Windows XP -> 7 - Samba4 a PPKE-n

Pásztor János
pasztor.janos@it.ppke.hu

2014-11-20

Outline

Windows XP

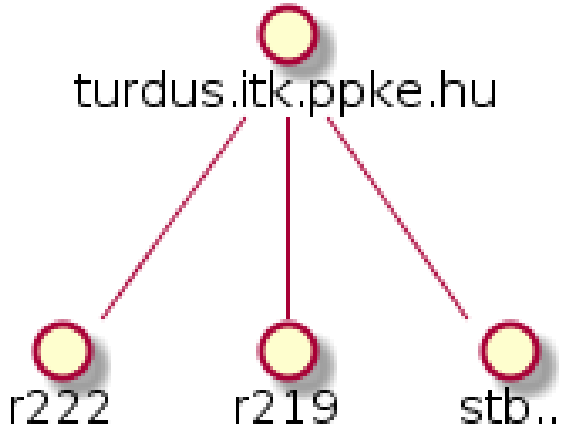
- „2014. április 8-án megszűnt a Windows XP támogatása és frissítési lehetősége.”

ITK

- egy kar
- 7 gépterem
- 175 pc

Szerver oldal

- Debian 5 (lenny)
- saját fordítású samba3
- NT4-es domain
- OpenLDAP backend
- PDC és fájlszerver egy gépen
- L2, netbios, sok vlan interface



Kliens oldal

- Windows XP
- 32 bit
- roaming profilok
- partíció alapú imagelő rendszer

Elvárások

- „Maradjon minden úgy ahogy volt, csak legyen jobb”

Realitások

- samba3 → samba4
- NT4 → AD
- directory és fájlszerver funkciók szétválasztása
- XP → 7
- 32 → 64 bit
- roaming profilok
- natív eszközök használata: gpo, powershell

DC

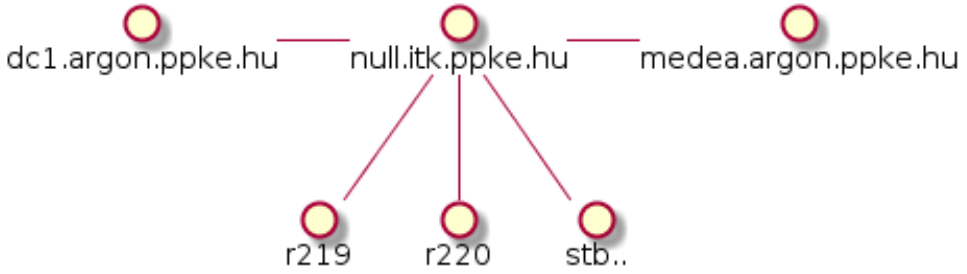
- argon.ppke.hu subdomain
- debian 7 backports csomagok
- `samba-tool domain provision --use-rfc2307 --interactive`
  - rfc2307 használata
  - internal dns
  - BIND9 alternatíva
- RSAT windows-os gépről

Fájlszerver

- Debian 7 backports csomagok
- `net ads join -U administrator`
- roaming profilok tárolása
- távolról ssh alapú elérés
- share jogokat natív windows-os eszközökkel lehet állítani

Tűzfal

- csak belső hálózat
- sok port
- tcp/upd külön port halmaz
- auth és dmz vlan, dump & write

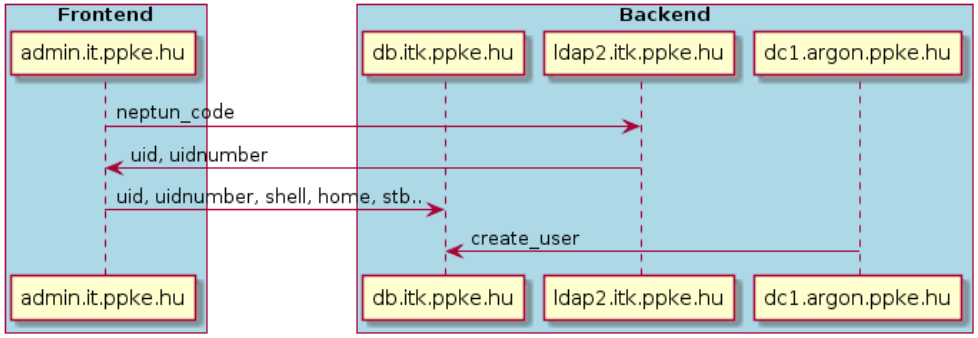


Userek létrehozása

- nincs OpenLDAP backend
- `samba-tool user add username password`
- perl és mojolicious

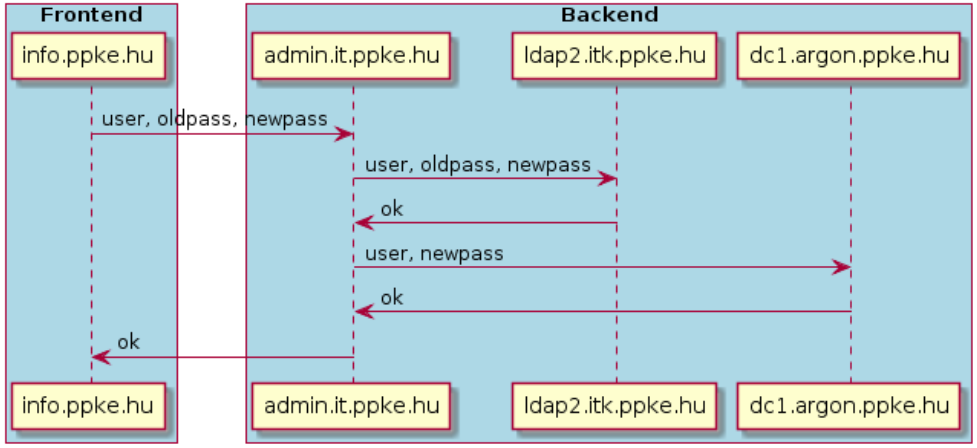
create-user

- webes form
- neptuncode, uid, uidnumber, profileserver, loginshell, gidnumber, state
- postgres adatbázis
- generált password



passwd-sync

- user plusz egy visszajelzést kap: ok/error/unknown
- kliensként idejön, itt is megváltoztatja a jelszót
- backend password változtató szkript kiegészítése



Userek a fájlszerveren

- winbind
  - nss
  - pam
- unix-os attribútumokat ki kell tölteni
- idmapd konfig, két át nem lapolódó tartomány
- domain users default group
- hasznos parancsok
  - `wbinfo -i username`
  - `getent passwd username`

Migráció

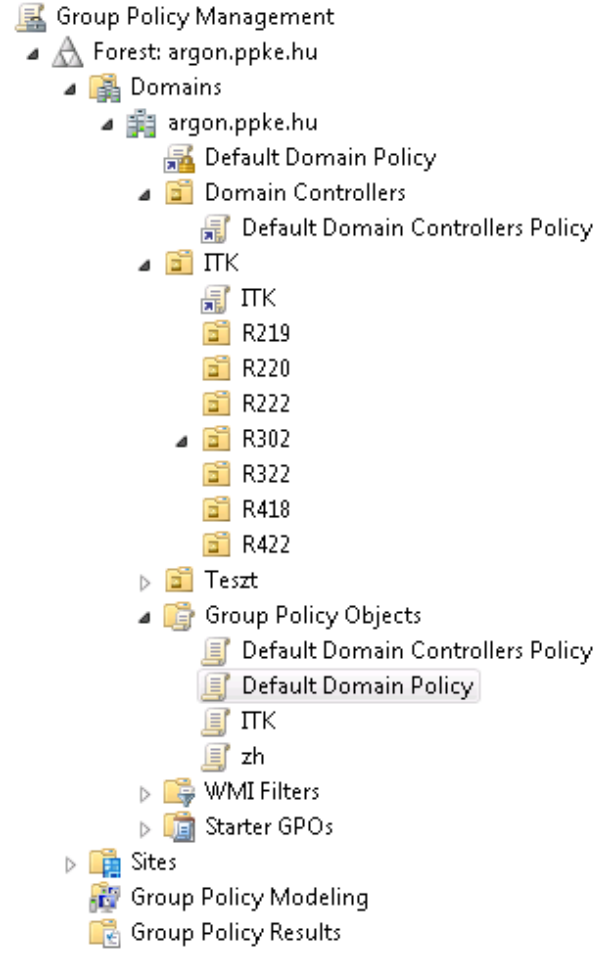
- szkriptelt tömeges user létrehozás
- kötelező jelszóváltás
- első belépéskor létrejött a profil
- a profilok nem kompatibilisek az XP-vel, profilnév.V2
- régi szerverről a user másolja át az adatait

Gépteremek

- imagelő rendszer maradt
- félévenkénti újrahúzás
- beléptetés két körös
  - gépek átnevezése & reboot
  - domain join
- powershell szkriptek

OU/GPO

- három szint
  - argon.ppke.hu → ITK → termek
- default domain policy
  - roaming profile törlése
  - Ctrl-Alt-Del jelszóváltás tiltása
  - sleep tiltása, csodagombok letiltása
- ITK
  - ntp szerver beállítása
- hasznos parancsok
  - `gpupdate`, `rsop.msc`, `gpresult`



Tapasztalatok

- hibernate GPO vs. `powercfg -h off`
- egy körös beléptetés nem megy, feles entry jön létre
- 10000 alatti uidnumber-rel rendelkező userek
- fölhasználói adatbázis, tartalmi hibák
  - egy neptunkód → több user
  - több user → egy uidnumber
- mentés
  - `getfacl & getfattr`

Limitációk

- `samba-tool` patch
- password policy `samba-tool` segítségével
- sysvol replikáció → rsync
- domain trust

Tervek

- dc2.argon.ppke.hu
- többi karon is használjuk
  - RODC & helyi profilszerver
- dolgozói gépek beléptetése
- csoporton belüli delegálás
- upgrade
- Windows 8 teszt
- print server
- NFS4
- stb. . .

Források

- wiki.samba.org
- samba-users levelezőlista
- Active Directory, 5th Edition
  - ISBN: 978-1-4493-2002-7
- Active Directory Cookbook, 4th Edition
  - ISBN: 978-1-4493-6142-6
- Windows PowerShell Cookbook, 3rd Edition
  - ISBN: 978-1-4493-2068-3
- technet.microsoft.com