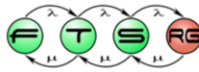


# Active Directory

Micskei Zoltán

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



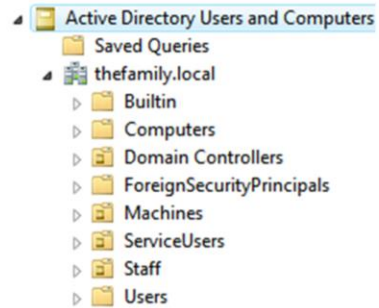
Utolsó módosítás: 2014. 03. 17.

## Az előző részek

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

# Active Directory (AD)

- 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

Zoltán Micskei Properties

Member Of: Dial-in Environment Sessions  
Remote control Terminal Services Profile CDM+  
General Address Account Profile Telephones Organization

Zoltán Micskei

First name: Zoltán Initials:

Last name: Micskei

Display name: Zoltán Micskei

Description: doktorandusz

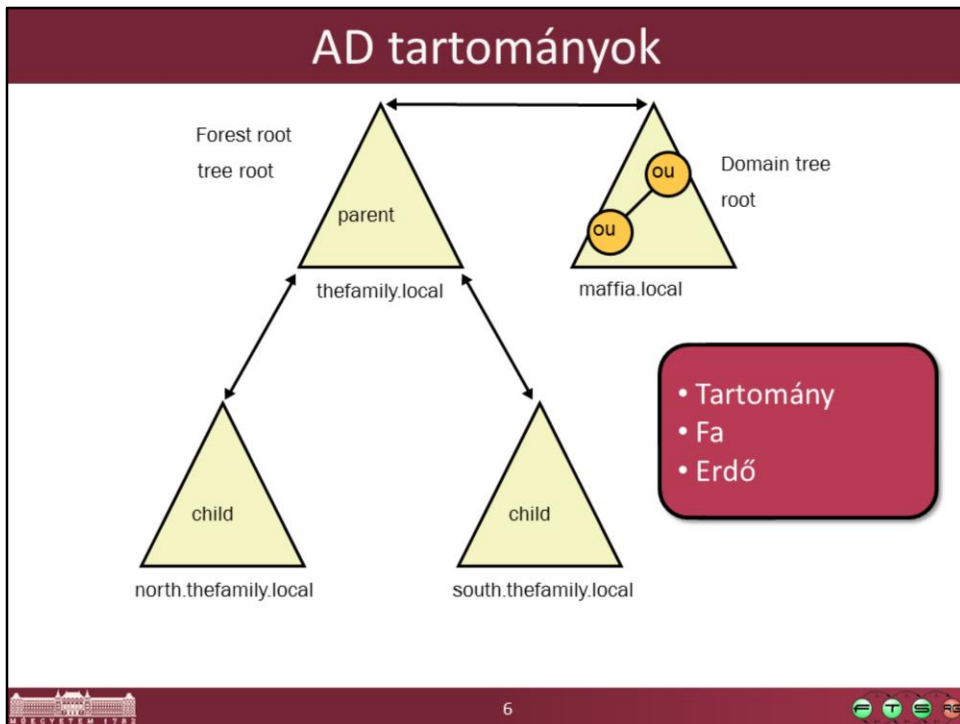
Office: IB414

Telephone number: 555-5555 Other...

E-mail: micskeiz@addemo.local

Web page: Other...

OK Cancel Apply



Az Active Directory (AD) egysége a tartomány (domain), az ebben lévő elemeket kezeljük közösen. A tartományon belül vannak az eddig megnézett elemek (felhasználók, szervezeti egységek...).

Van ezen kívül egy magasabb szintű szervezeti csoportosítás:

- 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.

## AD működése

- **Tartományvezérlő (Domain Controller, DC)**
- **Címtár adatbázis**
  - C:\WINDOWS\NTDS\ntds.dit
  - SYSVOL megosztás: házirend, logon script
  
- **DNS**
  - AD tartomány ↔ publikus DNS név  
thefamily.local ↔ thefamily.it
  - Szerverek megtalálása: SRV rekordok

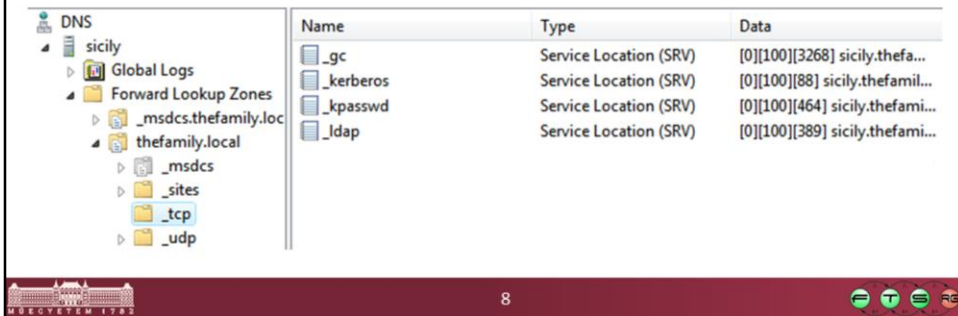


Tartományvezérlő: ezek a gépek tárolják magát a címtárat. Mindegyik tárol egy-egy példányt, és a változásokat egymás között szinkronizálják (úgynevezett multimaster replikáció segítségével, lásd később a fürtözés előadást a félév folyamán).

Fontos, hogy mindig válasszuk szét Active Directory esetén a belső AD tartomány nevét a külső DNS névtől, erre jó konvenció a .local végződés a belső tartomány DNS nevére (tipikusan egy Windows infrastruktúrában nem szeretnénk a tartományvezérlőt publikusan elérhetővé tenni).

## DEMO AD integrált DNS

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



The screenshot shows the Windows DNS console. The left pane displays the hierarchy: DNS > sicily > Forward Lookup Zones > thefamily.local. The right pane shows a list of SRV records for this zone.

Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268] sicily.thefa...
_kerberos	Service Location (SRV)	[0][100][88] sicily.thefamil...
_kpasswd	Service Location (SRV)	[0][100][464] sicily.thefami...
_ldap	Service Location (SRV)	[0][100][389] sicily.thefami...

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.



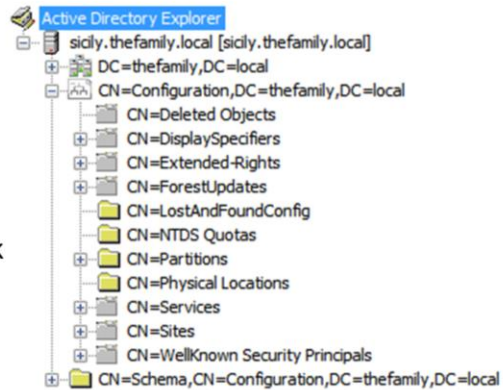
# AD belső felépítése

## ■ Partíciók

- Tartomány
- Konfiguráció
  - szerverek, telephelyek
- Séma
  - osztályok, attribútumok
- Egyéb alkalmazás

## ■ Gyakori attribútumok

- CN: common name
- DC: domain component



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

# DEMO Sysinternals AD Explorer

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

The screenshot shows the Sysinternals AD Explorer interface. The left pane displays a tree view of the Active Directory structure, with the path `CN=executive,OU=Executive,OU=Staff,DC=thefamily,DC=local,sicly.thefamily.local` selected. The right pane shows a table of attributes for this object.

Attribute	Syntax	Count	Value(s)
cn	DirectoryString	1	executive
description	DirectoryString	1	Heads of the family
distinguishedName	DN	1	CN=executive,OU=Executive,OU=Staff,DC=thefamily,DC=local
dsCorePropagationData	GeneralizedTime	1	160.1.0.1.0.1. 1:00:00
groupType	Integer	1	-2147483646
instanceType	Integer	1	4
member	DN	2	CN=Michael Mascarpone,OU=Executive,OU=Staff,DC=thefamily,DC=local
name	DirectoryString	1	executive
NTSecurityDescriptor	NTSecurityDescriptor	1	D:[DA]([RP]:46a9b11d-60ae-405a-b7e8-ffba58d456d2);S-1-5-32
objectCategory	DN	1	CN=Group,CN=Schema,CN=Configuration,DC=thefamily,DC=local
objectClass	OID	2	topgroup
objectGUID	OctetString	1	{5C8F537B-0503-4F1E-8F92-8F9EE18683F0}
objectSid	Sid	1	S-1-5-21-1710230559-89023312-1989996211-1105
sAMAccountName	DirectoryString	1	executive
sAMAccountType	Integer	1	268435456
uSNCreated	Integer8	1	0x4090
uSNChanged	Integer8	1	0x407B
whenCreated	GeneralizedTime	1	2009.01.17. 17:41:59
whenChanged	GeneralizedTime	1	2009.01.17. 17:37:54

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

## Csoportházi rend (Group Policy)

- Windowsos gépek adminisztrálásához alap
- ~3500 beállítás
  - start menü elemei, IE honlap...
- Kötelezően érvényre jutó beállítások
- Helyi rendszergazda nem tudja felülbírálni



*Csoportházi rend*: olyan technológia, amivel központilag definiálhatunk kötelezően érvényre jutó felhasználó és gépspecifikus beállítások tartományi környezetben.

## Csoportházirend fajtái

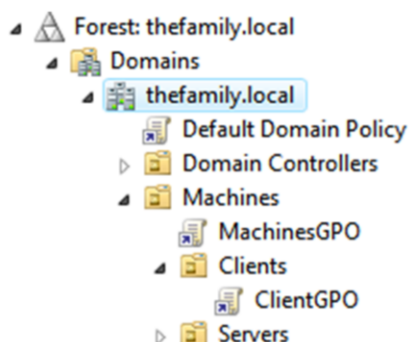
- Számítógép szintű
  - SW telepítés, tűzfal, Windows Update...
- Felhasználó szintű
  - mappa átirányítás, képernyő beállítás, nyomtatók
- Beépített: szoftver telepítés, biztonsági beállítás...
- Felügyeleti sablon (admx fájl): kiegészítések
- Policy vs. Preferences (Server 2008 óta)



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

## Csoportházi rend kiértékelés

- Házi rend: örökölhető, felül definiálható
- Tipikus értékek: Igen / Nem / Nem definiált



- Helyi szintű házi rend
- Telephely szintű
- Tartomány szintű
- OU szintű (legsőbb szintű felé)



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 házi rend szintjén, és NEM DEFINIÁLT értékű az alapértelmezett tartományi házi rendben. 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

The screenshot displays the Group Policy Management Console for a 'StudentGPO [demodc1.addemo.local] Policy'. The left pane shows the tree structure with 'Start Menu and Taskbar' selected. The right pane shows the 'Remove links and access to Windows Update' policy, which is currently 'Not configured'. Below the policy name, there is a 'Requirements' section stating 'At least Microsoft Windows 2000' and a 'Description' section explaining that the setting blocks user access to the Windows Update Web site at <http://windowsupdate.microsoft.com>. The main area of the console lists various settings with their current states:

Setting	State
Remove user's folders from the Start Menu	Not configured
Remove links and access to Windows Update	Not configured
Remove common program groups from Start Menu	Not configured
Remove My Documents icon from Start Menu	Not configured
Remove Documents menu from Start Menu	Not configured
Remove programs on Settings menu	Not configured
Remove Network Connections from Start Menu	Not configured
Remove Favorites menu from Start Menu	Not configured
Remove Search menu from Start Menu	Not configured
Remove Help menu from Start Menu	Not configured
Remove Run menu from Start Menu	Not configured
Remove My Pictures icon from Start Menu	Enabled
Remove My Music icon from Start Menu	Enabled
Remove My Network Places icon from Start Menu	Not configured
Add Logoff to the Start Menu	Not configured

**Group Policy Settings Reference for Windows and Windows Server**  
<http://www.microsoft.com/en-us/download/details.aspx?id=25250>

## 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

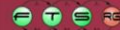
- Csoportházi rend: XML leíró (ADMX fájl)

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

- Saját alkalmazásunkhoz is készíthető ilyen
  - Nagyvállalati környezetben erősen ajánlott
- Pl. [Lenovo System Update Administrator Tools](#)



19



Felügyeleti sablonok helye: C:\Windows\PolicyDefinitions

A háttérben a csoportházi rendek registry beállítások. Készíthetők olyan felügyeleti sablon fájlok, amik ezeknek a registry beállításoknak a megadását vezetik ki a csoportházi rend felületre.

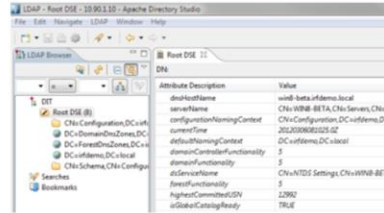
Példa külső csoportházi rend: Lenovo System Update Administrator Tools,  
[http://support.lenovo.com/en\\_US/detail.page?LegacyDocID=TVAN-ADMIN#tvsu](http://support.lenovo.com/en_US/detail.page?LegacyDocID=TVAN-ADMIN#tvsu)

# Tartalom

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

# AD elérése programozottan

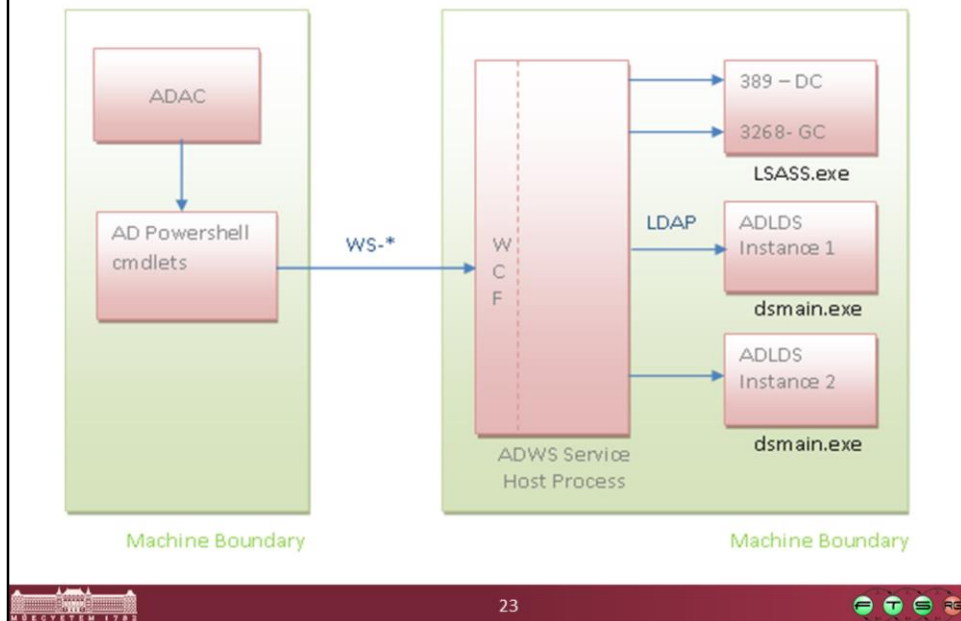
- **ds\* parancsok (pl. dsadd, dsquery)**
  - Egyszerű műveletek
- **Tetszőleges LDAP kliens**
  - Pl. Java-s kliensek is
- **.NET kódból**
  - System.DirectoryServices névtér osztályai
- **PowerShell**
  - AD Service Interface (ADSI)
  - Active Directory module (Windows Server 2008 R2)



## ActiveDirectory module for PowerShell

- Windows Server 2008 R2-ban megjelent:
  - ActiveDirectory modul PowerShellhez
  
- Natív PowerShell cmdletek AD-hez (147 db)
  
- AD Provider
  - AD: meghajtón keresztül elérhető a címtár

# ActiveDirectory modul architektúrája



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>

# ActiveDirectory cmdletek

**Active Directory Powershell**  
<http://blogs.msdn.com/adpowershell>

<b>Account Management</b> <b>Account Lifecycle Management</b> New-ADUser Get-ADUser Set-ADUser Remove-ADUser New-ADGroup Get-ADGroup Set-ADGroup Remove-ADGroup New-ADComputer Get-ADComputer Set-ADComputer Remove-ADComputer New-ADServiceAccount Get-ADServiceAccount Set-ADServiceAccount Remove-ADServiceAccount New-ADOrganizationalUnit Get-ADOrganizationalUnit Set-ADOrganizationalUnit Remove-ADOrganizationalUnit	<b>Account Settings Management</b> Search-ADAccount Disable-ADAccount Enable-ADAccount Unlock-ADAccount Set-ADAccountPassword Set-ADAccountControl Clear-ADAccountExpiration Set-ADAccountExpiration <b>Managed Service Account Management</b> Add-ADComputerServiceAccount Get-ADComputerServiceAccount Remove-ADComputerServiceAccount Install-ADServiceAccount Uninstall-ADServiceAccount Reset-ADServiceAccountPassword Get-ADUserResultantPasswordPolicy Get-ADDefaultDomainPasswordPolicy Set-ADDefaultDomainPasswordPolicy	<b>Group Membership Management</b> Add-ADGroupMember Get-ADGroupMember Remove-ADGroupMember Add-ADPrincipalsGroupMembership Get-ADPrincipalsGroupMembership Remove-ADPrincipalsGroupMembership Get-ADAccountAuthorizationGroup <b>Password Policy Management</b> New-ADIntraInePasswordPolicy Get-ADIntraInePasswordPolicy Set-ADIntraInePasswordPolicy Remove-ADIntraInePasswordPolicy Add-ADIntraInePasswordPolicySubject Get-ADIntraInePasswordPolicySubject Remove-ADIntraInePasswordPolicySubject Get-ADUserResultantPasswordPolicy Get-ADDefaultDomainPasswordPolicy Set-ADDefaultDomainPasswordPolicy
<b>Topology Management</b> <b>Domain Controller Management</b> Get-ADDomainController Move-ADDirectoryServerOperationMasterRole <b>Password Replication Policy Management</b> Add-ADDomainControllerPasswordReplicationPolicy Get-ADDomainControllerPasswordReplicationPolicy Remove-ADDomainControllerPasswordReplicationPolicy Set-ADDomainControllerPasswordReplicationPolicyInage Get-ADAccountResultantPasswordReplicationPolicy	<b>Optional Feature Management</b> Get-ADOptionalFeature Enable-ADOptionalFeature Disable-ADOptionalFeature <b>Domain and Forest Management</b> Get-ADBootDSE Get-ADDomain Set-ADDomain Set-ADDomainInfo Get-ADForest Set-ADForest Set-ADForestInfo	<b>Directory Object Management</b> New-ADObject Get-ADObject Set-ADObject Remove-ADObject Move-ADObject Rename-ADObject Restore-ADObject <b>Provider cmdlets</b> Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Set-Item Get-Item Remove-Item Move-Item Rename-Item Get-ItemProperty Set-ItemProperty Remove-ItemProperty Get-ChildItem Get-ACL Set-ACL

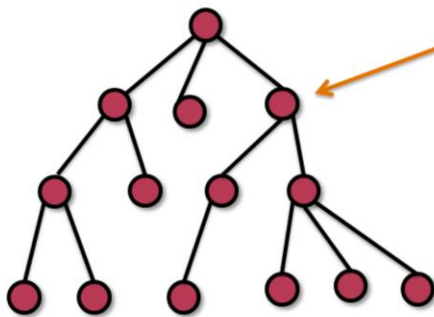
24

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



## Keresés LDAP címtárban



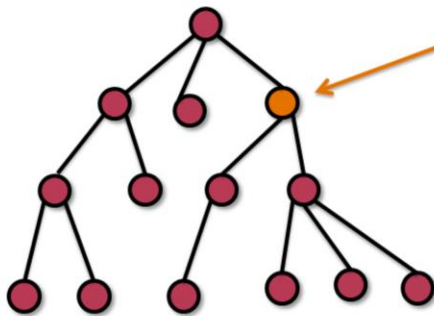
SearchRoot: honnan

PageSize: hány elemet

Scope: mik között

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

## Keresés LDAP címtárban



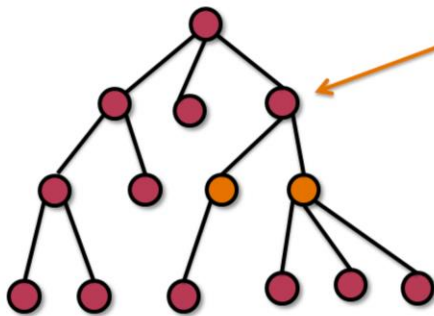
SearchRoot: honnan

PageSize: hány elemet

Scope: mik között

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

## Keresés LDAP címtárban



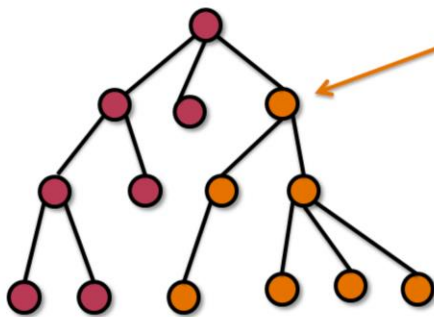
SearchRoot: honnan

PageSize: hány elemet

Scope: mik között

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

## Keresés LDAP címtárban



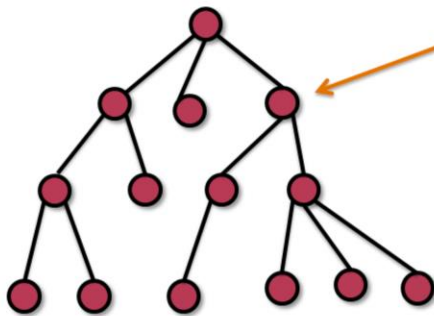
SearchRoot: honnan

PageSize: hány elemet

Scope: mik között

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

## 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

## 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\*



30



### Példák:

```
Import-Module ActiveDirectory
```

```
cd AD:
```

```
ls
```

```
cd '.\dc=irfdemo,dc=local'
```

```
ls -Recurse .\OU=People
```

```
ls -Recurse .\ou=people | ? { $_.objectClass -eq "group" }
```

```
Get-Command -Module ActiveDirectory
```

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

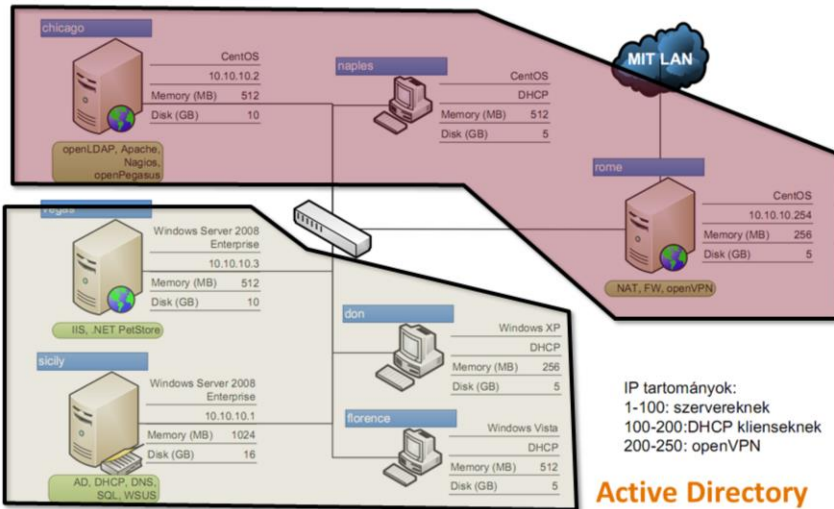
# Tartalom

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

# Kitekintés

## ▪ Készen vagyunk?

### OpenLDAP





# 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...

## További információ

### Active Directory:

- Gál Tamás, Szabó Levente, Szerényi László: [Rendszerfelügyelet rendszergazdáknak](#), Szak Kiadó, 2007.
- Gál Tamás: [Windows Server 2008 R2 – A kihívás állandó](#), JOS, 2011. (WS 2008 R2 újdonságok)
- Microsoft Technet: [Active Directory Services](#)
  - Planning, Deployment, Operations, Troubleshoot

### ActiveDirectory PowerShell modul:

- [Active Directory PowerShell](#) blog
- Soós Tibor: [Microsoft PowerShell 2.0 rendszergazdáknak – elmélet és gyakorlat](#), 2010.



35



- 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>