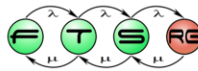


Active Directory

Micskei Zoltán

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



Utolsó módosítás: 2012. 03. 06.

Az előző részek

- Modellezés

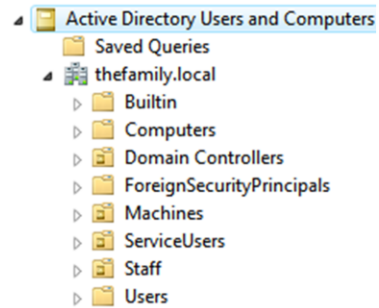
- Központosított felhasználókezelés, címtárak
 - LDAP
 - **Active Directory**

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

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: Initials:

Last name:

Display name:

Description:

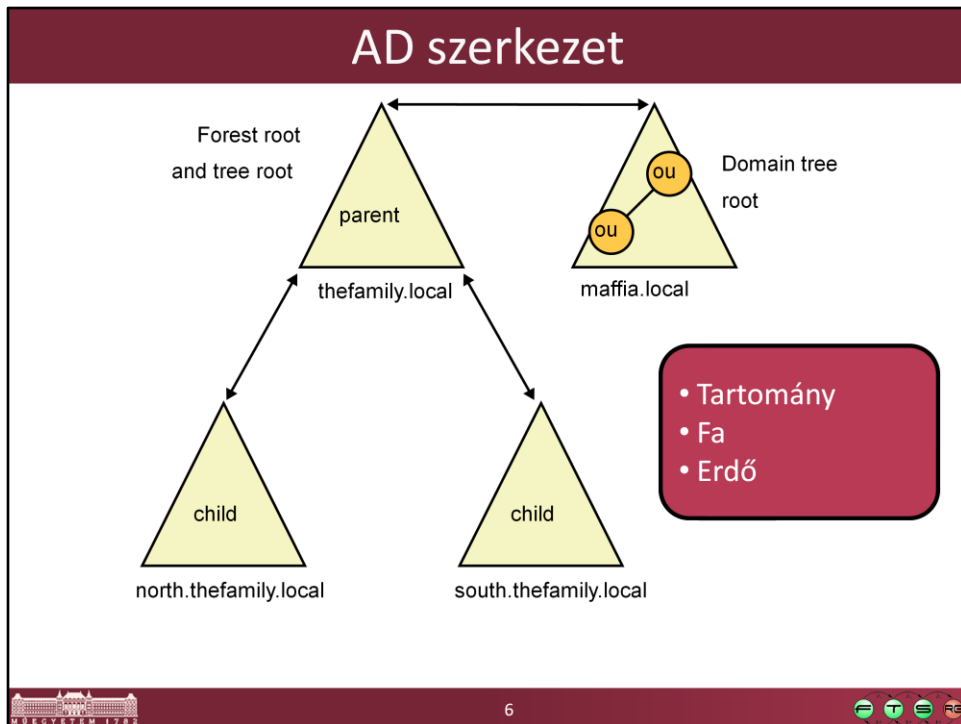
Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply



- 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.

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

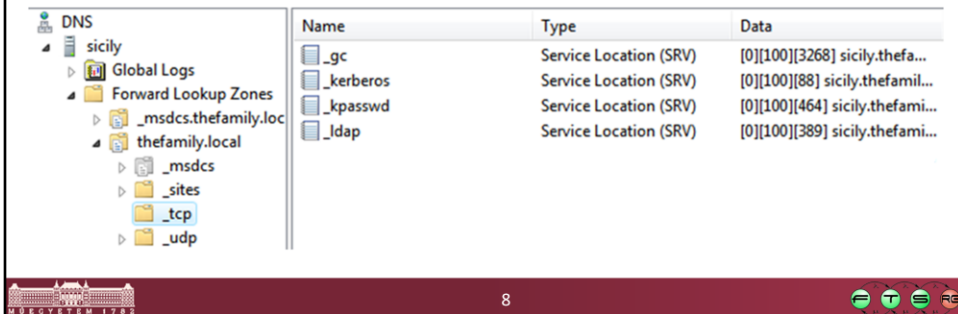


Tartományvezérlő: ezek a gépek tárolják magát a címtárat. Mindegyik tárol egy-egy példányt, és a változásokat egymás között szinkronizálják (úgynevezett multimaster replikáció segítségével, lásd később a hibatűrés előadásokat a félév folyamán).

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



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

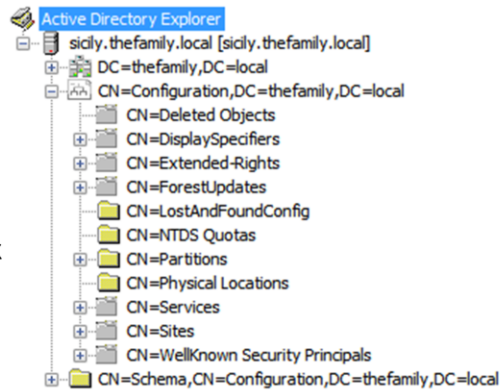
AD belső felépítése

■ Partíciók

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

■ Elem megnevezése

- CN: common name
- DC: domain component



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

DEMO Sysinternals AD Explorer

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

Path: CN=executive,OU=Executive,OU=Staff,DC=thefamily,DC=local,sicly.thefamily.local [sicly.thefamily.local]

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	160.1.0.1.01. 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;CN=Vito Mascarpone,OU=Executive,OU=Staff,DC=thefamily,DC=local
name	DirectoryString	1	executive
NTSecurityDescriptor	NTSecurityDescriptor	1	D:A(I)(CA);RP;A6a9b11d-60ae-405a-b7e8-ffba58d456d2;;S-1-5-32
objectCategory	DN	1	CN=Group,CN=Schema,CN=Configuration,DC=thefamily,DC=local
objectClass	OID	2	top:group
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
uSNCreated	Integer8	1	0x407B
whenChanged	GeneralizedTime	1	2009.01.17. 17:41:59
whenCreated	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

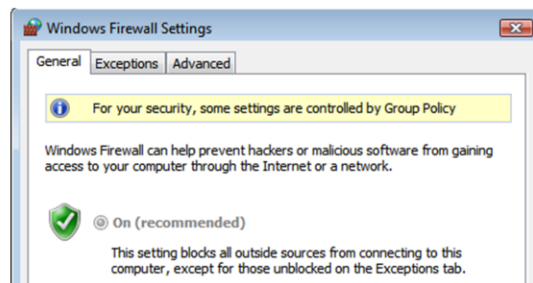
Központosított jogosultságkezelés

- 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

Csoportháziprend (Group Policy)

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



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

Csoportházi rend fajtái

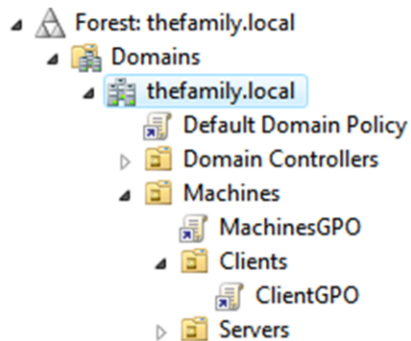
- Számítógép szintű
 - SW telepítés, tűzfal, Windows Update...
- Felhasználó szintű
 - mappa átirányítás, képernyő beállítás, nyomtatók
- Beépített: szoftver telepítés, biztonsági beállítás...
- Felügyeleti sablon (admx fájl): kiegészítések
- Policy vs. Preferences (Server 2008 óta)



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)



16



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 Csoportházi rend

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

The screenshot displays the Group Policy Management Console for a policy named 'StudentGPO [demodc1.addemo.local] Policy'. The left pane shows the tree structure with 'Start Menu and Taskbar' selected. The right pane shows the configuration for the 'Remove links and access to Windows Update' policy, which is currently 'Not configured'. Below the policy name, there are requirements and a description. A table lists various settings and their 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/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

- 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.

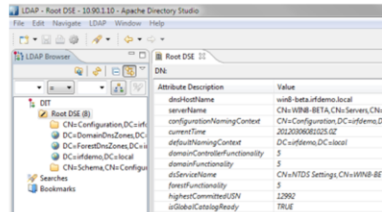
Példa külső csoportházi rend: Lenovo System Update Administrator Tools,
http://support.lenovo.com/en_US/detail.page?LegacyDocID=TVAN-ADMIN#tvsu

Tartalom

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

AD elérése programozottan

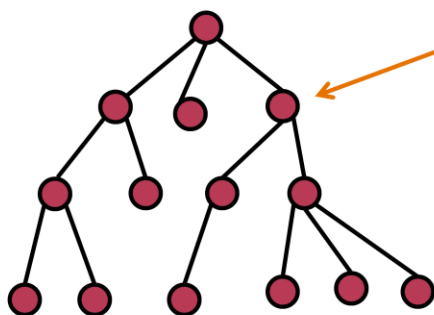
- `ds*` parancsok (pl. `dsadd`, `dsquery`)
 - Egyszerű műveletek
- Tetszőleges LDAP kliens
 - Pl. Java-s kliensek is
- .NET kódból
 - `System.DirectoryServices` névtér osztályai
- PowerShell
 - AD Service Interface (ADSI)
 - Active Directory module (Windows Server 2008 R2)



The screenshot shows the Apache Directory Studio interface. The 'LDAP Browser' window displays a tree view on the left with 'Root DSE (0)' selected. The main pane shows a table of attributes for the selected object.

Attribute	Description	Value
dn	dn	ldap://beta.mdemo.local
serverName	serverName	CN=WWW-BETA,CN=Servers,CN=DC
configurationNamingContext	configurationNamingContext	CN=Configuration,DC=ufidemo,DC
currentTime	currentTime	2012/09/06:10:05:02
dnstolNamingContext	dnstolNamingContext	DC=ufidemo,DC=local
domainControllerFunctionality	domainControllerFunctionality	5
domainFunctionality	domainFunctionality	5
dsServiceName	dsServiceName	CN=NTDS Settings,CN=WWW-BETA
forestFunctionality	forestFunctionality	5
highestCommittedUSN	highestCommittedUSN	12962
isGlobalCatalogReady	isGlobalCatalogReady	TRUE

Keresés LDAP címtárban



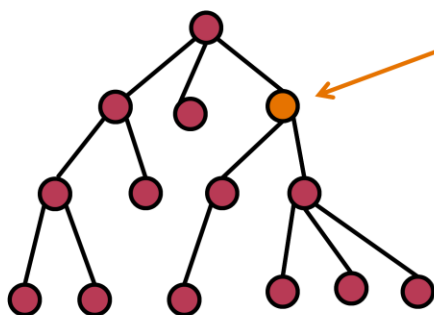
SearchRoot: honnan

PageSize: hány elemet

Scope:

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

Keresés LDAP címtárban



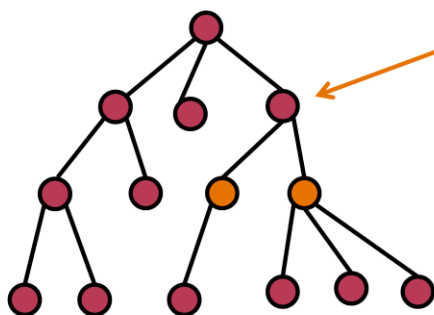
SearchRoot: honnan

PageSize: hány elemet

Scope: mik között

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

Keresés LDAP címtárban



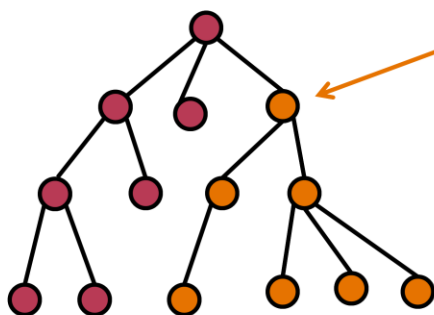
SearchRoot: honnan

PageSize: hány elemet

Scope: mik között

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

Keresés LDAP címtárban



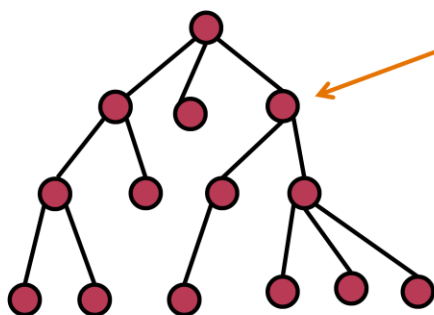
SearchRoot: honnan

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

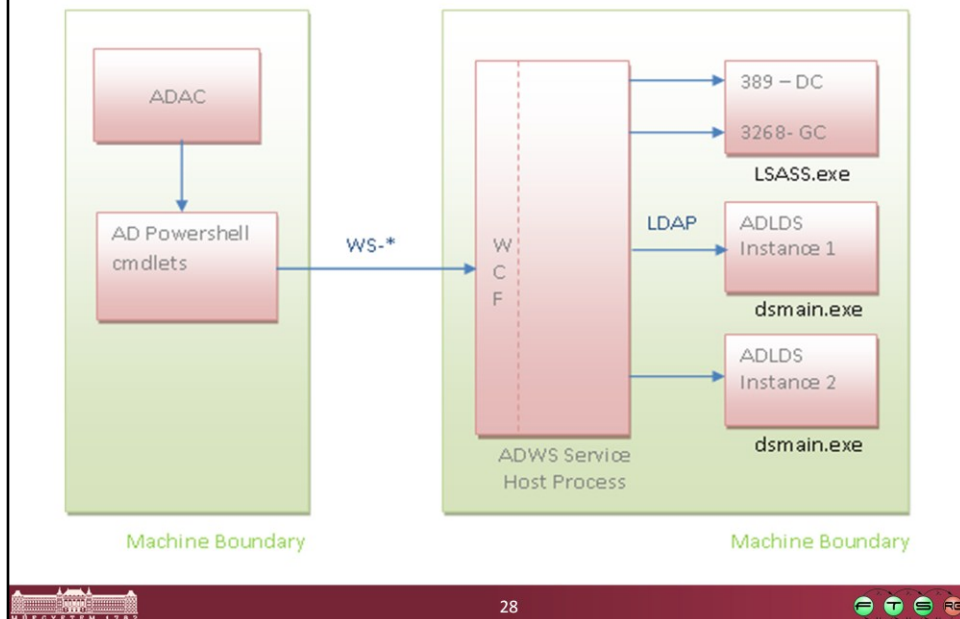
ActiveDirectory module for PowerShell

- 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

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>

Account Management Account Lifecycle Management 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	Account Settings Management Search-ADAccount Disable-ADAccount Enable-ADAccount Unlock-ADAccount Set-ADAccountPassword Set-ADAccountControl Clear-ADAccountExpiration Set-ADAccountExpiration Managed Service Account Management Add-ADComputerServiceAccount Get-ADComputerServiceAccount Remove-ADComputerServiceAccount Install-ADServiceAccount Uninstall-ADServiceAccount Reset-ADServiceAccountPassword	Group Membership Management Add-ADGroupMember Get-ADGroupMember Remove-ADGroupMember Add-ADPrincipalsGroupMembership Get-ADPrincipalsGroupMembership Remove-ADPrincipalsGroupMembership Get-ADAccountAuthorizationGroup Password Policy Management New-ADIneDrainedPasswordPolicy Get-ADIneDrainedPasswordPolicy Set-ADIneDrainedPasswordPolicy Remove-ADIneDrainedPasswordPolicy Add-ADIneDrainedPasswordPolicySubject Get-ADIneDrainedPasswordPolicySubject Remove-ADIneDrainedPasswordPolicySubject Get-ADUserResultantPasswordPolicy Set-ADDefaultDomainPasswordPolicy
Topology Management Domain Controller Management Get-ADDomainController Move-ADDirectoryServerOperationMasterRole Password Replication Policy Management Add-ADDomainControllerPasswordReplicationPolicy Get-ADDomainControllerPasswordReplicationPolicy Remove-ADDomainControllerPasswordReplicationPolicy Set-ADDomainControllerPasswordReplicationPolicyUsage Get-ADAccountResultantPasswordReplicationPolicy	Optional Feature Management Get-ADOptionalFeature Enable-ADOptionalFeature Disable-ADOptionalFeature Domain and Forest Management Get-ADRootDSE Get-ADDomain Set-ADDomain Set-ADDomainMode Get-ADForest Set-ADForest Set-ADForestMode	Directory Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Move-ADObject Rename-ADObject Restore-ADObject Provider cmdlets Get-PSProvider New-PSDrive Set-PSDrive Remove-PSDrive New-Item Get-Item Set-Item Remove-Item Get-ItemProperty Set-ItemProperty Remove-ItemProperty Get-Childitem Get-ACL Set-ACL

29

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*



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*"'
```

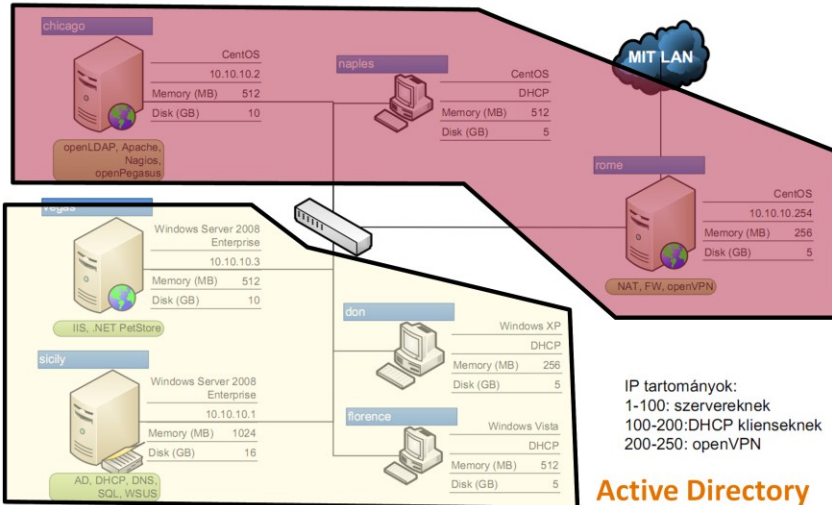
Tartalom

- 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. (WS2008R2 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>

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](#)



PowerShell + ADSI

- Keresés:
 - System.DirectoryServices.DirectorySearcher
- Leírás:
 - [Searching Active Directory with Windows PowerShell](#)
- Kereső kifejezés:
 - Példa: (&(cn=i*)(objectClass=group))
 - Segítség: Sysinternals AD Explorer
 - Search / Search Container -> GUI a kifejezés megírásához



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)" }
```

