Active Directory

25 mai 2010

Cuprins

- Integrarea DNS
- Ce înseamnă Active Directory?
- Domain Controller
- Organizational Unit
- Group Policy

Ce este Active Directory

- Brain of a Windows Server Network
- Baza de date ce tine evidenta mai multor date si ofera metode centralizate de a administra toate masinile, utilizatorii si resursele
- Obiecte din baza de date AD

Utilizatori si grupuri

Servicii (ex. Email)

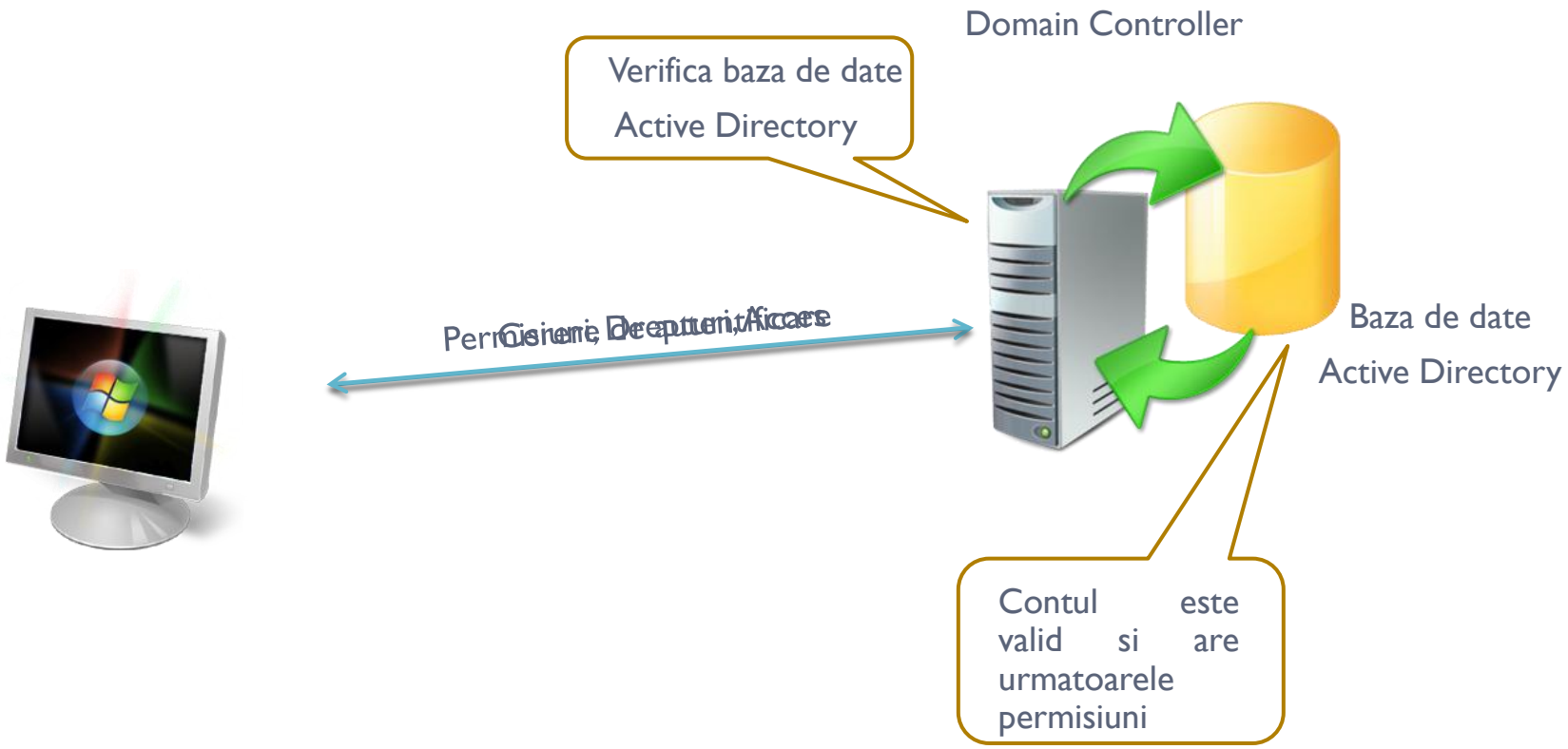
Resurse

(Imprimante, fisiere partajate, etc)

Server Role

- Domain Controller are de obicei 2 roluri:
  - Active Directory Domain Services
  - DNS – Active Directory nu poate functiona fara DNS
- Integrarea DNS cu Active Directory este foarte importanta, nu doar pentru o administrare mai usoara

Cum funcționează?



Domain Controller

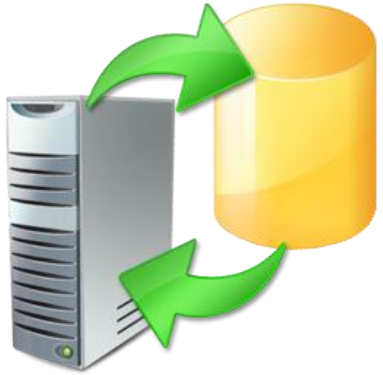
- Windows Server Machine ce rulează Active Directory Domain Services (rol de server)
- Boss of a network
  - Controlează domeniul Active Directory
  - Conține întreaga baza de date Active Directory
- Pot exista mai multe astfel de servere ce au copii ale aceleiasi baze de date Active Directory
  - Își partajează resursele intre ei prin replicare

Domeniu

- Namespace
- Un grup logic de calculatoare ce ruleaza versiuni Windows si partajează o bază de date centrală
- Mașinile conțin in nume denumirea Domeniului de ex. mssr.pub.ro (denumit si sufix) si sunt înregistrate in baza de date AD pentru a putea fi administrate (parte din namespace)

CLIENT1.mssr.pub.ro

CLIENT2.mssr.pub.ro



mssr.pub.ro

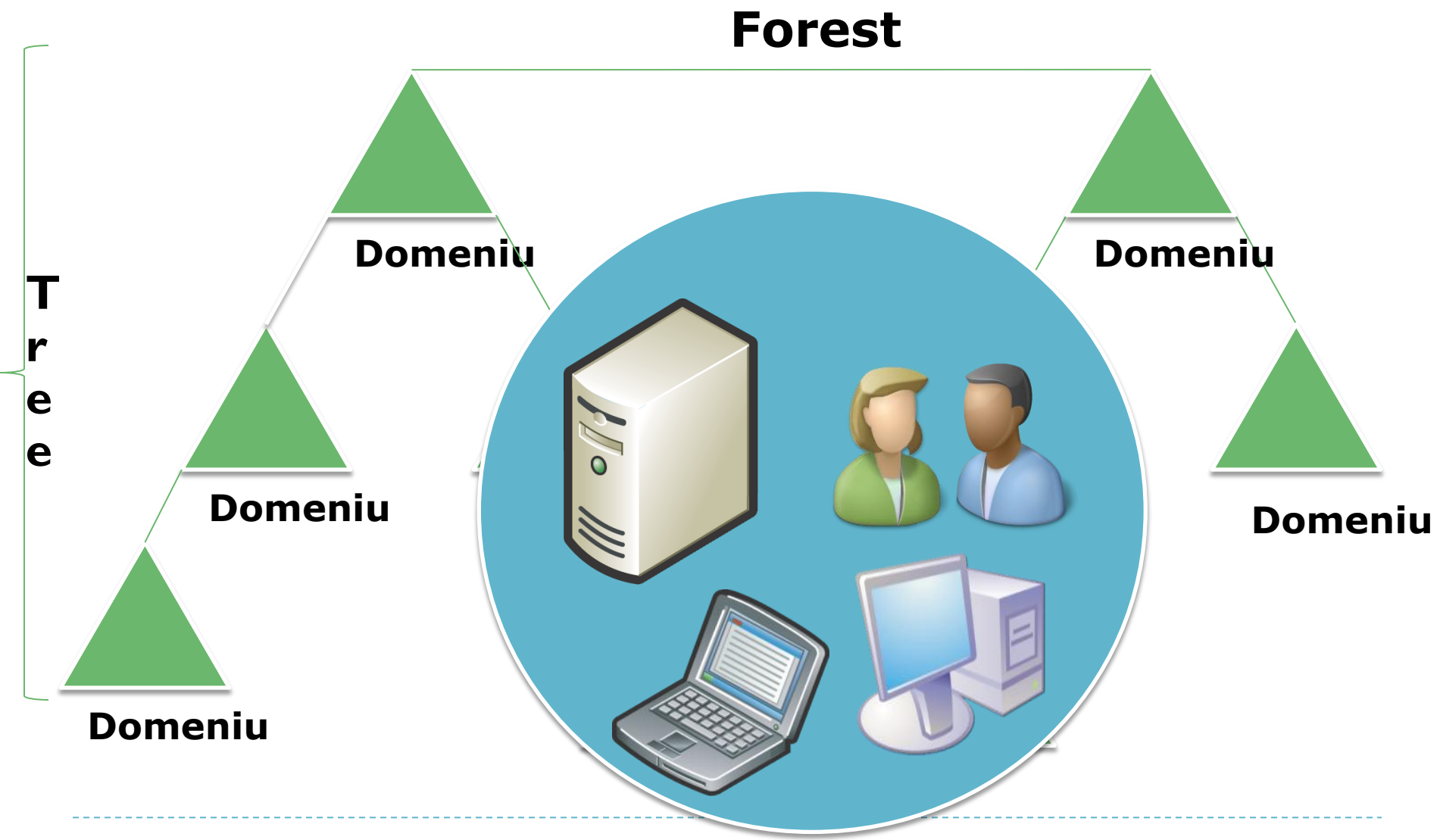
Domain Controller

SRV.mssr.pub.ro

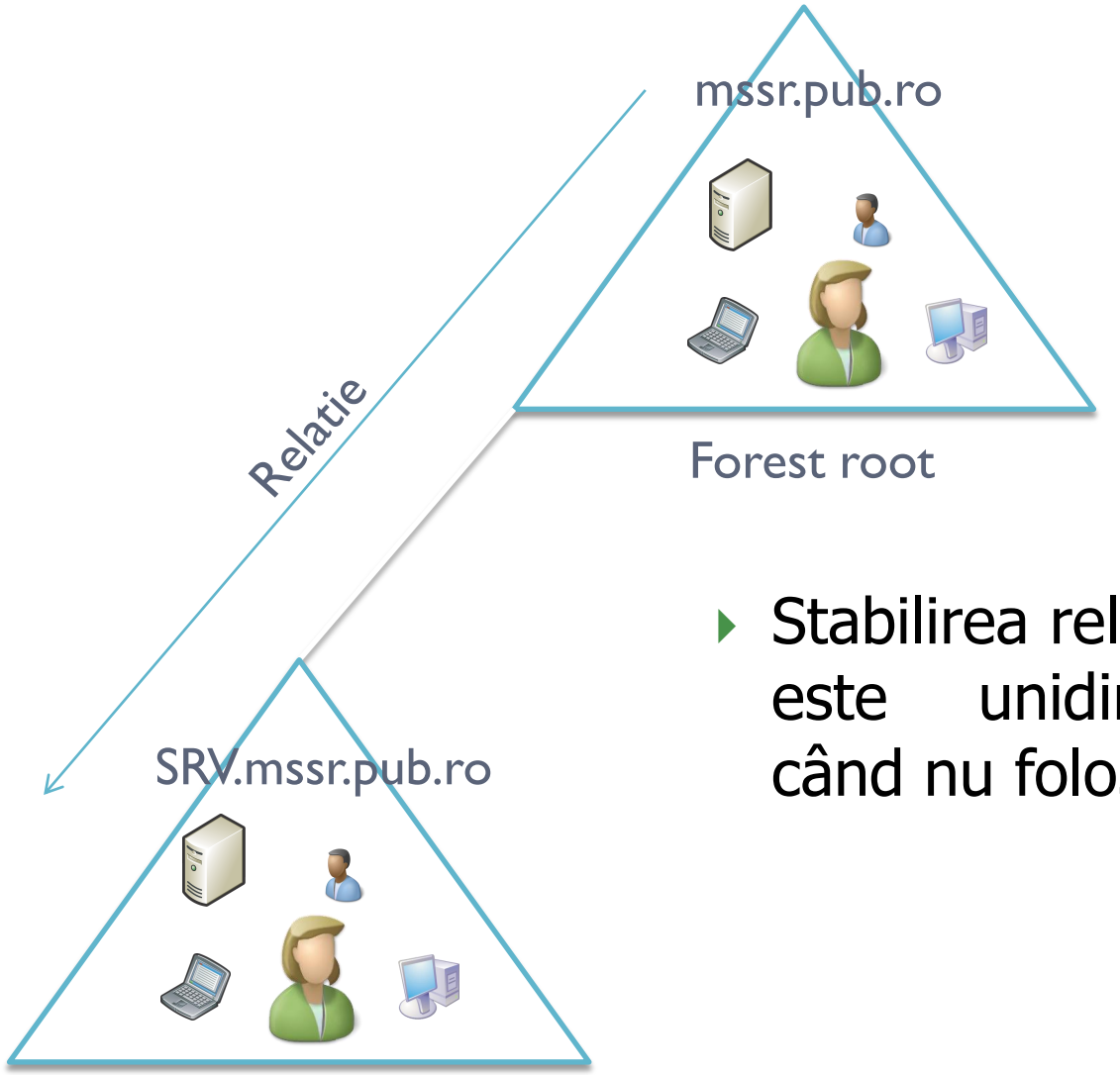
Domenii

- Utilizatorii fac parte din namespace
- Adresa de mail face parte din namespace
  - Ex: student@mssr.pub.ro
  - Email-like logins mai sunt denumite si “User Principle Names” la autentificarea intr-o retea win server

Structura Logică Active Directory



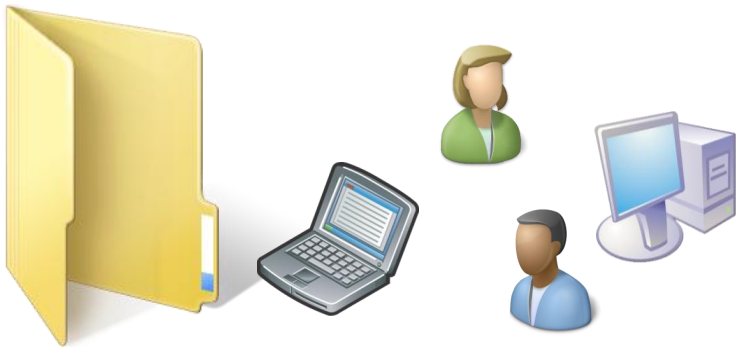
FBB – Forever best buddies



- Stabilirea relațiilor de încredere este unidirecțională atunci când nu folosim un forest

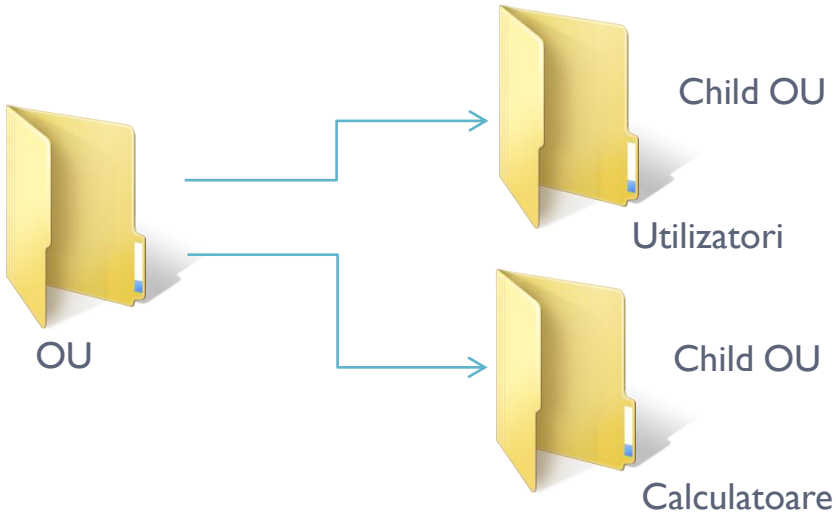
Organizational Unit

- Container pentru Obiecte AD, precum conturi de utilizatori, de calculatoare, grupuri



- Organizeaza Obiectele, dar mai sunt folosite si pentru a decide permisiuni pentru utilizatori
- Pot fi folosite pentru a delega controlul asupra unei sectiuni sub alta administratie

Organizational Unit



- E de preferat ca OU-urile pentru utilizatori si calculatoare sa fie separate
- OU-urile pot fi organizate in functie de:
  - Geografic
  - In functie de departamente, etc
- Remember: KISS!

Adăugarea utilizatorilor

- Command-line option pentru crearea utilizatorilor de la tastatura
  - *dsadd user "cn=Utilizator, ou=NumeOU, dc=Domeniu, dc=Sufix"*
- Exemplu
  - *dsadd user "cn=razvan, ou=profesori, ou=PoliOU, dc=acs, dc=pub.ro"*
- Configurari optionale
  - *dsadd user "cn=razvan, ou=profesori, ou=PoliOU, dc=acs, dc=pub.ro" –fn Razvan –ln Rughinis –pwd R@sv@n –mustchpwd yes*

Evidența calculatoarelor

- Conturile calculatoarelor permit AD sa tina evidenta si sa controleze calculatoarele dintr-o retea – un calculator fara un cont nu poate accesa reteaua
- Conturile calculatoarelor sunt stocate in OU-uri, ceea ce le va permite sa-si instaleze software-uri pe toate masinile dintr-un OU
- Cand un calculator devine membru intr-un domeniu, este automat creat si un cont calculatorului in AD – contul trebuie sa fie mutat in cel mai apropiat OU
- Conturile pot fi create manual – nu este o idee foarte buna

Diferențe între OU și Group

- Conturile din OU nu apartin vreunui grup – grupurile sunt tipuri diferite de obiecte
- OU-urile mentin obiectele organizate si sunt folosite pentru a controla permisiunile utilizatorilor si ale calculatoarelor
- Grupurile sunt Obiecte Active Directory ce controleaza permisiunile resurselor, precum imprimante si directoare
- OU-urile contin grupuri

Organizational unit

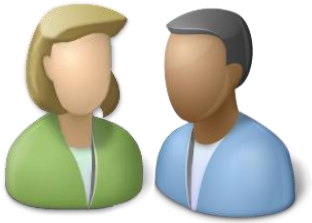
- OU decide ce au voie sau nu sa faca utilizatorii

- Utilizatorii pot:
  - Sa-si salveze fisierele pe desktop
  - Lock/hide taskbar
- Utilizatorii nu au voie sa:
  - Modifice wallpaper-ul desktop-ului
  - Instaleze software

Group

- Grupurile controleaza la ce resurse are acces un utilizator

Imprimanta pt bd



Grupul mssr

Imprimanta pt mssr

Imprimanta pt bd

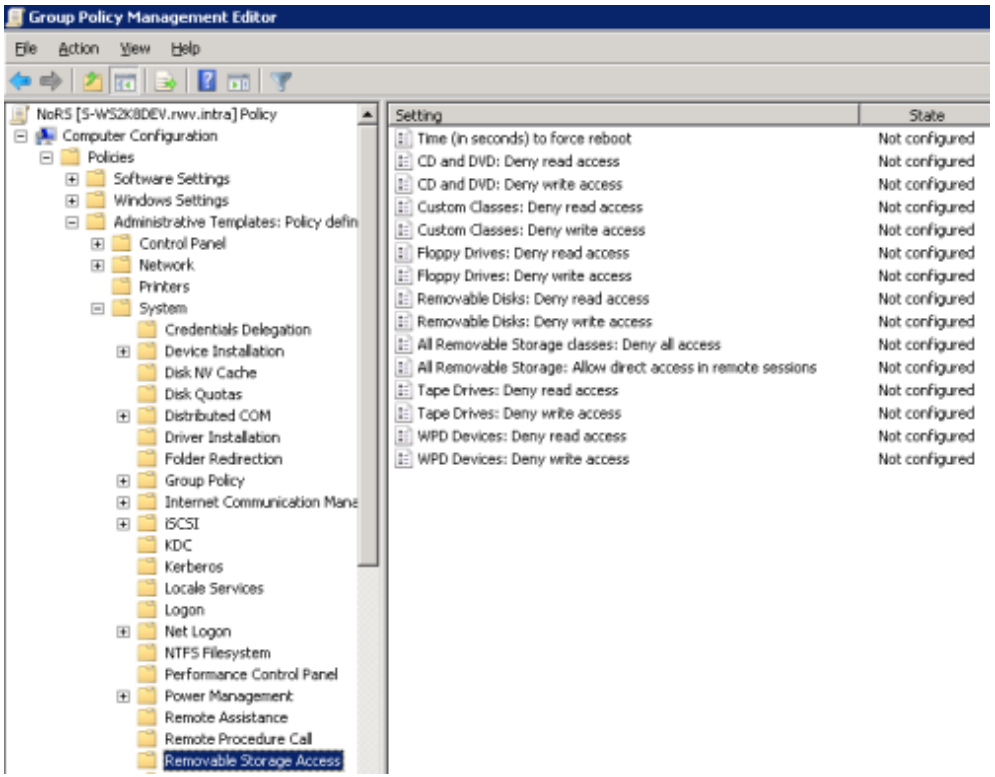
Imprimanta pt mssr

Terminologii OU

- User Account – Obiect Active Directory ce permite accesul utilizatorilor la resursele din retea
- Computer Account – Obiect Active Directory ce permite AD sa aiba o relatie de securitate cu un calculator si sa permita controlul asupra actiunilor calculatorului in retea
- Organizational Unit – Obiect Active Directory ce ofera un spatiu de stocare pentru User Accounts, Computer Accounts, si Grupuri. Mai ofera control asupra actiunilor calculatoarelor si utilizatorilor
- Group – Obiect Active Directory ce permite accesul la resursele dintr-o retea (precum fisiere) pentru utilizatori si calculatoare
- Distinguished Name – numele unui Obiect asa cum apare acesta in baza de date Active Directory

Group Policy Object

- Un GPO conține setări ce oferă control asupra acțiunilor calculatoarelor si utilizatorilor
- Mii de setări diferite pot fi configurate in interiorul fiecărui GPO
- GPO sunt folosite împreună cu containere (Domenii, Site-uri, OU-uri), dar nu se aplica Grupurilor



Local versus Domain

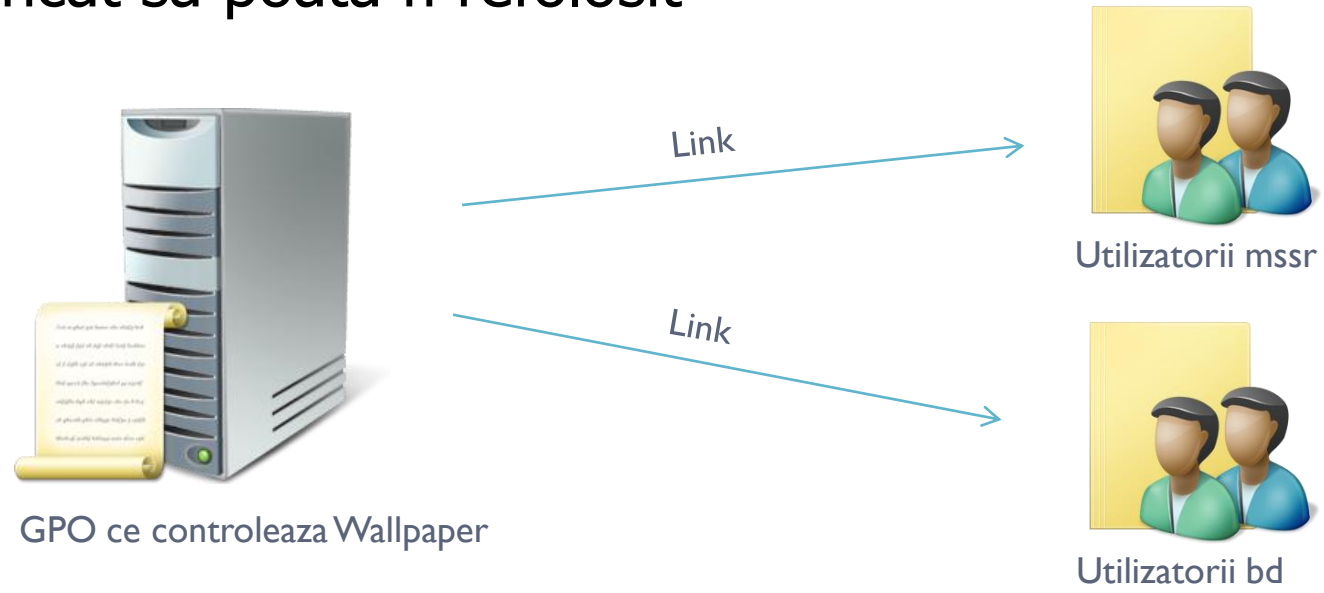
- Orice calculator are un Local Group Policy pentru a restricționa acțiunile acestuia – toate setările sunt îndeplinite manual
- Group Policy din Active Directory administrează controlul central

Fiecare calculator poate fi configurat separat, folosind politici locale..

.. sau poate fi administrat central împreună cu toate celelalte mașini

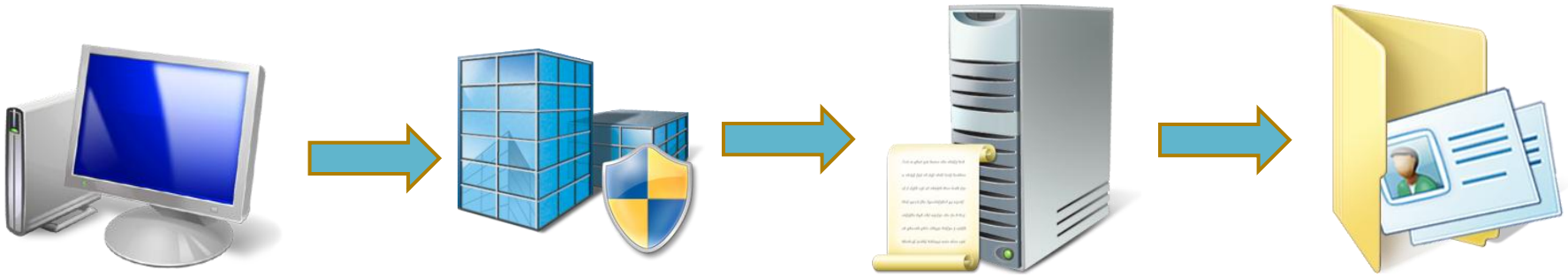
Creating and linking GPO

- Un GPO poate fi creat cu usurinta, dar trebuie sa-l corelam la cel mai apropiat Container (de obicei un OU), inainte de a avea efect asupra utilizatorilor si/sau calculatoarelor
- Un GPO poate fi corelat la mai multe Containere astfel incat sa poata fi refolosit



GPO

- Local Computer Policy -> Site Policy -> Domain Policy -> OU Policy

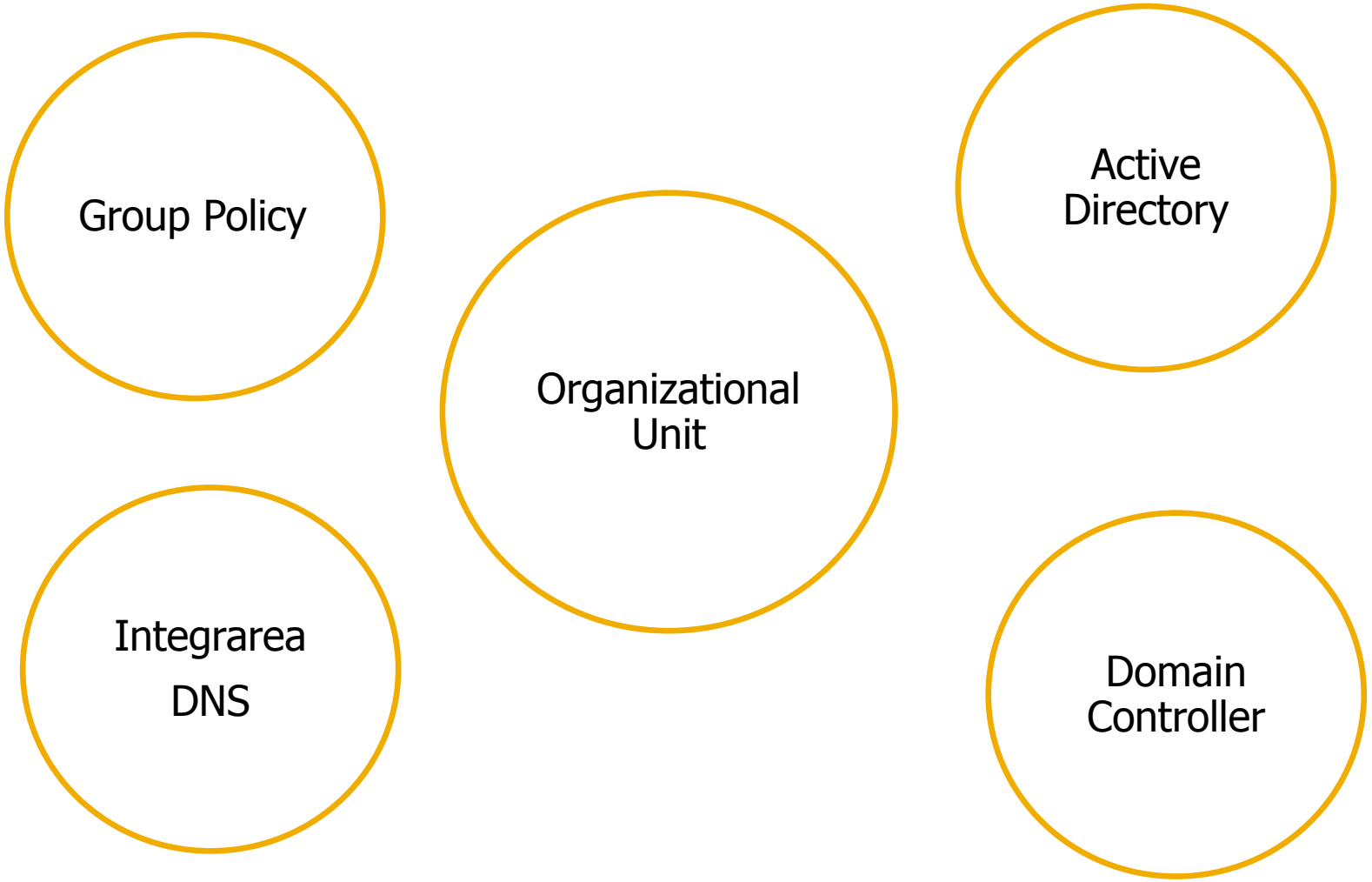


- L-S-D-OU
- Cum se alege:
  - The Last One Wins

Terminologii GPO

- Group Policy Object – Obiect Active Directory ce permite Administratorului sa controleze actiunile utilizatorilor pe un calculator prin Setari sau Politici – GPO
- Link – Obiect Active Directory ce permite unui GPO sa afecteze un Container (un intreg Domeniu sau OU)
- L-S-D-OU – Ordinea de procesare in care sunt aplicate GPO-urile
- GPMC – Group Policy Management Console, unde functioneaza toate politicile de grup
- Local Computer Policy – Politica de grup care se bazeaza pe un calculator local si afecteaza numai acel calculator

Obiective


Group Policy
Active Directory
Organizational Unit
Integrarea DNS
Domain Controller