Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Mitja Golob

Uporaba Microsoftovega AD za poenotenje IT-okolja in vpeljavo digitalnih identitet

DIPLOMSKO DELO NA UNIVERZITETNEM ŠTUDIJU

Mentor: prof. dr. Saša Divjak

Ljubljana, 2009

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
fax: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01529/2008
Datum: 15.12.2008

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MITJA GOLOB**

Naslov: **UPORABA MICROSOFTOVEGA AKTIVNEGA IMENIKA ZA POENOTENJE IT OKOLJA IN VPELJAVO DIGITALNIH IDENTITET**

UNIFICATION OF IT ENVIRONMENT AND INTRODUCTION OF DIGITAL IDENTITIES SUPPORTED BY MICROSOFT ACTIVE DIRECTORY

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Na primeru Pedagoške fakultete Univerze v Ljubljani proučite problematiko uvajanja sistema upravljanja digitalnih identitet. Konkretna implementacija naj temelji na sistemu strežnikov in odjemalcev MS Windows in na tehnologiji Aktivnega imenika. Opišite težave in ustrezne rešitve, ki jih boste ugotovili pri uvajanju Microsoftove domene.

Mentor:

prof. dr. Saša Divjak

Dekan:

prof. dr. Franc Solina

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01529/2008
Datum: 15.12.2008

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MITJA GOLOB**

Naslov: **UPORABA MICROSOFTOVEGA AKTIVNEGA IMENIKA ZA POENOTENJE IT OKOLJA IN VPELJAVO DIGITALNIH IDENTITET**

UNIFICATION OF IT ENVIRONMENT AND INTRODUCTION OF DIGITAL IDENTITIES SUPPORTED BY MICROSOFT ACTIVE DIRECTORY

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Na primeru Pedagoške fakultete Univerze v Ljubljani proučite problematiko uvajanja sistema upravljanja digitalnih identitet. Konkretna implementacija naj temelji na sistemu strežnikov in odjemalcev MS Windows in na tehnologiji Aktivnega imenika. Opišite težave in ustrezne rešitve, ki jih boste ugotovili pri uvajanju Microsoftove domene.

Mentor:

prof. dr. Saša Divjak

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Dekan:

prof. dr. Franc Solina

IZJAVA O AVTORSTVU

diplomskega dela

Spodaj podpisani/-a __**Mitja Golob**_____,

z vpisno številko __**24012412**_____,

sem avtor/-ica diplomskega dela z naslovom:

__**Uporaba Microsoftovega AD za poenotenje IT-okolja in vpeljavo digitalnih identit**__

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

  _____**prof. dr. Saša Divjak**_____

  in somentorstvom (naziv, ime in priimek)

  _____

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela

- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne __**19.1.2009**_____ Podpis avtorja/-ice: _____

Povzetek

Vsaka sodobna organizacija potrebuje sistem upravljanja digitalnih identitet, katerega uvajanje na Univerzi v Ljubljani smo na Pedagoški fakulteti s pridom izkoristili pri prenovi naših starih Unixovih strežnikov v Windowsove strežnike ter v celotno omrežje odjemalcev in strežnikov vpeljali in uskladili Microsoftovo domeno z njihovim Active Directoryjem 2003. Pri tem smo naleteli na zanimive težave, ker doslej Microsoftove domene sploh nismo imeli, ter med drugim odkrili, kako s trikom v registru neveščim uporabnikom omogočiti neopazen prehod, administratorjem pa z uporabo skupinskih politik olajšati upravljanje tako računalnikov kot uporabniških skupin in njihovih sodobnih potreb. Prikazan je optimiziran postopek uvajanja ter pasti na katere naletimo.

Ključne besede: AD, aktivni imenik, identiteta, skupinske politike, register, Windows, Unix

Abstract

Managing of every modern establishment requires a functioning digital identity service. We at Faculty of Education decided to use the one from our mother University of Ljubljana, when we decided to migrate our servers and users from Unix system to Microsoft domain using Active Directory 2003. We encountered interesting problems because of our non-domain IT environment and since most of our users were not prepared for the change; however, we managed with a hack-trick in registry to make transition for our users transparently invisible. In addition, Microsoft Group Policy considerably helped network administrators to alleviate management of enterprise computers and users, including users modern needs. We will show optimize proceedure and traps which you can encounter.

Keywords: AD, Active Directory, identity, group policy, register, Windows, Unix

Zahvala

Hvala mentorju za strokovno pomoč in usmerjanje pri izdelavi diplomske naloge, ljubeznivim staršem za potrpežljivo čakanje na mojo diplomo, moji družinici, ki je trpela med zadnjimi izpiti, mojim nadrejenim za vzpodbudo ter dovoljene izostanke, sodelavki Maji Hriberšek za nadomeščanje ob odsotnosti, pri iskanju rešitev in premlevanju problemov pa Andreju Govejšku (RCU), Roku Roglju (SRC), Gregorju Furlanu (IskraSistemi) in Dejanu Sraki (PeF).

Kazalo vsebine

Seznam slik

Seznam uporabljenih kratic

Kratica	Pomen	Slovenski prevod
AD	**Active Directory**	**Aktivni imenik**
ASP	**Active Server Pages**	**Skriptni jezik**
CGI	**Common Gateway Interface**	**Protokol za povezavo zunanjega programa in web-strežnika**
DC	**Domain Controller**	**Domenski strežnik**
DNS	**Domain Name Server**	**Imenski strežnik**
EFS	**Encrypting File System**	**Datotečni sistem s podporo enkripciji**
FTP	**File Transfer Protocol**	**Zastarel nezavarovan način prenosa podatkov**
GC	**Global Catalog**	**Globalni katalog**
GP	**Group Policy**	**Skupinska politika**
GPO	**Group Policy Object**	**Objekt skupinske politike**
IIS	**Internet Information Server**	**Web in ftp-windows strežnik**
IT	**Information Technology**	**Informacijska (računalniška) tehnologija**
IP	**Internet Protocol**	**Internetni protokol**
LDAP	**Lightweight Directory Access Protocol**	**Okleščen protokol za dostop do imenika**
NAT	**Network Address Translation**	**Prevajanje omrežnih naslovov**
OU	**Organizational Unit**	**Organizacijska enota, skupina v imeniku**
OWA	**Outlook Web Access**	**WWW-dostop do poštnega strežnika Exchange**
PHP	**PHP Hypertext Preprocessor**	**Skriptni jezik**
PVN	**Property Version Number**	**Številka verzije**
SSH	**Secure Shell**	**Novejši kodiran način prenosa podatkov**
TCP	**Transmision Control Protocol**	**Protokol za nadzor prenosa**
URL	**Unified Resource Locator**	**Unikaten web-naslov**
WMI	**Windows Managment Instrumentation**	**Orodje za nadzor nad rač.komponentami**

1 Uvod

Univerza v Ljubljani (UL) je v letu 2007 pričela s projektom upravljanja digitalnih identitet na podlagi Microsoftovega produkta "Identity LifeCycle Manager 2007" (ILM) [6]. Na Pedagoški fakulteti, kjer sem zaposlen kot računalniški operater, smo ravno v tem času razmišljali o poenotenju upravljanja vseh osebnih računalnikov, zamenjavi ostarelih strežnikov ter boljši povezavi tako med samimi uporabniki kot na relaciji uporabnik–strežnik. Akademska svoboda je nam, ki skrbimo za računalniške zadeve, v prejšnjih letih povzročala nemalo preglavic, izjem ter nepovezanosti. Nekateri so uporabljali Linux, Mac, WindowsXP, drugi pa še Windows98. Za elektronsko pošto, DNS in Web strežnik smo uporabljali Sunov Unix Solaris (sendmail, bind, apache). Strežnik je bil zanesljiv, a je zaradi velikih količin neželene pošte (spam) vedno bolj pešal. Sprejeti smo morali odločitev, ali v novih strežnikih nadaljevati s preverjeno Unixovo platformo ali pa se priključiti "čredi" ter skočiti v Microsoft okolje, ki je ravno zamenjevalo Alpha postaje na Univerzi v Ljubljani (UL). UL je tudi vpeljevala nove skupne storitve, ki so slonele na Microsoftu (digitalne identitete, kadrovska služba, e-študent, računovodstvo). Predvidevali smo, da bi si v prihodnje z drugačno tehnologijo, kot jo ima matična univerza, povzročili več preglavic kot prednosti.
Tudi trend uporabe operacijskih sistemov uporabniških (client) računalnikov na naši fakulteti se je oddaljeval od Linuxa, Maca in zastarelih Windows98 ter se vedno bolj ustaljeval na WindowsXP. K temu je zelo verjetno zelo pripomogla tudi MSDA-pogodba UL z Microsoftom, po kateri smo dobivali Microsoftove produkte brezplačno, ter večinoma družboslovna usmeritev naših profesorjev. Tako ni bilo daleč do odločitve, da se tudi sama administracija vseh PC-jev najlažje izvede z Microsoftovo domeno, ki je doslej sploh nismo imeli. Preko te domene pa poveže uporabnike tudi z novimi strežniki. Kljub Unix znanju, ki smo ga imeli na naši fakulteti, ter pomanjkanju znanja o Microsoftovih produktih smo domnevali, da nam bo veliko pomoči nudilo osebje Računalniškega centra Univerze v Ljubljani (RCU), kar se je izkazalo za resnično.
Tako smo začeli z "brainstormingom", vpeljavo novih Windows strežnikov, promoviranjem 400 uporabniških računalnikov v domeno ter vspostavljanjem skupnih pravil nmed uporabniki in računalniki. Pojavile so se zanimive težave, ki se jih prej ni nihče zavedal ali nanje pomislil in sicer tako na sami univerzi, ki je pripravljala ta projekt na zgornjem nivoju, kot pri Microsoftu, kjer so bili navajeni, da so vse ustanove že v svoji domeni.

In o tem potovanju, polnem čeri, bom pisal v svojem diplomskem delu ter o zelo uporabnih rešitvah pri težavah, nastajajočih pri omenjenem projektu.

1.1 Cilji diplomskega dela

Cilji diplomskega dela so:
- prenesti vse internetne storitve z Unix strežnikov na Windows strežnike;
- olajšati administracijo računalnikov z uporabo AD;
- pri računalniško neveščih uporabnikih čim bolj neboleče uvesti domeno, ki je doslej niso poznali, saj jim že ponovna izbira privzetega tiskalnika povzroča težave. Želeli smo uvesti postopek, pri katerem ni potrebna prisotnost uporabnika. Prav tako pa tudi, da po uvedbi ne potrebujejo pomoči administratorjev omrežja;
- določiti kadrovsko službo kot skrbnika digitalnih identitet zaposlenih, zunanjih zaposlenih ter drugih uporabnikov naših računalnikov, ter osveževanje njihovih podatkov, dodajanje novih, brisanje starih.

1.2 Metode dela

Moje diplomsko delo nima programerskega značaja, zato v njem ni veliko kodnih vrstic, razen nekaj enostavnih Windows skript ter Unix Apache httpd.conf kode, ki jo s klikanjem prevedemo na Microsoftov Internet Information Server (IIS).

Pred vsako implementacijo rešitve smo veliko razmišljali in iskali rešitve v literaturi in na internetu. Naleteli smo na težave, ker je zelo malo literature v slovenskem jeziku. Največ idej za rešitve smo našli na internetu, ki se v današnjih časih kaže kot aktualnejši in hitreje posodobljeni vir informacij kot knjige.

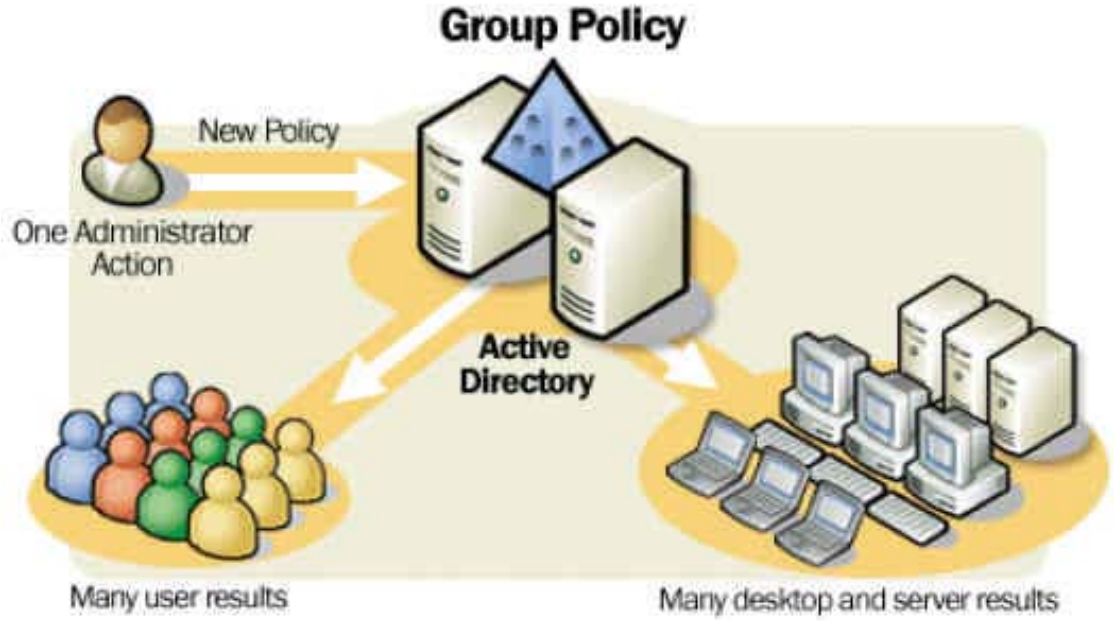
Sledili so prvi testi na nekaj uporabnikih, popravki, vpeljevanje novih, boljših rešitev in na koncu še testiranje na širši množici.

V delu, kjer smo želeli uporabniku nemoteče in neopazno vpeljati domeno, projekt že meji tudi na psihologijo uporabe računalnikov.

2 Aktivni imenik (AD)

2.1 Multi-master, X.500, (L)DAP, Kerberos

Aktivni imenik (Active Directory = AD) je Microsoftov multi-master sistem za upravljanje identitet, ki zelo olajša administracijo računalnikov in uporabnikov (slika 1).



Slika 1: Z enega mesta administriramo vse

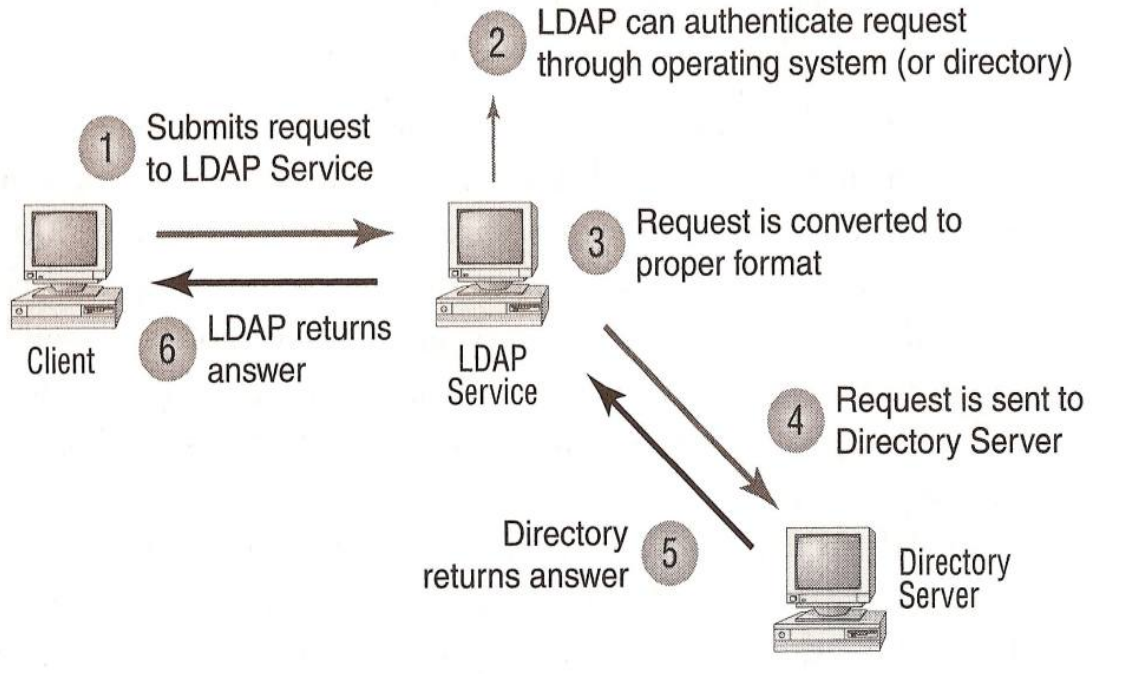
Olajšano je delo administratorjem, saj lahko celotno omrežje računalnikov, uporabnikov in pravice upravljamo iz enega uporabniškega vmesnika (Single Point of Managment). Prav tako je lažje tudi uporabnikom, ki se lahko z enakim uporabniškim imenom prijavljajo v več računalnikov (Single Logon) in v različne storitve (Pass-trough Authentication).

Kot mrežni imenik je sestavljen v stilu digitalne podatkovne baze. Temelji na X.500 priporočilu organiziranja imenikov, ki je bil narejen z namenom, da bi lahko imeniki različnih proizvajalcev lahko izmenjevali podatke. Specificira nam metodo organiziranja, poimenovanja in doseganja podatkov, ne pa same implementacije. Načrtovalci X.500 so že konec 80. let prejšnjega stoletja imeli v mislih tudi nalogo identifikacije in avtentikacije uporabnikov, ko bi lahko tak imenik služil kot edina točka za kontrolo nad informacijami in servisi.
Po pravilih X.500 je tudi v AD možno uporabljati različne vrste podatkov (AD jih imenuje objekti) z različno številnimi atributi. Mnogo uporabnih je že določenih v t.i. shemi (Schema),

ki se lahko v AD prosto spreminja. Imenik je hierarhično organiziran, ker je lahko struktura objektov zelo razvejana.

Pri dostopanju do teh podatkov v X.500 imenikih pa je potrebno določiti način, kako dostopati do njih v v shemi ter jih spreminjati. Za to so določili Directory Access Protocol (DAP), ki pa se je na sedanjih elektronskih napravah izkazal za neuporabnega.
DAP je namreč težišče vsega znanja o samem imeniku in dostopu vanj prevalil na odjemalca, ki je moral biti dovolj zmogljiv. Odjemalec je moral opraviti vso pravilno formatiranje zahtev ter je zato moral vsebovati popolno znanje o sestavi imenika. Strežnik je bil s tem sicer zelo razbremenjen. Takrat se je ideja zdela odlična, saj je komunikacija potekala hitreje. A sodobne mini napravice (telefoni, palmi) le nimajo tolikšne zmogljivosti in hitrih linij.

Tako se je sredi 90. let izoblikoval Lightweight Directory Access Protocol (LDAP), ki bolj razbremenjuje odjemalca. Ni vezan le na X.500 imenike, kot je DAP, zato predstavlja boljši vmesnik tudi drugim proizvajalcem. LDAP ne komunicira neposredno z imenikom, ampak svoje enostavne in kratke ukaze (ki so neprimerno bolj omejeni kot DPA) posreduje LDAP servisu na imeniškem strežniku. Ta pa potem komunicira z imenikom, kot nam kaže slika 2.



Slika 2: LDAP-razbremenitev odjemalca

To omogoča, da vsak proizvajalec sprogramira svoj LDAP-servis, ki teče na strežniku, ter

komunicira z njegovim imenikom, za katerega ni nujno, da je X.500. Odjemalci pa se kljub različnim proizvajalcem do vseh obnašajo enako – po standardnih LDAP-ukazih. [2]

LDAP-odjemalci vzpostavljajo sejo s strežnikom preko TCP-protokola in preko TCP pošiljajo zahtevke ter sprejemajo odgovore. Standardne LDAP-operacije se v Microsoftovi izvedenki AD izvajajo preko 389.vrat TCP, kodirane SSL preko 636.vrat TCP. Starejši Windows odjemalci (95/NT) za komunikacijo uporabljajo MAPI in RPC preko 135.vrat TCP/UDP.

Beseda "multi-master" pri AD pomeni, da je lahko domenskih strežnikov (DC), na katerih se hrani imenik, več, da so vsi glavni ter z enako vsebino. Torej se pri izgubi (okvari) enega od njih ne izgubi del vsebine. Hkrati pa je delovno breme lepo razporejeno med več strežniki in je tudi fizično bliže odjemalcu. S tem je Microsoft dokazal, da lahko sledi in celo utira pot in rešitve v razvoju multi-master sistemov ter konkurira drugim multi-master sistemom, kot sta npr. CA Directory ali Sun Java System Directory Server.

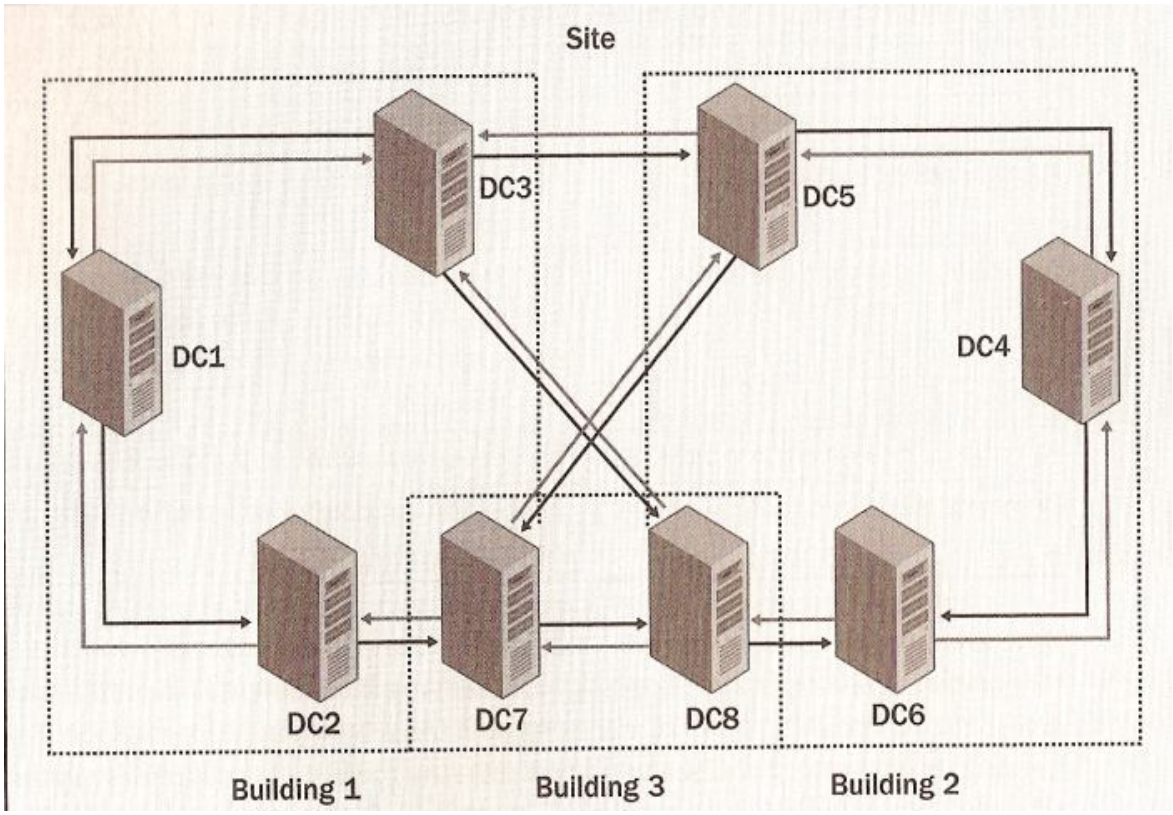
Za avtentikacijo uporabnikov se uporablja simetrično kriptografski Kerberos protokol "deljene skrivnosti" verzije 5, ko za uporabnikovo (Security Principal) geslo ve tudi vmesnik (Key Distributoin Center = KDC). Vlogo vmesnika v našem primeru igra kar AD sam, saj sta v njem shranjena tako uporabniško ime kot geslo. Tako je Kerberos popolno integriran v AD-okolje. Administratorji z njim nimajo popolnoma nobenega dela ali posebnega nastavljanja. Zaradi velike razširjenosti in stabilnosti Kerberos protokola je mogoče z njim celo izpeljati prepoznavanje z drugimi sistemi (Kerberized services).

Tudi pri zaupanju med domenami v gozdu ali pri dinamičnem DNS se uporablja Kerberos. Celo pri samem konzolnem prijavljanju (CTRL+ALT+DEL) v nove Windowse se uporablja tako, da Winlogon pokomunirica z AD, ter po avtentikaciji preda zagon UserInit.exe

Kerberos avtentikacija se v AD izvaja na 88.vratih TCP, kjer najprej "Principal" od KDC zahteva karto (Session Ticket), KDC ga prepozna po pravilnem geslu in mu izda karto, v kateri je shranjen uporabnikov SID (Security Identifier), SID vseh skupin, katerih član je "Principal", in ekriptan ključ KDC. S to karto se Principal predstavi želenemu naslovniku (Validating Server), ki lahko preko svojega ključa, tudi shranjenega pri KDC, preveri, če sta "Principal" in karta prava.

2.2 Podvojevanje (replication)

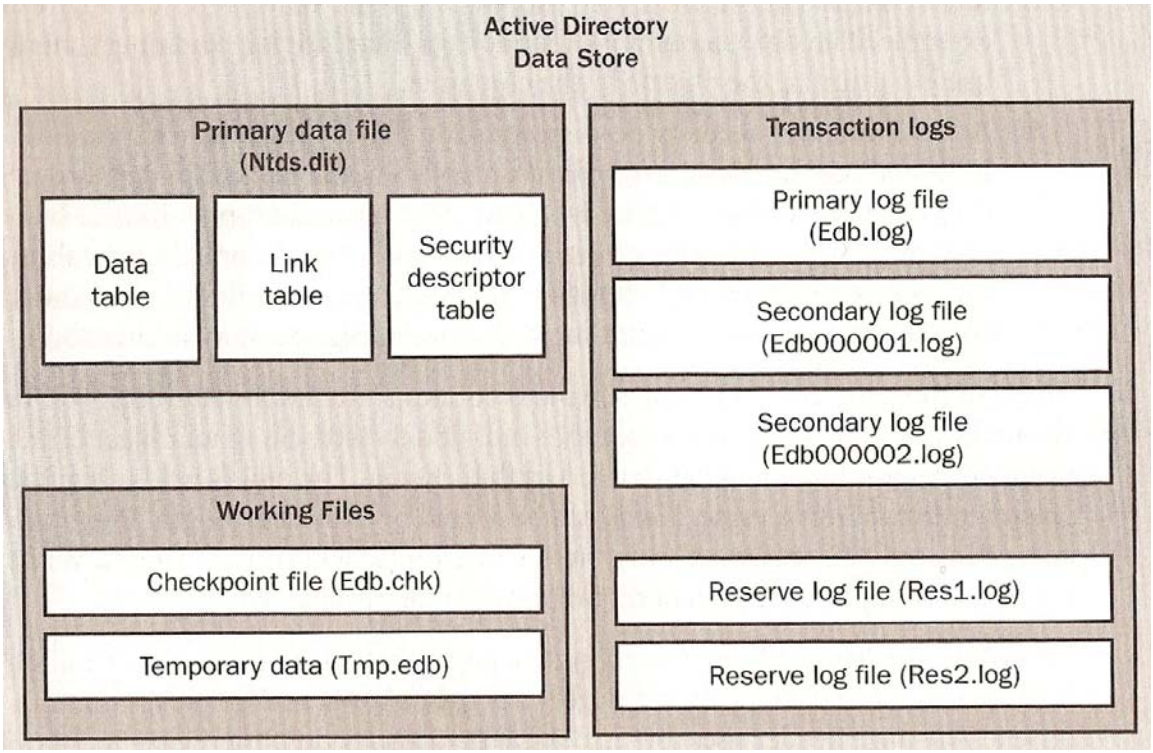
Aktivni imenik (AD) sestavljajo območja (site), domene, organizacijske enote ter objekti. AD je mehanizem, ki neprestano spreminja in prestavlja svoje objekte. Določen objekt se vedno spremeni pri uporabniku najbližjem DC, zato informacije na različnih "masterjih" (DC) niso nujno konsistentne v vsakem danem trenutku. Postale pa bodo konsistentne, če nekaj trenutkov ni sprememb. Za to sinhronizacijo med vsemi "masterji" (DC) skrbi podvojitev (replication). Ta temelji na verziji atributa, časovnem žigu (time-stamp), številki domenskega strežnika ter samozgrajeni topologiji. Pri velikem številu DC-jev je to geometrijsko zapleten (slika 3) in časovno dolg proces, ki skrbi da se ne izgubi nobena sprememba. Topologija se lahko prilagaja vsakih 15 minut, podvojevanje se znotraj domene izvede 15 sekund po spremembi, med območji pa preveri vsake 3 ure, ne glede na spremembe. [6]



Slika 3: Primer repliciranja osmih DC na več lokacijah

Za varnost samega spreminjanja podatkov v AD-ju enega DC skrbi Extensible Storage Engine (ESE), ki poleg indeksiranja vsake spremembe nudi tudi sledenje transakciji ter omogoča

povrnitev na prejšnje stanje (roll back) pri nenadni kritični napaki. Zato uporablja več datotek, ki nam jih prikazuje slika 4.



Slika 4: Katere datoteke sestavljajo aktivni imenik

Vsak podatek se ne zapisuje neposredno v podatkovno bazo – datoteko *ntds.dit*. Najprej se podatek, ki se bo spreminjal, zapiše tudi v *tmp.edb*. Želena transakcija se medtem zapiše v *edb.log* ter se poskuša uspešno zaključiti. Če se uspešno zapiše v *ntds.dit*, se označi kot "odkljukana" v *edb.chk* ter sprosti v *tmp.edb*. Če zmanjka elektrike, se ob povrnitvi strežnika preverijo te datoteke in z lahkoto ugotovi, katera je že bila "odkljukana" in katera ne. Nato se izvedejo nedokončani postopki iz *edb.log*. Dodatna izboljšava je, da se transakcija pred *edb.log* zapiše še v za to rezerviranih 100 MB pomnilnika "*version store*". Nato se namesto branja iz *edb.log* izvede prenos neposredno iz tega pomnilnika.
**.log* datoteke so natančno 10 MB velike. Ko podatki presežejo to velikost, se ustvarijo nove sekundarne datoteke (*edb000001.log, edb000002.log ...*). AD uporablja še rezervne datoteke *res*.log*, ki preventivno vnaprej omogočajo zasedbo prostora ter morebitno opozarjajo, da bo kmalu zmanjkalo diskovnega prostora. Služijo pa tudi čim hitrejšemu preklopu sekundarnih datotek na rezervne, da sistem ne izgublja kritičnega časa z njihovim ustvarjanjem.

Pri brisanju objekta se mora informacija o izbrisu podvojiti tudi pri ostalih domenskih strežnikih. Zato se namesto popolnega izbrisa nastavi atribut "isDeleted" na True, objektu pa se pobriše večina atributov in je prestavljen v skrito skladišče "Deleted Object", kjer čaka na podvojevanje. Čakanje dovolimo zato, da se vsi domenski strežniki seznanijo z izbrisom. Tu "preživi" 60 dni, potem pa ga ESE zbriše. Kot bomo videli v poglavju 2.3, imamo teh 60 dni tudi čas, da ga iz varnostne kopije restavriramo nazaj, če smo ga pobrisali po pomoti.
Vse te datoteke so shranjene v *Windows\NTDS* mapi. V sosednji mapi *Windows\SYSVOL* pa so shranjene še nekatere dodatne skripte in datoteke, ki skrbijo za politiko, in o katerih pišem v 4. poglavju. [5]

Območja (site) so v AD uvedeni, da se lahko z njimi bolje prilagodimo našemu fizičnemu omrežju. Tako lahko DC-je, ki so fizično oddaljeni ali povezani z manj zmogljivimi povezavami, ločimo od drugih v posamezna območja, ker ne bi zmogli tega hitrega 15-sekundnega podvojevanja [3].

Za avtomatsko spreminjanje topologije znotraj območji in med njimi skrbi Knowledge Consistency Checker (KCC). Ta poskrbi, da se podvojevanje znotraj območja nikdar ne opravi z več kot tremi preskoki (hups). Tako je zakasnitveni čas (latency) do najbolj oddaljenega DC-ja vedno manjši od minute [3].

Na Pedagoški fakulteti nimamo dislociranih enot, notranja mreža je zmogljiva 1 Gbps, tako da zaenkrat ne potrebujemo več kot dveh domenskih strežnikov (DC). Da bi se izognili motnjam pri sesutju omrežja v delu stavbe, smo ju fizično postavili v različni nadstropji.

Pri dostopanju do DC in branju podatkov iz AD se ustvarja velik promet, še posebej če je veliko računalnikov, ki posegajo po informacijah v domeni: če so na primer naše domene raztresene po celem svetu in bi morali za vsak vpogled samo v telefonsko številko sodelavca na drugi strani zemeljske oble opraviti poizvedovanje v njegovo domeno – na njegov nam zelo oddaljen DC, ki je po možnosti celo na slabi mrežni povezavi.

Zato se za hitrejše dostopanje uporabljata dve bližnjici.

Prva je "cashiranje" že prejetih informacij, ki se tičejo našega računa, lokalno na računalniku. Standardni čas je 7 dni, ki pa se lahko kot vse stvari v AD spremeni. "Cashiranje" omogoča, da se lahko sploh prijavimo v računalnik, čeprav ne bi bili na mreži, npr. doma na službenem prenosniku. Za še potrebneje pa se to izkaže pri dostopanju do enkriptiranih map (EFS), kjer se za odkriptiranje uporablja uporabnikov AD-ključ.

Druga bližnjica pa je vpeljava globalnih katalogov (Global Catalog – GC), ki podvojeno hranijo podmnožico vseh objektov vseh domen v našem gozdu, ampak ne celotnih objektov in vseh, temveč le najbolj dostopanih. Vrste atributov objektov, ki se hranijo v GC, so vnaprej določene, lahko pa jih v AD-shemi (Schema) poljubno dodajamo, če opazimo, da naši uporabniki zelo dostopajo do kakšne vrste njim pomembnih informacij, na katere Microsoft ni pomislil.

Na prvi pogled se zdi, da bi bilo najbolje, da imamo GC na čim več strežnikih v naši domeni, a bi se zaradi količine podvojevanja promet v omrežju preveč povečal, saj se tudi spremenjena GC-vsebina med njimi podvaja. Zato je treba v velikih omrežjih število GC in nove GC-objekte, ki smo jih dodali v podvojevalno shemo GC, skrbno načrtovati.
AD poskrbi, da GC postane prvi nameščeni DC v domeni. Vse naslednje moramo delegirati sami. GC poleg 389.vrat posluša tudi 3268.vrata TCP/UDP za LDAP-zahtevke. [2]

Dodatna izboljšava pri AD-ju verzije 2003 v primerjavi s staro različico 2000 je, da se replicirajo samo spremenjeni deli objekta in ne cel objekt (eden npr. spreminja telefonsko številko, drugi pa priimek). To prinaša manj prenesenih podatkov pri podvojitvi ter zmanjšuje pogostost podvojitvenih konfliktov. Če bi se podvajal cel uporabnik, bi že nastal konflikt, čeprav bi ta dva različna DC-ja spreminjala le vsak svoj delček informacije o uporabniku. AD 2003 to uvidi ter sinhronizira oba delčka istega uporabnika.

Konflikti se, če do njih vseeno pride, shranijo v *EventView*. Vendar se s pravo organizacijo administracije AD lahko temu popolnoma izognemo, če za različne delovne enote skrbijo različni ljudje ali celo za različne podatke ene osebe. Tudi sicer je malo verjetno, da bosta v istih 30 sekundah dva spreminjala isti podatek istemu uporabniku. Še največkrat pride do konfliktov pri premikanju ali brisanju uporabnikov.

V tem primeru lahko izkoristimo Pstoolsov eventlog *(http://technet.microsoft.com/en-us/sysinternals/default.aspx)*, ki v tekstovno datoteko izpiše vse "failed replication" v zadnjih 24 urah ter si jih z brezplačnim programom "bmail" pošljemo v poštni predal. (*http://www.beyondlogic.org/solutions/cmdlinemail/cmdlinemail.htm)*

Če je nekdo sprožil premik uporabnika v novo skupino (OU = Organizational Unit), drug upravitelj pa je v istem časovnem trenutku to OU pobrisal, se bo objekt znašel v "Lost & Found", kar vidimo v AD "Users and Computers", če vklopimo *Advanced view options*.

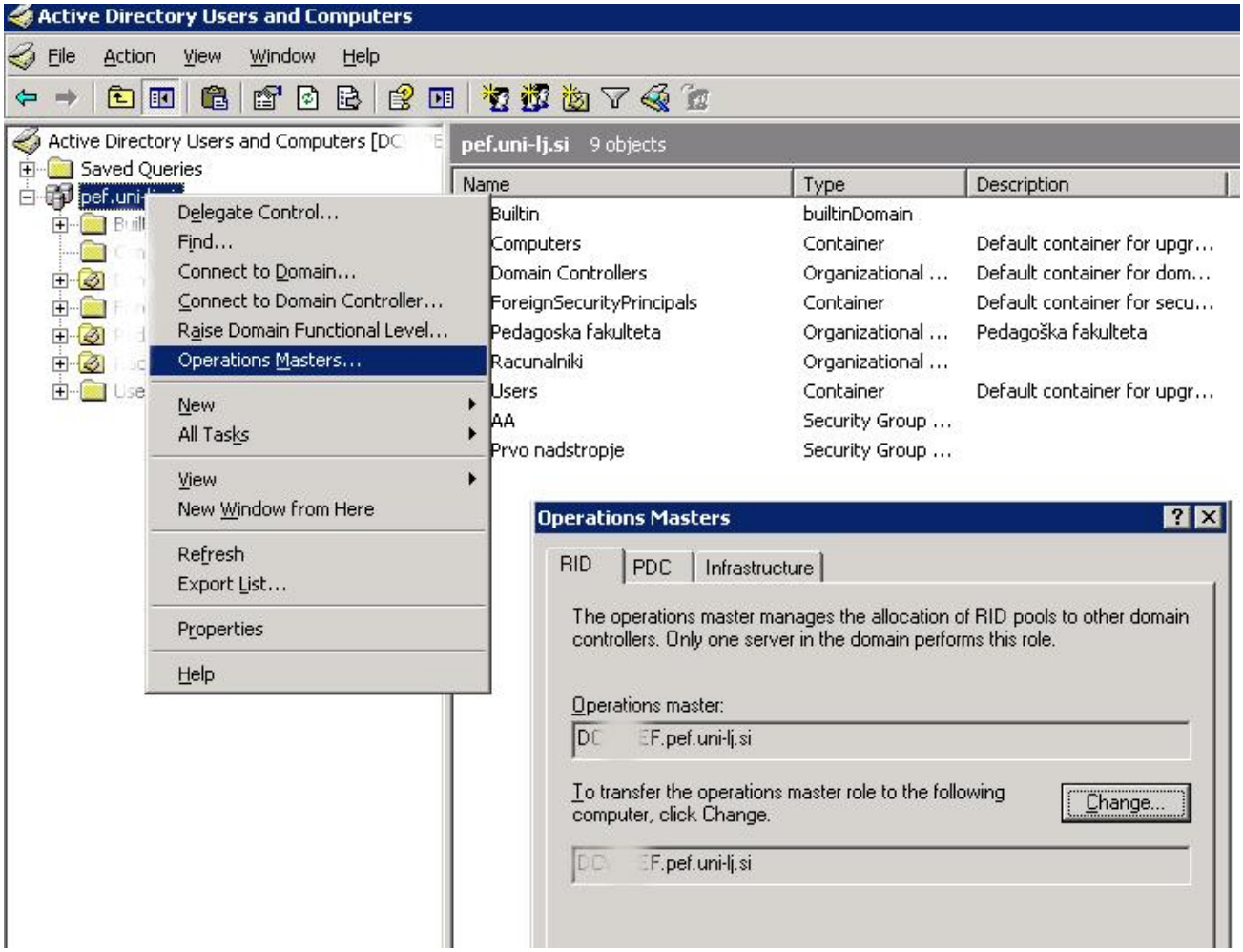
Podvojevanje lahko s pridom izkoristimo pri »sesutju« kakšnega od DC. Namestimo Windows 2003 server in AD ter ga določimo kot domenski strežnik. Podvojevanje pa bo poskrbelo za zapolnitev AD na tem novem DC.

Kljub popolni redundanci DC in brezskrbnemu odklopu kateregakoli DC v tem Microsoftovem multi-master sistemu pa moramo v AD 2003 le paziti na eno stvar – kateri DC je glavni razdeljevalec katere od petih vlog (Master roles).

Da je breme bolje porazdeljeno so glavni DC-ji (Operation Masterji) za eno od petih vlog lahko različni, za eno vlogo pa je vedno glavni le eden. Vloga poenostavljeno pomeni dodeljevanje unikatnih zaporednih številk objektom v AD ali spreminjanje strukture imenika. Kajti če bi tudi tukaj dovolili multi-master sistem, bi prihajalo do neskladij. Zato ga moramo, če nam iz omrežja izpade kateri od dodeljevalcev vlog, v doglednem času restavrirati nazaj iz varnostne kopije ali določiti nekoga drugega za glavnega »razdeljevalca vlog« (Operation Master).

To lahko za vlogo PDC Emulatorja in Infrastrukturo storimo iz AD Users and Computers Administrative toolsa, kot kaže slika 5.

Za spremembo Schema, Domain naming in RID »Masterja« pa moramo poseči po konzolnem orodju NTDSUTIL.



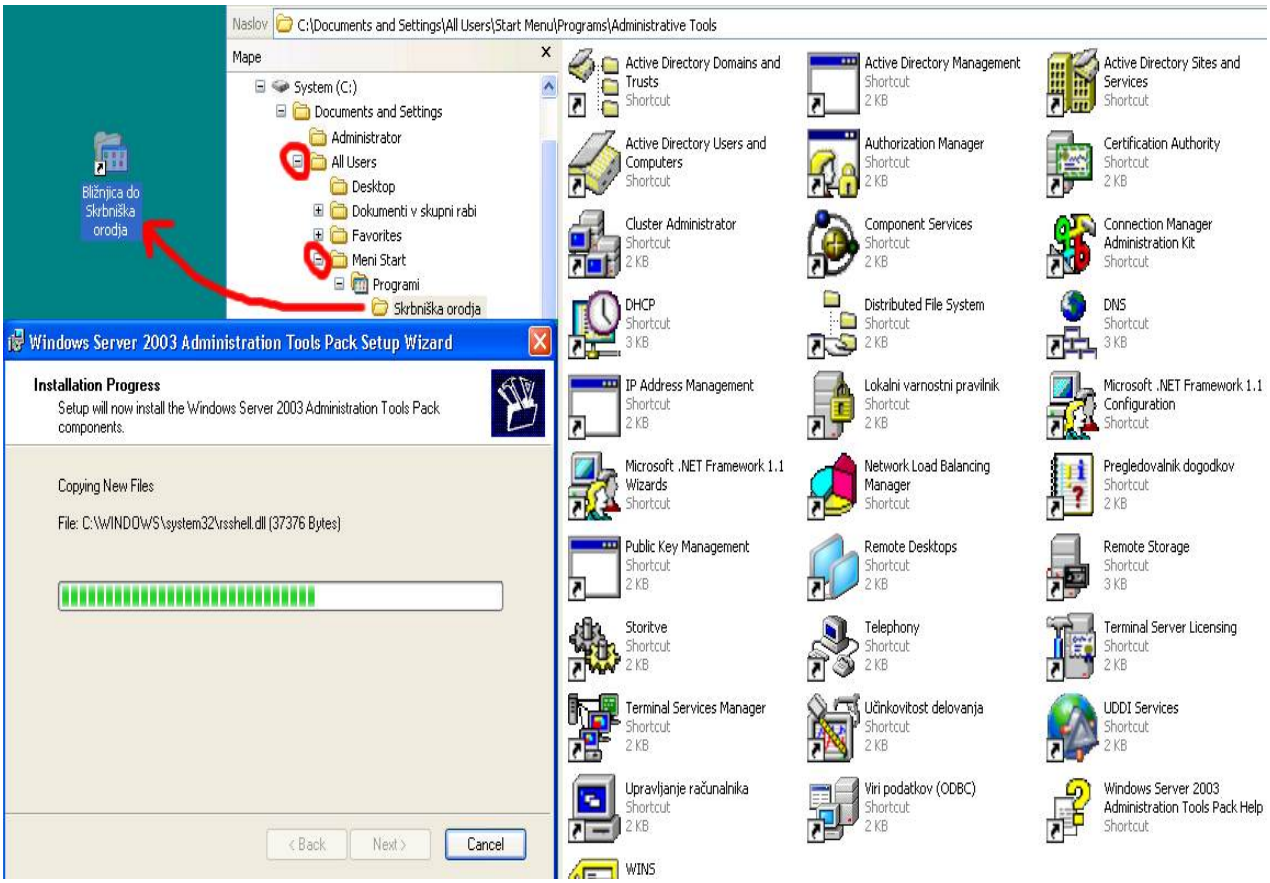
Slika 5: Kateri DC naj določa RID-vlogo (RID Role)?

2.3 Administracija, varnostne kopije

AD omogoča tudi napredne možnosti za določanje pravic skupinam uporabnikov, visoko stopnjo varnosti ter možnost za razširitev svojih identitet preko svojih meja v druge AD-je, če se med njihovimi gozdovi (forest) vzpostavi zaupanje.

Tako smo "napolnili" naš AD z našimi zaposlenimi (import iz Excel datoteke), ter jih potem delegirali v različne skupine (OU), ki so čim bolje odražale našo organizacijo.

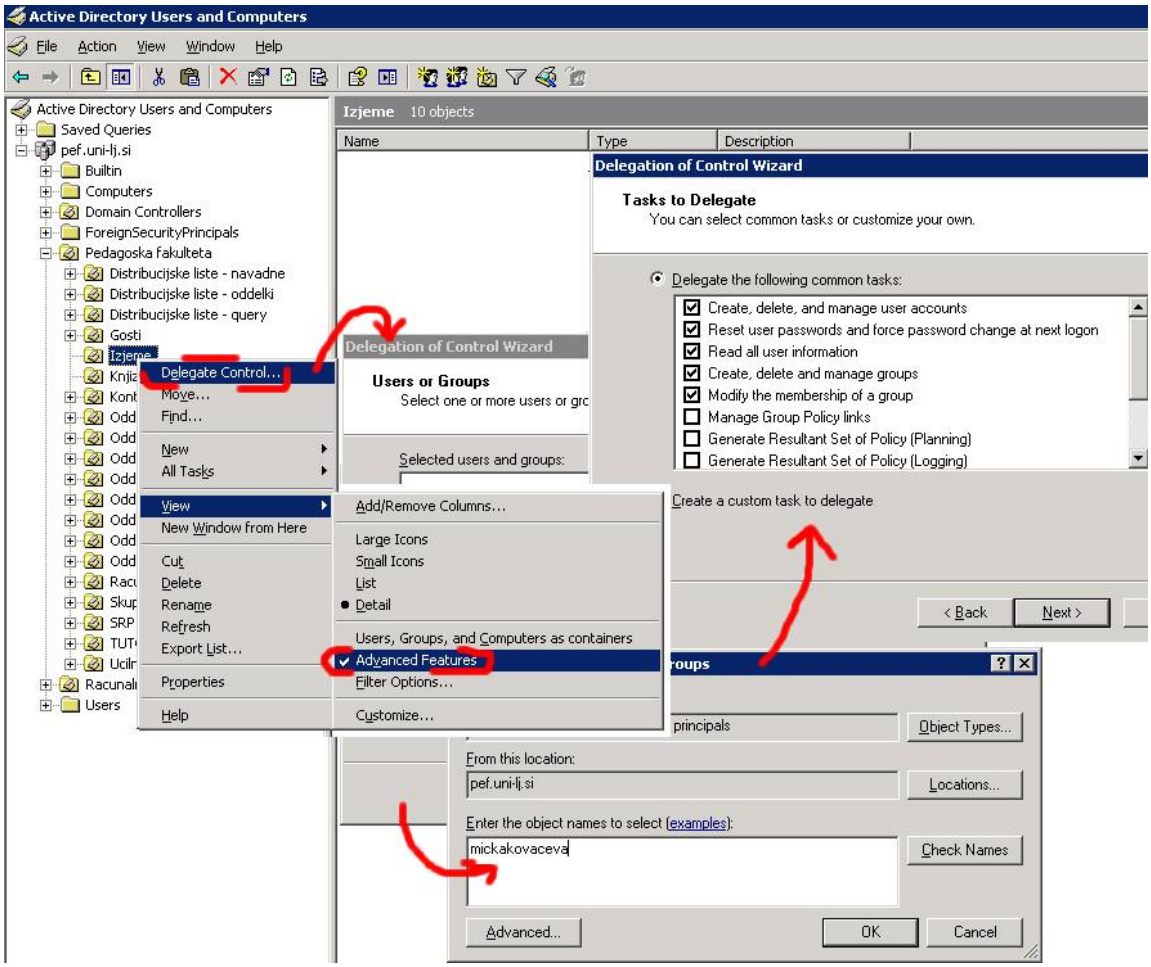
Uvedli pa smo drugačen način delegiranja novih uporabniških računov (digitalnih identitet). Tega ne počnejo več računalničarji, ampak kadrovska služba. Ta najbolj ve, kdo je nov zaposleni, v kateri OU spada ter kdaj ni več zaposlen.
Seveda nismo učili delavcev kadrovske službe, kako se povežejo na AD-strežnik, zaženejo določene programe, ampak smo v ta namen namestili posebno orodje *Windos Server 2003 Administration Tools Pack*, ki je dosegljivo na naslovu *http://www.microsoft.com/downloads/details.aspx ?FamilyID= C16AE515-C8F4-47EF-A1E4-A8DCBACFF8E3&displaylang=en*



Slika 6: Administration Tools Pack

Kot nam kaže slika 6, se nam je sprva zdela namestitev malo skrivnostno skrita, saj je nihče od navadnih uporabnikov računalnika ni videl (kljub namestitvi v *All Users*). A hitro ugotovimo, da je verjetno to namenoma, saj nam omogoča dodatno zaščito ter dodelitev pravic branja nad mapo (kjer so orodja) le določenim osebam na tem računalniku.
Ko smo jim prikazali orodja na njihovo namizje, jim je bilo potrebno še ustrezno odkleniti dostop do spreminjanja določenih OU in drugih objektov AD.

To smo storili kot domenski administrator preko opcije Delegate, kot nam kaže slika 7.

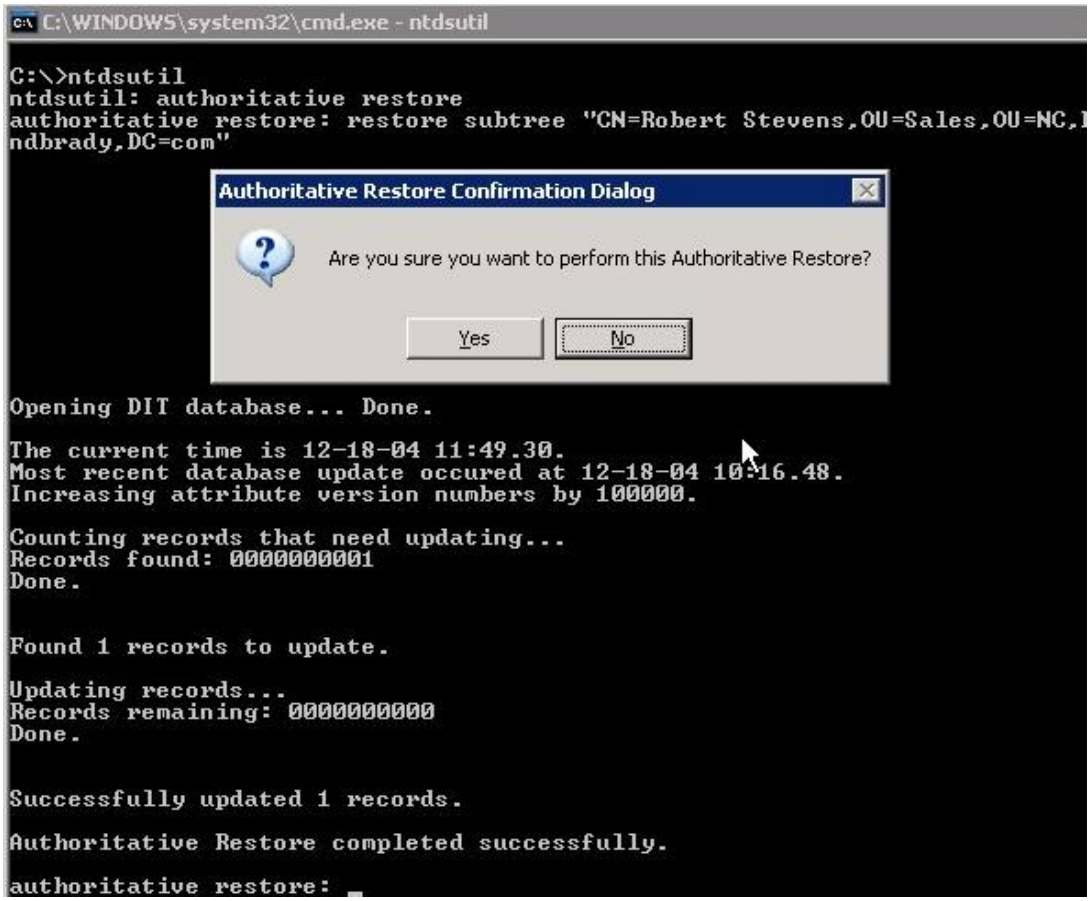


Slika 7: Odklep pravic v AD

S popravki snapina lahko še dodatno oklestimo ogled AD, da res vidijo le tiste objekte, ki jih zanimajo. Pravice pa jim lahko odvzamemo, če vklopimo Advanced Features View, kot tudi kaže slika 7.

S tem smo vpeljali novo osebje v popravljanje AD-ja, s čimer se je možnost napačnih vnosov in izbrisov povečala. Prav tako smo dobili dodatne vstopne točke za vdor na strežnik.
Zato je kljub multi-master sistemu, ki se samostojno podvaja, postalo zelo pomembno, da vsakodnevno (ali večkrat dnevno) delamo varnostno kopijo AD. V nasprotnem primeru bi se ob izbrisu ta takoj podvojil na vse strežnike in lahko bi ostali brez večine uporabnikov, uporabniških skupin ali skupinskih politik.
Kot smo videli v poglavju 2.2, ostane informacija o izbrisanem objektu v imeniku "živa" še 60 dni. Po 61. dnevu postane varnostna kopija imenika neuporabna! V nasprotnem primeru, bi

se velikost podatkovne baze imenika oz. položaj (ne)izbrisanega objekta med različnimi DC-ji razlikovala ter vodila v pokvarjen imenik.
V šestdesetih dneh pa moramo narediti "Authorative Restore", saj bi v nasprotnem primeru ostali DC-ji takoj označili naš "restavriran" objekt nazaj, kot da je izbrisan. [2]



Slika 8: "Authorative Restore" izbrisanega objekta iz sveže varnostne kopije

Pri "Authorative Restore" uporabimo konzolni ukaz NTDSUTIL, kot kaže slika 8, navesti pa moramo točen LDAP "Distinguished Name" objekta v imeniku, da ga orodje najde. "Authorative Restore" ne naredi drugega, kot da številko PVN (Property Version Number) objektu poveča za 100000, s čimer poskrbi, da je gotovo najnovejši v bazi. A hkrati velja tudi pozornost, da pomotoma ne restavriramo starejšega podatka, z novejšim. "Authorative restore" se izvede le, če smo prepričani, da je točno ta objekt v naši obstoječi bazi pomotoma napačno vnesen ali pobrisan (v zadnjih 60 dneh).

Ko smo imeli AD pripravljen za populacijo, smo pričeli s prenosom strežniških storitev in samih uporabnikov v domeno.

3 Prehod strežniških storitev in odjemalskih računalnikov v AD

3.1 E-Mail: s POP3 sendmaila na RPC Exchange

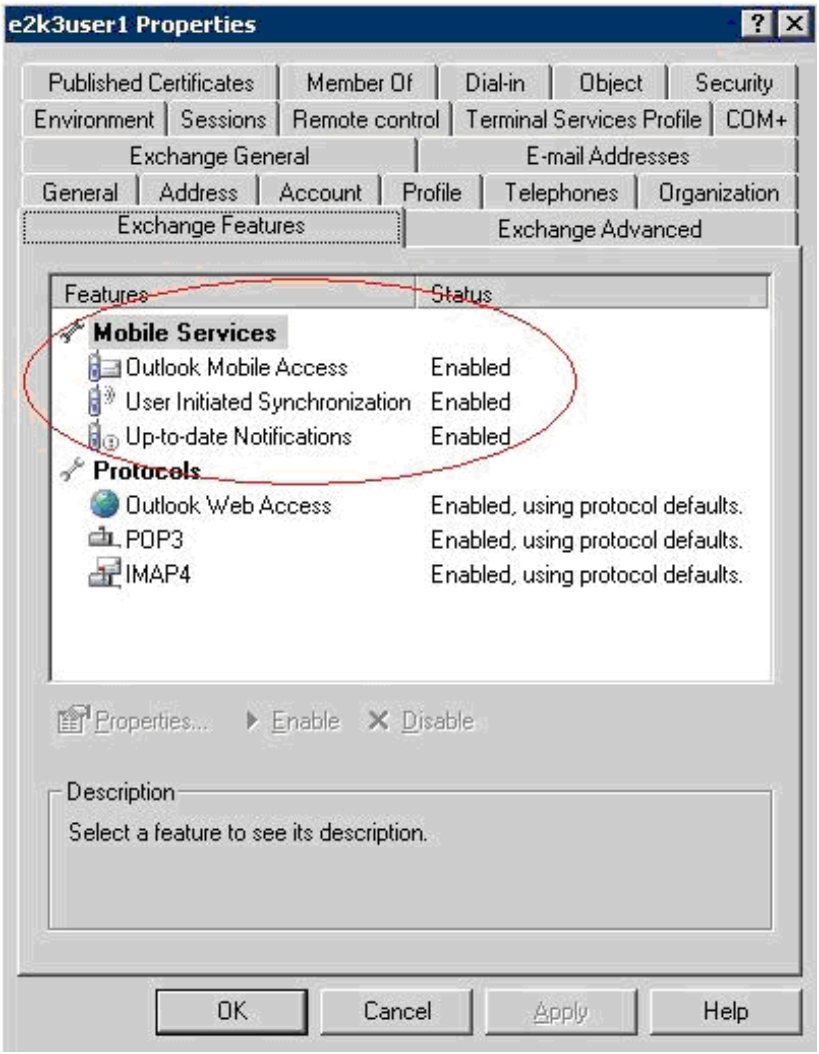
Na začetku smo si zadali težko nalogo, da bomo tudi nadalje še vedno sami skrbeli za naš novi, a tokrat Windowsov poštni strežnik - vse v stilu Microsoftove domene in Web strežnika. Preizkusiti smo želeli Windowsovo rešitev. Izkušenj z Windowsovim Exchangom sicer nismo imeli, a smo domnevali, da bo z nekaj tečaji ter dobro voljo pač šlo, saj smo navsezadnje dolgo brez težav vzdrževali Unixov sendmail.

Pri neformalnih pogovorih z administratorji Exchanga ter brskanju po internetu smo dobivali vedno več namigov, naj tega ne počnemo tako na hitro, češ da nas neuke čakajo nepremostljive težave. Nihče nam ni napovedoval več kot enomesečnega uspešnega delovanja e-mail sistema.

3.1.1 S poštnim strežnikom raje gostujte

V luči teh strahov in ponudbe s strani Računalniškega centra Univerze v Ljubljani, da gostujemo na njihovem strežniku Exchange, smo uvideli, da bo to res najboljša rešitev, strojno opremo in svoj čas pa usmerimo v datotečno gostovanje – FILE-strežnik.
Rešitev "outsourcinga" se je izkazala za briljantno. Instalirali smo Exchange konzolo [1], preko katere na AD zavihkih svojih uporabnikov poleg ostalih stvari reguliramo še Exchange mailbox nastavitve. Z vzdrževanjem poštnega sistema pa se zdaj ukvarjajo drugi.

Kot nam kaže slika 9, je seveda zadeva popolnoma drugačna od Unix */etc/aliases* vrstice ali *sendmail.cf*.
Pri prenosu uporabnikov nas je čakalo ogromno dela z raznimi mailing listami, a ves ta čas se nam bo obrestoval kasneje, ko ne bo potrebno administrirati strežnika.



Slika 9: Dodatni Exchange zavihki pri uporabnikih

Uporabnikom smo pri obisku kabineta, ko smo uvajali njihov računalnik v domeno (poglavje 3.6) in kopirali dokumente ter profil, v njihov priljubljeni bralnik pošte dodali nov račun, ter tako poskrbeli še za eno nevidno dejanje: e-pošta se bo, ko bo preusmerjena na novi strežnik, začela pojavljati v tem novem zavihku (računu) njihovega poštnega programa.

3.1.2 OWA - ko ne vidijo novih 25 mailov, pride prav operativen stari strežnik

Uporabnikom, ki so občasno brali pošto preko Web brkljalnika, je še največjo težavo predstavljalo navajanje se na novi on-line način branja e-pošte. Pri Exchangu se imenuje Outlook Web Access (OWA).

Kot vedno so se težave pojavile tam, kjer smo jih najmanj pričakovali. Najzanimivejši se nam je zdel preskok na naslednjih 25 e-pisem. Stvar, ki sem nam zdi samoumevna, je povprečnemu uporabniku nedoumljiva.

Slika 10: Skok na naslednjih 25 mailov OWE

Začelo se je s težavami, da uporabniki ne dobivajo več pošte. V resnici pa je seveda bilo krivo to, da so videli le prvih 25 elektronskih pošt urejenih po padajočem vrstnem redu. Kot kaže slika 10, pa se niso znali prestaviti na naslednjih 25 elektronskih pošt. Ta privzeta nastavitev se sicer na prvi pogled zdi neumna, a razmislek pove, da bi bila obratna še veliko slabša – da bi vedno videl le najnovejših 25. Tako so sami hitreje ugotovili, da imajo težave.
Odločitev, da stari poštni strežnik še vedno pustimo nekaj časa v delovanju (pod drugim imenom), se je pri tem (in kot bomo videli v poglavju 3.2 tudi pri Webu) izkazala za rešilno. Preko njega smo lahko vse uporabnike podučili z obvestilom, kako si naj nastavijo OWA ter v meniju Options nastavijo, da bodo hkrati na eni strani videli vsaj 100 e-pisem.

Takšne malenkosti so še en dokaz, da način uporabe informacijske tehnologije potrebuje ogromen preskok k bolj instinktivno naravnanim uporabniškim vmesnikom in rešitvam.

3.2 DNS

3.2.1 S Solarisovega BIND na Windows 2003 DNS

Unixov DNS, imenovan bind, ima datoteke shranjene v direktoriju /var/named:

-rw-r--r-- 1 root other 571 Jul 9 db.127.0.0
-rw-r--r-- 1 root other 10265 Nov 26 db.193.2.74
-rw-r--r-- 1 root other 18634 Oct 17 16:37 db.pef.uni-lj

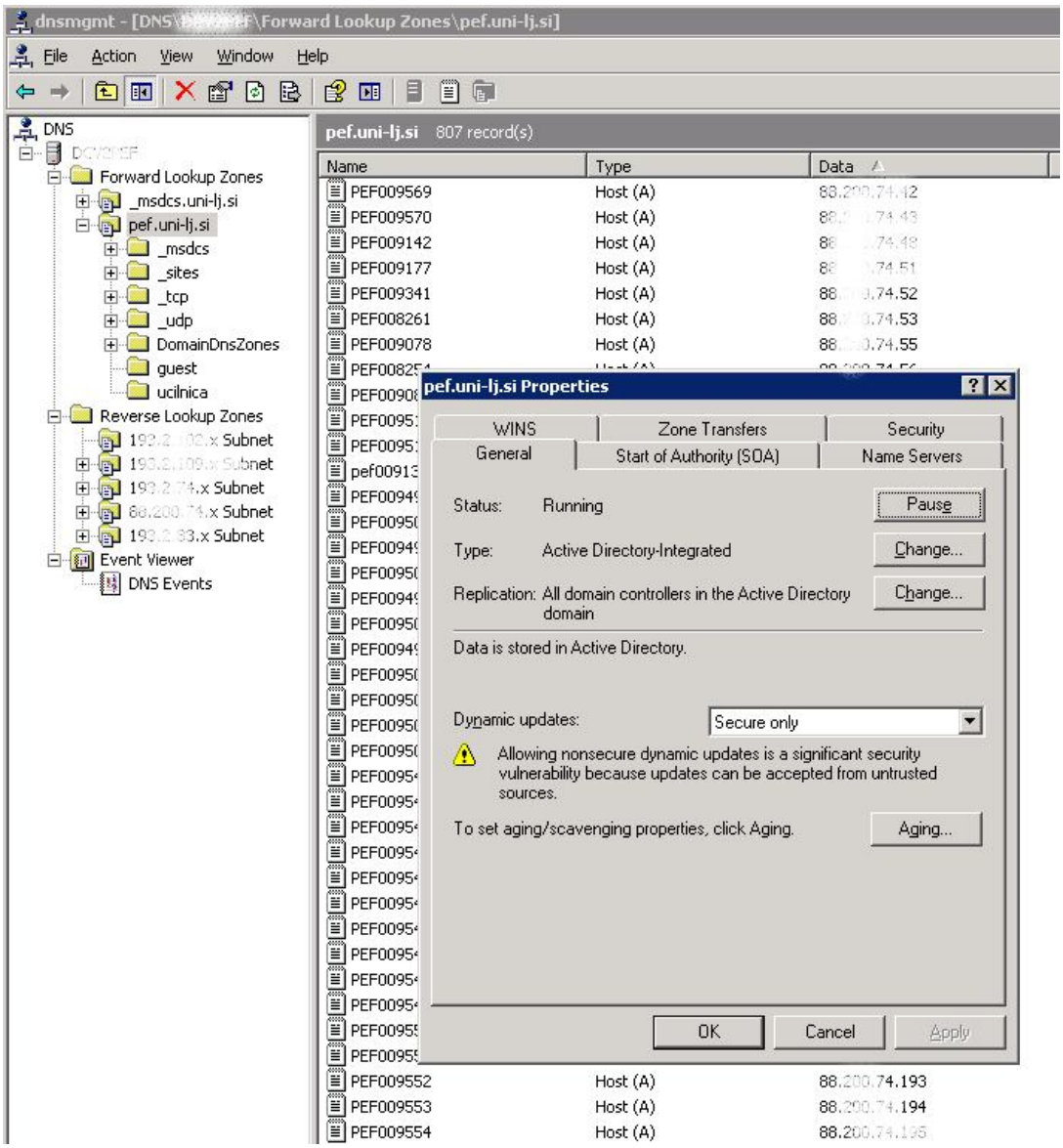
in direktoriju /etc:

-rw-r--r-- 1 root other 454 Dec 8 2004 named.boot
-rw-r--r-- 1 root other 1397 Jun 17 10:39 named.conf
-rw-r--r-- 1 root root 4 Oct 17 16:37 named.pid

Te se popravljajo v tekstovnem urejevalniku, restart, ki sproži uporabo novih nastavitev, se izvede z ukazom:

*kill –HUP _pid_*

DNS Windows na drugi strani upravljamo z grafičnim orodjem (slika 11), ponovni zagon pa se opravi s klikom miške.

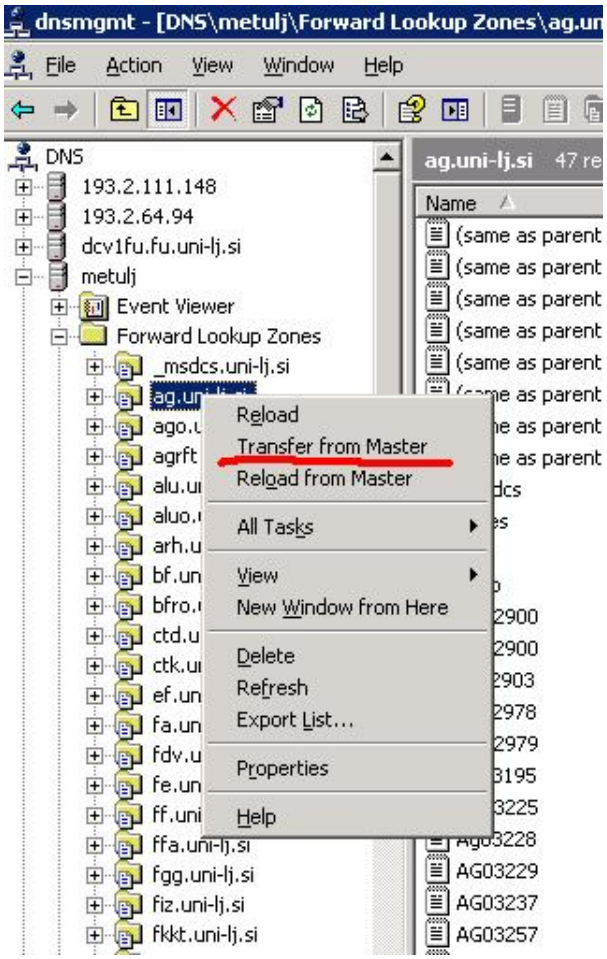


Slika 11: Windows DNS-konzola

Ker orodje nima opcije Import, da bi lahko tekstovne datoteke iz Unixa prenesli vanj, smo uporabili prenos. Na Unixu smo dovolili izvoz/transfer na naš novi Windows DNS strežnik s sledečim stavkom v datoteki *named.conf*:

```
options {
        allow-transfer {  _ip_od_novega_windows_DNSja;  };
        directory      "/var/named";
};
```

V Windows DNS smo vključili, da je slave, nato na Windows strežniku izbrali Transfer from Master, kot kaže slika 12.



Slika 12: DNS transfer iz Unixa v Windows

Da bomo popolnoma v duhu Microsoftovih rešitev, smo nameravali prenehati z bind Unix master/slave načinom con (Zone) ter izbrali AD-Integrated. Microsoft sicer tudi omogoča

ekvivalent primary/secondary, a prednost "integrated" je, da so zapisi redundančno podvojeni na vseh DC-jih, ter se sproti avtomatsko osvežujejo, kot se izvaja podvajanje. Popravki se s tem lahko izvajajo (in so redundančno posneti) na kateremkoli DC, ne le glavnem. DNS-zapisi pa niso zapisani v posebni Zone datoteki na trdem disku, ampak so v bazi AD ter tako podvrženi dodatni varnosti.

Aktivni imenik ne temelji več na NetBIOS-imenih kot v starejših verzijah AD, temveč na hostnamih: pravem internetnem DNS-ju. Brez odličnega delovanja DNS je prijavljanje AD-uporabnikov počasno, vse ostale AD-komunikacije odjemalec–strežnik pa onemogočene. [3] Ker se pojavi vprašanje, katero DNS-strežniško strukturo izbrati, da bo zmožna dovolj zanesljivo servisirati AD, se večini administratorjem odgovor prikaže avtomatsko: uporabimo kar same AD-domenske strežnike! Izgleda, kot da je to tudi Microsoftov namen - nam namigniti, da je najbolje, če je kar sam AD tudi primarni DNS, unixov bind pa slave; če se že nismo odločili, da unix bind povsem ukinemo iz našega IT-okolja.

Naš stari unix bind je bil preslaboten, zato smo unixov servis bind pri nas tako ali tako nameravali ugasniti, vendar se je vse skupaj še malo zavleklo, ker so se pojavile težave, ki jih bom opisal v naslednjem poglavju.

3.2.2 Kratki URL-ji, enaki imenu domene, v Windows DNS niso podprti

Na uporabo kratkega URL *http://pef.uni-lj.si* domače strani (namesto *http://www.pef.uni-lj.si*) lahko v Windows IIS pozabite, če je slučajno domena istega imena (*pef.uni-lj.si*).

Sami smo imeli nekaj uporabnikov s takimi okrajšanimi naslovi, ki so te strani imeli polinkane in objavljene po celem svetu, torej tudi v iskalnikih.
Rešili smo se tako, da smo za en mesec zavlekli uvedbo Web strežnika ter pustili vzporedno delujoč star DNS strežnik, ki smo ga navedli med Name Serverji Forward Lookup Zone.

Integracije modula Rewrite v naš stari Apache ni bila možna, zato smo se poslužili 301 Redirecta. Za domače strani uporabnikov, ki so bile prizadete, smo uvedli httpd.conf nastavitev:

```
#
# Redirect allows you to tell clients about documents which used to exist in
# your server's namespace, but do not anymore. This allows you to tell the
# clients where to look for the relocated document.
# Format: Redirect   old-URL   new-URL
#

Redirect   301   /~uporabnik       http://www.pef.uni-lj.si/~uporabnik
```

Ta nastavitev ni povzročila le začasnega (nepotrebnega) preusmerjanja, ampak smo z njo povzročili, da si je npr. Google ob naslednjem obisku to daljše ime zapisal v svojo bazo ter pozabil naše daljše URL-je, ki pod novim DNS-jem ne bodo več delovali!

3.3 FILE-strežnik ter avtomatska skrb za varnostne kopije uporabnikov

Povprečni uporabniki ne delajo varnostnih kopij. Povprečni uporabniki ne znajo uporabljati orodij za snemanje na optične nosilce (CD, DVD), zato je potrebno splošno urediti varnostno kopiranje njihovih dokumentov.
Uporaba roaming profilov to reši najelegantneje, če imamo dovolj zmogljiv strežnik in povezave. V nasprotnem primeru je edina izbira vpeljava dodatnega diska, ki je fizično na strežniku, uporabnik pa ga na svojem računalniku vidi kot dodatno črko pogona (npr. X:) in ga uporablja. Mi pa poskrbimo za varnostno kopiranje vsebine tega strežnika na kakšen zunanji USB disk, ki so trenutno zelo poceni in hitri, kasetni sistemi pa predragi.

V Windows backup orodju imamo na izbiro razne vrste varčnih "backupiranj", ki ne snemajo celotne vsebine: "incremental", "diferential", "daily". Za prvo silo smo, ker velikost datotek še ni bila prevelika, izbrali za obnovitev podatkov najhitrejšo, ter poenostavljeno spodnjo rešitev, ki za ceno petkratnika velikosti osnovnega diska varnostno kopira celoten mesec.
Za dobro prakso se je izkazala uporaba dveh kompletov zunanjih diskov. Vsake toliko časa jih med sabo zamenjamo, drugi komplet pa shranimo na drugi lokaciji. Drugače pri požaru, v stavbi, kjer je strežnik, izgubimo tudi varnostno kopijo (slika 13).

Slika 13: Primer backupiranja na dva kompleta

Ker je velikost diska omejena, vsebino snemamo vsak drugi dan v tednu, da se lahko vrnemo na zgodnjo zgodovino, ter vsako sredo v mesecu, da se lahko vrnemo za en mesec nazaj. Za vrnitev na obdobje npr. pol leta nazaj, se uporabi drugi komplet, ki je na varnem v sefu na drugi lokaciji.

Ko bo velikost varnostnih datotek narastla, se bomo lotili mešanega načina backupiranj, npr. vsako nedeljo popolni backup, potem med tednom pa le incrementalni, dnevni ali diferencialni.

Šele ko količina ogromno naraste, se nam bo splačalo investirati v tračne sisteme, ki so v osnovi dragi, a so kasete, ki jih je veliko, cenejše.

Pri nekaterih večjih USB-diskih se nam je pojavila težava gonilnikov, ker osnovni Windows gonilniki niso podpirali tako velikih zunanjih diskov. Težavo smo rešili s posebnimi proizvajalčevimi gonilniki ali zamenjavo proizvajalca.

3.4 FTP, SSH

Naši uporabniki so na starem WWW strežniku za prenos datotek uporabljali FTP-protokol. Ker smo se zavedali problema nekodiranega prenosa uporabniškega imena ter gesla pri tem prenosu, smo protokol ohranili le za določen čas, pa še to z drugimi (nedomenskimi) uporabniškimi imeni, ki smo jih prenesli iz Unix strežnika [12].
V tem kratkem obdobju smo naleteli na dve veliki FTP-težavi v Windows okolju, o katerih pišem v poglavjih 3.4.1 in 3.4.2. Nato pa smo s pospešenim korakom odšli raziskovat tri boljše načine za prenos datotek:
- uporabo zastonjskega free SSH deamona [19];
- implementiranje komercialne rešitve kodiranega kanala Point-to-Point Tunneling Protocol (PPTP), na katerega obesimo FTP;
- posodobitev na Windows verzijo IIS 7.0.

3.4.1 Nevarnost skeniranja administratorskega gesla preko FTP-servisa

Žal Microsoft v svojem IIS-servisu ne omogoča onemogočanja administratorskega računa. Posledično lahko vsakdo preko FTP-protokola prosto preizkuša administratorsko geslo, kar predstavlja veliko varnostno luknjo v celem domenskem sistemu.
Našli smo dve rešitvi:
- spremeniti prvotno administratorsko uporabniško ime. Tako preizkušajo neobstoječega uporabnika "Administrator";
- avtomatsko onemogočiti IP, iz katerega pride zahtevek po vstopu z administratorskim geslom s skripto *banftpips.vbs* [13].

3.4.2 FTP 530 Error

Sprejeli smo še en ukrep. FTP-servis smo prestavili na nestandardna, zelo visoka vrata, kar je presenetljivo popolnoma ukinilo neprestana "skeniranja" in ugibanja gesel. Predvidevali smo, da se bo intenzivnost "hackerskega skeniranja" zmanjšala, nismo pa pričakovalo, da bo celo popolnoma izginila!
Takrat pa smo naleteli na hrošča v IIS.

Samo nekaterim uporabnikom se je začela pojavljati nerazumljiva napaka »nepovezovanja - Error 530«. Pojavila se je naključno ne glede na nastavitve požarnega zidu, njihovega routerja, če so na internetu preko NAT ali ne ter četudi so uporabljali istega internetnega ponudnika.

Uporabnik pri istem internetnem ponudniku, brez vklopljenih požarnih zidov je imel težave, drugi, ki je bil v internet povezan celo preko dveh NAT-ov pa ne.

WINSOCK.DLL: WinSock 2.0

WS_FTP95, Copyright C 1992-1996 Ipswitch, Inc. All rights reserved.

- -

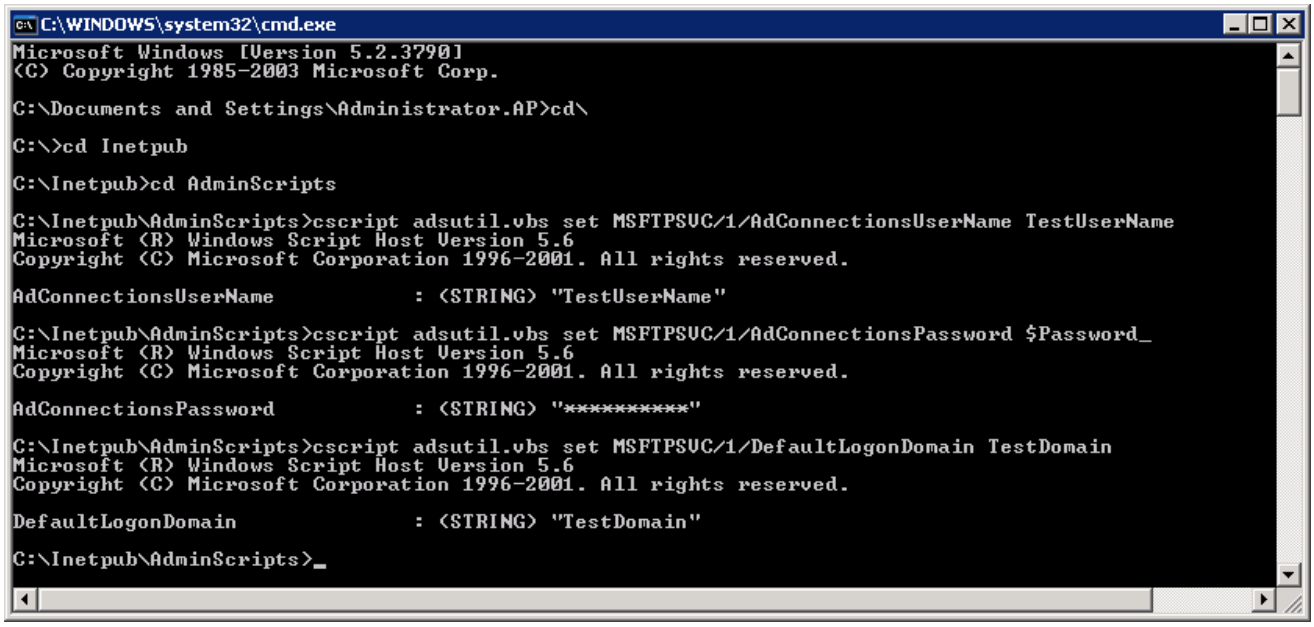
connecting to 200.6.94.102 ...

Connected to 200.6.94.102 port 21

530 Connection refused, unknown IP address.

unk open msg "530 Connection refused, unknown IP address." 530

Pri uporabi več FTP-servisov na različnih vratih se je izkazalo, da se včasih nastavitve med sabo pomešajo, ker je v ipsecurity še vedno nastavljena napačna zastavica.
Rešili smo se tako, da smo s skripto *adsuti.vbs*, ki smo jo zagnali iz konzole (slika 14), pobrisali datoteko *ipsecurity,* v katero IIS zapiše te nastavitve, ter ponovno zagnali FTP [11].



Slika 14: Močno orodje adsutil.vbs

Izgleda, da se tudi v Windowsih vse le ne reši samo s pomočjo klikanja.

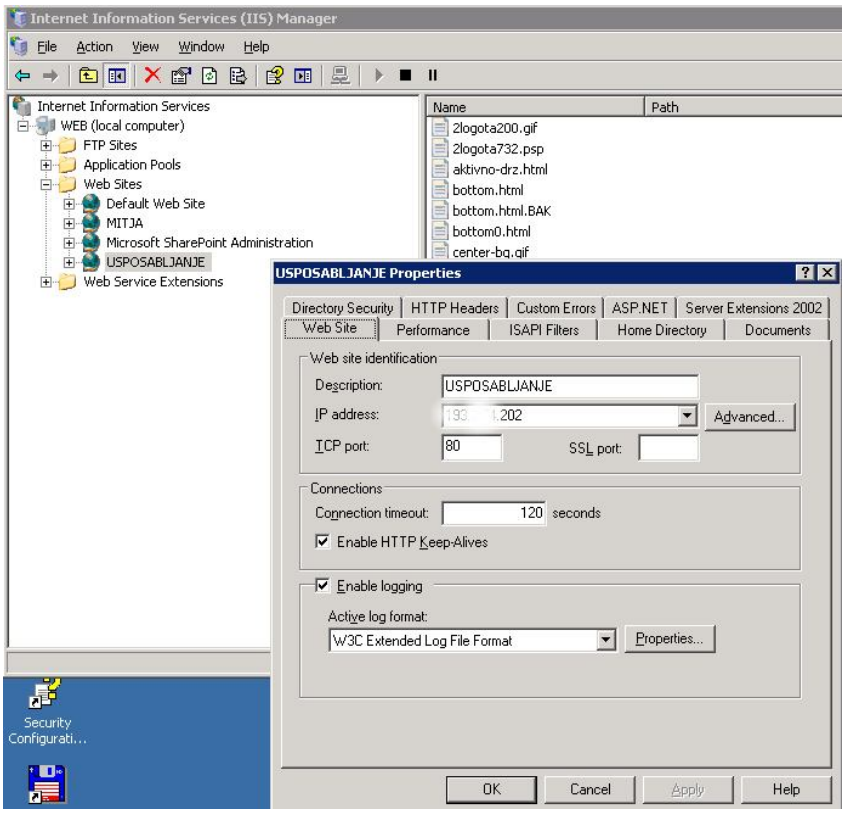
3.5 WWW: prehod z Apache + CGI na IIS + ASP + php

Kot pri vseh orodjih in storitvah se že v sami osnovi vidi razlika med operacijskima sistemoma Unix in Windows. Pri Unixu je filozofija zgrajena na tekstovnih konfiguracijskih datotekah, pri Windows pa na klikanju grafičnega vmesnika.
Tudi varnostna politika se v IIS drugače nastavlja, kjer smo najprej onemogočili Directory Browsing ter nastavili Access Control Options [16].

3.5.1 Virtualhost/website, redirect

Virtualni gostitelji, ki so na istem IP-ju, se v Apache Unix *httpd.conf* datoteki napišejo takole:

<VirtualHost ceps.pef.uni-lj.si>
ServerAdmin webmajster@pef.uni-lj.si
DocumentRoot /users/ceps/public_html
ServerName ceps.pef.uni-lj.si
ErrorLog logs/ceps_error_log
CustomLog logs/ceps_access_log common
</VirtualHost>

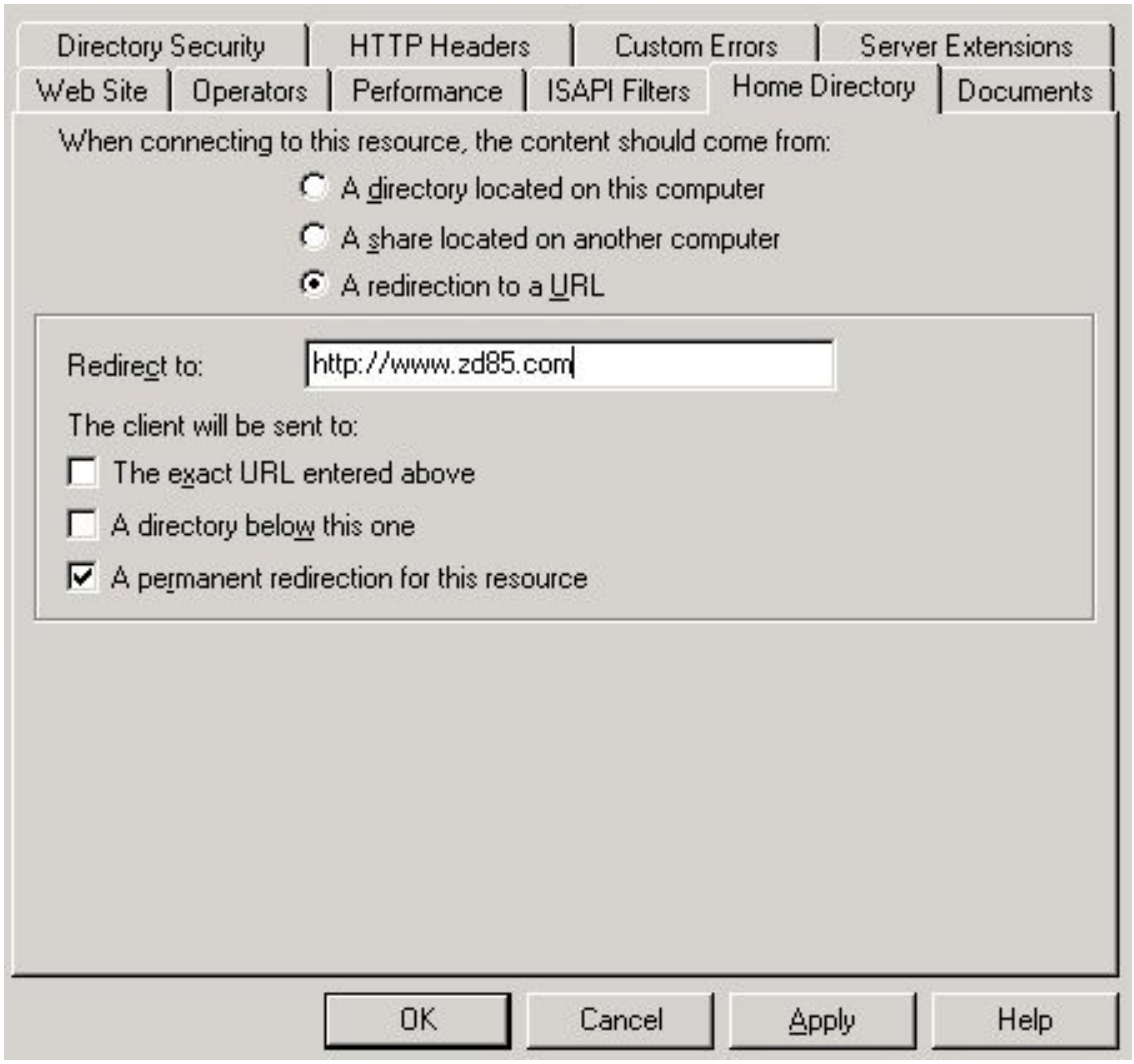


Slika 15: IIS konzola - nov website

Pri Windows IIS pa se za to ustvari nov Website [4], dodeli isti IP in 80.vrata, v filtru ISAPI nastavi servise, popravi "home direktorij", omogoči "anonymous access" ter tudi zanj nastavi politiko zaganjanj skript (slika 15).

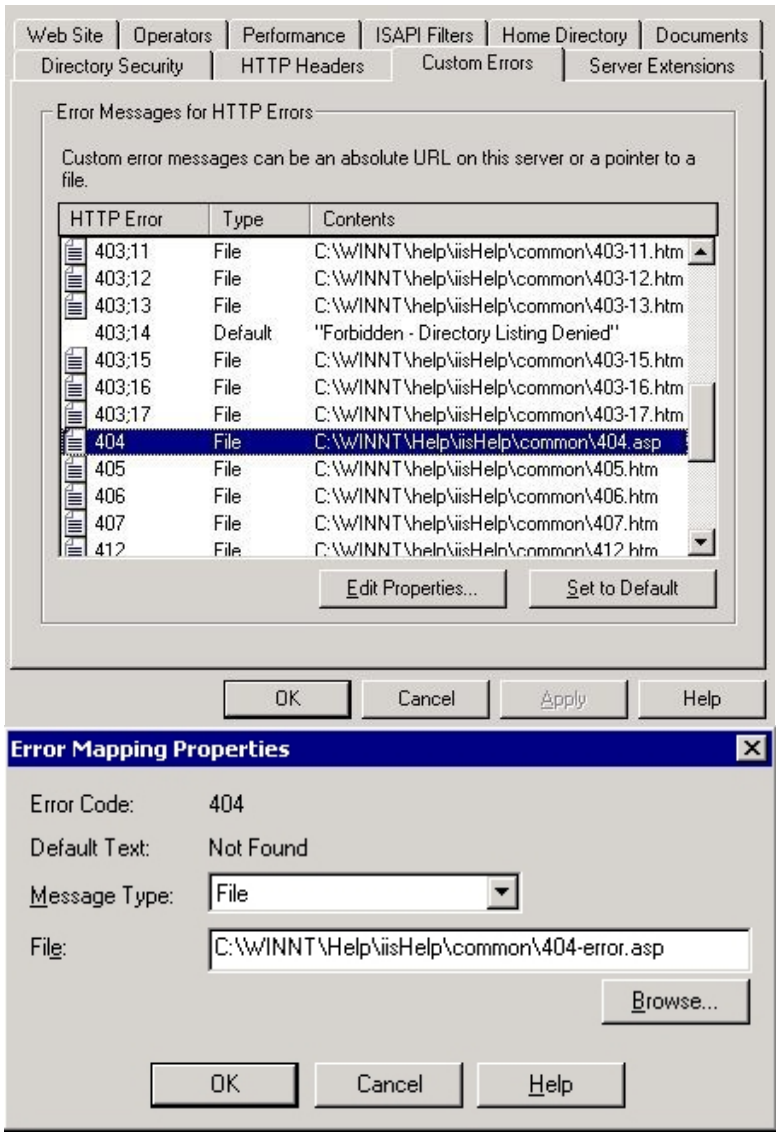
Na starem strežniku smo uporabljali skripte CGI. V času ASP in PHP nismo več želeli nadaljevati z njimi, zato smo tiste CGI, katerih izvorno kodo smo še imeli na voljo, ponovno prevedli na tem strežniku ter uporabili ExecCGI filter. Ostale smo programirali v PHP ali ASP.

Kako se v *httpd.conf* uporablja redirect, smo videli v poglavju 3.2.2, v Windows pa gre zopet preko nekaj klikov (slika 16).



Slika 16: IIS konzola - redirect

Katero obvestilo naj se pojavi pri neobstajanju strani (napaka 404), nastavimo v IIS, kot kaže slika 17.

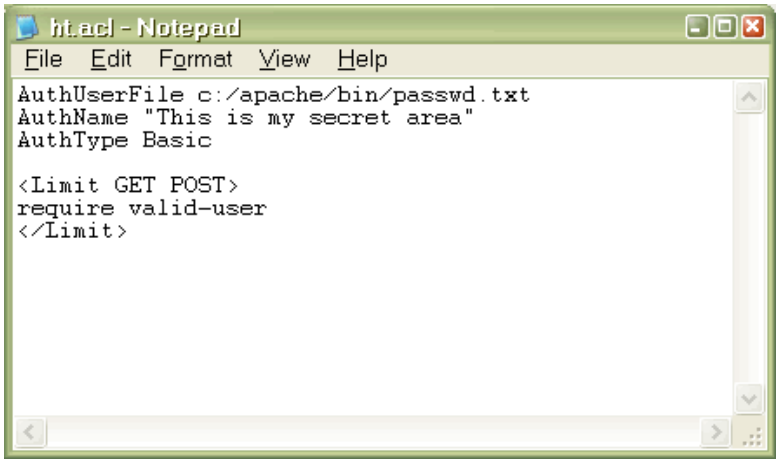


Slika 17: IIS-konzola - redirect na neobstoječi strani

3.5.2 .httaccess

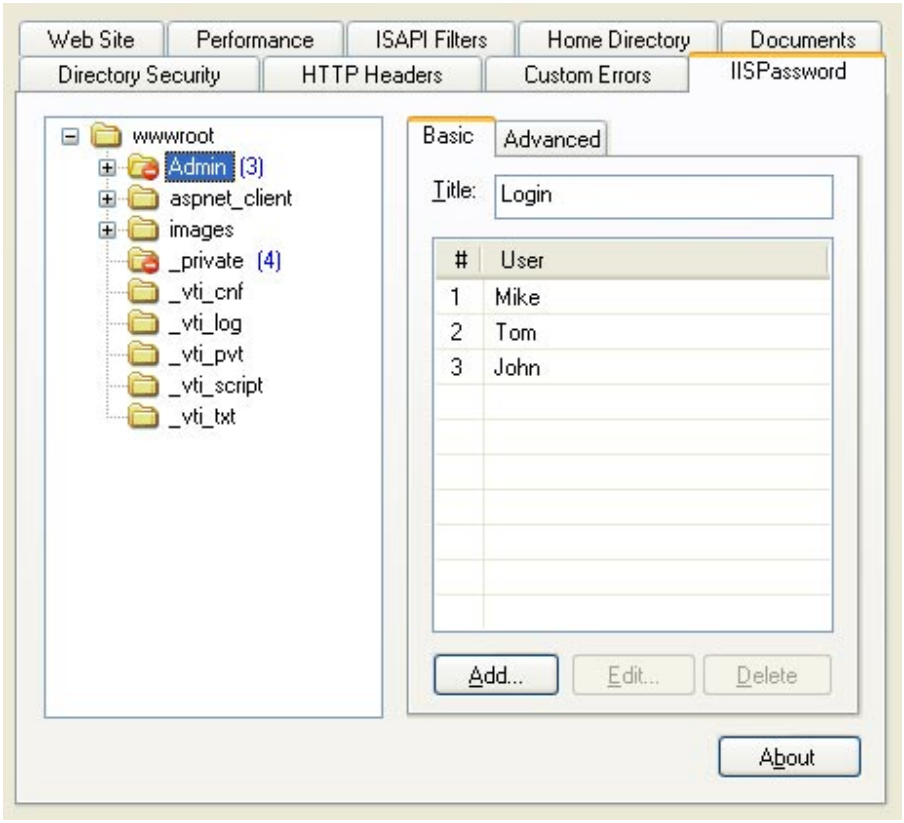
Windowsov IIS se pravic nad "web" mapami loteva popolnoma drugače kot Unixov Apache. Rešitev .htaccess, ki v Apacheju ščiti celoten direktorij (slika 18), se je v prvih verzijah IIS reševala tako, da smo izklopili uporabnika IUSR_XXX ter vpeljali nove Windows uporabnike in jim dodelili ustrezne pravice nad želenimi mapami [15].

Žal lahko nove uporabnike v Windows strežniku dodeljuje le administrator. V Apache .htaccess rešitvi uporabnike, skupine ter gesla kreira v svoji mapi uporabnik sam.



Slika 18: Primer .htaccess datoteke

Po novem obstajajo tudi komercialni moduli kot je npr. ISAPI_Rewrite .htaccess [14] ali bolj usklajena Microsoftova *web.config* rešitev s tehnologijo ASP.NET [18].
Sami smo našli za nas zadovoljujočo komercialno rešitev IISpassword [17], ki omogoča brezplačno uporabo .htaccess za tri uporabnike (slika 19).



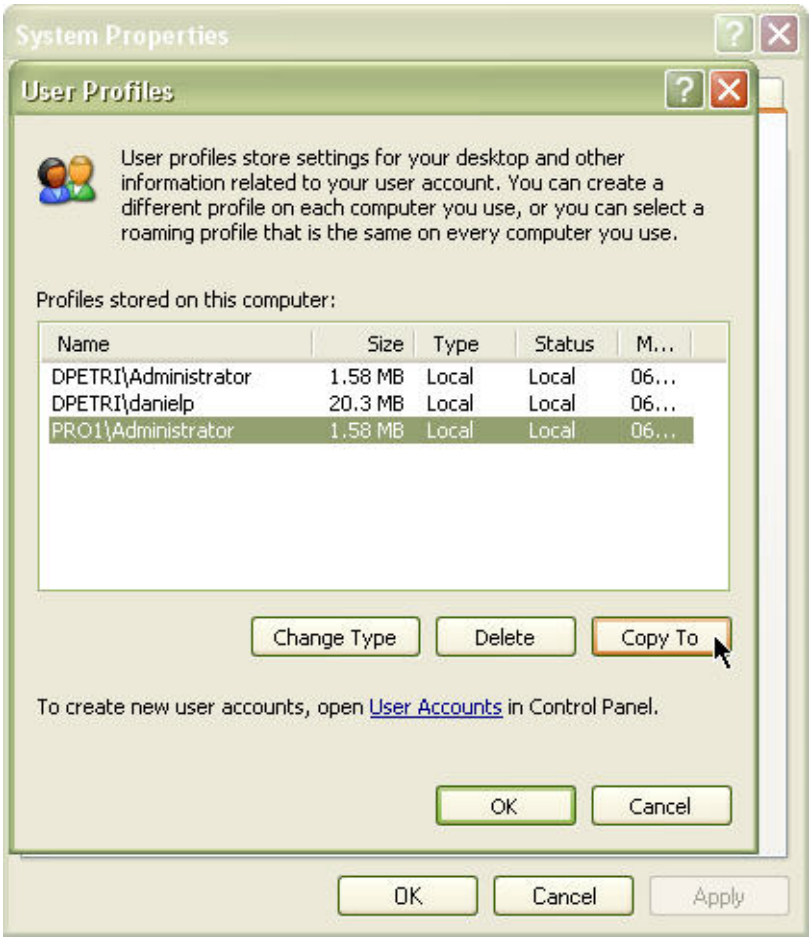
Slika 19: IISpassword

Možnost bi bila tudi zamenjava IIS z Apachejem za Windows. A v bodoče nameravamo preizkusiti še ostale Microsoftove rešitve, kot sta ASP in SharePoint, zato smo vztrajali pri IIS.

3.6 Odjemalci: obisk pri uporabniku

3.6.1 Regedit trik »dveh kazalcev« za popolnoma neopazen prehod v domeno

Standarden Microsoftov postopek (slika 20) pretvorbe nedomenskega uporabniškega profila v domenskega [7] se pri naših uporabnikih ni dobro obnesel.

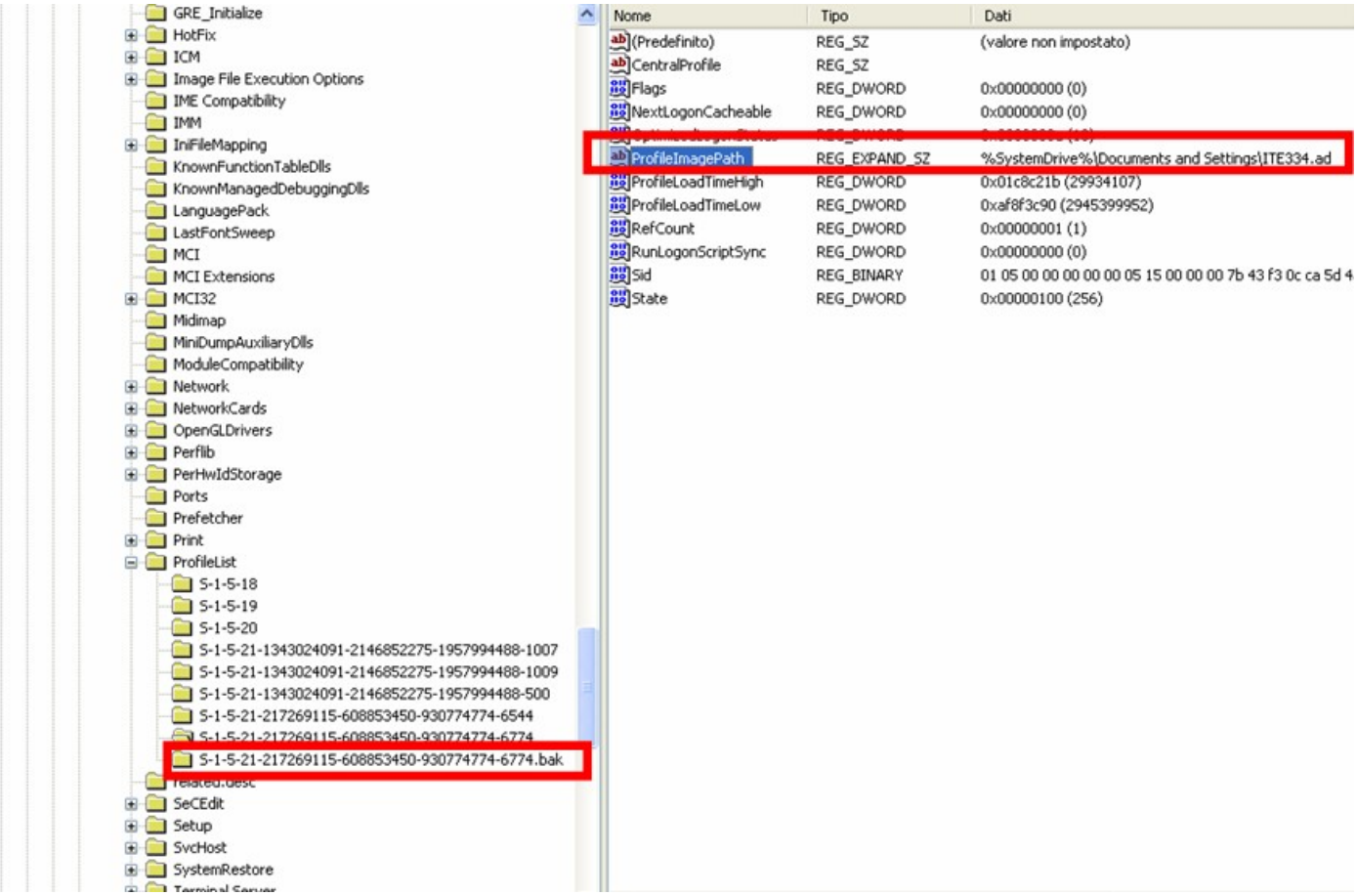


Slika 20: Kopiranje profilov po standardnem postopku

Ta postopek prenese datoteke, elektronsko pošto, a neveščim uporabnikom spremeni izgled namizja, glavni tiskalnik, zadnje odprte dokumente in še druge stvari. Uporabnik, navajen postavitve ikon, tiskanja s klikom, zaide v težave ter kliče računalniško pomoč.

Da bi se vsemu temu izognili, smo na internetu izbrskali zanimivo rešitev [8], ki že malo meji na "hackerstvo". Vsak Windowsov uporabnik ima v registru zapisane vse svoje nastavitve. Še prej pa je v registru zapisan sam uporabnik in nato sledi kazalec (pointer) na njegov del

registra. Torej lahko uporabniku B preusmerimo kazalec na nastavitve uporabnika A, ter tako B prevzame vse nastavitve uporabnika A (slika 21)?



Slika 21: Regedit nastavitev dveh kazalcev

HK_LOCAL_MACHINE/Software/Microsoft/Windows NT/Current version/Profile List/ #SID domenskega uporabnika# -> ProfileImagePath:

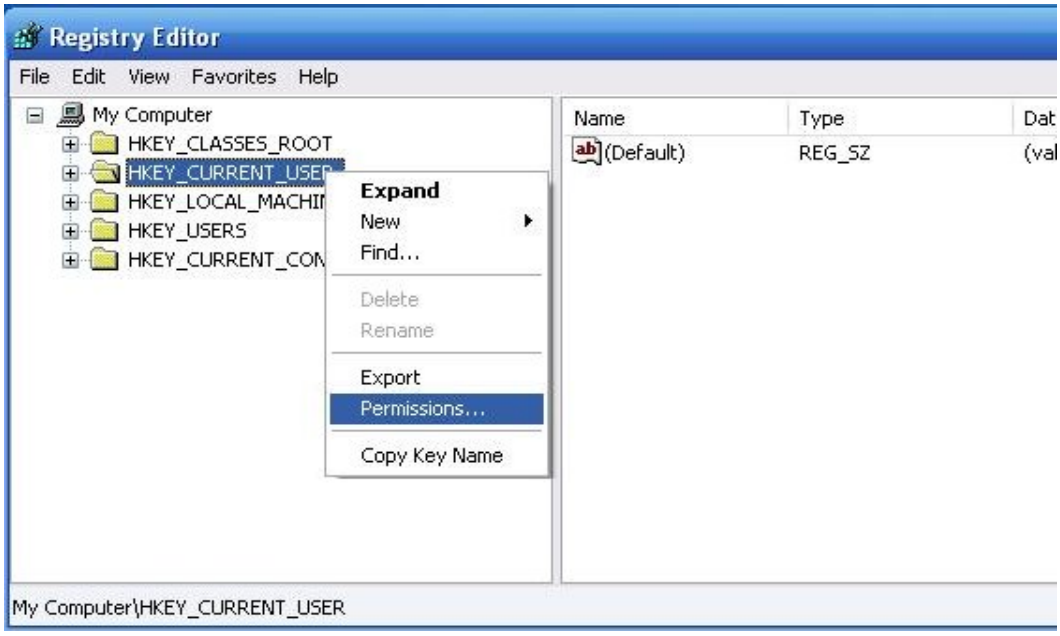
kjer namesto:

%SystemDrive%\Documents and Settings\domenski-novi-user

vpišemo

%SystemDrive%\Documents and Settings\stariuser-ki-ni-bil-v-domeni

Na srečo je res tako, saj nič v nastavitvah ni pogojeno z uporabniškim imenom in se lahko leta poljubno prepletajo. Le na pravice (permissions) ne smemo pozabiti. Del registra uporabnika A (stari uporabnik, ki ni bil v domeni) moramo nastaviti, da bo v njem imel pravice pisati in brati tudi uporabnik B (novi, ki je v domeni), kot nam kaže slika 22.



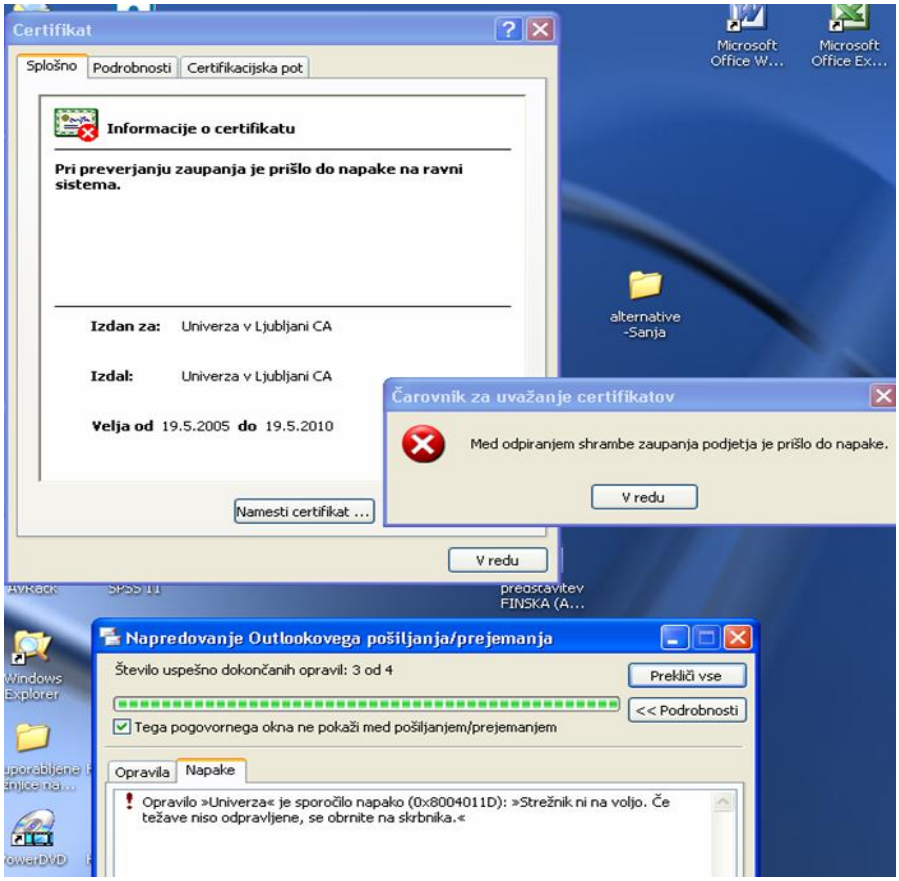
Slika 22: Regedit nastavitev permissiona

V nekaterih primerih se vseeno zaplete. Rešitev je prijava v računalnik kot uporabnik A, nato izvoz panja registra uporabnika A (*Export* je ena opcija nad *Permissions*) ter odjava in prijava kot uporabnik B. Sledi uvoz panja uporabniku B. V postopku uvoza panja se sicer pojavi napaka, za katero kasneje nismo ugotovili, da bi vplivala na delovanje, ter smo jo ignorirali. Narediti pa smo morali še eno odjavo uporabnika B ter prijavo nazaj v sistem.

Seveda pred postopkom nismo smeli pozabiti uporabniku B dodeliti popolne pravice tudi nad celotno mapo *C:\Documents and Settings\uporabnika-A*, saj bo to mapo zdaj uporabljal s "trikom". Največ časa smo porabili ravno s spreminjanjem pravic vseh datotek, map in podmap. Kadar je uporabnik administratorjem odvzel pravice nad uporabnikovo mapo, smo morali najprej prevzeti lastništvo [10].

3.6.2 Znižanje pravic Poweruserjev v NormalUser v Windows ni podprto

Če so administratorji računalnikov uporabnikom dovolili vse pravice (t.i. PowerUser) in jih kasneje želijo odvzeti, se lahko znajdejo v veliki težavi. Zanimivo nam je bilo, da se je to dogajalo le v Microsoftovem programju, pri ostalih proizvajalcih pa ne, kot da bi Microsoft uporabljal kakšne nedokumentirane procedure, ki imajo hrošča v registru ali "LocalSettingsih".



Slika 23: Https problem pri "demotanju" uporabnika

Problematičnega uporabnika na računalniku odkrijemo tako, da mu po znižanju pravic neha delovati protokol https://, npr. dostop na stran *http://www.gmail.com* vrne error 404. Pojavijo se tudi težave z e-certifikati v Internet Explorerju, onemogočen pa je Outlookov RPC-dostop do Exchange strežnika (slika 23).
Mozilla ni prizadeta.

Ostali (prej NormalUser) uporabniki na istem računalniku ali isti uporabnik na drugem računalniku ni imel težav. Tudi domena ni kriva, ker na enako težave naletimo, četudi računalnik ni v domeni [9]. Standardni Microsoftov postopek za kopiranje profila [7] ne odpravi te https:// težave.

Rešitvi, ki smo ju našli, sta dve:
- kopirati vse dokumente uporabnika brez lokalnih nastavitev; pobrisati stari profil; ustvariti novega; kopirati dokumente v nov profil;
- na tem računalniku uporabniku dodeliti PowerUser pravice, a mu z AD-skupinskimi pravicami onemogočiti namestitev programske opreme ter ogled datotek drugih uporabnikov.

3.6.3 Postopek

Celoten postopek smo zaradi porabljenega časa želeli čim bolj časovno skrajšati. Začeli smo na testnem računalniku, a ker "v laboratoriju" ne moremo nikdar predvideti vseh izjem in nepredvidljivih situacij, se je postopek izpopolnil šele po obiskih nekaj uporabnikov.
Na koncu je bil prečiščen in optimiziran postopek tak:

****
** *V kabinet pridemo s pozdravnim listom uporabniku, kaj se je delalo in kakšne prednosti* **
** *domene bo zdaj deležen, ter obvestilom, da ga v njegovem recepcijskem predalčku čaka* **
** *list z domenskim uporabniškim imenom in geslom.* **
****

Vstopimo v računalnik kot lokalni Administrator (to geslo kot upravljalec omrežja imamo)
Popravimo primarni DNS na IP novega Windows domenskega strežnika (brez tega ne bo šel v domeno),
Ponovnem zaženemo PC, ga damo v domeno pef.uni-lj.si in še enkrat restartamo

Prijavimo se kot domenski Administrator.
v Moj racunalnik | Manage | Grupe | Administrators | Dodaj | ---- dodamo vse lokalne userje kot Member of Administrators

****
** *GLAVNI KORAK - Migracija vsakega posameznega userja na tem računaniku* **
****

DOMENSKI USER se prijavi, da mu ustvarimo regedit vnos. Odjavi se.

LOKALNI user se prijavi (ki je zdaj member of Administators in lahko počne vse).
// Če ne vemo gesla, mu ga spremenimo, saj ga bomo po opravljenem delu tako ali tako ukinili //
Pogledamo trenutne nastavitve lokalnega profila (izgled desktopa, recent documents...), si to zapomnimo.
Izvozimo "HK_Current_User" iz registra na C: disk za primer, če bo šlo kaj narobe.

Dodamo pravice v registru lokalnega "HK_Current_User" na Full control za domenskega userja.
// ja, samega sebe - ker se včasih zgodi, da nimaš pravice pisati po tej mapi /
// ker se je le-ta prenesla od starega lokalnega uporabnika //
//to naredimo tako, da v registru z desnim kliknom na HK_CURRENT_USER, izberemo Permissions //
//kliknemo ADD in dodamo domenskega uporabnika ter mu dodelimo vse pravice //

Pregled uporabnikovih certifikatov in jih izvozimo ter nato izbrišemo.
// nekateri uporabniki jih bodo imeli na CD-ju/disketi //

Pregled diska, če je uporabnik uporabljal tudi kakšne druge mape na particijah.
// da mu lahko kasneje nastavimo pravice branja //
Pogledamo ime domače mape (Documents and settings\#mapa#) in si jo zapišemo.
//pazi na Velike/male črke). Če je user imel v imenu šumnike, je verjetnost, da prenos v domeno ne bo uspel //
Nad celotno mapo lokalnega userja moramo dati FULL pravice DOSTOPA domenskemu userju
// Medtem ko čakamo pravice nad direktorij,i opravimo še kakšen drug želen postopek na računalaniku
ter njegovega DOMENSKEGA userja damo med ADMINE !!!
// Moj racunalnik | Manage | Grupe | Administrators | Dodaj | pef\xxxxx

Popravimo v registru pot na starega userja (trik dveh kazalcev):
HK_LOCAL_MACHINE/Software/Microsoft/Windows NT/Current version/Profile List/
#SID domenskega uporabnika# -> ProfileImagePath:
kjer namesto:
%SystemDrive%\Documents and Settings\noviuser
vpišemo
%SystemDrive%\Documents and Settings\stariuser

Lokalni uporabnik se odjavi.

DOMENSKI USER login - pregled namizja in ostalih lastnosti starega uporabnika
Če še vedno ni uspelo, naredi uvoz v register prej izvožene nastavitve "HK_Current_User"
// JA ! tukaj na koncu uvoza javi napako je normalno! //
Logout, zopet login nazaj kod domenski user, da preverimo, če je zdaj šlo?

Dodamo nov account "Exchange mailbox" v njihov priljubljen poštni bralnik (v ta novi account se bodo stekali vsi maili, ko naredimo preskok s starega mail strežnika na novega)

****
** END OF LOOP
****

Pobrišemo vse datoteke izvoženih panjev registra

Umik vseh domenskih in lokalnih accountov iz local admins grupe.
Vse lokalne userje disablamo, da je mogoč vstop le z domenskimi.

List z njegovim novim domenskim usernamom + geslom mu po končanem postopku v recepcijskem predalčku.

3.6.4 Pravni vidiki ter varstvo osebnih podatkov na uporabniških računalnikih

Pri postopku migracije se nam je pojavilo zanimivo pravno vprašanje varstva zasebnosti zaposlenih. Bo varovana pravica do zasebnosti delavca z delom računalniškega administratorja na računalniku delavca ali že s samim dejstvom vstopa administratorja v njegov računalnik kršena? Saj je vendar administrator uporabniku celo resetiral geslo!

Pri reševanju navedene dileme je pomagala naša pravna služba, ki je poskrbela, da vsak zaposleni delavec podpiše izjavo soglasja s pravili uporabe službenih računalnikov ter pravili ravnanja v omrežju Metulj. Vsak zaposleni je tudi podal soglasje in privolitev, da računalniški administratorji delodajalca na službenih računalnikih redno opravljajo vzdrževalna dela ter imajo zato možnost dostopa do vsebine njihovih morebitnih osebnih dokumentov.

Računalniški administratorji so se v sklopu varovanja osebnih podatkov oz. zasebnosti delavcev, do katerih imajo možnost dostopa pri opravljanju svojega dela, s pisno izjavo zavezali, da bodo pri svojem delu na računalnikih drugih delavcev izvajali zgolj posege, ki sodijo v vsebino njihovih delovnih nalog. Če bodo pri izvajanju vsebin svojega dela nehote naleteli tudi na podatke oz. dokumente, ki imajo pravno naravo osebnih podatkov delavca, bodo varovali tajnost teh podatkov, razen če omenjeni podatki nimajo narave kaznivega dejanja.

Ker naj bi bila po razlagah Zakona o varstvu osebnih podatkov (ZVOP-1) pravica varstva osebnih podatkov delavca bolj varovana od poslovnih interesov delodajalca oz. organizacije, kjer je delavec zaposlen, je delodajalec delo računalniških administratorjev organizacijsko uredil tako, da morajo ti praviloma opraviti posege v službeni računalnik delavca med delovnim časom delavca in ob njegovi prisotnosti pri posegu, vsakemu delavcu pa so kljub zgoraj sprejetim ukrepom, katerih namen je zagotoviti varovanje delavčeve pravice do zasebnosti, omogočene tudi pravica in možnosti, da je v postopku migracije vedno osebno prisoten in da lahko osebno nadzoruje poseganje v podatke na njegovem službenem računalniku.

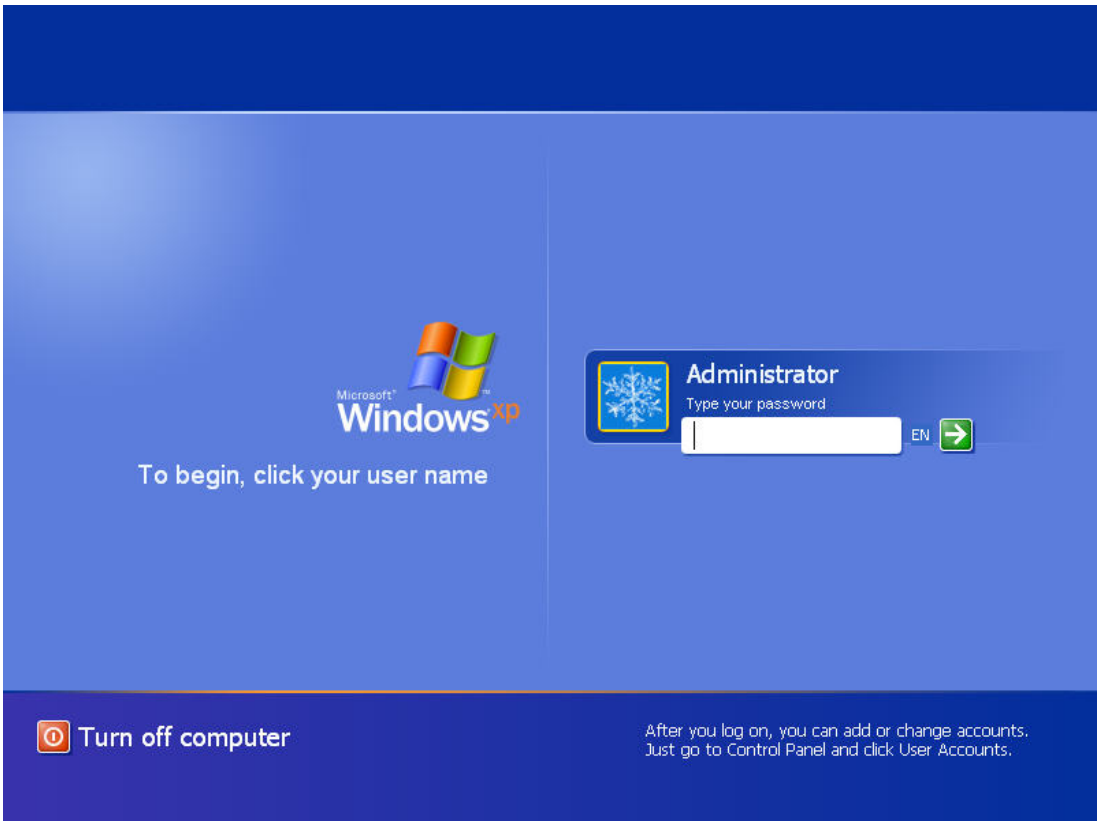
3.6.5 Uporabniki s šumnikom v imenu

Izogibanja šumnikov v imenih datotek smo bili vajeni v starejših Windowsih, na nekaterih strežniških izvedenkah pa še dandanes.

A nihče ni pričakoval, da lahko težavo predstavlja tudi uporaba šumnika v imenu uporabnika. Nastala je velika težava, kajti takega uporabnika z našim trikom "dveh kazalcev" ali z Microsoftovim postopkom sploh nismo mogli prenesti. Potreben je bil reformat računalnika.

3.6.6 Novo prijavno okno: CTRL + ALT + DEL uganka povprečnega uporabnika?

Uporabniki v nedomenskem Windowsovem okolju imajo najverjetneje izbran lažji način prijave: preko slikovne ikone, kar nam prikazuje slika 24. Enostavno z miško izberejo svojo ikono, po možnosti vpišejo še geslo in se pripravijo na delo v Windowsovem namizju.



Slika 24: Pozdravno okno, ko nisi v domeni

V domenskem okolju ta način prijave ni več možen. Obvezno se na začetku pojavi prijavno okno z napisom "pritisnite CTRL + ALT + DEL" (slika 25).

Slika 25: Ctrl + alt + del uganka prijave v domeni

Neveščim uporabnikom to lahko predstavlja veliko težavo. To smo predvidevali ter jo rešili tako, da smo vsakemu uporabniku natisnili razumljiva slikovna navodila. Nismo pa predvideli, da se povprečen uporabnik doslej še ni nikdar srečal s kombinacijo CTRL + ALT + DEL, ter da ne ve kaj mu pravi to sporočilo.

Pri ozaveščanju nam je pomagala slika 26, ki smo jo priložili navodilom.

Slika 26: Slika tipk ctrl, alt, del

3.7 Tečaje osebja organizirajte pravočasno

Seveda je samoiniciativno učenje novih tehnologij zaželena lastnost informacijskega kadra. A velikokrat se izkaže, da že teden tečaja ne le skrajša končni čas razumevanja tehnologije, temveč tudi napoti po pravi poti uvajanja, brez pasti zahajanja v stranske slepe ulice.

Zato je potrebno seznanjanje s tehnologijo in novimi orodji opraviti dovolj zgodaj, saj povsem lahko odkrijemo, da tehnologija za nas sploh ni primerna, ter se še pravočasno usmerimo v konkurenčno.

3.8 Uvedba portala za izmenjavo izkušenj v projektu

Univerza v Ljubljani je poskrbela za skupen portal za izmenjavo mnenj. Žal pa se je vse skupaj sprevrglo bolj v suhoparno podajanje navodil, na konkretne težave uvajalcev, ki so jih navajali na portalu, pa ni nihče odgovarjal.
Poskrbeti bi bilo treba za tim ljudi (ali enega človeka), ki bi opravljal to nalogo, saj se nemalo težav v organizacijah ponavlja ter se nepotrebno ponovno odkriva rešitve, ki jih nekdo že ima.

3.9 Strogo sledenje varnostnim pravilom

Administratorji nedomenskega okolja niso seznanjeni z raznimi vrati in izjemami Microsoftove domene. Microsoftova pomoč, ki nam je pomagala uvajati okolje, pa ne več na nedomensko okolje.
Ugotovili smo, da je potreben tretji član, ki budno pazi in usklajuje vse nekonsistentnosti, ter krpa varnostne luknje za obojimi.

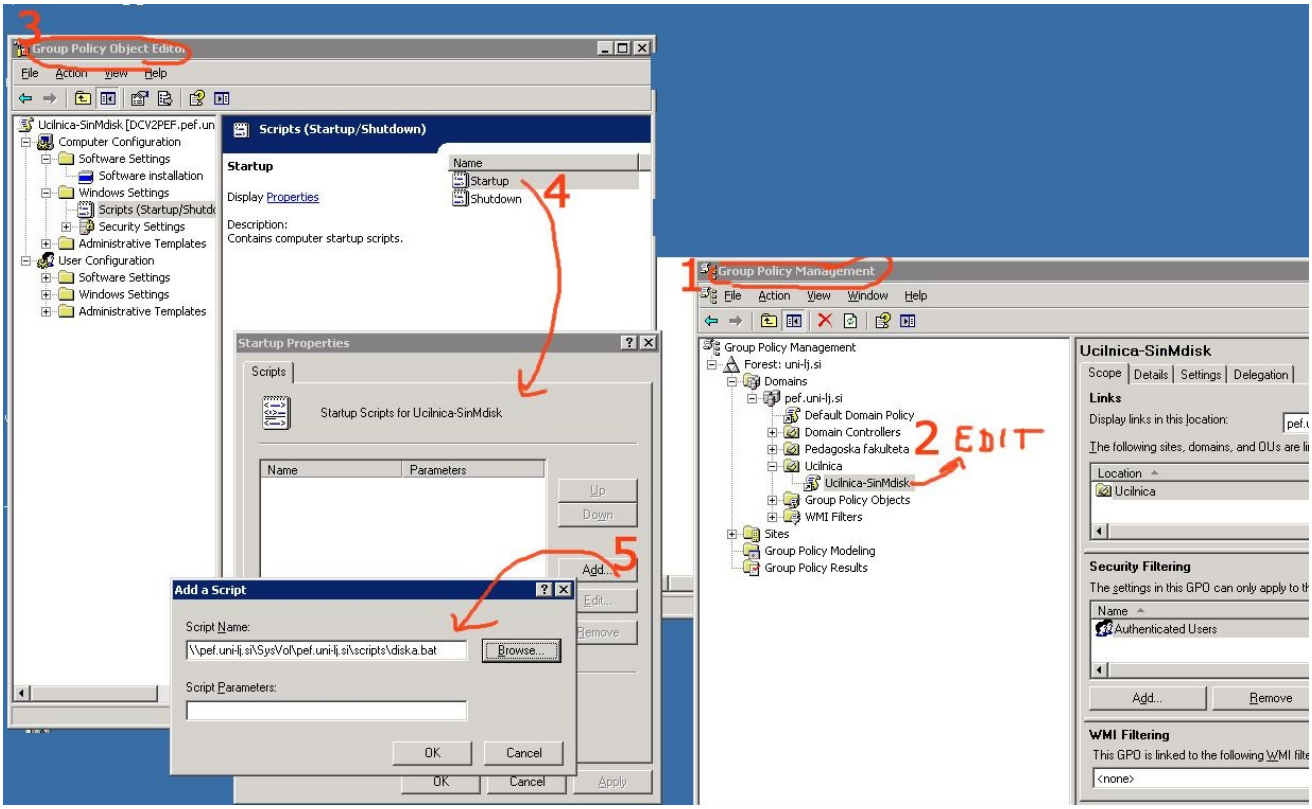
V našem primeru se je to zgodilo z vrati 3389. Po navadi so vrata nad 1023 namenjena povratnim klicom. Teh višjih vrat se v Unix okolju ne zapira, saj so strežniški servisi na nižjih vratih. Windowsovi strežniki pa za terminalski dostop uporabljajo omenjena visoka vrata Administratorji Unixa tega nismo vedeli. Administratorji Windows pa niso bili seznanjeni s tem, da mi tega ne vemo ter da imamo vrata na požarnem zidu odprta. In prvi vdor je bil tu.

4 Uporaba AD-skupinskih politik

4.1 Group Policy Manager Console

Windowsovi računalniki, odjemalci in uporabniki si vse pravice, kaj smejo in česa ne smejo, naložijo na začetku iz t.i. Group Policyja (GP). Kot nam pove že ime "skupinska pravila", z enim objektom nastavimo več pravil, politik.

Če zelo poenostavimo, se najprej zažene lokalni Group Policy, ki je na samem računalniku, če je računalnik v domeni, pa ob naslednji prijavi izvede še domenski AD Group Policy (GP) za ta računalnik in nato trenutnega uporabnika. Domenski Group Policy je objekt AD-ja [4], ter v resnici razdeljen na tri različne GP-je: območja, domene in organizacijske enote. V tem vrstnem redu se politike tudi izvajajo. Kasnejša pa popravlja zgodnejšo. [3]



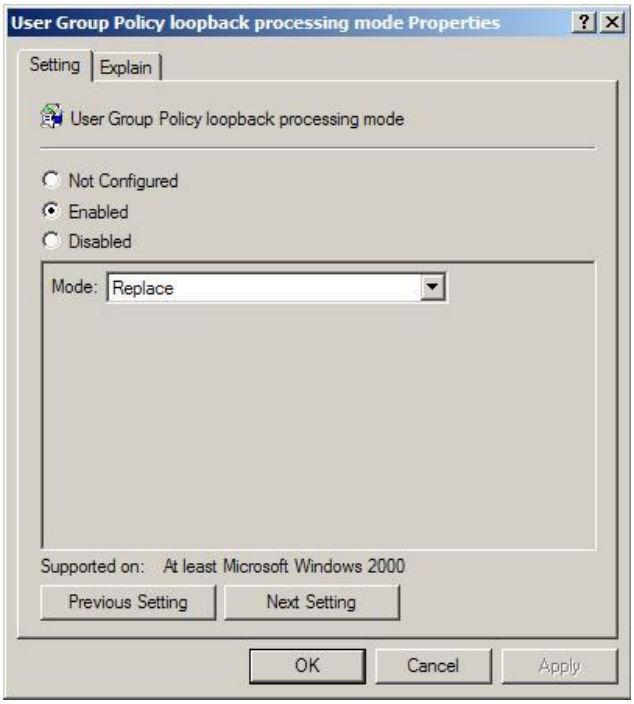
Slika 27: Primer dodelitve pravila v GPO

Poleg dobimo orodje za nadzor Group Policy Manager Console [5]. Z njim lahko z domenskimi nastavitvami GP popolnoma razveljavimo lokalni GP, uporabnike in/ali

računalnike pa uredimo v skupine, ki se v AD imenuje Organizational Unit (OU). Nad OU lahko določimo enako GP-politiko, ne glede na lokalne posebnosti posameznih računalnikov.

Tako npr. enostavno uvedemo dostop do skupnega diska (
Slika 27 27). Takoj ko uporabniku ne želimo več omogočati dostopa do tega diska, ga prestavimo iz te skupine. Če se skupni disk prestavi na drugo lokacijo, to povemo v GP Objectu (GPO) te nastavitve.

Uporabnik se seli od računalnika do računalnika. Tako se zgodi, da računalnik, na katerem dela, spada v neko GPO, njegov uporabniški račun pa v drugi GPO. Ker se pri vsaki skupni politiki najprej izvede GP za računalnik, kasneje pa GP za uporabnika, nam lahko na kakšnem računalniku (npr. ki je prosto dostopen v knjižnici) to z varnostnega vidika predstavlja problem, saj bi uporabniški GPO lahko dovolil nekaj, kar mi točno na tem računalniku izrecno prepovedujemo – ne glede na vrsto uporabnika, ki se bo prijavil nanj.
Takrat spremenimo "loopback processing mode properties", kar povzroči, da se GP za računalnik izvede kasneje kot GP za uporabnika ali pa se uporabnikov sploh ne izvede. Kako lookback vklopimo in katerega od dveh načinov izberemo, nam kaže slika 28.



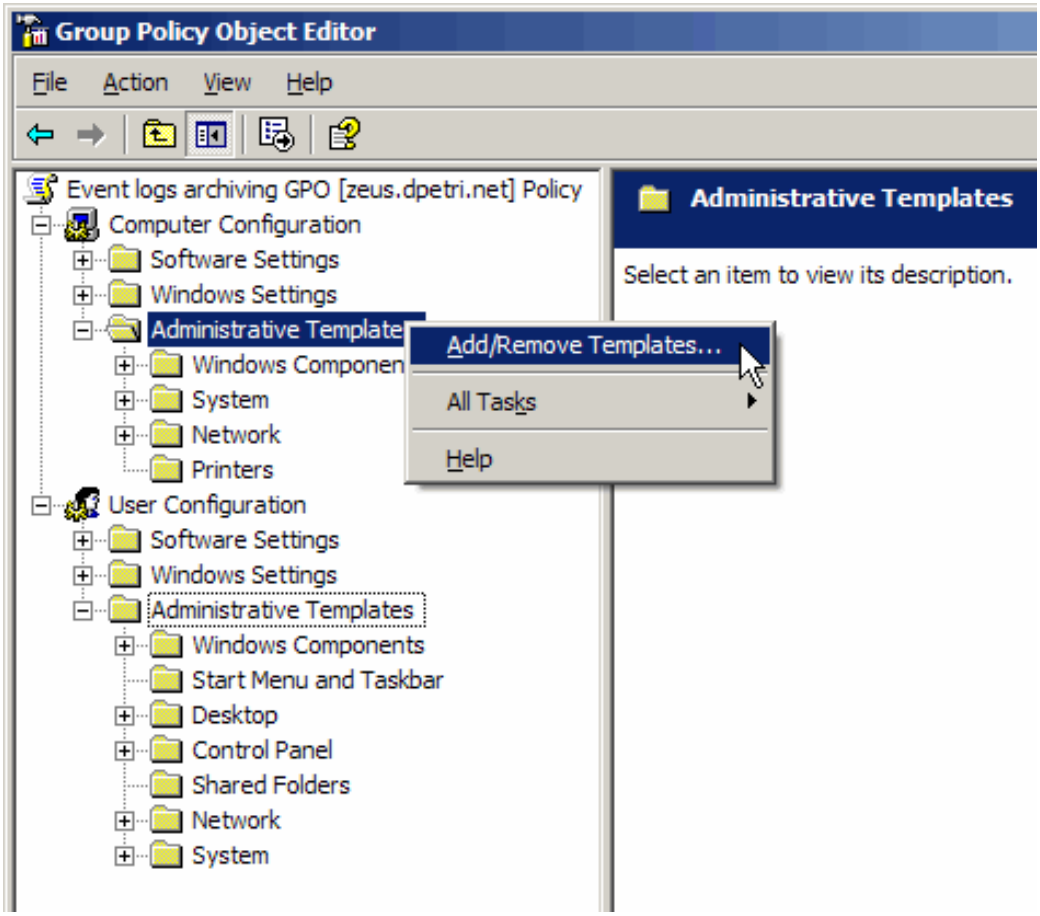
Slika 28: Preklic uporabniških GP

Pri "Merge" se bo najprej izvedel računalnikov GP, nato uporabniški ter nato zopet še enkrat računalnikov GP. Pri "Replace" pa se uporabniški GP sploh ne bo izvedel.

Pri slabi povezavi se lahko zgodi, da se v izogib počasnega prijavljanja ne izvedejo vse GP-nastavitve, ampak le varnostne [3]. To je vgrajena funkcija AD-ja, ki je na začetku vklopljena. Lahko jo spremenimo ali onemogočimo v *"slow link detection properties"*, če se bojimo, da bi kakšen "hackerski" napad, ki bi nasilno obremenjeval omrežje, povzročil, da se pomembna GP nastavitev ne bi izvedla.

Potrebna je velika pazljivost pri brisanju GPO, saj lahko povzročimo nepovratno okvaro registra pri uporabnikih, ki so bili v tem GPO-ju. Najprej je treba odlinkati GPO uporabnikov, da se spremembe zapišejo v njihov register.

Na voljo imamo več že narejenih predlog (Administrative Templates), ki jih lahko najdemo na internetu (npr. za Office 2003), da s pomočjo AD GPO Editorja hitreje najdemo in nastavimo želene nastavitve. Vplivamo lahko na več kot 700 nastavitev. Predloge se zapisujejo v datoteke .ADM in jih po potrebi nalagamo, kot kaže slika 29. [21]

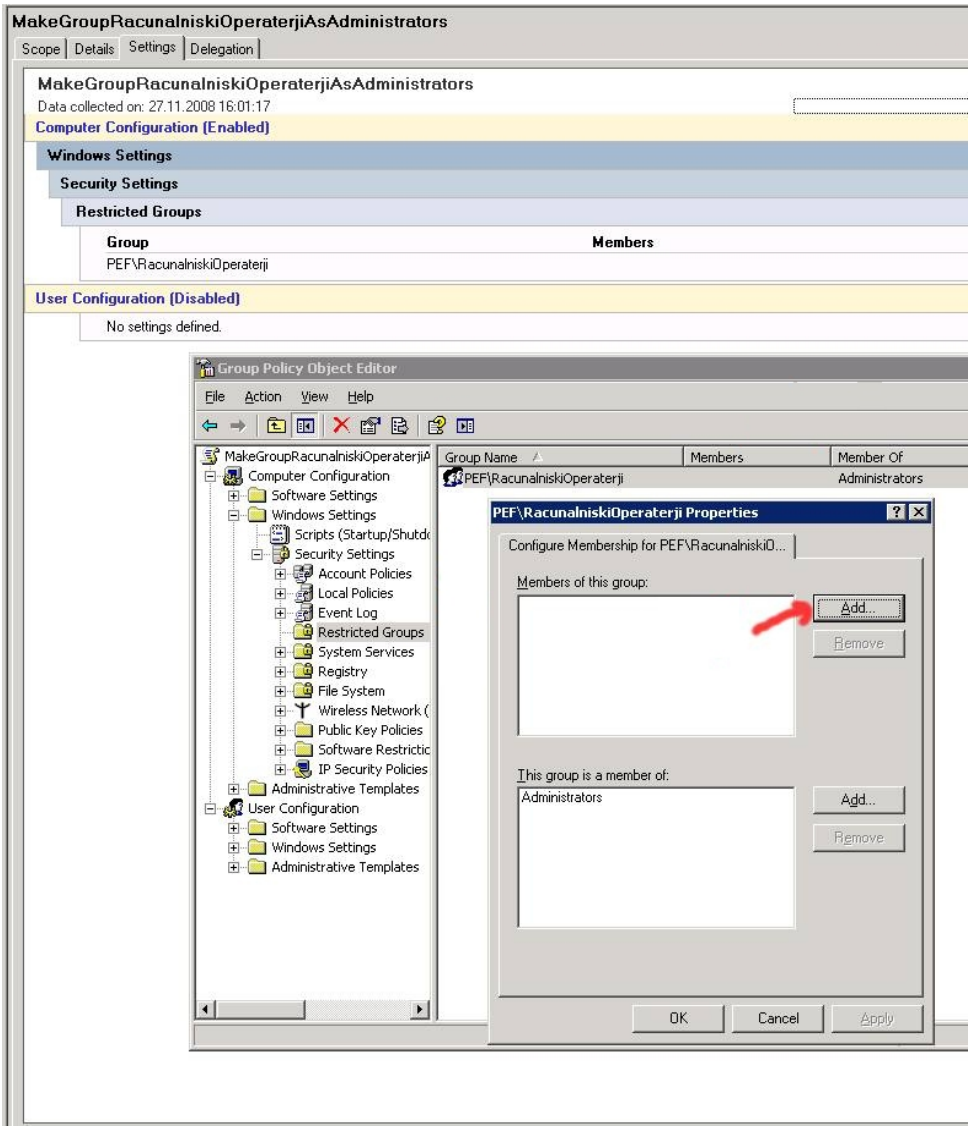


Slika 29: Nalaganje Administrative Templates

Kot rečeno, je nastavitev skupinskih politik zelo veliko, navedel pa bom le tri, ki smo jih kot prve s pridom uporabili.

Prva je bila določitev administratorjev v učilnicah. V nedomenskem okolju je to potrebno storiti na vsakem računalniku posebej. V domenskem pa lahko s kreiranjem nove "PowerUser" OU skupine ter nastavitvijo politike nad to skupino enostavno s klikanjem premikamo nove uporabnike v "PowerUser" OU-skupino ali jih iz nje umikamo.
Politiko pa izvedemo le nad to določeno skupino računalnikov, v kateri želimo, da je ta "PowerUser" OU-skupina administrator.
Nastavitev se, kot nam kaže slika 30, nastavlja v GP:

- *Computer Configuration | Windows Settings | Security Settings | Restricted Groups*



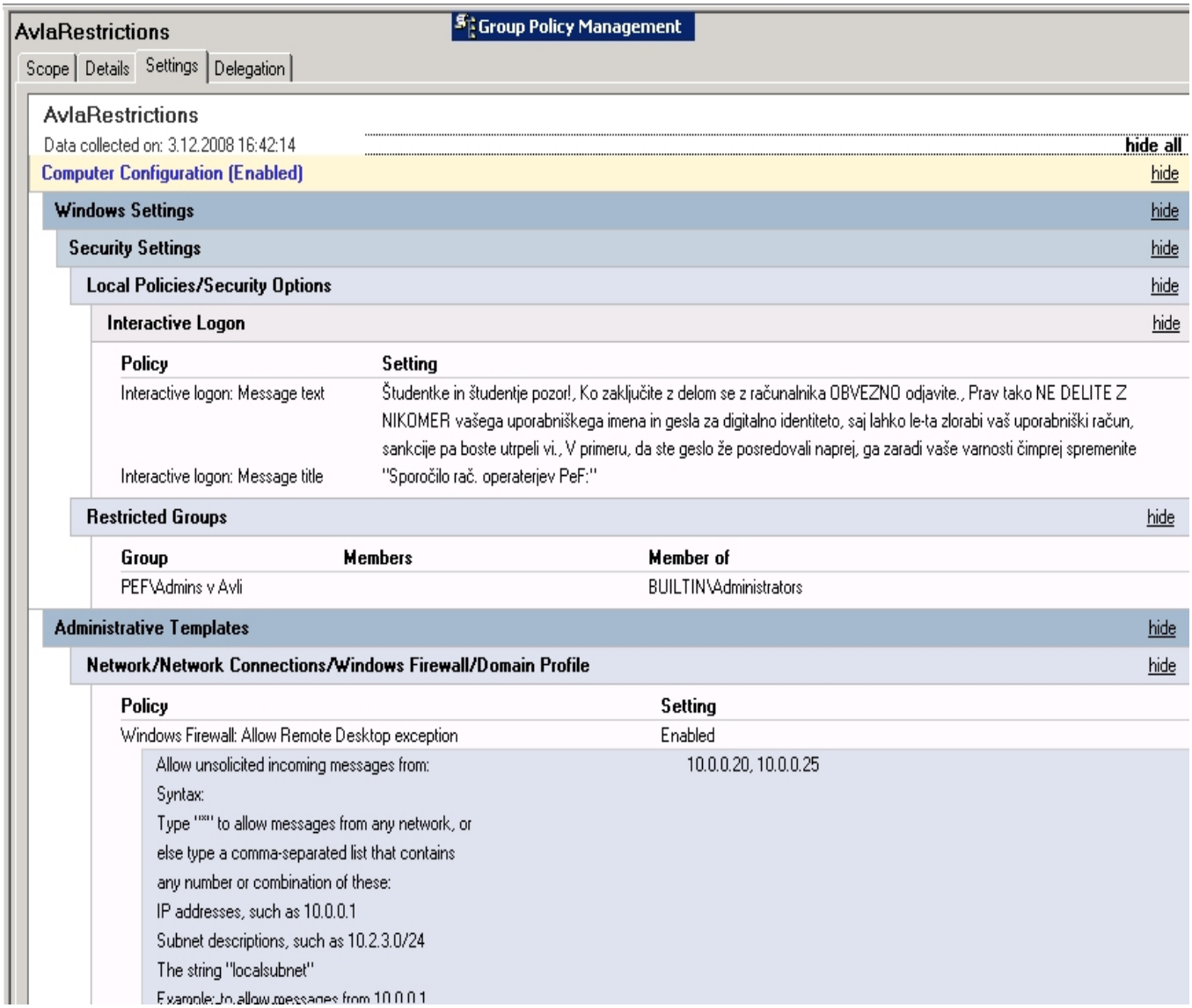
Slika 30: Domensko nastavljanje administratorskih pravic v določeni OU

Kot nam kaže slika 31, sta zanimivi še dve nastavitvi v *Computer Configuration* :

- *Windows Settings* | *Security Settings* | *Local Policies* | *Interactive Logon*

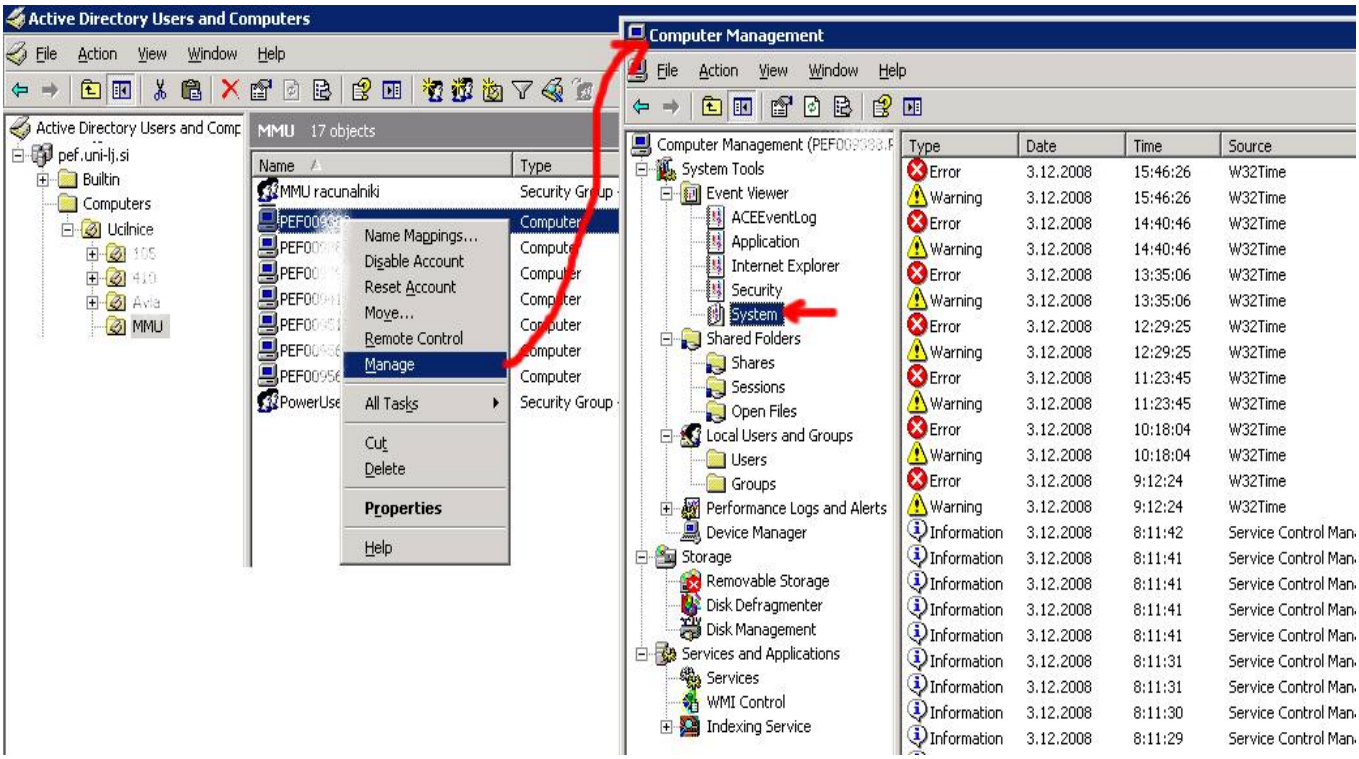
- *Administrative Templates* | *Network* | *Network Connections* | *Windows Firewall* | *Domain Profile* | *Allow Remote Desktop Exceptions*

Prva obvešča uporabnike, naj se strogo odjavljajo ter ne posojajo gesel, druga pa odklene požarni zid oddaljenemu namizju samo za določene IP-je.



Slika 31: Sporočila in požarni zid

Domena nam omogoča tudi "Remote Managment" (slika 32) vključenih računalnikov, ko na daljavo opravimo in pogledamo marsikatero napako kar iz AD-imenika vseh računalnikov.

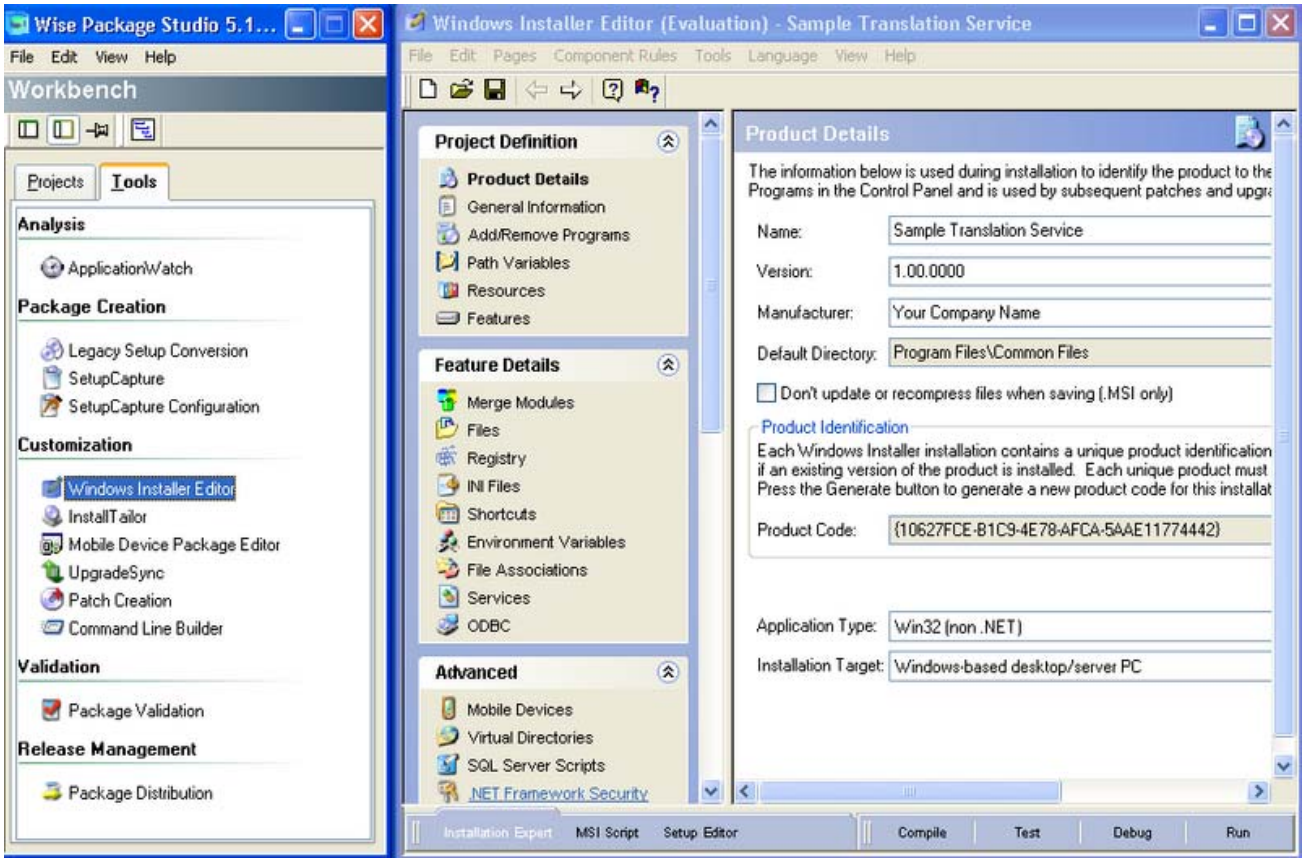


Slika 32: Enostavno oddaljeno upravljanje domenskih računalnikov

4.2 Namestitve programja s pomočjo Group Policy in .msi

V AD lahko za dodajanje in odstranjevanje programov na uporabniškem računalniku, ki je v domeni, uporabimo Microsoft Windows Installer tehnologijo [3], ki vsebuje dve komponenti:
- instalacijski paket (.msi datoteke "native Windows installer file");
- Windows Installer servis (msiexec.exe).

V povezavi z GP postane močno orodje za nastavitve tako novih programov kot osveževanje obstoječih. Preprosto lahko dodelimo, da se program A osveži vsem, ki so v skupini "uporabniki A", nov tiskalnik B v 2. nadstropju pa nastavi vsem, ki so v skupini "2. nadstropje". Vse to se naredi v ozadju brez interakcije uporabnika.
Vsi podatki o sami namestitvi so shranjeni v .msi datoteki. Msiexec.exe pa z uporabo DLL-knjižnice poskrbi za izvedbo .msi paketa. Isti .msi paket se lahko uporablja tudi za popravljanje programa, ki smo ga namestili, npr. ko se program po kliku z miško noče zagnati, ker mu manjka kakšna datoteka ipd.



Slika 33: Izdelava paketa za instalacijo s komercialnim orodjem

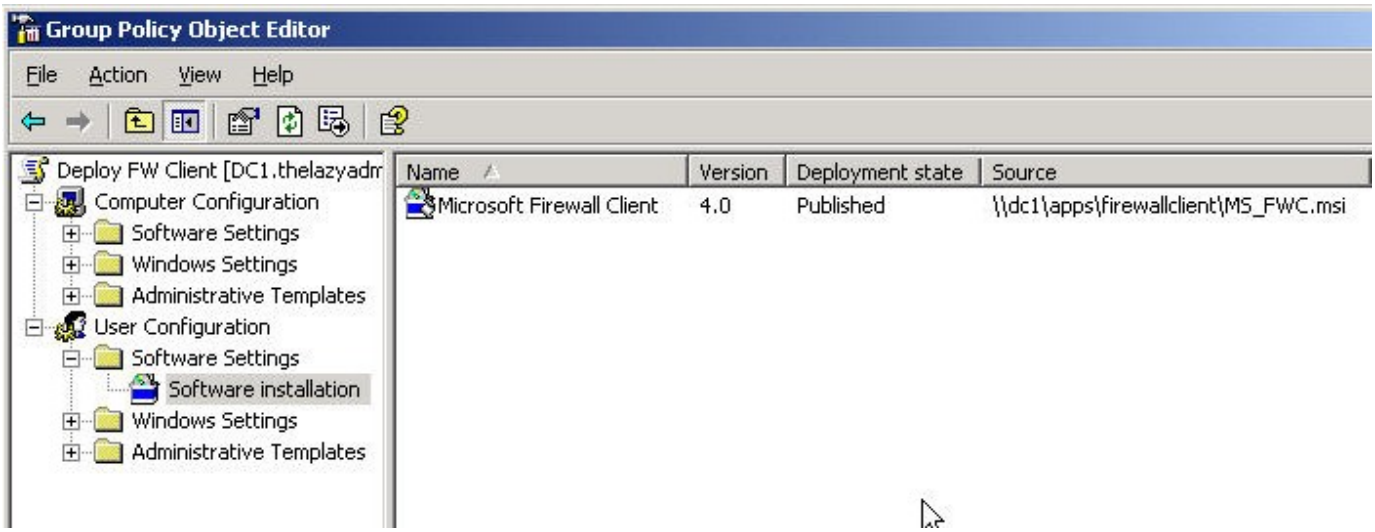
Windows Installer servis se lahko uporablja tudi za starejše Windowsove operacijske sisteme, vendar pa se GP lahko uporablja le na Windows 2000/XP/2003/Vista/2008. Po navadi je potrebno imeti za različne verzije operacijskega sistema različne .msi pakete. Prav tako je vprašljivo, če bi Windows95/98/NT še sploh podpiral programje, ki ga z .msi nalagamo. Če proizvajalec ni priskrbel svoje .msi datoteke, lahko za izdelavo (slika 33) uporabimo brezplačna ali komercialna orodja, kot so Advanced, WinINSTALL, Wise ipd. [20].

Obstaja tudi nekaj komercialnih .msi datotek za programje *http://www.appdeploy.com* , ki ga v osnovi proizvajalci niso ponudili v .msi obliki. Brezplačni AdvancedInstaller pa dobimo na *http://advancedinstaller.com*

Potem ko imamo .msi datoteko, je na vrsti vpeljevanje (deploy).

Datoteko .msi moramo objaviti na nekem mrežnem disku, do katerega imajo vsi le bralni dostop. Dobro je tako mapo preventivno skriti, kar storimo z dodatnim znakom $ na koncu imena "sharane" mape.

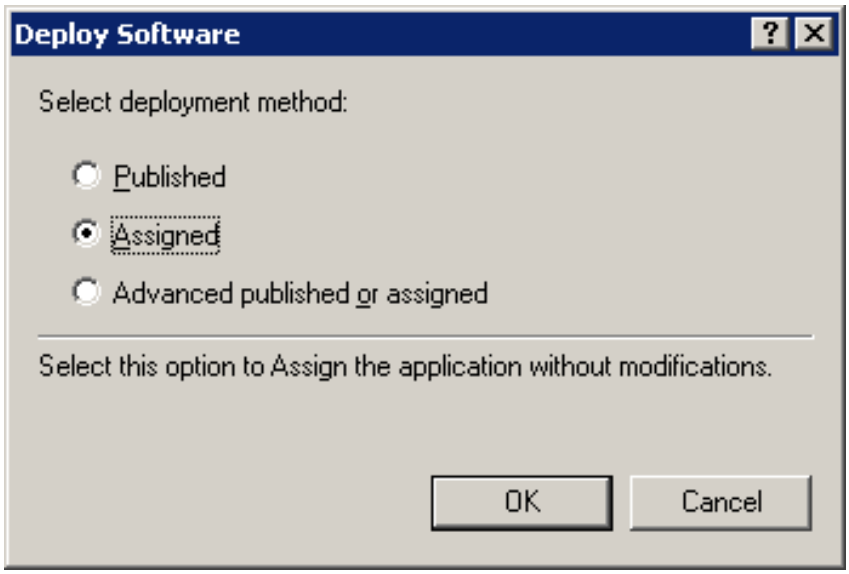
V GP | Software Setings | Software Installation določimo, komu se naj paket zažene (slika 34), ter določimo način vpeljevanja.



Slika 34: GPO za deploy

Osnovna načina vpeljave sta dva (slika 35):

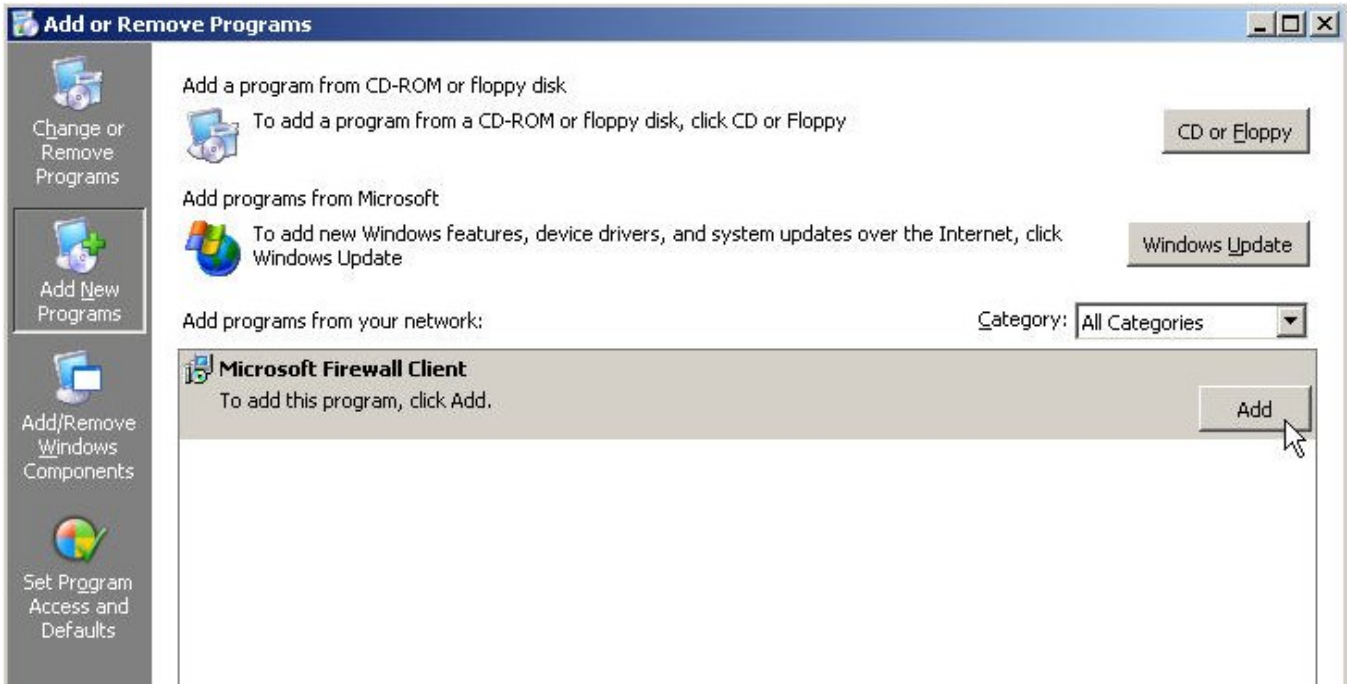
- Assign;
- Publish.



Slika 35: Vpeljava (deploy) softwara

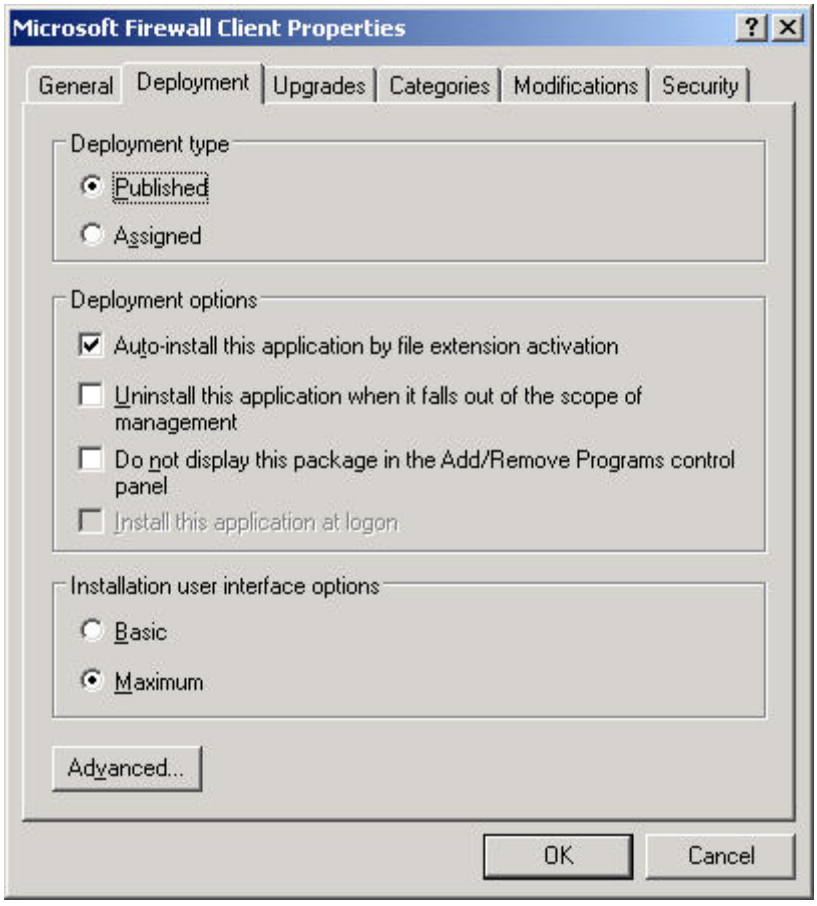
"Assingamo" lahko na računalnik ali na uporabnika. Kadar to naredimo na računalnik, se bo ob naslednjem zagonu računalnika aplikacija namestila vsem, ki delajo na njem. Kadar to storimo na uporabnika, pa se bo namestila v bodoče, kjerkoli se bo ta uporabnik prijavil, a šele ko bo poskušal izvesti operacijo, ki je povezana s tem programjem. Torej se to ne bo zgodilo avtomatsko pri sami prijavi uporabnika.

"Publishiranje" pa pomeni, da bo novo programje le navedeno kot možnost v Nadzorni plošči med Dodaj/Odstrani programe (slika 36), ki jo uporabniki lahko sami izvedejo. Za to bodo izvedeli z obvestilom pri prijavi.



Slika 36: Publish deploy v nadzorni plošči

Nastavlja se lahko še nekaj ostalih možnosti, kar nam kaže slika 37.



Slika 37: Dodatne nastavitve pri publish deploy

Največja težava, ki se lahko kaj hitro zgodi, je, da vpeljemo zadevo za preveč oseb ali računalnikov naenkrat, saj mreža preprosto ne prenese tolikšnih hkratnih namestitev.

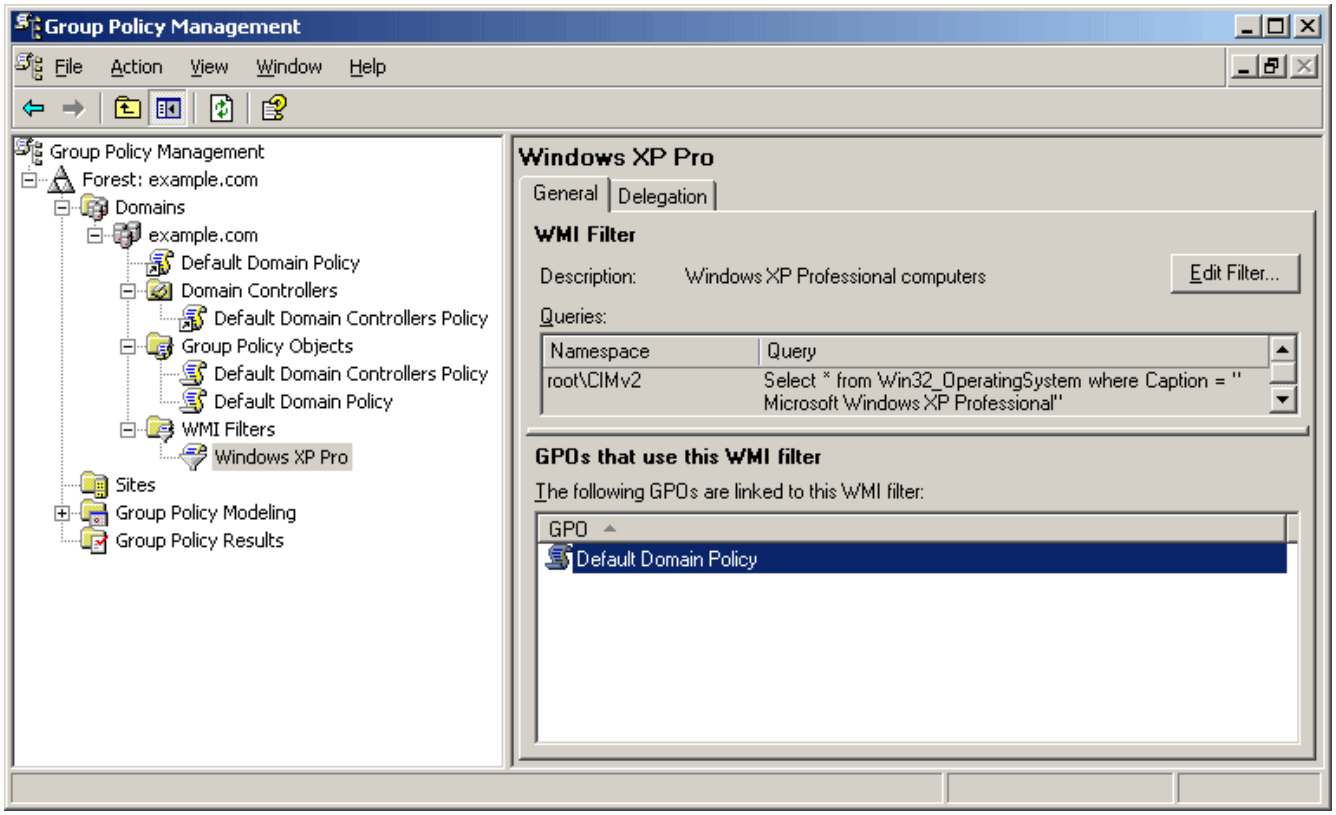
Kaj hitro tudi uvidimo razne omejitve, ki jih odpravita Microsoft System Managment Server (SMS) ali Intel LANdesk [3].
Prva je, da lahko uvedemo uvajanje softwara mimo GP, torej tudi na starejše Windows sisteme.
Pomembnejša je možnost uvedbe časovnega urnika. Z njim lahko programje na računalnike nameščamo v nočnem času. Zbudimo jih z "wake-up-LAN" tehnologijo, namestimo programje ter nato ugasnemo.

Pri velikem številu namestitev se v normalnem načinu "unicast" vsi podatki prenašajo k vsakemu posameznemu računalniku ter tako nepotrebno porabljajo podatkovno širino. Izberemo lahko "multi-cast" način, ko se podatki prenašajo samo v enem paketu po celem omrežju, odjemalski računalniki pa jemljejo podatke iz tega "multi-cast paketa".
Pri SMS in LANdesku lahko dobimo tudi poročilo, kaj se je na posameznem računalniku izvedlo od načrtovanih namestitev in kaj ne, ter vodimo popoln spisek.
Njun spisek ne vsebuje le tega, kaj je bilo nameščeno, ampak tudi popolno poročilo o strojni opremi računalnika. To lahko dodatno izkoristimo pri "izbirčnem" nalaganju nekega programja, npr. če ima dovolj pomnilnika, če ima močno grafično kartico itn.

Tudi v AD-skupinskih politikah je podobno, a bolj omejeno orodje, ki nam omogoča implementacijo nekega pravila (ali namestitve) le na računalnikih z določenimi strojnimi ali programskimi karakteristikami. To so filtri WMI (Windows Managment Instrumentation), ki s podmnožico ukazov SQL, ki jih imenujejo WQL, omogočajo poizvedbo, npr.:

*SELECT * from Win32_Processor WHERE currentclockspeed > 600*
*SELECT * from Win32_OperatingSystem WHERE caption=""Microsoft Windows 2000""*

Vsakemu GPO lahko dodelimo le en filter, kot nam kaže slika 38.



Slika 38: Filter WMI

5 Sklepne ugotovitve

Naš namen čim bolj nemotene in neopazne vpeljave novega domenskega okolja na uporabniške (odjemalske) računalnike smo celo presegli, saj razen spremenjene začetne prijave uporabnik nikjer ni zaznal spremembe. Tega si pred začetkom nismo upali pričakovati.
Sicer so se pojavili zapleti na področjih, kjer jih sploh nismo pričakovali, a smo vse rešili na način, ki ga uporabnik ni zaznal.
Začelo se je že z drobnim trikom v Windowsovem registru, ki kazalec novega uporabnika preusmeri na starega. To povzroči, da uporabnik uvedbe sploh ne zazna (namizje, certifikati, zadnji odprti dokumenti, privzeti tiskalnik – vse to ostane nedotaknjeno). Ugotovili smo, da to drži le v 90 % primerov, saj se Microsoft drži nekaj nedokumentiranih stvari, ki uporabnikom, nekdanjim PowerUserjem, samo v Microsoftovem programju povzroča težave.
Nadaljevalo se je z ugotovitvijo, da povprečni družboslovni uporabnik ne ve, kaj pomeni napis CTRL + ALT + DEL v prijavnem oknu, ki ga pričaka v domeni. Navajen je bil le klika na uporabniško ikono ter vpisa gesla. Po tej spremembi je bilo mnogo klicev računalniškega osebja, kaj se je zgodilo z njegovim računalnikom.

Tako lahko trdimo, da smo našli zelo uporabne rešitve s praktičnimi primeri za podjetja, ki se bodo lotila prenove. Skupaj z diplomskim delom Roka Roglja (december 2007) "Vzpostavitev sistema za upravljanje življenjskega cikla identitet Univerze v Ljubljani" [6] naše rešitve predstavljajo odličen ter popoln komplet za olajšanje vpeljave aktivnega imenika (AD).

Naše strežniške storitve smo uspeli z večjimi težavami prenesti na Windowsovo okolje, njihova stabilnost pa se bo pokazala v prihodnjih letih. Zaenkrat je odlična, a to je tudi posledica posodobitve strojne opreme.
Poenotenje in olajšanje upravljanja vseh računalnikov v hiši s pomočjo AD je proces, ki se ne bo nikoli končal, in že zdaj vsak dan odkrivamo nove rešitve ter boljše načine administracije. Dosegli smo, da lahko sproščeni čas usmerimo na druga področja, ki so bila prej vedno na čakanju.

Čaka nas še integracija AD in programa za kadrovsko evidenco, saj se zdaj ukvarjamo z nepotrebnim dvojnim popravljanjem podatkov uporabnikov.

Zelo zanimivo bi bilo takšno nadaljevanje našega dela:

- raziskati, kje natančno v Windowsovem registru oz. Local Settingsih je zanka, da PowerUserjem pri degradiranju v Normal User v Microsoftovem programju neha delovati https://. Namig: ni v povezavi z domeno – isto se zgodi tudi lokalnem računalniku, ki ni v domeni. Predlagamo uporabo ali izdelavo "hackerskih" orodij za sledenje odpiranja procesov, datotek ter pisanja v register (Sysinternals Russinovicha?);

- raziskati, če je mogoče po kakšnem drugem načinu vpeljati krajše URL-je, morda na višjem nivoju izven Windows DNS – v našem primeru ne fakultetnem, ampak univerzitetnem ali celo pri Arnesu, če so URL-ji imensko enaki kot domena članice, kar zdaj ni mogoče (Windows DNS-omejitev);

- raziskati mehanizem brisanja objektov v AD in hranjenja kot "thumbstone" v mapi "Deleted Object" 60 dni ter možnost uvedbe dodatnega mehanizma pri uporabi starejših varnostnih kopijah kot 60 dni, ki zdaj sesujejo imenik. Verjetno bi se dalo takšen starejši "thumbstone", ki se ne zna replicirati na ostale DC-je prestaviti v mapo "Lost & Found" ter jo preko nje replicirati na vse DC-je, ne da bi se pokvarila konsistentnost imenikov.

6 Viri

[1] Robbie Allen, *Windows Server Cookbook for Windows 2003 and 2000*, Sebastopol: O'Reilly, 2005, pogl.17

[2] Robert R.King, *Mastering Active Directory for Windows Server 2003, Third Edition*, San Francisco, London: Sybex, 2003, pogl.3, 4, 8, 15

[3] Stein Reimer, Mike Mulcare, *Active Directory for Microsoft Windows Server 2003*, Redmond: Microsoft, 2003, pogl.3, 4, 5, 11, 12, 13, 15

[4] Jeffrey R.Shapiro, Jim Boyce, Marcin Policht, Brian Patterson, and Scott Leathers, *Windows Server 2003 Bible*, Indianapolis: Wiley, 2003, pogl.14, 29

[5] William R.Stanek, *Microsoft Windows Server 2003 Inside Out*, Redmond: Microsoft, 2004, pogl.7, 38

[6] Rok Rogelj, *Vzpostavitev sistema za upravljanje življenjskega cikla identitet Univerze v Ljubljani*, diplomsko delo FRI UL, december 2007

[7] (2008) how do I copy one user profile to another?
Dostopno na: http://technet.microsoft.com/en-us/library/cc781200.aspx

[8] (2008) CHANGING a local user profile to a domain profile
Dostopno na: http://www.petri.co.il/forums/showthread.php?t=6286

[9] (2008) Weird Outlook bug when running as limited user
Dostopno na: http://discuss.joelonsoftware.com/default.asp?joel.3.564874.13

[10] (2008) How to take ownership of a file or folder in Windows XP.
Dostopno na: http://support.microsoft.com/default.aspx?scid=kb;en-us;308421

[11] (2008) Could not login to the FTP
Dostopno na: http://www.chicagotech.net/msapps/ftp1.htm

[12] (2008) HOW TO: Migrate User and Group Information
Dostopno na: http://support.microsoft.com/kb/324222/

[13] (2008) IIS: Instantly Ban IPs Attempting to Login to MS-FTP as Administrator
Dostopno na: http://blog.netnerds.net/2006/07/iis-instantly-ban-ips-attempting-to-login-to-ms-ftp-as-administrator/

[14] (2008) ISAPI_Rewrite 3 - Apache .htaccess mod_rewrite compatible module for IIS
Dostopno na: http://www.helicontech.com/isapi_rewrite/

[15] HOW TO: Migrate .Htaccess Data in a UNIX-to-Windows Migration
Dostopno na: http://support.microsoft.com/kb/324064/

[16] How to secure IIS in a UNIX-to-Windows migration
Dostopno na: http://support.microsoft.com/kb/324216/EN-US/

[17] (2008) IISPassword
Dostopno na: http://www.iistools.com/en/iispassword.html

[18] (2008) The ASP.NET Web.config File Demystified
Dostopno na: http://www.sitepoint.com/article/web-config-file-demystified/

[19] (2008) FreeSSHd
Dostopno na: http://www.freesshd.com/

[20] (2008) MSI Packaging Tools
Dostopno na: http://www.windowsnetworking.com/articles_tutorials/MSI-Packaging-Tools.html

[21] (2008) What are Administrative Template in Group Policy Objects?
Dostopno na: http://www.petri.co.il/understanding_administrative_templates_in_gpo.htm