vaikutusalueita, jotka määräävät, millä alueella ryhmät toimivat ja kelpaavat. Huonosti suunnitellut ryhmät vaikeuttavat järjestelmänvalvojan tehtäviä. Toimivuusalueille pyritään helpottamaan näitä hallintaan liittyviä ongelmia ja tehtäviä. Ryhmien toimivuusalueet ovat:

- Toimialueen paikalliset ryhmät (domain local groups) Nämä ryhmät ovat voimassa vain yksittäisen toimialueen ohjauspalvelimessa. Jäseninä voivat olla vain toimialueeseen luodut tilit (esim. käyttäjätilit).

- Sisäänrakennetut paikalliset ryhmät (built-in local groups) Näillä ryhmillä on vain toimialueen paikalliset oikeudet. Näitä ryhmiä ei voi luoda eikä poistaa, vain muokkaus onnistuu.

- Universaalit ryhmät (universal groups) Ryhmiä voidaan luoda laajemmalle alueelle, muihin toimialueisiin tai vielä laajemmin metsän alueisiin. Tällaiset ryhmät ovat käytännöllisiä lähinnä suurissa yrityksissä, joissa ryhmiä hallita ja monistaa laajalle alueelle

- Yleiset ryhmät (global groups) Näiden ryhmien avulla voidaan luoda vaikuttamaan minkä tahansa toimialueen tai metsän objekteihin. Perusperiaatteena jäseniä voivat olla vain toimialueen objektit, jotka sijaitsevat kyseisien ryhmien määritysalueella. Opinnäytetyössäni esimerkkifirmassa käytetään näitä yleisiä ryhmiä. (Kivimäki 2004: 557-561, Stanek 2003: 181-185)

4.3 Ryhmien suunnittelu

Kuten edellä mainitsin, suunniteltaessa ryhmiä monen seikan huomioon ottaminen muodostuu tärkeäksi. Pohja kannattaa rakentaa järkevällä periaatteella, esimerkiksi yksi peruste voisi organisatorisen asema yrityksessä. Ryhmätilit kannattaa luoda samantyyppisiä käyttäjiä varten. Yrityksien järjestelmissä ryhmien luonnit voivat perustuvat resurssien tarpeisiin, esimerkiksi osastokohtaisesti, yrityksen eri toimijoiden tehtävät huomioon ottaen. Samalla osastolla työskentelevät tarvitsevat todennäköisesti samoja resursseja, ja myös ohjelmistot on jaettava ryhmittäin. Johtajilla, suunnittelijoilla ja muilla käyttäjillä on oltava joitakin erilaisia käyttöoikeuksia. Monien eri toteutustapojen yhdistäminen luo hallinnan vaikeuksia. Ryhmiä joudutaan lisäämään toisiin ryhmään ja sisäkkäisten tasojen määrä kasvaa. Tämä johtaa siihen, että ongelmatapauksissa järjestelmänvalvojan käyttöoikeuksien metsästäminen hankaloituu. Sisäkkäisten tasojen määrä tulisi siis pitää pienenä jos se on vain mahdollista. Mutta isomman ja monen erilaisten objektijoukkojen kanssa määritys saattaa olla vaikeaa. Jokainen järjestelmänvalvoja voi miettiä, että haluaako hän suorittaa toistuvia käyttöoikeusmäärityksiä vai luoko hän vain muutamia sisäkkäisiä tasoja. (Kivimäki 2004: 572)

Ryhmistä ja niiden jäsenyyksistä tulisi tehdä dokumentaatio, jotta tiedetään millaiset käyttöoikeudet ovat voimassa. Yrityksessä tapahtuu liikehdintään, järjestelmänvalvoja, ylläpitäjä tai tekninen tuki saattaa vaihtua ajansaatossa. Tämä auttaa myös muokkausta ja suunnittelua tulevaisuuden kannalta. (Stanek 2003: 217)

5 Ryhmäkäytännöt

5.1 Ryhmäkäytäntöjen suunnittelu

Järjestelmänvalvojan/suunnittelijan kannattaa ottaa huomioon muutamia seikkoja suunniteltaessa toimialueella vallitsevia ryhmäkäytäntöjä. Ensinnäkin hyödyllisesti ryhmäkäytännöstä on turha puhua, jos se kohdistuu pelkästään vain yhteen objektiin. Tällöin ei myöskään päästä hyödyntämään ryhmäkäytäntöjen tärkeää ominaisuutta periytymistä. Sitä tulisi käyttää kaikissa mahdollisissa tilanteissa, jotta ryhmäkäytännöt voitaisiin suunnitella koskemaan mahdollisimman suurta joukkoa objekteja. Näin edelläkin mainittu ryhmien ”paimentaminen” yksinkertaistuu ja täten myös helpottuu.

Ryhmäkäytännöt tulee ryhmitellä järkevästi. Niitä kannattaa sijoittaa suhteellisen harvoihin ryhmäkäytäntöobjekteihin. Suurpiirteisemmät säännöt (Koko yritystä tai osastoa koskevat käytännöt) voidaan sijoittaa toimialuetasolle, joka periyttää ne kaikille organisaatioyksiköille. Yksittäisen organisaatioyksikön käyttäjiä koskevat asetukset taas voidaan määritellä ryhmäkäytäntöobjektissa, joka on sijoitettu kyseiset käyttäjätilit sisältävään organisaatioyksikköön. Samaa tapaa kannattaa noudattaa muidenkin objektien kanssa. (Kivimäki 2004: 595-596)

Hyvä suunnittelu on kaiken A ja O. Ryhmäkäytännöt tulee suunnitella yrityksen ja sen toiminnan tarpeiden mukaisesti. Ilman järkevää politiikkaa, objektien ja niistä koostuvien ryhmien hallitseminen vaikeutuu ja sen myötä inhimillisten virheiden määrä kasvaa. Ryhmäkäytännöt kannattaa testata hyvin ennen todellista käyttöönottoa. Huonosti toimivat ryhmäkäytännöt riskeeraavat toimialuetta monella eri tapaa, esimerkiksi tietoturva saattaa kärsiä pahasti. Täytyy myös muistaa, että ”mitä enemmän keittäjiä sen isompi soppa”, joten kannattaa rajoittaa myös ryhmäkäytäntöjä hallitsevien järjestelmänvalvojien määrää. Ryhmäpolitiikan monimutkaisuuden myötä vaikeutuvat ylläpitäminen ja hallitseminen.
(Shimonski, Chellis, Desai 2006: 383)

5.2 Ryhmäkäytännön käsittely ja jakaminen

Ryhmäkäytäntöjä voidaan jakaa eri alueille. Niitä voidaan tehdä paikallisesti, palvelinjoukolle, toimialueelle ja organisatoriseen yksikköön. Ne jakautuvat kahteen luokkaan, työasemiin liittyvät asetukset ja käyttäjiin liittyvät asetukset. Serveri käsittelee ryhmäkäytännöt järjestelmän käynnistyksessä ja sammutuksessa (työasemiin liittyvät) sekä käyttäjien kirjautuessa järjestelmään sisään, käytännöt huomioidaan myös uloskirjautumisen yhteydessä (käyttäjiin liittyvät) (Stanek 2003: 86-87)

Ryhmäkäytännöt ovat olemukseltaan dynaamisia; ne käsitellään oletuksena 90 minuuttia + 0….30 minuutin välein, ohjauspalvelimissa 5 minuutin sisällä. Tämä johtaa siihen, että esimerkiksi suojausasetukset voivat olla paikallisessa järjestelmässä korkeintaan kaksi tuntia (enintään 90+30min) jotakin muuta kuin toimialueen ryhmäkäytäntö on määrittänyt. Jos toimialueen ja paikallisen työaseman ryhmäkäytännöt eivät täsmää toistensa kanssa, ottavat toimialueen ryhmäkäytännöt määräävämmän aseman ja jakavat omat suojausasetuksensa työasemalle. Näin ollen paikallisia suojausasetuksia (esim. salasanakäytäntöjä) voidaan ohjata toimialueen ryhmäkäytäntöjen avulla. Myös ajallisesti katsottuna ristiriitatilanteessa myöhemmin asetetut käytännöt korvaavat aiemmin asetetut. (Kivimäki 2004: 595)

5.3 Linkittäminen ja periytyminen

Ryhmäkäytäntöjen tärkeimpiä ominaisuuksia ovat linkittäminen ja periytyminen. Niiden avulla ryhmäkäytäntöjen käyttäminen tehostuu, koska käytännöt saadaan koskemaan laajempaa joukkoa. Perusneuvona ryhmäkäytäntöjen määrä kannattaa pitää mahdollisimman pienenä helpottaen niiden hallintaa ja välttäen ristiriitaisuuksia. Linkittäminen mahdollistaa aiemmin luotujen ryhmäkäytäntöjen liittämisen toiseen organisaatioyksikköön tai toimialueeseen. Näin järjestelmänvalvojan/suunnittelijan ei tarvitse aina tehdä uuttaa ryhmäkäytäntöä. Linkitys toimii, kun muokkaat kohteen ryhmäkäytäntöä, niin muokkaat samalla ryhmäkäytäntöobjektin alkuperäistä kopiota. ja myös näin ollen muutokset vaikuttavat kaikkiin niihin objekteihin, joihin tämä ryhmäkäytäntö on linkitetty.

Periytyminen ei ole pakollista, mutta sitä tulisi käyttää niin paljon kuin vain mahdollista. Ryhmäkäytännöt tulisi suunnitella, niin että periytymisominaisuutta ei tarvitsisi ottaa pois turhan takia. Mutta halutessa alisäilöille voidaan määritellä omat ryhmäkäytäntönsä, jolloin ne korvaavat isäntäsäiliön. Käytännöt voidaan kytkeä pois, jolloin ne eivät ainakaan pääse periytymään, mutta tällöin ne eivät kohdistu mihinkään, eikä niistä ole silloin mitään hyötyä.
(Kivimäki 2005: 611-614)

6. Active Directory Users and Computers-hallintakonsoli

6.1 Yleisesti AD:n hallintakonsoleista

Palvelimen hallintaa ohjataan Active Directory-hallintatyökalun avulla. Työkalu sisältää monta erilaista hallintakonsolia, joita keskitetysti hallitaan MMC-työkalupakin avulla. MMC-konsolin avulla AD-suunnittelijalla on mahdollisuus rakentaa omanlaisensa hallintapaketti, jossa voidaan käyttää vain haluttuja hallintatyökaluja. Tätä pakettia voidaan kutsua myös tietynlaiseksi suunnittelijan työkalupakiksi. AD:n tärkeitä hallintakonsoleja ovat Active Directory Users and Computers, Active Directory Domains and Trust, Active Directory Sites and Services ja Resultant Set of Policy. (MSPress 2004: 2-1)

Opinnäytetyöni päätyökalu on Active Directory Users and Computers-hallintakonsoli, jonka avulla voidaan hallita toimialuetta. Edellä mainittuun hallintaan liittyvät ohjauspalvelinten roolien käsittely, toimialueen toimintatilan määritteleminen, sekä objektien luominen ja hallitseminen. Toimialueen objektit koostuvat esimerkiksi käyttäjistä, ryhmistä, tietokoneista, organisaatioyksiköistä ja ryhmäkäytännöistä. Tämän opinnäytetyön pääpaino on enimmäkseen toimialueen objektien suunnittelussa ja hallinnassa.(Stanek 2003: 155-157)

Active Directory Users and Computers -hallintakonsolin käyttö edellyttää AD-suunnittelijalta riittäviä oikeuksia hallittavaan toimialueen objektiin nähden. Hänen tulee olla Domain Admins-ryhmän jäsen, joka on jäsen toimialueen paikallisessa Administrator-ryhmässä. Ensimmäiseksi AD-suunnittelijan on saatava yhteys toimialueen ohjauspalvelimeen, jotta käyttäjätilien ja niihin liittyvien objektien suunnittelu ja luominen voivat alkaa. Kun yhteys ohjauspalvelimeen ja hallittavaan toimialueeseen saadaan muodostettua, voidaan alkaa käyttää kyseisen konsolin palveluja. Niistä tärkeimmät voidaan kiteyttää kolmeen toimintoon, luo, etsi, jaa ja delegoi. Voit luoda uusia objekteja ja antaa niille erilaisia arvoja, atribuutteja. Voit etsiä ja tarkastella luomiasi objekteja, lähinnä niiden ominaisuuksia ja tilitietoja. Voit jakaa resursseja käyttäjien kesken. AD:n User and Computers-hallintakonsolilla voi myös delegoida hallintatehtäviä toisille järjestelmänvalvojille. Vähän hallintaa vaativia perustehtävät (esim. salasanojen resetointi) voidaan osoittaa helpdeskille tai vaikkapa sihteereille. (Kivimäki 2005: 34-37,541)

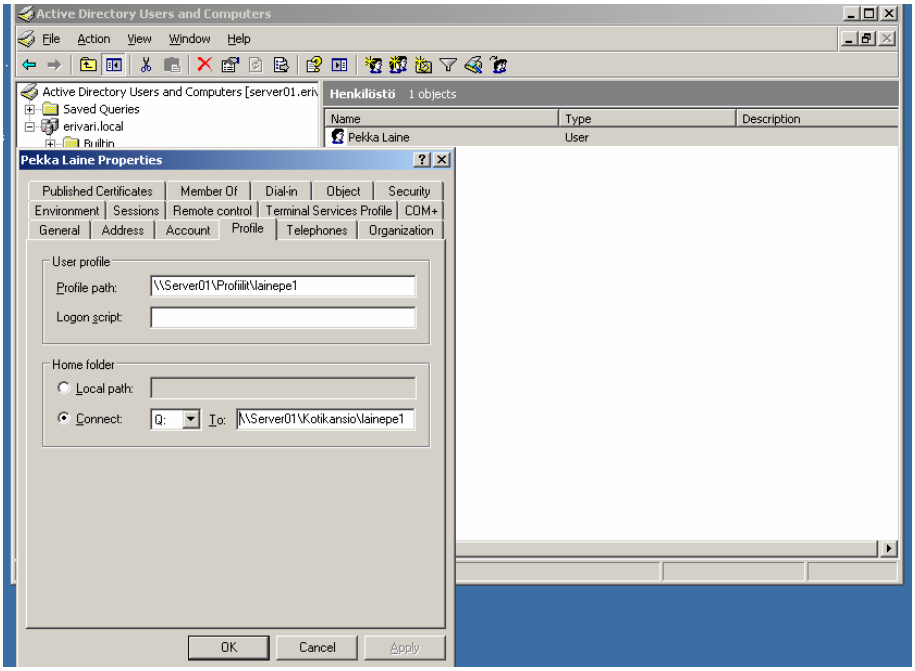
AD-suunnittelija voi säilyttää luomansa objektit perustamalla oman järjestyksensä niille. Mutta on myös mahdollista käyttää ns. vakiosäiliöitä. Esimerkiksi käyttäjä- ja tietokonetilin järjestämiseen voidaan käyttää niille tarkoitettuja vakiosäiliötä Users, Computers. Ne ovat oletustallennuspaikkoja toimialueen sisällä toimiville objekteille.

Käyttäjäympäristön AD-suunnittelussa kannattaa ottaa huomioida myös säiliö, nimeltään Builtin, joka sisältää luettelon sisäänrakennetuista ryhmätileistä, joita voidaan käyttää hyväkseen luodessa oletusobjektien suojauskäytäntöjä. (Stanek 2003: 158-164)

6.2 Käyttäjätilien suunnittelu ja toteuttaminen AD:n avulla

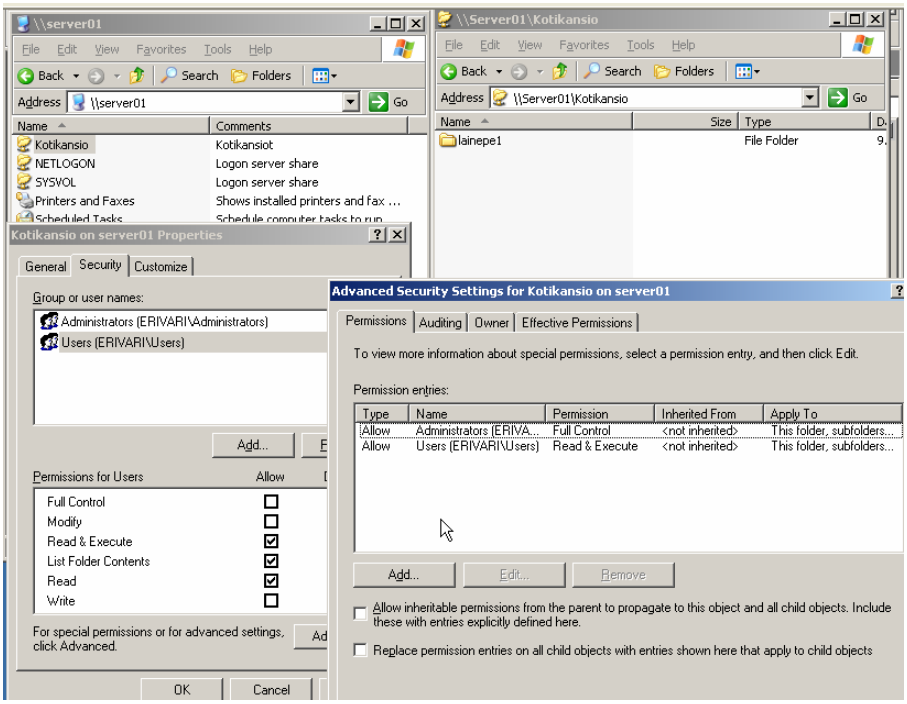
Käyttäjätilejä voidaan luoda monella eri tavalla. Graafisesti Active Directory User and Computers-hallintakonsolilla tai vaikkapa AD:ta tukevien erilaisten komentojonojen, skriptien avulla (ks. luku 7). Niiden avulla käyttäjiä voidaan luoda isoja määriä kerrallaan. Active Directory Users and Computers-hallintakonsolissa on myös mahdollisuus monistaa käyttäjiä (Copy Object User Wizard), tämän toiminnon uudet monistetut käyttäjätilit saavat myös mallitiliin sisältyneet asetukset. (MSPress 2003: 3-31, 3-32)

Hyödyllisiä skriptejä ja apuohjelmia ovat esimerkiksi Net user, DS-komennot, Windows Script Host ja Addusers.exe, Ldifde.exe ja Csvde.exe. Näistä lisää luvussa 7. Active Directory User and Computers-hallintakonsolin avulla käyttäjän luominen toimialueelle on suhteellisen helppoa, mutta työlästä. Suurten massaryhmien luonti samanaikaisesti on lähes mahdotonta. AD-konsolin avulla käyttäjän luonti, käyttöoikeuksien ja resurssien jakaminen on selkeää ja helposti ymmärrettävää, kun taas skriptien ja komentojen kanssa yksikin kirjain voi olla kohtalokas ja myös inhimillisten virheiden mahdollisuus on suuri. Seuraavassa toteutetaan käyttäjän tili, kotikansio ja profiili Active Directory Users and Computers-hallintakonsolin avulla. (Kivimäki 2004: 466)



Kuva 1 AD:n avulla käyttäjälle lainepe1 on luotu kotikansio

Kuvassa 1 käyttäjälle luodaan oma kotikansio palvelimelle. Se tehdään käyttäjän ominaisuudet-ikkunan profiili-välilehdellä. Kotikansion oikea polku on lisätty Connect-kohtaan, tiedostopolun määrityksessä käytetään muuttujaa ”%username%”, jolloin toiminto luo käyttäjänimelle olevan kansion. Palvelimella sijaitseva profiili määritellään samaan tapaan. Kohtaan User profile - Profile path on määritetty oikea polku, joka viittaa palvelimella sijaitsevaan jaettuun profiilitkansioon.



Kuva 2 Kotikansioiden luonti

Kuvasta 2 voidaan todeta, että käyttäjän kotikansio sijaitsee Server01-palvelimelle. Kansio on jaettu ja sen käyttöä varten on määritetty käyttöoikeudet. Järjestelmänvalvojalle on annettu täydet käyttöoikeudet, jotta hän voisi tarpeen mukaan ylläpitää jaettua kansiota. Muilla käyttäjille on asetettu luku- ja katseluoikeudet, koska se riittää, heidän ei tarvitse päästä muokkaamaan kansion sisältöä mitenkään. Kansion oikeuksien periytyminen on myös hyvä poistaa, jotta käyttäjät eivät pääsisi tallentamaan tiedostoja jaetun kansion juurikansioon. Samantyyppinen esimerkkiratkaisu tehdään Net user-komentojonojen avulla luvussa 7.

6.3 Ryhmien ja ryhmäkäytäntöjen suunnittelu AD:n avulla

Kuten jo edellä mainittiin, Active Directory-hallintatyökalu tarjoaa monia järjestelmän valvontaa helpottavia työkaluja, käytäntöjä ja proseduureja. Järjestelmänvalvojan ei kuulu valvoa tai opastaa jokaista käyttäjää erikseen. Hänen ei myöskään tarvitse keskittyä jokaiseen rutiinitehtävään, vaan hän voi automatisoida monia tehtäviä erilaisten hallintamenetelmien avulla. Niitä ovat esim. ryhmäkäytännöt, suojausmallit ja tehtävien ajastaminen. (Stanek 2003: 85-86),

Ryhmäkäytännöillä (Group Policy) tarkoitetaan järjestelmän kokoonpanoasetuksia, joilla voidaan vaikuttaa Active Directoryn objekteihin (Organisaatioyksiköt, ryhmät, käyttäjät yms.). Ryhmäkäytännöt ovat resursseja, joilla voidaan hallita keskitetysti käyttäjistä ja työasemista

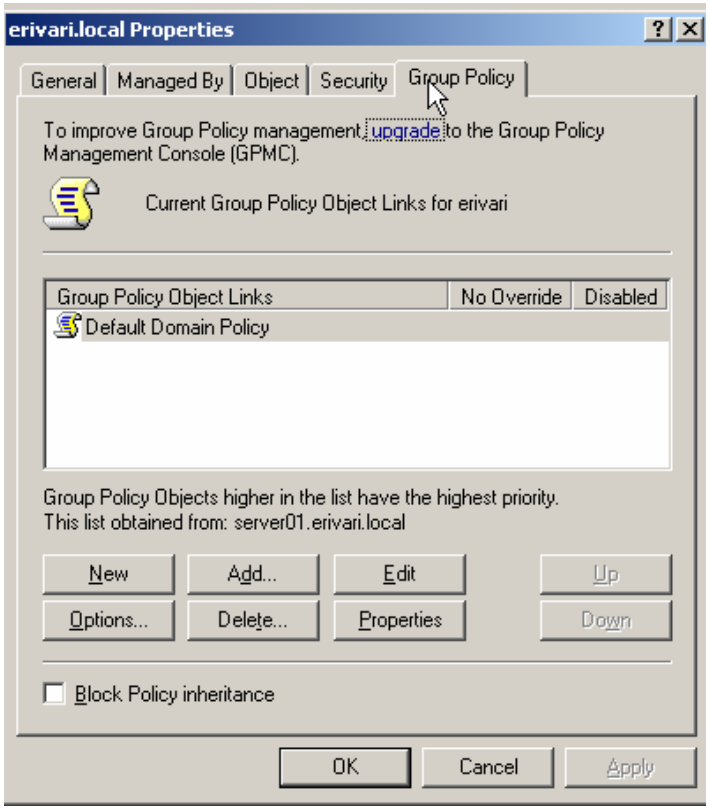
muodostettuja ryhmiä AD-toimialueen sisällä. Niiden avulla järjestelmänvalvojat voivat määrittää esim. käyttäjän ympäristöasetuksia, ohjelmien jakeluasetuksia, salasanakäytäntöjä, ja muita tarvittavia asetuksia. Ryhmäkäytännöt itse ovat objekteja (GPO), joihin nämä asetukset tallennetaan. Ryhmien luominen tapahtuu Active Directoryn Users and Computers-konsolin avulla. Työkalulla tehdään myös muut ryhmään liittyvät hallintatehtävät, kuten jäsenien lisääminen, ryhmän poistaminen ja niiden vaikutus alueitten muuttaminen yms. (Kivimäki 2004: 595)

6.4 Ryhmäkäytäntöjen periytymisen ohjaaminen ja linkittäminen AD:lla

Active Directoryssa ryhmäkäytännöt määritellään objektien avulla. Tällöin niiden ominaisuuksiin liittyy myös periytyminen. Tässä tapauksessa sillä tarkoitetaan, että oletuksena ryhmäkäytännöt siirtyvät pääsäiliöstä alisäiliöön. Tarvittaessa objektien ominaisuuksien periytyminen voidaan estää toiminnolla Block Policy inheritance. Tällöin toiminto estää objektia perimästä ylemmän tason ryhmäkäytäntöjä. Objektin Properties - Group Policy - Options-kohdassa on kaksi periytmiseen kohdistuvaa asetusta. Erikoistapauksena No override-asetus, joka pakottaa periytymisen Block Policystä huolimatta. Tällöin aliobjekteihin tehdyt omat ryhmäkäytännöt eivät korvaa ylempien, isäobjektien määrityksiä.

6.5 Ryhmäkäytäntöobjektien käyttäminen AD:n avulla

Ryhmäkäytäntöä luotaessa on ensin luotava ryhmäkäytäntöobjekti käyttäen Active Directory Users and Computers -konsolia toimialueelle tai sen objekteille. Ryhmäkäytäntöobjektin luominen tehdään halutun toimipaikan, toimialueen tai organisaatioyksikön Properties-ikkunan Group Policy -välilehdeltä (kuva 3) näemme toiminnot, jotka ryhmäkäytäntöobjektia tehdessä voidaan suorittaa:



Kuva 3 Group Policy-toiminnot

- Group Policy Object Links: tehdyt ryhmäkäytännöt
- New: ryhmäkäytäntöobjektin luominen
- Add: ryhmäkäytäntöobjektin linkittäminen
- Edit: haluttua ryhmäkäytäntöobjekti voidaan muokata tämän toiminnon avulla. Toiminto avaa Group Policy -hallintakomponentin (Group Policy object editor)
- Options: ryhmäkäytäntöobjektin ominaisuudet
- Delete: ryhmäkäytäntöobjektin poistaminen
- Properties: ryhmäkäytäntöobjektin ominaisuudet
- Up / Down: voit muuttaa ryhmäkäytännön prioriteettia. (ks. myös ryhmäkäytännön käsittely ja jakaminen)

Kuten yllä ryhmäkäytäntöjen suunnittelukappaleessa mainittiin, liian monia ryhmäkäytäntöjen muokkaaja saattaa synnyttää ristiriitaa käytäntöjen välille. Ryhmäkäytäntöobjekteille voidaan antaa tietynlaisia

käyttöoikeuksia. Niitä voidaan tarkastella ryhmäkäytäntöobjektin Properties ja Security -välilehdellä.

Oletuksena voimassa ovat:

Järjestelmävalvojalla: luku, muokkaus, luominen: kaikki aliobjektit, poistaminen.

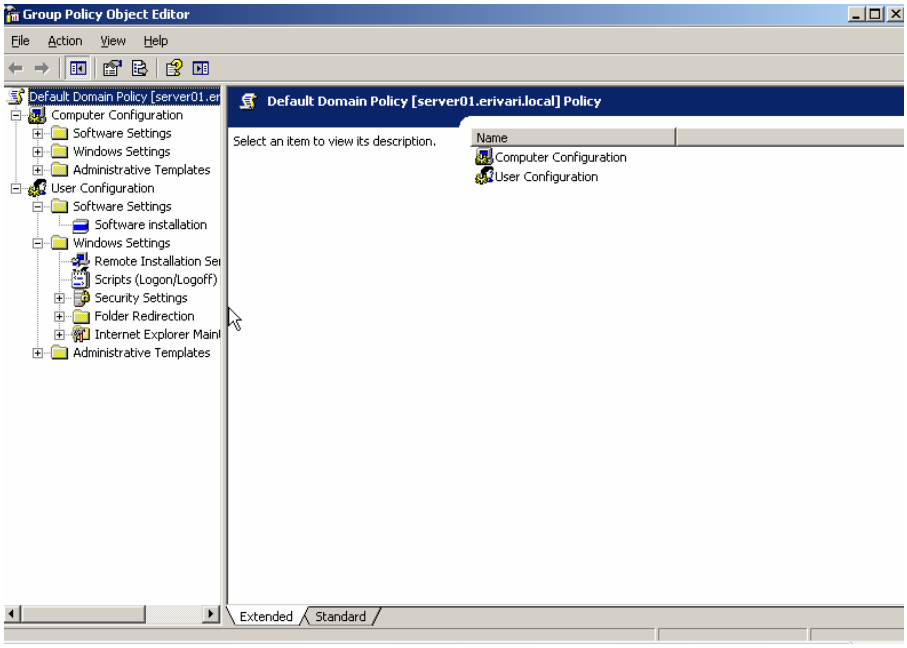
- Creator Owner: Objektin omistaja, annetaan erityisluvat, jotka mahdollista ryhmäobjektin aliobjektienkin hallinnan

- Authenticate User: luku ja Apply Group Policy (ryhmäkäytäntöä sovelletaan tähän ryhmään) Nämä oikeudet tulee laittaa ryhmälle, jonka tulee noudattaa tätä haluttua käytäntöä.

- Deny-atribuutti taas poistaa koskevuuden haluttuun ryhmään. Tätä arvoa ei kumminkaan kannata käyttää ryhmäkäytäntöobjektien muokkauksen tai päivityksen aikana. Tässä käytetään Properties, Options - Disabled-valintaa, jolloin käytäntö jää säilöön, mutta se poistetaan väliaikaisesti käytöstä.

6.6 Ryhmäkäytäntöasetukset Group Policy-konsolissa

Ryhmäkäytäntöjen asetuksia lähemmin katsottuna voidaan havaita tiettyjä ominaisuuksia (kuva 4). Tarkastellessamme kahden luokan (työasema- ja käyttäjäasetukset) sisältäviä asetuksia:



Kuva 4 toimialueen Group Policy-Objekti

- Administrative Templates: rekisteriperusteiset ryhmäkäytännöt, joiden avulla voidaan määritellä käyttöjärjestelmäkomponentit, työpöydän käyttäytymistä ja ulkoasua ohjaavat asetukset. Kolmelle rekisteriparametrilla (enabled, disabled, not configured) voidaan asettaa vaikkapa tietynlainen työpöytä tiettyineen taustoineen ja kuvaikkeineen.

- Software Setting / Software installation: vaikuttaa käyttäjän sovelluksiin. Sovellusten asennusta voidaan automatisoida kahdella eri tavalla: Sovellusten liittäminen käyttäjiin, tämä ryhmäkäytäntö asentaa tai päivittää yrityksen työaseman sovellukset automaattisesti tai tarjoaa käyttäjän käyttöön sovelluksen, jota hän ei voi poistaa. Sovellusten julkaisemisessa taas käyttäjä voi poistaa sovelluksen lisää/poista sovelluksia -toiminnolla. Sovelluksen julkaisemisen tekee järjestelmänvalvoja.

- Remote Installation Services: Etäasennukset, jotka näkyvät käyttäjälle, kun hän käyttää ohjattua Client Installation-toimintoa.

- Internet Explorer Maintenence: Internet Explorerin asetukset

- Folder Redirection: käyttäjän kansioiden uudelleenohjaus palvelimen jakamaan kansioon, jossa niitä voidaan hallita keskitetysti.

7 Komentojonojen käyttö käyttäjäympäristössä

7.1 Yleisimmät komennot

Objekteja voidaan luoda ja muokata perinteisellä tavalla Active Directory Users and Computer-hallintokonsilla tai aikaisemmin mainituilla komentojonoilla, skripteillä. Yleisimpiä komentoja ovat Ds-komennot, Net user, Ldifde.exe tai Csvde.exe. Komentojonojen käyttö helpottaa ja nopeuttaa monien kymmenien objektien luontia ja käsittelyä. Tiettyjen parametrien avulla käyttäjälle saadaan muutamalla rivillä kaikki tarvittavat ominaisuudet. Näin vältytään myös ikuisuuksia kestävältä asetusvälilehtien selausrumbalta, kuten myös totaaliselta kyllästyneisyydeltä.

Windows Server 2003-käyttöjärjestelmä tukee ensimmäistä kertaa komentorivillä käytettäviä DS-alkuisiakomentoja. Ne ovat monipuolisia, hyvin ymmärrettäviä komentoja ja niiden avulla voidaan luoda, poistaa, tarkastella, siirtää sekä tehdä hakuja että muuttaa atribuutteja. Niitä käytetään eri objektien edellä. Kappaleessa 7.3 kerrotaan enemmän kyseisistä komennoista.
(MSpress 2004: 3-17, 3-26)

7.2 Käyttäjien toteuttaminen ja kehittäminen komentojonojen avulla

Käyttäjätilejä voidaan luoda Net user-komennolla. Se ei sovellu kovin hyvin suurten käyttäjämäärien käsittelyyn. Net user-komennolla käyttäjätilit sijoitetaan automaattisesti Active Directorysta löytyvään vakiosäilöön Users. Halutessaan järjestelmänvalvoja voi järjestää käyttäjät organisaatiorakenteen mukaisesti, Users-oletussäilöstä käyttäjä voidaan siirtää sopivan organisaatioyksikön alle. Net user-komennon eduksi voidaan laskea, että sen käyttö ei vaadi kauhean kovia ohjelmointitaitoja. Komentoa voidaan käyttää ohjelmoinnissa käytettävien silmukoiden avulla vaikkapa käyttäjätilien testaukseen.

Jyrki Kivimäen (Kivimäki 2004: 484) tekemä esimerkki testauskomentojonosta silmukoineen:

// Komentojono tekee 500 testikäyttäjää nimellä Testi lisäten järjestysnumeron Testi-käyttäjien nimiä erottamaan.

For /L %i in (1,1,500 do net user Testi%i /add

ja poistaa ne

For /L %i in (1,1,500) do net user Testi%i /delete /yes
463-464

Net user-komennon perussyntaksi on:

Net user [käyttäjätunnus [salasana| *] [asetukset]] [/domain]
Net user [käyttäjätunnus {salasana |*} /add [asetukset] [/domain]
Net user käyttäjätunnus [/delete] [/domain]

[ei mitään]: jos net user-komentoa käytetään ilman parametreja, se näyttää kaikkien tietokoneen tai toimialueen käyttäjätilien luettelon

käyttäjätunnus: Määrittää lisättävän, poistettavan, muokattavan tai näytettävän käyttäjätilin nimen. Käyttäjätunnuksessa voi olla enintään 20 merkkiä.

salasana: Asettaa tai muuttaa käyttäjätilin salasanan. Salasanan on täytettävä salasanakäytännössä määritetty vähimmäispituus. Salasanassa voi olla enintään 127 merkkiä; on suositeltavaa käyttää enintään 14 merkin pituisia salasanoja.

*: salasana pyydetään kehotteella. Kehotteen jälkeen kirjoitettua salasanaa ei näytetä.

/domain: Suorittaa komennon toimialueella (käyttäjätili voidaan luoda myös paikallisena)

/add: lisää käyttäjätilin

/delete: poistaa käyttäjätilin

Seuraavat asetukset ovat käytettävissä:

/active: {no | yes}: ottaa käyttäjätilin käyttöön tai poistaa käytöstä. Jos käyttäjätili ei ole aktiivinen, käyttäjä ei voi kirjautua toimialueelle. Oletus on arvona aktiivinen.

/fullname:”nimi” : käyttäjän koko nimi (ei käyttäjänimeä.) Niin on kirjoitettava lainausmerkkeihin.

/homedir: polku: käyttäjän kotikansion sijainti. Polun on oltava olemassa.

/passwordchg: {yes|no}: voivatko käyttäjät muuttaa omia salasanojaan. Oletuksena voivat

/passwordreq {yes|no}: onko käyttäjätileillä oltava sanasala, oletuksena kyllä

/profilepath: [polku] käyttäjän profiilin kansiopolku

/scriptpath: path: käyttäjän kirjauskomentojonotiedoston kansipolun

Luvun 6.2 kuvaan 2 pohjautuva samantyyppinen käyttäjän ja hänen kotikansionsa luominen voidaan siis tehdä myös Net user-komentoja hyväksikäyttäen:

```
MD \Server01\Kotikansio\
Net user lainepe1 /ADD /passwordreq:yes /fullname:”Pekka Laine”
/eriväri.local /homedir:\Server01\kotikansio\lainepe1

// Luo Kotikansio-nimisen kansion Server01:lle.
// Luo käyttäjän, jolla on oltava salasana
// Luo käyttäjälle kotikansion
```

Kansioihin tarvitaan vielä käyttöoikeudet, jotka voidaan määrittää CACLS-komennolla.

```
CACLS \Server01\kotikansio\lainepe1 /G lainep1:F
CACLS \Server01\kotikansio\lainepe1 /E /G Adminstrators:F

//CACLS-komento asettaa käyttöoikeudet. Ensimmäinen lause luo
käyttäjäoikeusluettelon valitsin /E muokkaa sitä. Kummatkin
käyttäjät saavat Full Control-oikeudet F, aivan kuten graafisestikin
tehtiin hallintakonsolin ja kansionjakamisen kanssa. Net user-
komentojono tekee käyttäjän
```

7.3 DSADD ja Muut DS-alkuiset kommennot

DS-komennot ovat tulleet ensimmäistä kertaa Windows Server 2003 mukana. Komennot ovat: DSADD, DSGET, DSMOD, DSMOVE, DSQUERY, DSRM. Niiden avulla voidaan määritellä ja yksilöidä objekti ja objektin tyyppi. Komentojen avulla voidaan paikantaa niiden vaikutusalue ja määrittää millä oikeuksilla ne vaikuttavat kyseiseen alueeseen. (MSPress 2003: 3-15-24)

Komentojen tarkoitukset ovat:

DSADD-komennon avulla voidaan luoda ja antaa asetukset kaikentyyppisille objekteille toimialueella.

DSGET-komento näyttää objektin ominaisuudet

DSMOD-komennolla voidaan muuttaa objektin atribuutteja

DSMOVE-komennolla siirretään objektejä

DSQUERY-komennolla voidaan tehdä kyselyjä toimialueella. Sen avulla voidaan tuoda esille erilaisia listauksia toimialueen objekteista

DSRM-komennolla voidaan poistaa objekteja

DS-alkuinen komento näyttää yksinkertaisimmiltaan (esim. DSADD):

dsadd <objektityyppi> <objektin yksikäsitteinen tunnus>

Parametrit voidaan lisätä haluttu määrä esimerkkikomennon perään. Tärkeimpiä parametreja ovat mm.

-samid / käyttäjätunnus
-pwd /salasana *-merkin jälkeen se voidaan antaa
-memberof /ryhmänjäsenyys
-display / näyttönimi
-hmdir / kotikansio
-profile / profiili

(Microsoft Windows Server TechCenter 2005)

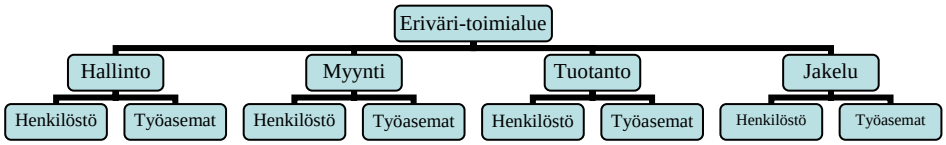
7.4 Ldifde.exe ja Csv.exe-apuohjelmat

Hyviä objektien luontiin käytettäviä välineitä ovat myös ohjelmapohjaiset Ldifde.exe ja Csv.exe. Ne ovat windows 2000-käyttöjärjestelmän mukana tulevia sovelluksia. Ldifden avulla voidaan tuoda valmiita esimerkiksi käyttäjätietoja koostuvia tekstitiedostoja, jotka määritelty niille tarkoitettuihin organisaatioyksiköihin. Ohjelman avulla onnistuvat myös muidenkin toimialueen objektien muokkaus ja poistaminen. Tiedostossa eri käyttäjätilit on eroteltu tyhjällä rivillä. Ldifde -apuohjelma erottelee eri käyttäjätilit ja niiden attribuutit eri riveille. Csv.exeä käytetään hyväksi Dcpromon luodessaan ensimmäistä ohjauspalvelinta Active Directoryyn. Kuten Ldifdekin kanssa, myös CSV-sovelluksella määritellyt tilit voidaan tuoda AD-hakmistoon. Erona CSV-sovelluksen tapauksessa on, että objektit on eroteltu pilkku-erottimella, eikä objekteja voi olenkaan muokata tai poistaa. Ldifde.exe apuohjelmalla luodaan eriväri-toimialueen objekteja luvussa 8. (Kivimäki 2005: 470-475)

8 Esimerkkiyrityksen toteuttaminen (Eriväri-toimialue)

8.1 Eriväri-toimialueen organisaatioyksiköt

Pienyrityksen organisatorinen rakenne ei ole yleensä kovin monimutkainen. Toimialuerakenne kannattaa silti suunnitella jonkinlaisen toimintamallin mukaan, jotta sen hallinta olisi tehokkaampaa. Pienyrityksen näkökulmasta mahdolliset rakenteet voisivat olla esimerkiksi järjestelmähallinnallisia, osastokohtaisia tai liiketoimintaan perustuvia. Esimerkkifirmassa Erivärin organisaatioon kuuluvat neljä osastoa (Hallinto, Myynti, Tuotanto, Jakelu). Organisaatioyksiköiden suunnittelu ja luominen perustuvat näin ollen liiketoiminnalliseen malliin. Jokaisella neljällä pääorganisaatioyksiköllä on kullakin samanlaiset aliorganisaatioyksiköt (Henkilöstö ja Työasemat). Henkilöstön aliorganisaatioyksikössä sijaitsevat kaikki käyttäjät ja niihin kohdistuvat ryhmät. Työasema-organisaatioyksikköön sijoitetaan yrityksessä käytettävät tietokoneet. (Kaaviossa 1. Eriväri-toimialueen organisaatioyksikkörakenne)



Kaavio 1 Eriväri-toimialueen organisaatioyksiköt

8.2 Eriväri-toimialueen organisaatioyksiköiden luonti skriptien avulla

Eriväri-toimialueen objektit toteutan erilaisten komentojen avulla. Lähtökohtana sovellan erilaisia skriptejä monipuolisesti, lähtien liikkeelle pääorganisaatioyksiköistä jatkaen aliorganisaatioyksikköön ominaisuuksineen. Jokaisen yrityksen osaston luon eri skriptejä hyväksikäyttäen.

Liikkeelle lähdetään luomalla yrityksen pääorganisaatioyksiköt, joita on siis neljä (Myynti, Tuotanto, Jakelu, Hallinto). Näistä jokainen omistaa aliorganisaatioyksiköt Henkilöstö ja Työasemat. Organisaatioyksiköt luodaan Windows Script Hostilla, (*.vbs) asettamalla muuttujille arvot, joita sovelletaan itse luomisvaiheessa.

Luodaan Organisaatioyksikot.vbs

```
//Asetetaan skriptille Toimialue arvo, jota voidaan käyttää hyväkseen
sen eri vaiheissa. Toimialue on siis dc=erivari, dc=local

Set Juuri = Getobject(“LDAP://RootDSE”)
Toimialuekohde = Root.Get(“DefaultNamingContext”)
Set Toimialue = GetObject(“LDAP://” & Toimialuekohde)

//Tehdään toimialueelle pääorganisaatioyksiköt

Set ouMyynti = Toimialue.Create(”organizationalUnit”,
”OU=Myynti”)
ouMyynti.Put”Description”, “Myyntiorganisaatioyksikkö”
ouMyynti.Setinfo

Set ouTuotanto = Toimialue.Create(”organizationalUnit”,
”OU=Tuotanto”)
ouTuotanto.Put”Description”, “Tuotanto-organisaatioyksikkö”
ouTuotanto.Setinfo

Set ouJakelu= Toimialue.Create(”organizationalUnit”, ”OU=Jakelu”)
ouJakelu.Put”Description”, “Jakeluorganisaatioyksikkö”
ouJakelu.Setinfo

Set ouHallinto = Toimialue.Create(”organizationalUnit”,
”OU=Hallinto”)
ouHallinto.Put”Description”, “Hallinto-organisaatioyksikkö”
ouHallinto.Setinfo


//Luodaan Myynti-organisaatioyksikön sisään aliorganisaatioyksikkö
Henkilöstö

Set ouAli = GetObject(”LDAP://OU=Myynti, ” & Toimialuekohde
Set ouHenk = ouAli.Create(”organizationalUnit”, ”OU=Henkilöstö”)
ouHenk.Put”Description”, “Henkilöstö”
ouHenk.Setinfo

// Luodaan Myynti-organisaatioyksikön sisään aliorganisaatioyksikkö
Työasemat

Set ouAli = GetObject(”LDAP://OU=Myynti, ” & Toimialuekohde
Set ouTyoasemat = ouAli.Create(”organizationalUnit”,
”OU=Työasemat”)
ouTyoasemat.Put”Description”, “Työasemat”
ouTyoasemat.Setinfo
```

```
//Luodaan muiden organisaatioyksiköiden aliorganisaatioyksiköt. Se
voidaan tehdä käyttämällä hyväkseen edellä tehtyä skriptiä, muuttaen
vain kohdetietoja.

Set ouAli = GetObject(”LDAP://OU=Jakelu, ” & Toimialuekohde
Set ouHenk = ouAli.Create(”organizationalUnit”, ”OU=Henkilöstö”)
ouHenk.Put”Description”, “Henkilöstö”
ouHenk.Setinfo

Set ouAli = GetObject(”LDAP://OU=Jakelu, ” & Toimialuekohde
Set ouTyoasemat = ouAli.Create(”organizationalUnit”,
”OU=Työasemat”)
ouTyoasemat.Put”Description”, “Työasemat”
ouTyoasemat.Setinfo

Set ouAli = GetObject(”LDAP://OU=Tuotanto, ” & Toimialuekohde
Set ouHenk = ouAli.Create(”organizationalUnit”, ”OU=Henkilöstö”)
ouHenk.Put”Description”, “Henkilöstö”
ouHenk.Setinfo

Set ouAli = GetObject(”LDAP://OU=Tuotanto, ” & Toimialuekohde
Set ouTyoasemat = ouAli.Create(”organizationalUnit”,
”OU=Työasemat”)
ouTyoasemat.Put”Description”, “Työasemat”
ouTyoasemat.Setinfo

Set ouAli = GetObject(”LDAP://OU=Hallinto, ” & Toimialuekohde
Set ouHenk = ouAli.Create(”organizationalUnit”, ”OU=Henkilöstö”)
ouHenk.Put”Description”, “Henkilöstö”
ouHenk.Setinfo

Set ouAli = GetObject(”LDAP://OU=Hallinto, ” & Toimialuekohde
Set ouTyoasemat = ouAli.Create(”organizationalUnit”,
”OU=Työasemat”)
ouTyoasemat.Put”Description”, “Työasemat”
ouTyoasemat.Setinfo

// Seuraavaksi tehdään vielä Myynti- ja Jakeluorganisaatioyksikköön
kuuluvat ryhmät (Myyjät, Myyntijohtajat, Jakelijat, Jakelusuunnitteli-
jat) Hallinto- ja Tuotanto-organisaatioyksiköiden ryhmät luodaan
myöhemmin luvussa 8.3

Set KohdeOU = GetObject(”LDAP://OU=Henkilöstö, OU=Myynti”
& Toimialuekohde)

Set KohdeOU2 = GetObject(”LDAP://OU=Henkilöstö, OU=Jakelu”
& Toimialuekohde)
```

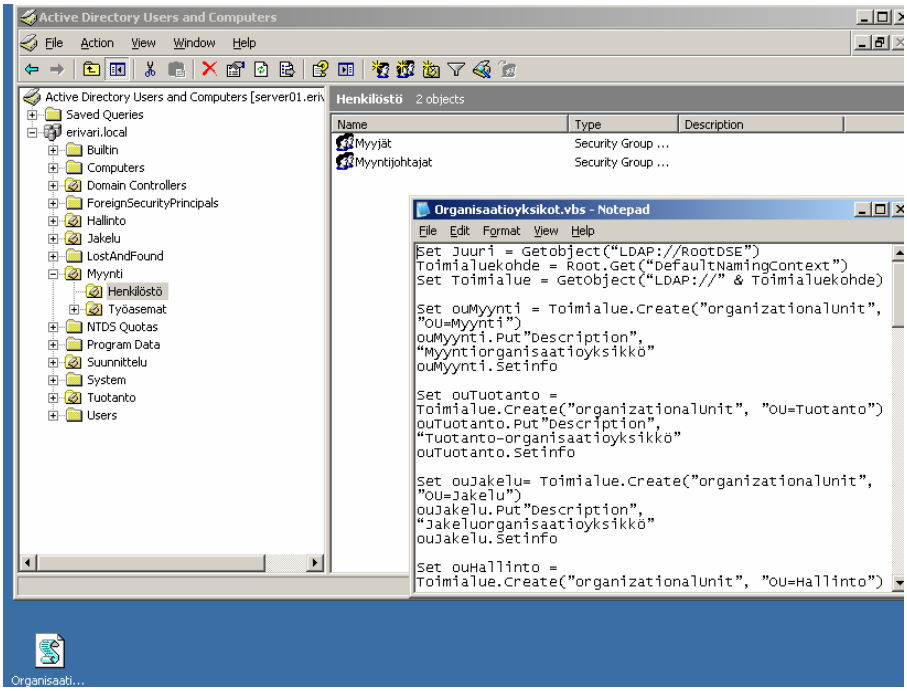
```
Set objgrp =KohdeOU.Create(”group”, ”CN=Myyntijohtajat”)
objgrp.Put “samAccountName”, “Myyntijohtajat”
objgrp.SetInfo

Set objgrp =KohdeOU.Create(”group”, ”CN=Myyjät”)
objgrp.Put “samAccountName”, “Myyjat”
objgrp.SetInfo

Set objgrp =KohdeOU2.Create(”group”, ”CN=Jakelusuunnittelijat”)
objgrp.Put “samAccountName”, “Jakelusuunnittelijat”
objgrp.SetInfo

Set objgrp =KohdeOU2.Create(”group”, ”CN=Jakelijat”)
objgrp.Put “samAccountName”, “Jakelijat”
objgrp.SetInfo
```

(Microsoft Script Center 2008)



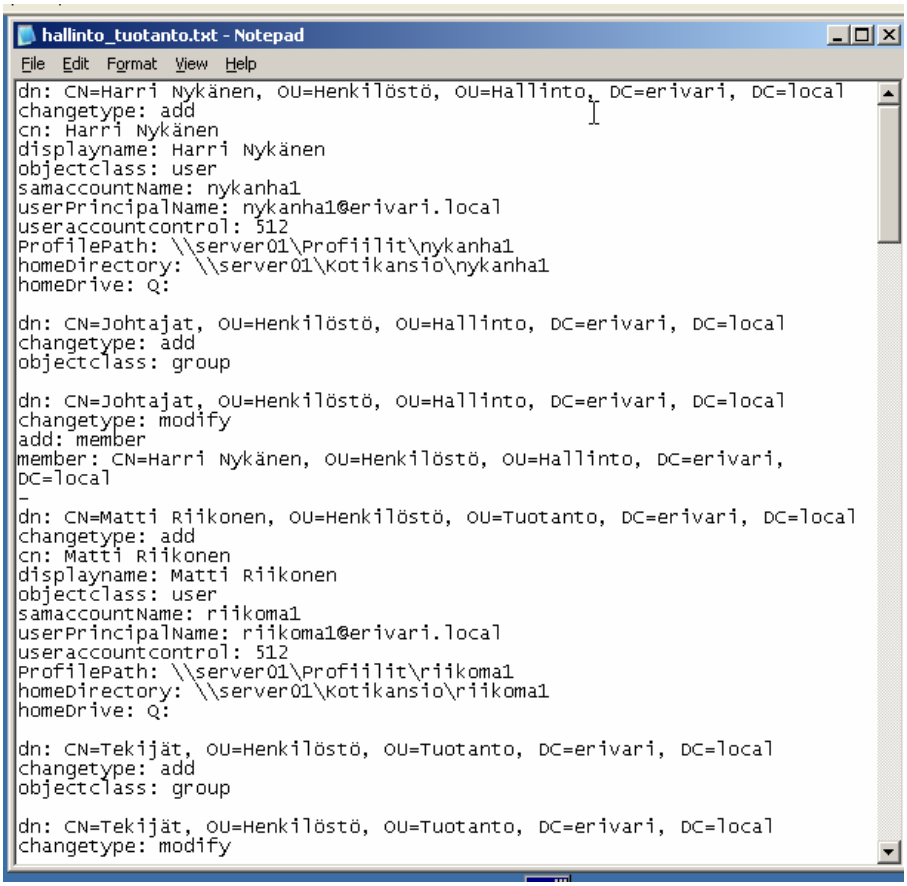
Kuva 5 Organisaatioyksikot.vbs avulla tehdyt organisaatioyksiköt ja ryhmät

8.3 Hallinto- ja Tuotanto-organisaatioyksiköiden käyttäjätilien luonti Ldifde-skriptin avulla

Hallinto- ja Tuontantoyksikön käyttäjätilit tuodaan AD:hen aikaisemmin esiteltyä Ldifde.exe-apuohjelmaa käyttäen. Näihin kahteen yksikköön kuuluu yhteensä 10 työntekijää, joista kerätään tarvittavat käyttäjätiedot tekstitiedostoon hallinto_tuotanto (kuva 6). Tekstitiedosto tuodaan AD:hen käskyllä ldifde -i -f hallinto_tuotanto.txt

Käyttäjät ovat:
Hallinto - Harri Nykänen (Johtajat), Tuomo Kanerva (Osastopäälliköt), Seppo Takanen (Osastopäälliköt), Teemu Rehula (Johtajat), Leena Rahunen (Sihteerit)

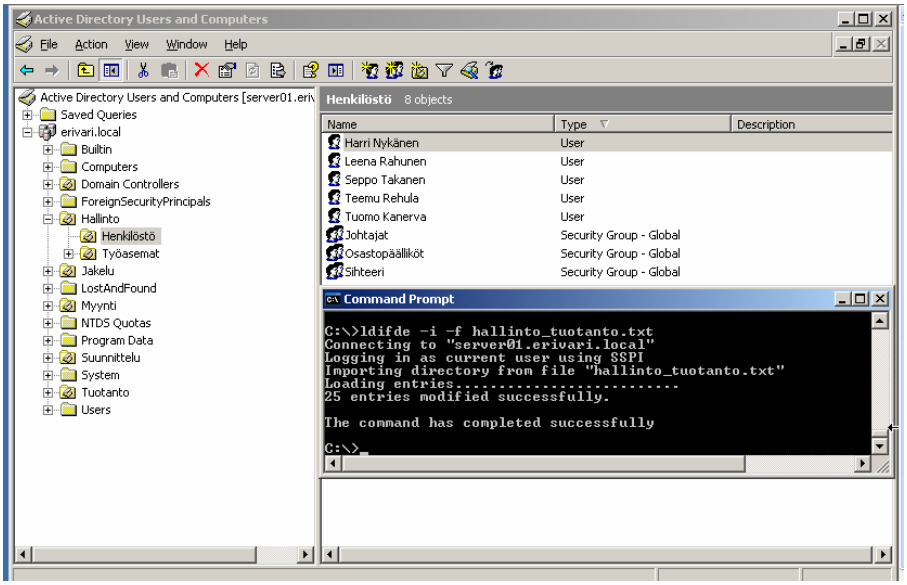
Tuotanto - Matti Riikonen (Tekijät), Merja Siltanen (Tuotantosuunnittelijat), Rami Poranen (Tekijät), Risto Nevalainen (Tuotantosuunnittelijat), Sami Niiranen (Tekijät)



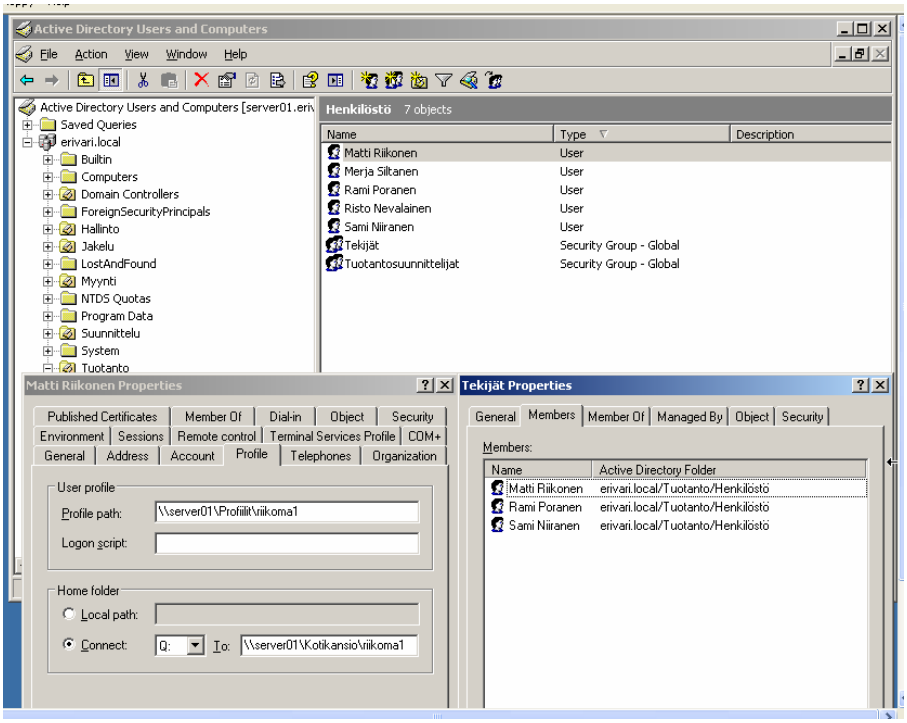
Kuva 6 hallinto_tuotanto-skriptitiedosto

Skripti luo kymmenen käyttäjää, joiden kotikansio ja profiili sijaitsevat palvelimella Server01. Käyttäjätunnukset ovat muotoa viisi kirjainta sukunimestä, kaksi etunimestä ja järjestysnumero. Käskyllä ”useraccountcontrol: 512” käyttäjätilit asetetaan käyttöön. Skripti luo myös Hallinnon ja Tuotannon ryhmät, joita on viisi (Johtajat, Osastopäälliköt, Sihteeri, Tuotantosuunnittelijat, Tekijät), ja niihin lisätään vielä oikeat jäsenet. Soveltamalla erilaisia komentoja toisiinsa saadaan luotua Hallinnon ja Tuotannon Henkilöstö-organisaatioyksiköiden objektit. Skripti suorittaa 25 toimintoa (Kuva 7) pienellä vaivalla, ilman Ominaisuus-välilehtien selailua. Skriptin

avulla vältytään myös käyttäjien manuaalilisäysten aikana tapahtuvista mahdollisista lyöntivirheistä. (Kuvassa 8 käyttäjätilin asetukset ja ryhmien jäsenyydet skriptin ajon jälkeen)



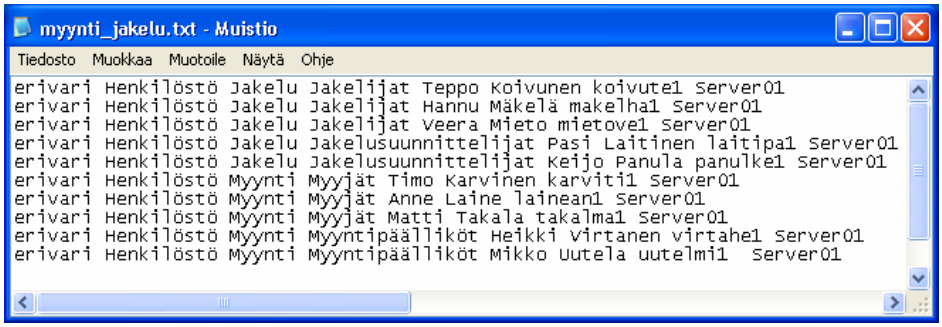
Kuva 7 ldifde.exe avulla tehdyt objektit



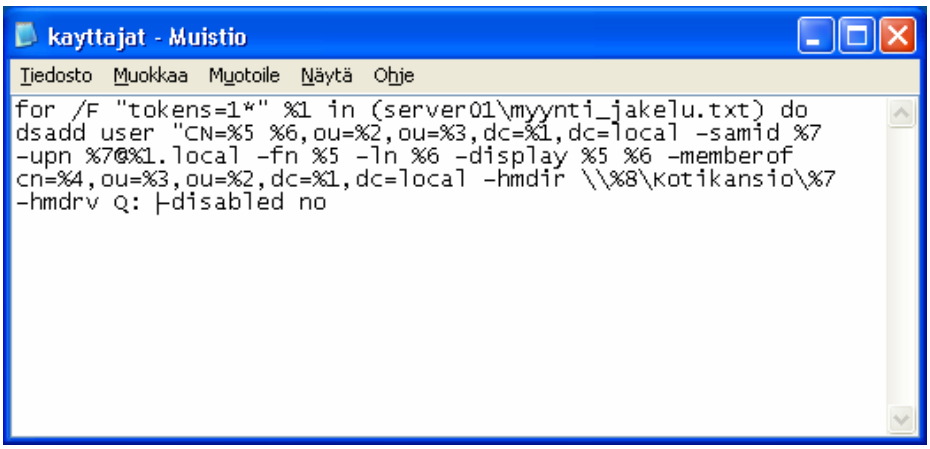
Kuva 8 käyttäjätilin asetukset ja ryhmien jäsenyydet

8.4 Myynti- ja Jakeluorganisaatioyksiköiden käyttäjätilien luonti For-lausekkeella

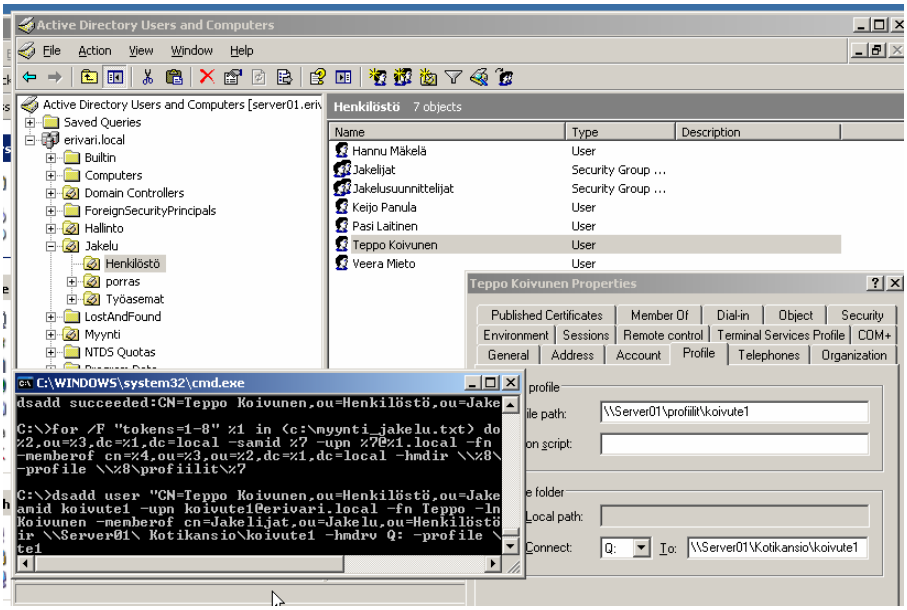
Seuraavaksi luodaan Myynti- ja Jakelu-organisaatioyksiköihin käyttäjätilit ja siirretään ne oikeisiin ryhmiin (lopputulos kuvassa 11). Tiedot näiden organisaatioyksiköiden käyttäjistä on saatu myynti_jakelu.txt-tiedostosta (sijaitsee palvelimella Server01), joka luetaan ja käsitellään kayttajat.bat-komentojonossa For-lausekkeen avulla. Komento lukee tekstitiedostoa sana kerrallaan ensimmäisestä rivistä ja sanasta lähtien (For /F ”tokens=1*” %1) tehden sanoille paikannustiedot (%1=erivari, %2=Henkilöstö, %3=Jakelu, jne..). Do-vaiheessa lauseke tekee käyttäjän ja sille tietyt ominaisuudet käyttäen hyväksi edellä mainittuja paikannustietoja (CN=%5, viides paikka tekstitiedostossa on Teppo). For-lauseke on voimassa niin pitkään kuin käyttäjiä riittää. Tiedostojen sisällöt on esitetty kuvissa 9 ja 10.



Kuva 9 myynti_jakelu.txt sisältö



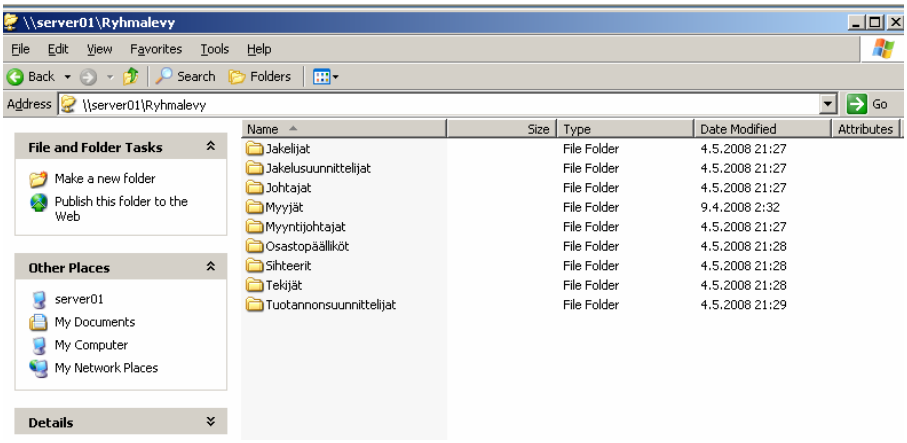
Kuva 10 Kayttajat.batin for-lauseke



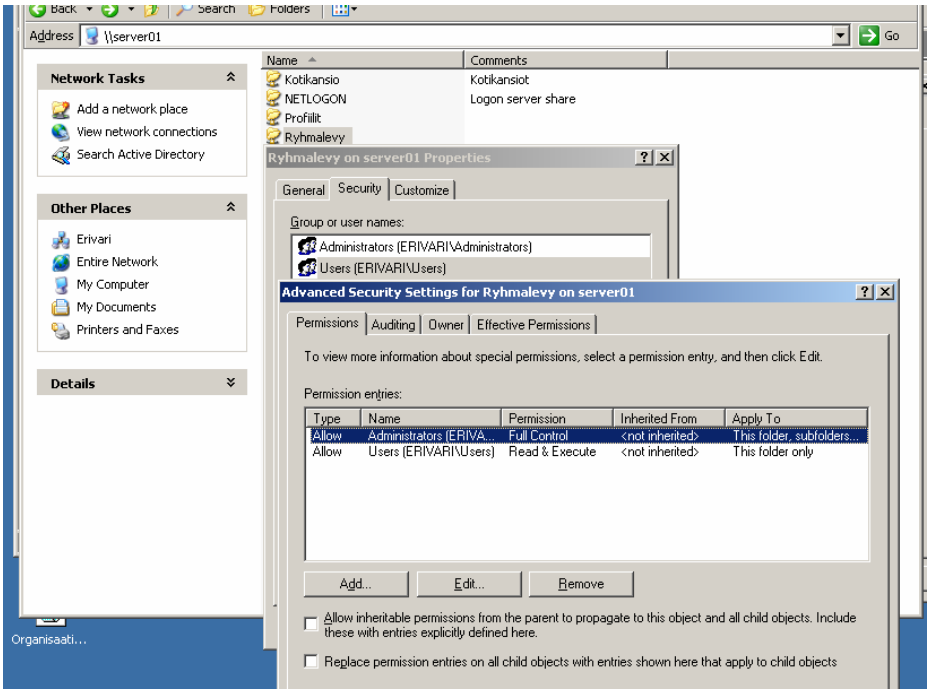
Kuva 11 Kayttajat.batilla luodut käyttäjätilit

8.5 Ryhmäkansioiden luonti Eriväri-toimialueella

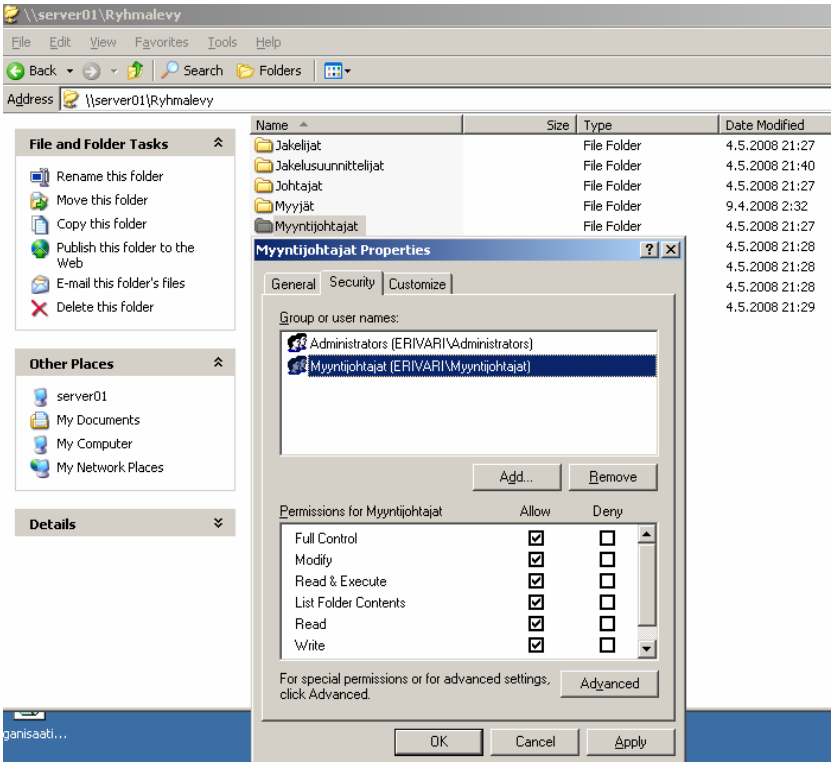
Yrityksen yhteinen tallennustila löytyy Server01:lta Ryhmälevykansiosta, joka sisältää jokaiselle käyttäjäryhmälle oman osastokansionsa (kuva 12). Jokaisella yrityksen työntekijällä (toimialueen käyttäjällä) on lukuoikeus tähän Ryhmälevykansioon. Jotta lukuoikeus ei kummittelisi myös alikansioissa, on poistettava periytyminen. Kuten voimme kuvasta 13 huomata toimialueen kaikilla käyttäjille ei ole enää lukuoikeutta Myyntijohtajat-kansioon. Ryhmälle itselleen on asetettu täydet oikeudet, jotta oman kansion sisällön muokkaus onnistuisi (kuva 14). Järjestelmänvalvojalle on jätetty täydet oikeudet tuki- ja tiedostojenpalautustehtävien varalta. Tarvittaessa ryhmille/käyttäjille voidaan luoda väliaikaisia oikeuksia tiettyjen työtehtävien puitteissa, mutta silloin ns. ryhmäoikeuspyynnöt menevät johtajien hyväksynnän kautta. Yleisesti projekteja varten luodaan erilliset projektikansiot.



Kuva 12 yrityksen ryhmäkansiot



Kuva 13 suojausten asettaminen

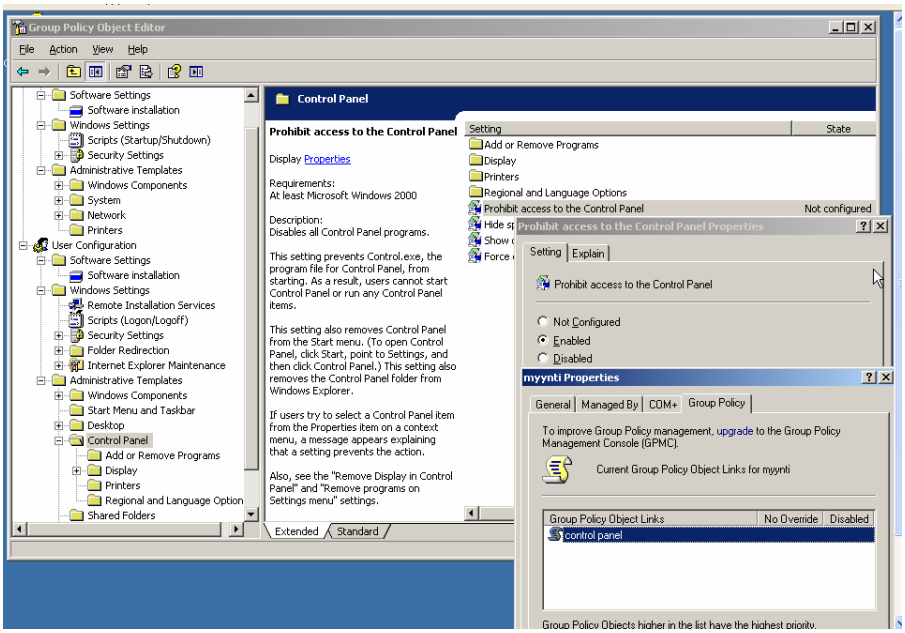


Kuva 14 Myyntijohtajilla täydet oikeudet omaan kansioonsa

8.6 Esimerkki Eriväri-toimialueen ryhmäkäytännöstä

Eriväri-toimialueella on neljä pääorganisaatioyksikköä, jotka on luotu osastokohtaisesti. Jokaisella osastolla on omat työtehtävänsä, jotka vaativat omat asetuksensa ja työkalunsa. Jotta homma pysyisi hallittavana ja toimivana, on myös säädettävä rajoituksia.

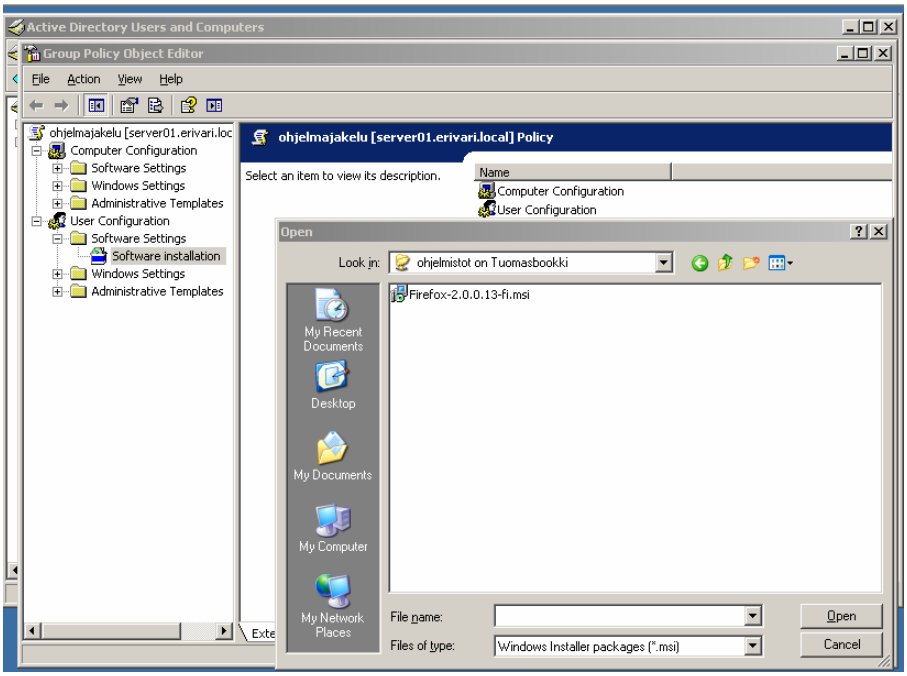
Esimerkkitapauksessa Eriväri-toimialueen Myynnin organisaatioyksikön käyttäjät tarvitsevat vain myyntiin tarkoitettuja asetuksia ja ohjelmistoja. Heiltä voidaan kieltää Control Panelin käyttö, jotta he eivät pääse itse muuttamaan asetuksiaan ja sotkemaan tällä tavalla osaston työasemien yhtäläisyyttä (kuva 15). Yrityksessä muille organisaatioyksikölle Control Panelin käyttö on sallittu, koska heidän pitää päästä muuttamaan työaseman asetuksia työtehtävien vaatimalla tavalla. Myynti-organisaatioyksikköön liitetty ryhmäkäytäntö periytyy Henkilöstö-organisaatioyksikölle kaikkine ominaisuuksineen, sama koskee myös käyttäjä- tai muita objekteja, joten Pekka tai tulevaisuudessa Myyntiosastolle tulevat uudet työntekijät eivät tule pääsemään ohjauspaneeliin vaan he tulevat saamaan samat ”Myyntiyksikön säännöt” tai yleensäkin Eriväri-toimialueeseen liitetyt käytännöt, kuten muut sen toimialueen aliobjektit. Periytyminen voidaan tarvittaessa tietysti poistaa.



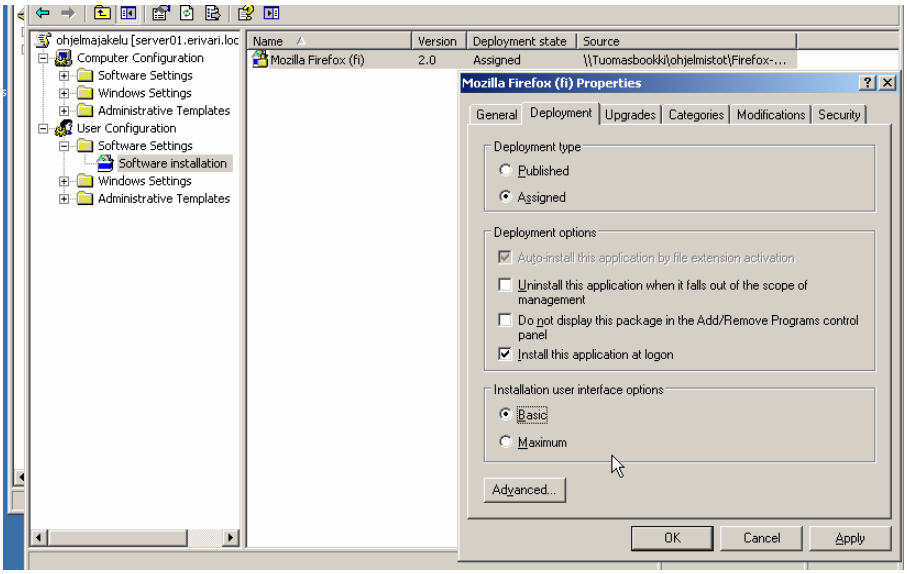
Kuva 15 ryhmäkäytäntöobjekti: Control Panel

8.7 Esimerkki Ohjelmapaketin jakelusta ryhmäkäytännön avulla Erivä-ri-toimialueella

Esimerkissä (kuva 16 ja 17) Myynti-organisaatioyksikössä tarvitaan toinen nettiselain Microsoft Explorerin rinnalle, jotta voidaan tarkastella, miltä netissä julkaistut myyntiesitteet näyttävät eri selaimilla. Tällainen nettiselaimen asennus voidaan tehdä keskitetysti kaikille Myyntiorganisaatioyksikön käyttäjille Ohjelmajakelu-nimisen ryhmäkäytännön avulla. Mozilla Firefox.msi -ohjelmapaketti (Group Policy – Software Installation tukee vain *.msi-päätteisiä ohjelmapaketteja) liitetään (Assigned) Myynti-organisaatioyksikön käyttäjille.



Kuva 16 ohjelmapaketin lisääminen jakeluun

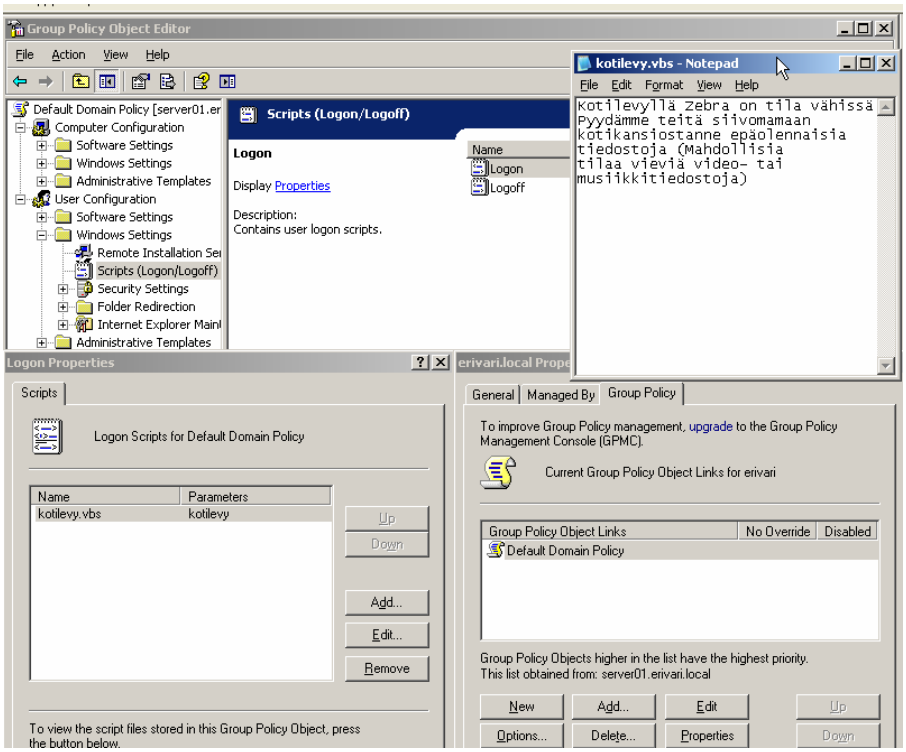


Kuva 17 ohjelmapaketin asetukset

8.8 Windows Script Hostin soveltaminen ryhmäkäytäntöön Eriväri-toimialueella

Toimialueen ryhmäkäytäntöasetuksista löytyy Scripts-toiminto, jolla järjestelmänvalvoja voi määrittää erilaisia skriptejä. Niitä voidaan suorittaa käyttäjien kirjautumisen tai järjestelmän käynnistymisen yh-

teydessä. Esimerkissä (Kuva 18) yrityksen työntekijät ovat tallentaneet kotikansioihinsa paljon myös ylimääräistä materiaalia. Kotilevypalvelimen levytila alkaa olla lopussa, joten järjestelmänvalvojan on informoitava yrityksen järjestelmän käyttäjiä. Hän on tehnyt kotilevy.vbs -tiedoston (skriptipohjainen), jota käytetään tarvittaessa ilmoittamaan kotilevypalvelimen tilan vähyydestä. Käyttäjien kirjautuessa työasemilleen heidän työpöydälleen ilmestyy viestilaatikko, jossa kehotetaan siivoamaan epäolennaiset (esim. *.avi- tai *mp3-tiedostot) kotilevyltään.



Kuva 18 skripti: kotilevytila vähissä

9. Päätelmiä ja pohdintaa

Voidaan todeta, että mitä suurempi käyttäjämäärä, sen parempi hyöty skripteistä voidaan saada irti. Mutta työn edetessä huomasin, että jo yhdenkin organisaatioyksikön käyttäjien naputtelu ja niiden kaikkien ominaisuuksien asettaminen yksi kerrallaan, vaati hieman kärsivällisyyttä. Sitä vaatii tietysti skriptienkin teko (virheiden korjaukseen saa menemään tuntikausia), mutta onnistuessaan yksi tuplaklikkaus tekee kaiken vaivan puolestani, ja myöhempi hyöty muutaman muuttajan muutoksen myötä on myös taattu.

Muutamien komentojonokokeilujen myötä löysin ne, joilla halusin yritykseni käyttäjäympäristön toteuttaa. Windows Script Host, Ldifde.exe ja Dsadd tuntuivat mielekkäimmiltä ja jokseenkin ymmärrettäviltä tämän tyyppiseen toteutukseen. Täydellinen komentojonojen hyödyntäminen olisi vaatinut laajempia ohjelmointitaitoja, mutta jonkinlaisella For-lausekeopiskelulla päästiin liikkeellä. Soveltamalla ja yhdistämällä eri komentoja toisiinsa, saatiin luotua muutakin kuin vain yhdenlaisia toimialueen objekteja. Muodostamalla kahden organisaatioyksikön käyttäjiä, ryhmiä ja niiden yhteyksiä yhteen komentojonoon, päästiin puntaroimaan sen hyötyjä yksittäisten käsin tehtävien objektilisäyksien hyötyihin. Selkeimmät hyödyt ovat komentojonojen avulla säästetty aika ja inhimillisten virheiden poiston mahdollisuus.

Palatakseni esimerkkiyritykseni mahdollisiin tulevaisuuden ratkaisuihin, yrityksen laajentuessa edellä esitettyä organisaatioyksikkörakennetta voitaisiin muuttaa esimerkiksi toimipiste- tai paikkakuntakeskeiseksi. Organisaatioyksiköiden siirtäminen paikasta toiseen on mahdollista, koska niiden ominaisuudet siirtyvät mukana kuten objektien kanssa yleensä. Jo tehdyistä skripteistä on varmasti hyötyä tulevaisuudessa, uusien toimipisteiden synnyissä ja niiden käyttäjäympäristöjen luonnissa.

Uskon, että opinnäytetyöstäni on hyötyä järjestelmävalvojille, käyttötuen henkilöille tai yleisesti niille, jotka haluavat perehtyä tai laajentaa yrityksen käyttäjäympäristöön liittyvää osaamistaan. Työni edetessä oman ymmärrykseni ja taitojeni kohentuminen on näkynyt mielenkiinnon lisääntymisenä omaa alaani ja tämän hetkistä työtehtävää kohtaan.

Lähteet

Kivimäki, Jyrki 2005. Active Directory - Tehokas Hallinta. Jyväskylä: Gummeruksen Kirjapaino Oy.

Kivimäki, Jyrki 2005. Windows Server 2003 - Tehokas Hallinta. Jyväskylä: Gummeruksen Kirjapaino Oy.

Kivimäki, Jyrki 2004. Inside Active Directory - Verkonhallinta. Helsinki: Edita Prima Oy

Microsoft Script Center 2008. Active Directory [online] [viitattu 20.4.2008]
http://www.microsoft.com/technet/scriptcenter/hubs/ad.mspx

MSPress 2004. Managing and Maintaining a Microsoft Windows Server 2003 Enviroment. Canada: H.B. Fenn and Company Ltd.

Microsoft Windows Server TechCenter 2005. DSADD [online] [viitattu 28.4.2008]
http://technet2.microsoft.com/windowsserver/en/library/8d37ecb0-ac28-4e05-aa05-da82dc36b54b1033.mspx?mfr=true

Shimonski, Robert. Chellis, James. Desai, Anil 2006. Windows Server 2003 Active Directory Planning, Implementation and Maintenance. Indianapolis, IN: Wiley Publishing, Inc.

Stanek, William R 2003. Microsoft Windows Server 2003: asiantuntijan käsikirja. Helsinki: Edita Prima Oy