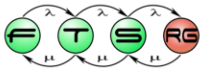
Intelligens rendszerfelügyelet

Active Directory

Micskei Zoltán

http://mit.bme.hu/~micskeiz/



Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

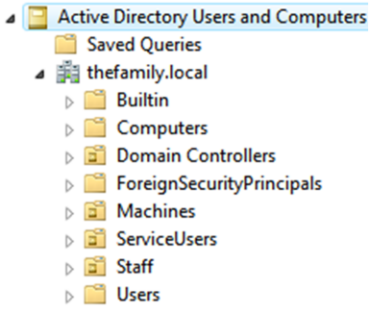
Utolsó módosítás: 2012. 03. 06.

Az előző részek

- Modellezés
- Központosított felhasználókezelés, címtárak
  - LDAP
  - **Active Directory**

Active Directory

- Microsoft címtár implementációja
- Infrastruktúra alapja
  - hitelesítés, menedzsment
  - sok szervertermék és alkalmazás igényli
- Tárolt elemek
  - felhasználók, csoportok
  - gépek, nyomtatók
  - megosztott könyvtárak
  - …



AD címtár szerkezete

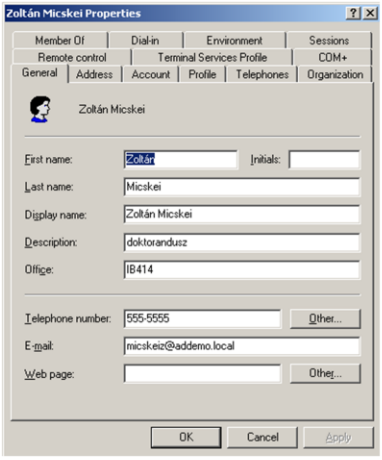
- Fa szerkezet, LDAP címtár (csak el van fedve:)
- Hierarchia eleme: **szervezeti egység** (organizational unit)
- Struktúra kialakításának alapja:
  - Delegálás
  - Házirendek

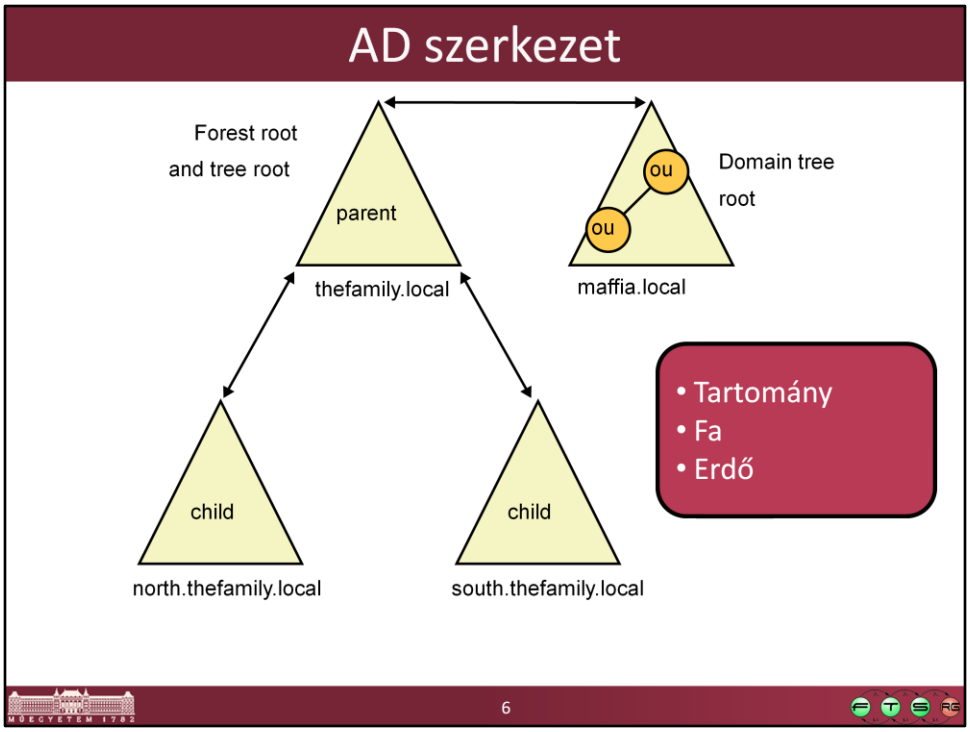
Delegálás: adott részfa menedzselését át tudjuk adni másoknak. Nagy szervezet esetén hasznos ez. A címtár szerkezetét úgy kell kialakítani, hogy egybe tartozó elemek felügyeletét lehessen együtt delegálni.

Házirendek: működést szabályozó beállítások összessége (lásd később). Házirendeket is OU-ra lehet definiálni.

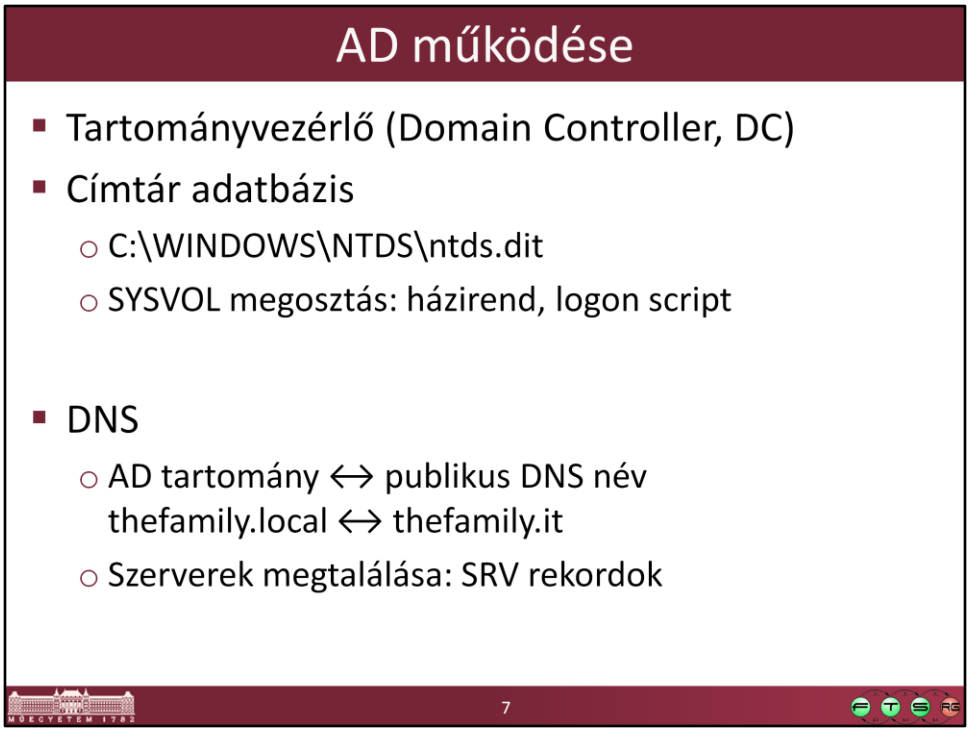
DEMO AD Users and Computers

- fa szerkezet, tárolók és elemek
- felhasználó létrehozása
  - nevek, jelszó opciók
- felhasználó tulajdonságai
  - adatok, címek, profil, dial-in
- csoport
  - jogosultságosztás (RBAC)
  - levélküldés





- Az Active Directory (AD) egysége a tartomány (domain), az ebben lévő elemeket kezeljük közösen.
- A tartományoknak lehetnek gyerek tartományaik (child domain). A szülő felhasználói is elérhetőek a gyerek tartományokban, azonban a két tartomány között a szinkronizálás már szabályozható, így egymástól távoli telephelyeken is lehetnek, amik lassú hálózati kapcsolattal vannak összekötve. Így alakul ki egy fa (tree).
- Az AD legnagyobb egysége az erdő (forest). Egy erdőbe tartozó tartományoknak közös a sémája, van egy közös katalógusok a kereséshez, és a tartományok között kétirányú bizalmi kapcsolatokat (trust) vannak.

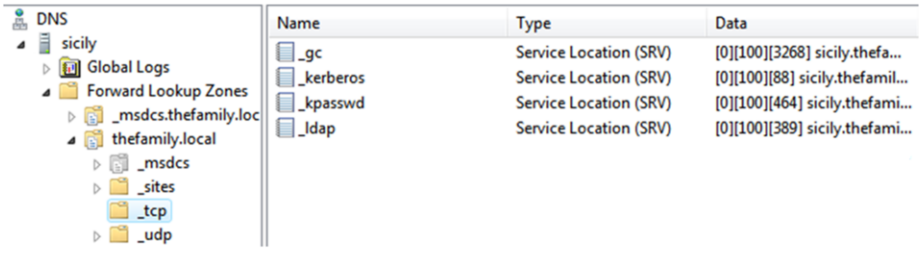


Tartományvezérlő: ezek a gépek tárolják magát a címtárat. Mindegyik tárol egy-egy példányt, és a változásokat egymás között szinkronizálják (úgynevezett multimaster replikáció segítségével, lásd később a hibatűrés előadásokat a félév folyamán).

Fontos, hogy mindig válasszuk szét a belső AD tartomány nevét a külső DNS névtől, erre jó konvenció a .local végződés a belső tartomány DNS nevére.

DEMO AD integrált DNS

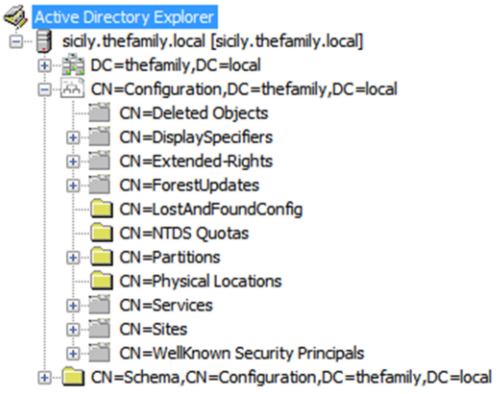
- Forward Lookup Zones
  - A rekordok
  - SRV rekordok
- Reverse Lookup Zones
- Forwarders



Az Active Directory esetén a kliensek ezeknek az SRV rekordoknak a segítségével találják meg, hogy hol találhatóak az egyes szolgáltatások, pl. ki az LDAP szerver.

AD belső felépítése

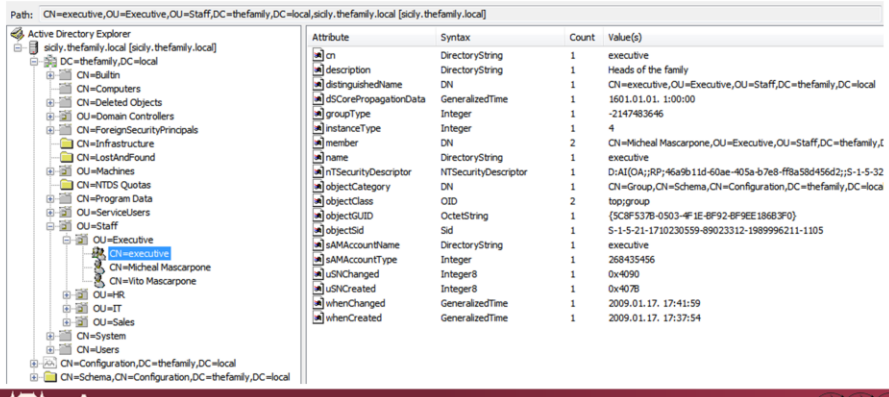
- Partíciók
  - Tartomány
  - Konfiguráció
    - szerverek, telephelyek
  - Séma
    - osztályok, attribútumok
  - Egyéb alkalmazás
- Elem megnevezése
  - CN: common name
  - DC: domain component



Ha megnézzük a sysinternals AD Explorer eszközével, akkor belül ez is egy LDAP címtár.

DEMO Sysinternals AD Explorer

- Elem: belső attribútum nevek
- Configuration
- Séma: pl. User, People, Computer



A képen egy csoportnak az attribútumai láthatóak. Vannak szabványosak, pl. objectClass vagy a cn, és vannak a Windows specifikusak, pl. objectSID, sAMAccountName.

További AD szolgáltatások

- Active Directory Domain Services
  - Címtár, erről volt szó eddig
- Active Directory Rights Management Services
  - DRM megoldás
- Active Directory Federation Services
  - Címtárak összekapcsolása más felhasználókezelővel
- Active Directory Certificate Services
  - Tanúsítványok kiállítása, központi kezelése
- Active Directory Lightweight Directory Services
  - Saját alkalmazásunk adatainak tárolása a címtárban

Tartalom

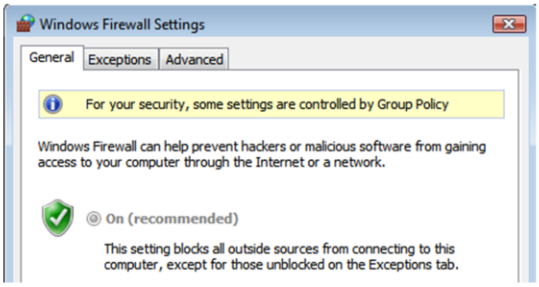
- Az Active Directory felépítése
- **Központosított felügyelet és jogosultságkezelés**
- AD elérése programozottan
- Kitekintés

Központosított jogosultságkezelés

- Egy gépen beállítottam a böngészőt, vírusirtót…
  - Mi lesz a többi 10-zel??
- Megoldás:
  - Kézzel végigmegyek mindegyiken: 1000 gép esetén?
  - Szkript: aktuális állapot, frissítés?
  - Központi tárolás, érvényesítés, lekérdezés

Csoportházirend (Group Policy)

- Windowsos gépek adminisztrálásához alap
- ~3200 beállítás
  - start menü elemei, IE honlap…
- Kötelezően érvényre jutó beállítások
- Helyi rendszergazda nem tudja felülbírálni

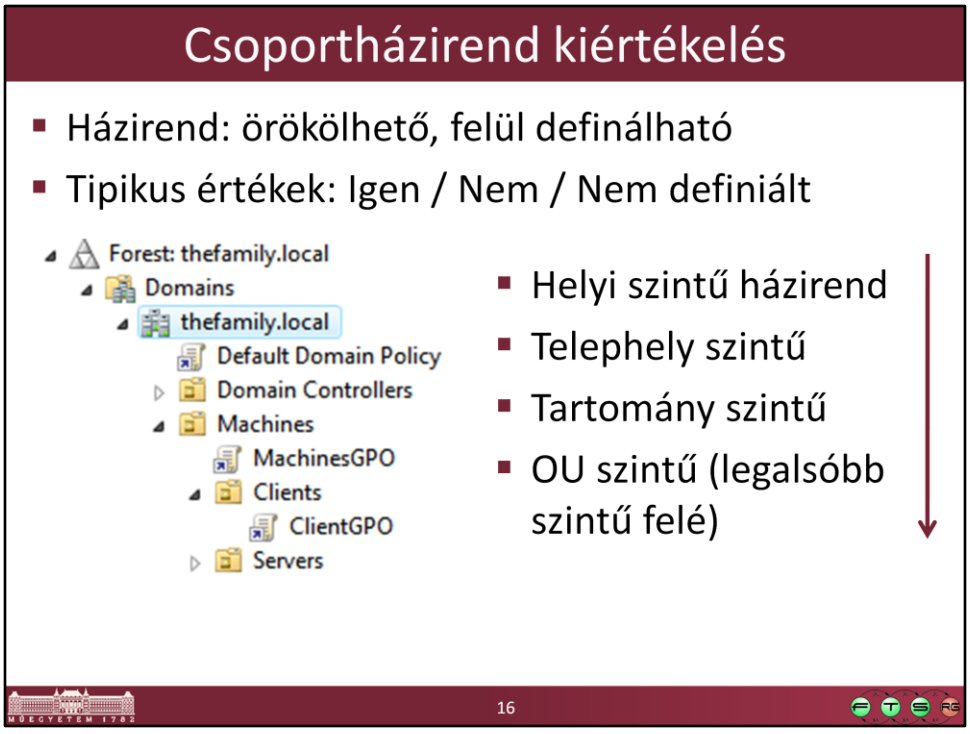


Csoportházirend: olyan technológia, amivel központilag definiálhatunk kötelezően érvényre jutó felhasználó és gép specifikus beállítások tartományi környezetben.

Csoportházirend fajtái

- Számítógép szintű
  - SW telepítés, tűzfal, Windows Update…
- Felhasználó szintű
  - mappa átirányítás, képernyő beállítás, nyomtatók
- Beépített: szoftver telepítés, biztonsági beállítás…
- Felügyeleti sablon (admx fájl): kiegészítések
- Policy vs. Preferences (Server 2008 óta)

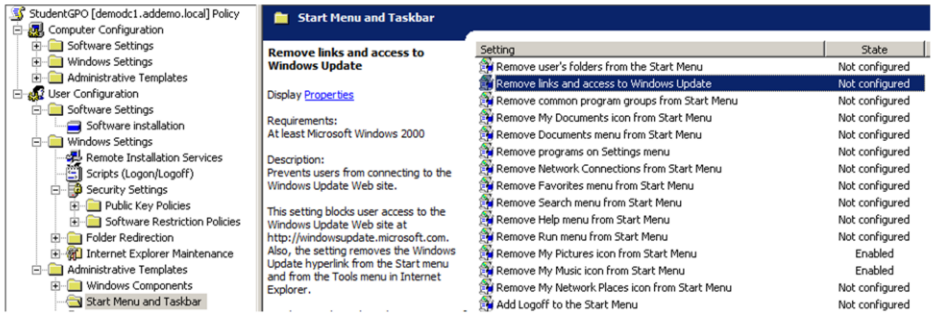
A Policy részben kötelezően érvényre jutó beállítások vannak, a Preferences részben olyan beállítások vannak, amit a felhasználó később felül tud definiálni.



Ha egy adott beállítást több helyen is definiálunk, és azok értéke ütközik egymással, akkor mindig a legspecifikusabb jut érvényre. Például nézzünk egy olyan számítógépet, ami benne van a Clients OU-ban. A „komplex jelszó használata kötelező” beállítás NEM értékre van állítva a helyi házirend szintjén, és NEM DEFINIÁLT értékű az alapértelmezett tartományi házirendben. Ilyenkor, bár a tartományi beállításnak nagyobb a prioritása, de mivel annál nem definiált érték van megadva, ezért a helyi jut érvényre. Ha viszont a MachinesGPO-ban is meg van adva (NEM), és a ClientGPO-ban is (IGEN), akkor a helyi beállítást figyelmen kívül hagyja, és az adott géphez legközelebb eső OU beállítása jut érvényre (tehát a ClientGPO IGEN értéke).

DEMO Csoportházirend

- Group Policy Management Console
  - szerkesztés
  - eredő házirend
- Group Policy Settings Reference XLS



Group Policy Settings Reference for Windows and Windows Server
http://www.microsoft.com/downloads/details.aspx?FamilyID=18c90c80-8b0a-4906-a4f5-ff24cc2030fb&displaylang=en

DEMO Csoportházirend

- Group Policy Management Console
  - Keresés (Angol billentyűzetkiosztás legyen!)
- Beállítások:
  - Számítógép szintű: tűzfal bekapcsolása (helyi gépről nem kapcsolható ki)
  - Felhasználó: profil méretének korlátozása
- Frissítés:
  - `gpupdate /force`

Saját GP készítése

- Csoportházirend: XML leíró (ADMX fájl)

```
<policy name="NoAutoUpdate" class="User"
  key="Software\Microsoft\Windows\CurrentVersion\Policies\Exp
  lorer" valueName="NoAutoUpdate">
      <enabledValue><decimal value="1" /></enabledValue>
</policy>
```

- Saját alkalmazásunkhoz is készíthető ilyen
  - Nagyvállalati környezetben erősen ajánlott
- Pl. Lenovo System Update Administrator Tools

Felügyeleti sablonok helye: C:\Windows\PolicyDefinitions

A háttérben a csoportházirendek registry beállítások. Készíthetőek olyan felügyeleti sablon fájlok, amik ezeknek a registry beállításoknak a megadását vezetik ki a csoportházirend felületre.

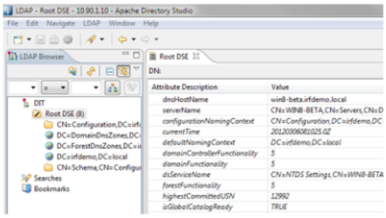
Példa külső csoportházirend: Lenovo System Update Administrator Tools, http://support.lenovo.com/en_US/detail.page?LegacyDocID=TVAN-ADMIN#tvsu

Tartalom

- Az Active Directory felépítése
- Központosított felügyelet és jogosultságkezelés
- **AD elérése programozottan**
- Kitekintés

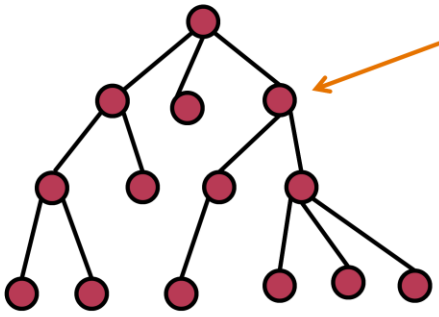
AD elérése programozottan

- `ds*` parancsok (pl. `dsadd`, `dsquery`)
  - Egyszerű műveletek
- Tetszőleges LDAP kliens
  - Pl. Java-s kliensek is



- .NET kódból
  - `System.DirectoryServices` névtér osztályai
- PowerShell
  - AD Service Interface (ADSI)
  - Active Directory module (Windows Server 2008 R2)

Keresés LDAP címtárban

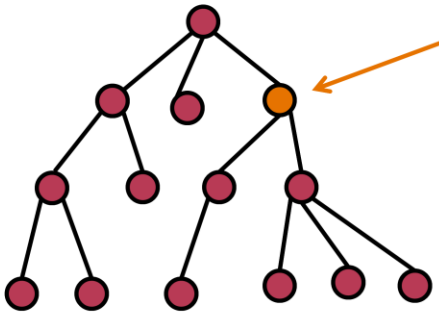


SearchRoot: honnan

PageSize: hány elemet

Scope:
- Base: csak az az egy elem
- OneLevel: gyerek közt
- Subtree: teljes részfa

Keresés LDAP címtárban

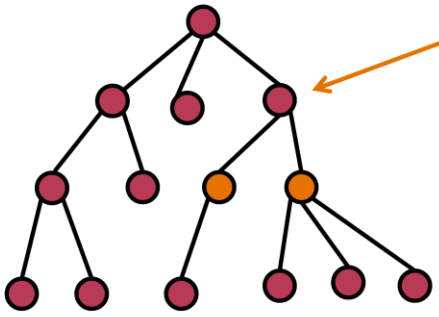


SearchRoot: honnan

PageSize: hány elemet

Scope: mik között
- Base: csak az az egy elem
- OneLevel: gyerek közt
- Subtree: teljes részfa

Keresés LDAP címtárban

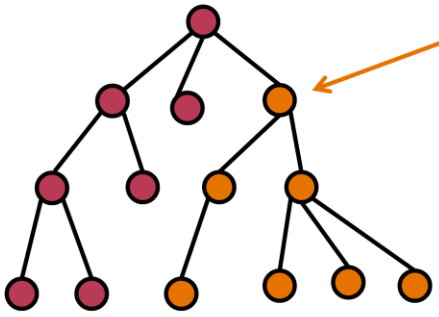


SearchRoot: honnan

PageSize: hány elemet

Scope: mik között
- Base: csak az az egy elem
- OneLevel: gyerek közt
- Subtree: teljes részfa

Keresés LDAP címtárban

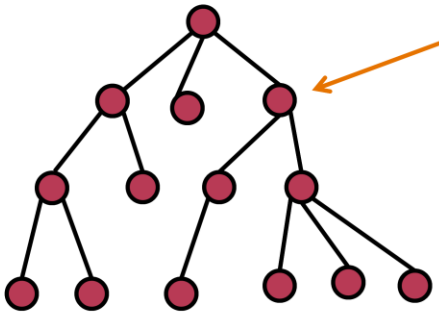


SearchRoot: honnan

PageSize: hány elemet

Scope: mik között
- Base: csak az az egy elem
- OneLevel: gyerek közt
- Subtree: teljes részfa

Keresés LDAP címtárban



SearchRoot: honnan

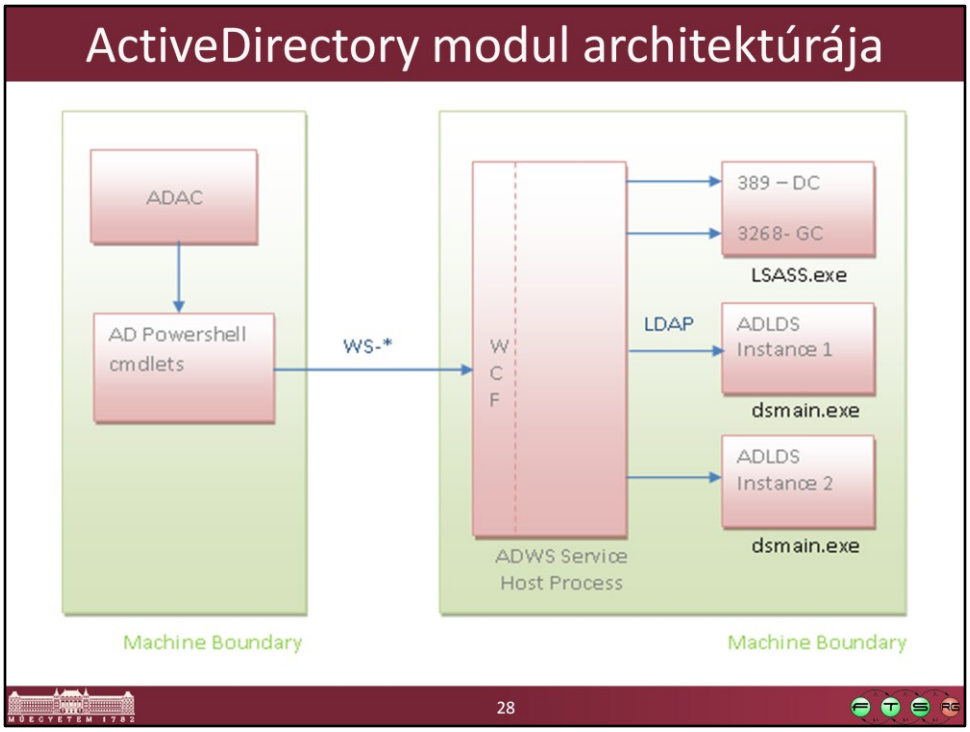
PageSize: hány elemet

Scope: mik között
- Base: csak az az egy elem
- OneLevel: gyerek közt
- Subtree: teljes részfa

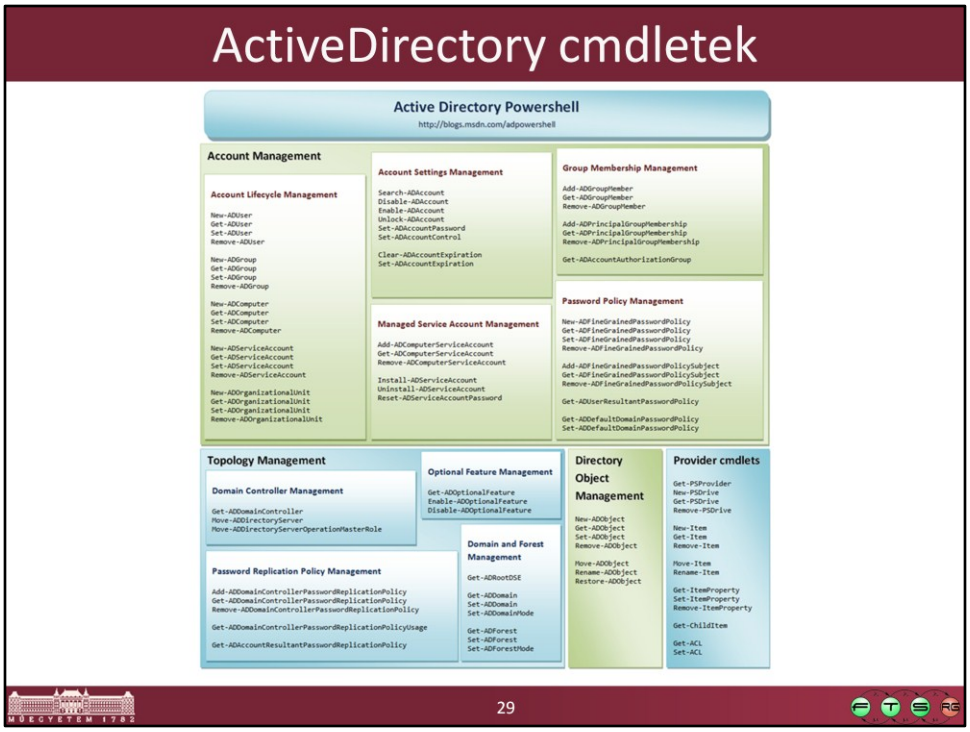
Filter: mit keresünk

ActiveDirectory module for PowerShell

- Windows Server 2008 R2-ban megjelent:
  - ActiveDirectory modul PowerShellhez
  - (Elérhető régebbi verziókhoz is részben)
- Natív PowerShell cmdletek AD-hez (76 db)
- AD Provider
  - AD: meghajtón keresztül elérhető a címtár



Forrás: Active Directory PowerShell Blog. „Active Directory Web Services Overview”, 6 Apr 2009, elérhető online: http://blogs.msdn.com/b/adpowershell/archive/2009/04/06/active-directory-web-services-overview.aspx



Kép forrása: Active Directory PowerShell Blog. „Active Directory PowerShell Overview”, 4 Mar 2009, elérhető online: http://blogs.msdn.com/b/adpowershell/archive/2009/03/05/active-directory-powershell-overview.aspx

Néhány példa cmdlet: Get-ADUser, Get-ADGroup, New-ADUser, New-ADOrganizationalUnit, Set-ADAccountPassword, Set-ADObject, Search-ADAccount

DEMO AD module for PowerShell

- AD Provider használata:

```
cd AD:
cd "DC=irfhf,DC=local"
```

- Keresés:

```
Get-ADGroup -Filter 'CN -like "e*"' -SearchScope Subtree
-SearchBase "OU=People,DC=irfhf,DC=local" | % {echo
"Name: $($_.name), DN: $($_.DistinguishedName)"}
```

- Lásd még:
  - Get-Help about_ActiveDirectory*

Példák:

Import-Module ActiveDirectory
cd AD:
ls
cd '.\dc=irfdemo,dc=local'
ls -Recurese .\OU=People
ls -Recurse .\ou=people | ? { $_.objectClass -eq "group" }

Get-Command -Module ActiveDirectory

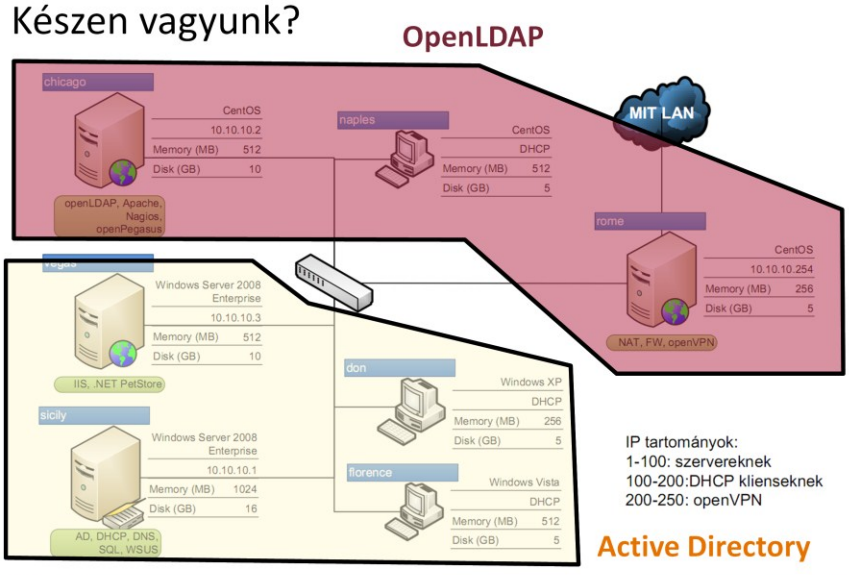
Get-ADUser -filter 'name -like "m*" '

Tartalom

- Az Active Directory felépítése
- Központosított felügyelet és jogosultságkezelés
- AD elérése programozottan
- **Kitekintés**

Kitekintés

- Készen vagyunk?



Identity management

- Több, különböző felhasználói siló jött létre
- Megoldások
  - Címtárak szinkronizációja
  - Metacímtár
  - Identity mgmt rendszer
  - …
- További feladatok:
  - Munkafolyamatok: új alkalmazott, elbocsátás…
  - Jelentések készítése, elemzések

Összefoglalás

- Active Directory
  - Windows alapú IT rendszer lelke
  - Kötelező ismerni vállalati környezetben
- Csoportházirend
  - Központi felügyelet és jogosultság kezelés
- Sokféle API az AD kezelésére
- Felhasználókezelés:
  - Címtár: OK ✓
  - Identity management: még csak most kezdődne…

- Gál Tamás, Szabó Levente, Szerényi László. „Rendszerfelügyelet rendszergazdáknak”. Szak Kiadó, 2007., elérhető online: https://technetklub.hu/Downloads/Browser.aspx?shareid=1&path=PDF

- Gál Tamás: Windows Server 2008 R2 – A kihívás állandó, JOS, 2011., elérhető online: https://technetklub.hu/Downloads/Browser.aspx?shareid=1&path=PDF/E-Book+-+Windows+Server+2008+R2+-+A+kih%C3%ADv%C3%A1s+%C3%A1lland%C3%B3

- Active Directory Powershell Blog, http://blogs.msdn.com/b/adpowershell/

- Soós Tibor, „Microsoft PowerShell 2.0 rendszergazdáknak – elmélet és gyakorlat”, Microsoft Magyarország, 2010., elérhető online: https://technetklub.hu/Downloads/Browser.aspx?shareid=1&path=PDF

PowerShell + ADSI

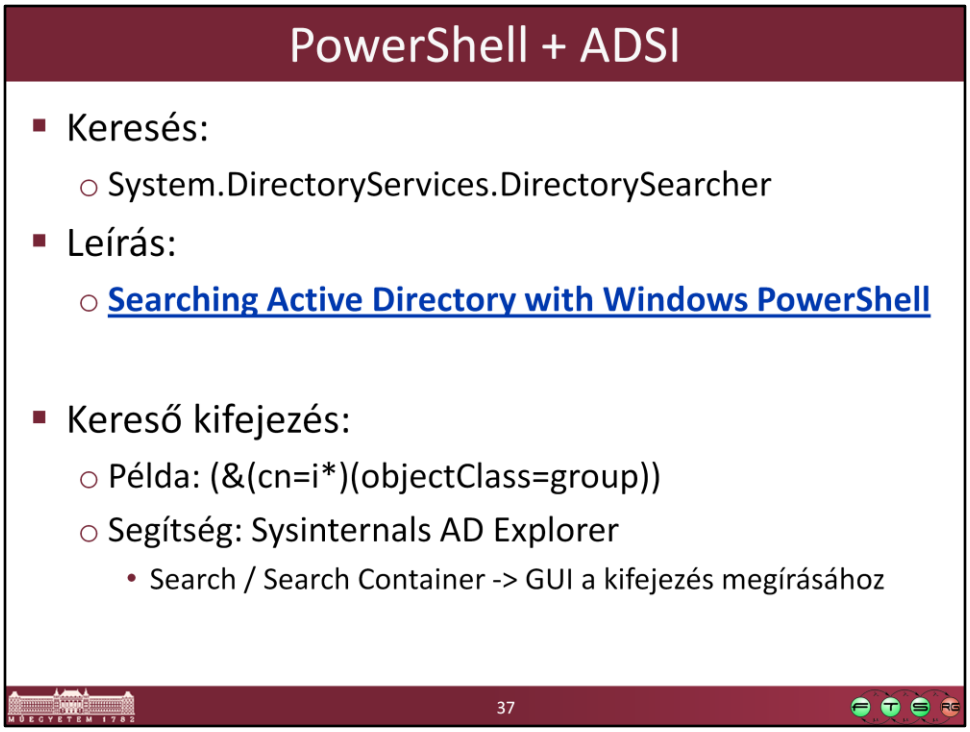
- LDAP objektum lekérése:

```
PS C:\> $root = [ADSI]"" # binds to default domain
PS C:\> $root
   distinguishedName : {DC=thefamily,DC=local}
   Path              : LDAP://dc=thefamily,dc=local
   …
```

- Objektum módosítása:

```
$don = [ADSI]"LDAP://CN=Vito Mascarpone,OU=Executive,
   OU=Staff,DC=thefamily,DC=local"
$don.Description = "the Don of the family"
$don.SetInfo()
```

- Bevezető: Working with Active Directory



A fenti cikk nagyon részletesen leírja, hogy hogyan kell keresni AD-ban PowerShellből.

Bonyolultabb keresőkifejezés előállításához pedig az AD Explorer tényleg jó segítség.

DEMO Keresés az AD-ben (ADSI)

```
$strFilter = "(&(cn=i*)(objectClass=group))"

$objDomain = [ADSI]"LDAP://DC=thefamily,DC=local"
# create searcher, set search properties
$objSearcher = New-Object System.DirectoryServices.DirectorySearcher
$objSearcher.SearchRoot = $objDomain
$objSearcher.PageSize = 1000
$objSearcher.Filter = $strFilter
$objSearcher.SearchScope = "Subtree"

# property name should be lower case!
$colProplist = "name", "distinguishedname"
$colPropList | % {$objSearcher.PropertiesToLoad.Add($_) > $null}

# search for matching entries in the LDAP
$colResults = $objSearcher.FindAll()

# write out results
$colResults | % {echo "Name: $($_.Properties.name), DN:
   $($_.Properties.distinguishedname)" }
```