# Címtárak kezelése

*Gyakorlati útmutató*
*Készítette: Micskei Zoltán*
*Utolsó módosítás: v1.3, 2013.03.21.*

A segédlet célja, hogy bemutassa az LDAP címtárak általános fogalmait, majd az openLDAP és a Microsoft Active Directory használatának alapjait.

**Figyelem**: A leírásban szereplő utasításokat ne másoljuk, hanem tényleg gépeljük is be. Különben nem sok mindent tanulunk belőle, nem rögzül a szintaktika.

## Tartalomjegyzék

1 Az LDAP-ról általánosan ..... 2
2 Linux: openLDAP, phpLDAPadmin ..... 4
2.1 Ismerkedés az LDAP címtárral ..... 4
2.2 Az LDAP címtár kezelése parancssori eszközökkel ..... 8
3 Windows: Active Directory ..... 13
3.1 Active Directory Users and Computers ..... 13
3.2 AD Explorer ..... 17
3.3 Lekérdezés PowerShellből ..... 19
3.4 Csoportházirendek ..... 24
4 Összefoglalás ..... 26
4.1 További információ ..... 26
5 Függelék ..... 28
5.1 DIGEST-MD5 hitelesítés használata openLDAP esetén ..... 28
5.2 ADSI használata ..... 31

# 1 Az LDAP-ról általánosan

Az LDAP ajánlások [1] többek között definiálnak egy adatmodellt [2], ami megszabja, hogy az LDAP alapú címtáraknak hogyan kell felépülniük, egy protokollt a címtár elérésére (az LDAP-ot [3]) és egy szöveges formátumot a címtár elemeinek leírására (LDIF [6]).

A címtár *bejegyzés*ekből (entry) áll. Egy bejegyzés *attribútum*ok (attribute) halmaza. Az attribútumok lehetnek felhasználói vagy műveleti (operational) attribútumok, ez utóbbiak a címtár működéséhez szükséges adatokat tárolják. Egy attribútum egy leírásból (kb. az attribútum neve, pl. givenName) és egy vagy több értékből áll. A bejegyzéseknek van egy vagy több típusa, ezek az *objektumosztály*ok (object class), ezek határozzák meg többek között a bejegyzés lehetséges attribútumait és helyét a címtárban. Az objektumosztályok definícióját a címtár *séma*ja (schema) tartalmazza, minden objektumosztályt egy *objektumazonosító* (object identifier – OID) azonosít.

A bejegyzések között lehetnek *kapcsolat*ok (relationship). A bejegyzések egy fastruktúrába vannak szervezve, ez a *Directory Information Tree* (DIT). Az LDAP hierarchikus elnevezést használ. Egy adott szinten belül egy bejegyzést a *Relative Distinguished Name* (RDN) neve azonosítja, ez az attribútumainak egy olyan halmaza, ami egyedi az adott szinten belül. A teljes címtáron belül a bejegyzést a *Distinguished Name* (DN) neve azonosítja, ezt a bejegyzés RDN-jének és a szülője DN-jének összefűzésével kapjuk.

Egy címtár szerveren belül a címtár csúcsa az úgynevezett *root DSE*[1], ez a szerverrel kapcsolatos működési információkat tárolja. A root DSE-hez tartozó DN az üres sztring. Többek között az van a root DSE-ben feljegyezve, hogy a szerver milyen úgynevezett *naming context*eket tárol, ezek a bejegyzések egy szerveren belül tárolt részfája[2]. Egy naming contextet az úgynevezett *root DN*-jével azonosítják[3], ami a gyökérelemének DN-je. A kliensek általában egy adott naming context root DN-jéhez kapcsolódnak, a root DSE-hez való kapcsolódást külön, speciális módon kell kérni.

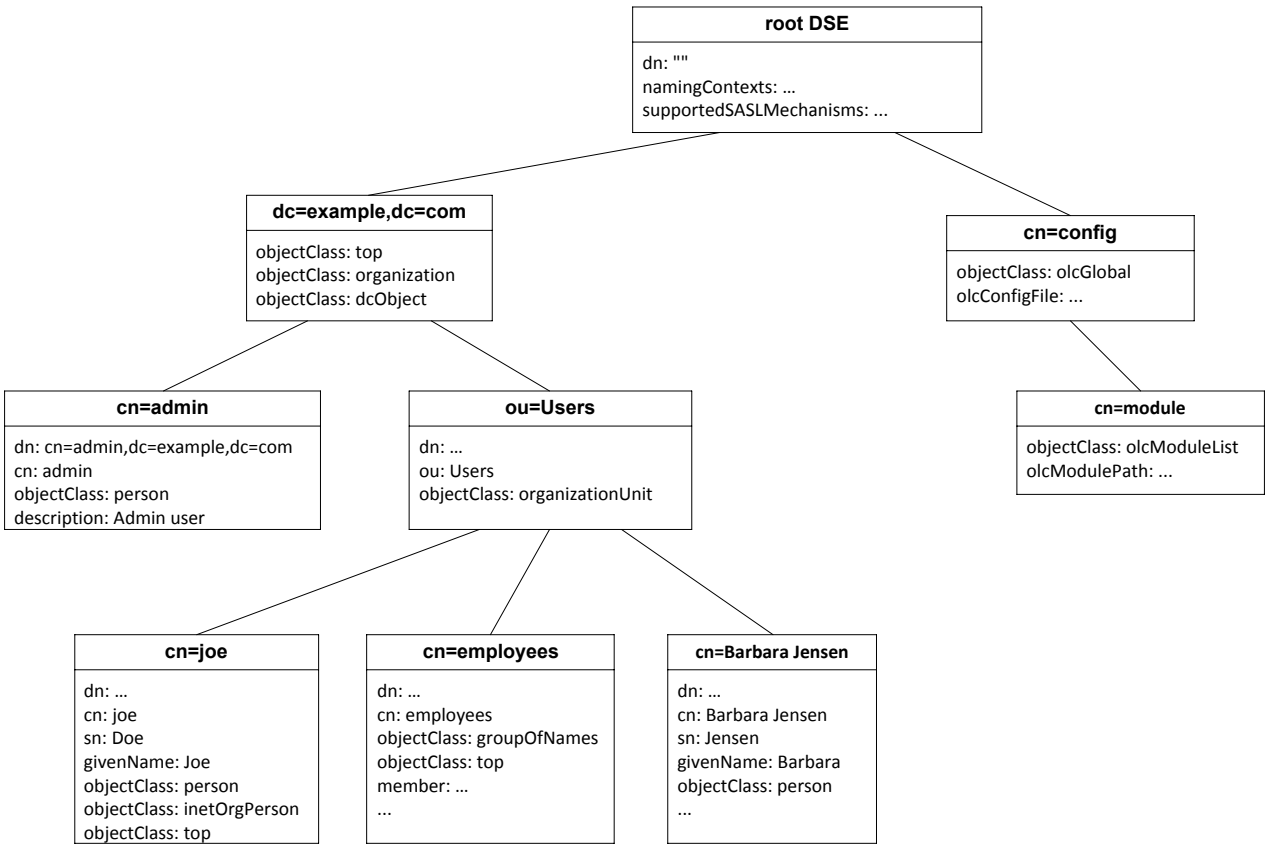
Nem kevés fogalom, igaz? És ezek még csak az alapok. Nézzük meg egy példán keresztül ezeket még egyszer. Az alábbi ábra egy DIT részletét ábrázolja (1. ábra). Az érthetőség kedvéért sok részletet lehagytunk, csak a legfontosabbakra koncentrálunk. A címtárat most egy UML diagram jellegű ábrán szemléltetjük, ahol névként a bejegyzések RDN-je szerepel. Ez talán egy kicsit szemléletesebb megjelenítés, mint a szabványos puszta szöveges információ. A DIT gyökéreleme a root DSE. A címtár jelenleg két naming contextet tárol, az egyik gyökere a `dc=example,dc=com`, a másiké pedig `cn=config`. A fa struktúrában az elemek következő csoportjaira hivatkozhatunk. Egy bejegyzésnek lehetnek *gyerek*ei (child), és egy *szülő*je (parent). Egy elem összes ősére a *felmenő*k (ancestor), az összes gyerekére, unokájára stb. pedig a *leszármazott*ak (descendant) névvel hivatkozunk. Egy adott elem gyerekei *testvér* (sibling) viszonyban vannak. Tehát például a `dc=example,dc=com` bejegyzés gyereke a `cn=admin` és `ou=Users` elemek, a leszármazottai az alatta levő 5 elem. A `cn=joe` testvére a

[1] A DSE a *DSA-specific entry* rövidítése, ahol a DSA a *Directory System Agent* rövidítése, ami a címtárat tároló szervert jelöli.
[2] Az LDAP lehetővé teszi, hogy részfák kezelését és tárolását delegáljuk másik szervereknek.
[3] Pontosabban a szabvány ezt *context prefix*nek hívja, de a gyakorlatban erre root DN néven hivatkoznak.

`cn=employees` és `cn=Barbara Jensen` elemek. Az ábra alapján az egyes bejegyzések DN-jét is könnyű származtatni: `cn=joe` DN-je `cn=joe,ou=Users,dc=example,dc=com`.

Egy bejegyzés lehet többféle objektumosztály példánya is, például a `dc=example,dc=com` bejegyzésnél is három szerepel. Egy elem CN[4] (common name) attribútumát bárhogy megválaszthatjuk, arra kell csak figyelni, hogy ha ez az RDN-je, akkor a testvérei között egyedinek kell lennie. Vannak általános objektumosztályok, de lehetnek teljesen gyártó-specifikusak is, pl. a `cn=config` részfában az openLDAP saját kiegészítéseit használtuk.

(Ez így most elég tömény, de remélhetőleg a gyakorlat elvégzése után már érthetőbbé válik.)




**1. ábra: Példa Directory Information Tree**

[4] Az LDAP nem érzékeny a kis- és nagybetű közötti különbségre.

# 2 Linux: openLDAP, phpLDAPadmin

A feladatok megoldásához például a kiadott VMware virtuális gépbe telepített openSUSE rendszert lehet használni. Ez a virtuális gép előre telepítve tartalmazza a következőket:

- openLDAP[5] 2.4.31 – LDAP címtár,
- phpLDAPAdmin[6] 1.2.2 – webes felület a címtárhoz,
- SuperHotels[7] példa címtár elemei.

## *2.1 Ismerkedés az LDAP címtárral*

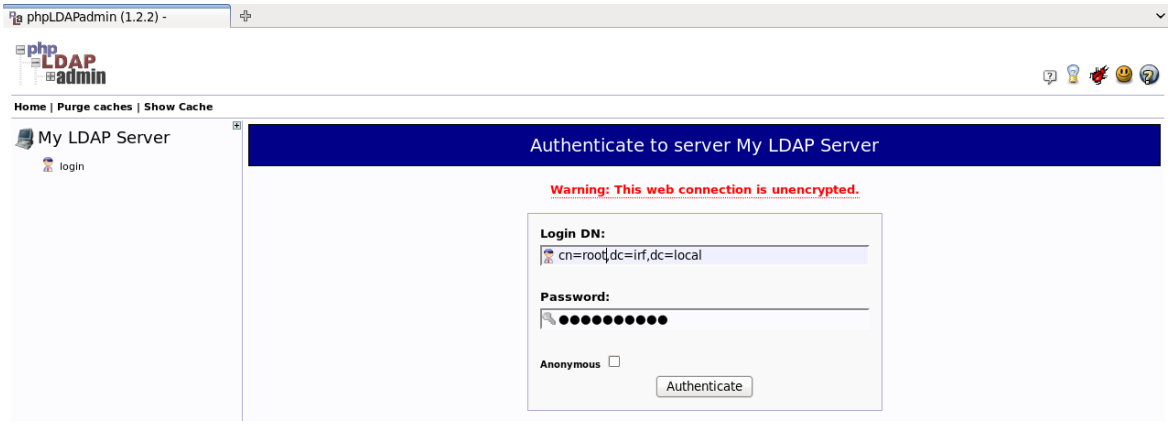
Az első feladatban a címtár webes felületén keresztül megvizsgáljuk annak felépítését, majd elvégzünk néhány alapfeladatot, mint például felhasználók létrehozása vagy csoportokhoz adása.

1. Indítsuk el a virtuális gépet!

   A gépre van grafikus felület is telepítve, használhatjuk azt, de bejelentkezhetünk rá akár távolról SSH segítségével is.

2. Bejelentkezés a címtár webes felületén

   A phpLDAPAdmin komponens egy webes felületet biztosít a címtár elérésére. A felületre a virtuális gépen belül a `http://localhost/phpldapadmin` weboldalon tudunk belépni (kívülről pedig a `localhost` nevet cseréljük le a virtuális gép aktuális IP-címére). Figyeljünk arra, hogy a belépéshez már egy, az LDAP-ban definiált felhasználót kell megadni, mégpedig a DN-jével (2. ábra).

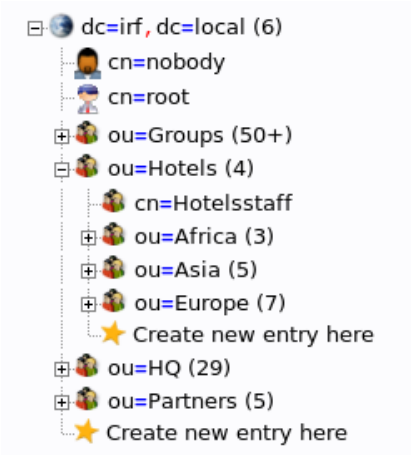



**2. ábra: Belépés a phpLDAPAdmin felületen**

3. A címtár struktúrája

   Egy LDAP címtár egy fastruktúra tulajdonképpen. A tárgyhoz tartozó példa címtár felépítését az alábbi ábra szemlélteti.

[5] http://www.openldap.org/
[6] http://phpldapadmin.sourceforge.net/
[7] Darvas Dániel. „Active Directory tesztadatok generálása” URL: http://blog.inf.mit.bme.hu/?p=394

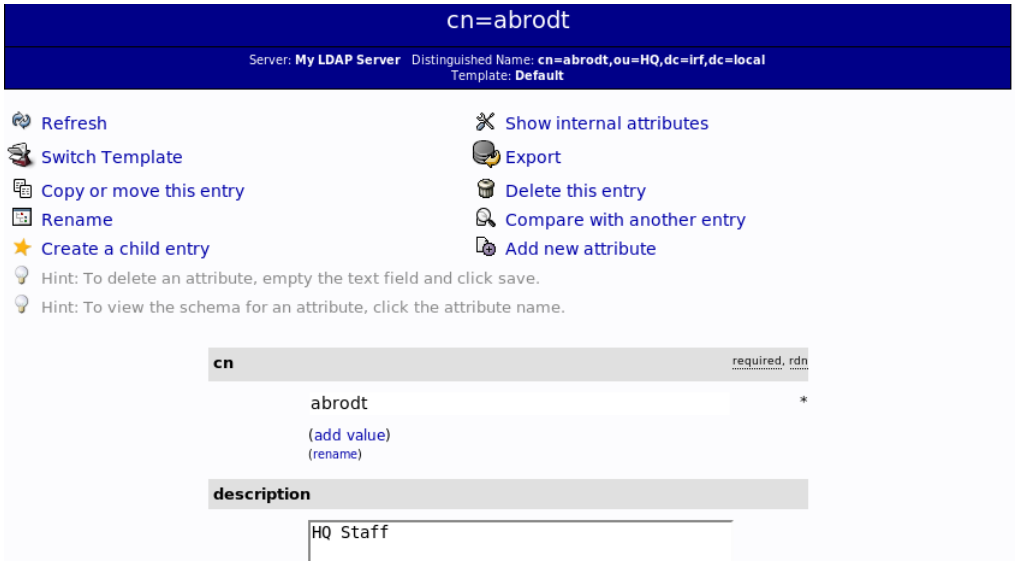



**3. ábra: A példa címtár felépítése**

A címtár gyökérelemének neve `dc=irf,dc=local`. Ez alatt találhatóak felhasználók, szervezeti egységek (*organizational unit* – OU) és csoportok. A phpLDAPAdmin felület kiírja az egy csomóponthoz tartozó gyerekelemek számát is, például az `ou=Partners` szervezeti egységnek 5 darab gyerekeleme van.

4. Egy elem részletes tulajdonságai

   Keressünk ki a címtárból egy felhasználót, és nézzük meg a tulajdonságait (4. ábra).




**4. ábra: Felhasználó tulajdonságai és a rajta végezhető műveletek**

Az ábrán látszik, hogy a felhasználó DN-je `cn=abrodt,ou=HQ,dc=irf,dc=local`. Ebből a CN (*common name*) tulajdonsága az abrodt, ez a tulajdonság az RDN-je is egyben (*relative distinguished name* – az adott hierarchia szinten belül egyedi, megkülönböztető név). Az ábrán ezen kívül csak a *description* attribútuma látszik.

   a. Módosítsuk és frissítsük is az objektumot (*Update Object* gomb legalul), például írjuk át a leírását.

A többi attribútumát is könnyedén meg tudjuk nézni, ha exportáljuk LDIF formátumba az elemet (*Export* gomb). A következő eredményt kapjuk:

```
# Entry 1: cn=abrodt,ou=HQ,dc=irf,dc=local
dn: cn=abrodt,ou=HQ,dc=irf,dc=local
cn: abrodt
description: HQ Staff
displayname: Alexa Brodt
gidnumber: 1000
givenname: Alexa
homedirectory: /home/users/abrodt
loginshell: /bin/sh
mail: abrodt@superhotels.com
objectclass: top
objectclass: inetOrgPerson
objectclass: person
objectclass: posixAccount
sn: Brodt
telephonenumber: 774-2134-710
uid: abrodt
uidnumber: 2004
```

A tulajdonságok között látunk általános LDAP attribútumokat (pl. *displayname*, *description*) és Linux-specifikusakat is (például *uid* – a felhasználó azonosítója). Az objectclass többértékű attribútum sorolja fel, hogy milyen, az LDAP sémában szereplő osztályoknak példánya az adott elem.

5. Új elem létrehozása

Ha egy adott OU-n belül a *Create new entry here* linkre kattintunk, akkor a következő típusú elemek közül választhatunk.


**5. ábra: Sablonok új elem létrehozásakor**

Az egyes sablonok a létrehozandó elem típusait és így az attribútumainak halmazát határozzák meg.

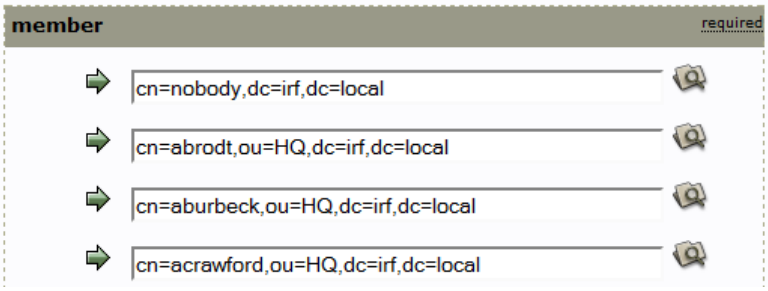
a. Hozzunk létre egy új felhasználót (*Generic: User Account*)! A felület a vezetéknév és keresztnév megadása után a felhasználónevet, CN-t és a home könyvtár elérési útját kitölti megfelelően, de ezeket is megváltoztathatjuk, ha más konvenciót szeretnénk alkalmazni.

Más típusú elemet is hasonlóan lehet létrehozni.

6. Csoportok kezelése

Válasszunk ki egy csoportot (például `cn=HQstaff,ou=HQ,dc=irf,dc=local`). A csoporttagságot a *member* attribútum tárolja. Figyeljünk meg, hogy minden tagról annak a DN-jét tároljuk, az LDAP címtár a DN-jével hivatkozik az egyes objektumokra.

a. Módosítsuk a csoport tagjait (*modify group members* link), és adjuk hozzá az újonnan létrehozott felhasználónkat.




**6. ábra: Csoporttagság tárolása**

7. Keresés a címtárban

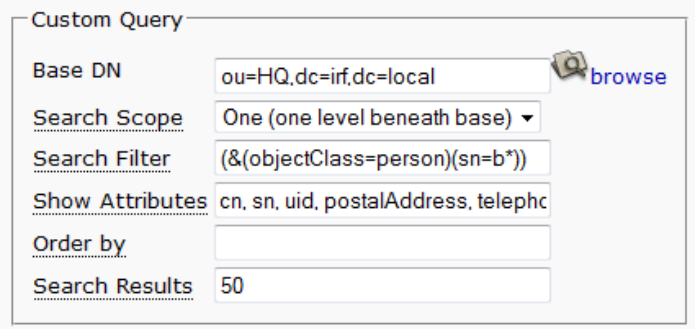
A bal oldali menü *Search* gombjával tudunk a címtárban keresni. Kereséshez a következőket kell megadni:

- *Base DN*: melyik csomóponttól kezdve akarunk keresni,
- *Search Scope*: csak az adott elemben (*Base*), az adott elem közvetlen gyerekelemei között (*One*) vagy az összes leszármazottja (*Sub*) között akarunk keresni,
- *Search Filter*: a keresési kifejezés az LDAP saját prefix nyelvén,
- *Show Attributes*: milyen attribútumokat kérünk majd le,
- *Search Results*: korlátozza a visszakapott elemek számát.

A következő keresési kifejezés például megadja azokat a felhasználókat, akiknek a vezetéknevük *b* betűvel kezdődik:

```
(&(objectClass=person)(sn=b*))
```

Ezt felhasználva az alábbi ábrán látható beállítások megkeresik az ilyen felhasználókat közvetlenül a HQ nevű szervezeti egységben (7. ábra).




**7. ábra: Keresés a címtárban**

## 2.2 Az LDAP címtár kezelése parancssori eszközökkel

Ha tömeges módosításokat akarunk elvégezni vagy valamilyen szkriptből szeretnénk elérni az LDAP címtárat, akkor hasznosak következő LDAP parancsok:

- `ldapadd`: új elem hozzáadása (a háttérben az `ldapmodify` parancsot hívja meg a `-a` kapcsolót megadva),
- `ldapmodify`: meglévő elem vagy elemek módosítása és hozzáadása,
- `ldapsearch`: keresés a címtárban.

Módosítás és létrehozás esetén a változtatásokat meg lehet adni a *standard input* bemeneten vagy pedig fájlban, mindkét esetben az LDIF [6] formátumot kell használni. Ha a standard inputot használjuk, akkor a `Ctrl+D` kombinációval tudunk majd kilépni, miután beadtunk az összes változtatást.

A legalapvetőbb közös parancssori paraméterek:

- `-H`: LDAP URI megadása, ez jelzi, hogy hol és milyen protokollon keresztül éri el a címtár szervert.
  - A formátuma `proto://host:port`, ahol `proto = {ldap, ldaps}`, `host` a szerver neve vagy IP-címe, az `ldap` port pedig tipikusan 389, az `ldaps` pedig 636.
  - Tehát például a helyi gépről nézve és nem SSL kapcsolatot választva a következő URI használható: `ldap://localhost:389`
- `-v`: verbose mód, hibakereséshez hasznos információkat is kiír (néha).

Ezen kívül meg kell még adni a hitelesítés módjára vonatkozó kapcsolókat. Az openLDAP (és maga az LDAP szabvány is) sokféle hitelesítési módot támogat [5]:

- *Simple*: Egyszerű hitelesítés, amit kötelező a szabvány szerint támogatni. A `-x` kapcsolóval lehet aktiválni. Különböző üzemmódjai vannak:
  - *Anonymous*: alapesetben a legtöbb LDAP kiszolgáló támogatja az adatok egy részének név nélküli lekérdezését, kereséshez például lehet ezt használni.
  - *Unauthenticated*: nevet adunk meg, de jelszót nem, lényegében a név nélküli hozzáféréshez lesz hasonló az eredmény.

  - *Név/jelszó*: nevet és jelszót is megadunk a hitelesítés során, és az LDAP kiszolgáló ezt ellenőrzi. Ez egy az LDAP-ban definiált felhasználó, tehát a nevét a DN-jével kell megadni. Figyelem: nyílt szövegben küldi át a jelszót a csatlakozás során!

- *Simple Authentication and Security Layer (SASL)*: keretrendszer, amely többféle hitelesítési módszert is támogat. Ezek egy része már biztosítja az átvitt adatok integritásának védelmét és a bizalmasságukat. A támogatott hitelesítési mechanizmusok (a `-Y` kapcsolóval lehet megadni, hogy melyik fajtát akarjuk használni):
  - *DIGEST-MD5*: MD5 hash-t használó challange-response protokoll,
  - *GSSAPI*: Kerberos V5 hitelesítés,
  - *EXTERNAL*: külső forrás használata, például Linux IPC hitelesítés,
  - …
- *SSL/TLS*: az előzőektől teljesen független, alapvetően nem hitelesítési módszer, de a teljesség kedvéért érdemes itt megemlíteni. Lehetőség van a teljes kommunikációt a szállítási réteg szintjén titkosítani, és így használható az egyszerű név/jelszó módszer.

Az openLDAP ezen kívül számos biztonsági módszert biztosít még (IP-szintű szűrés, jelszavak tárolásának kérdése, hozzáférés szabályozása stb.), ezekre nem térünk itt most ki.

1. Keresés a címtárban

   Első körben próbáljuk meg ugyanazt a lekérdezést végrehajtani parancssorból is, amit már a webes felületen sikeresen elvégeztünk. Az `ldapsearch` a következő formában várja a paramétereket:

   ```
   ldapsearch <kapcsolók> <szűrő> <attribútumok listája>
   ```

   Tehát a keresett lekérdezés (a válaszban csak az *sn* és *cn* attribútumokat kérjük):

   ```
   ldapsearch -H ldap://localhost:389 -x -b "ou=HQ,dc=irf,dc=local" -s one
   "(&(objectclass=person)(sn=b*))" cn sn
   ```

   Az eredmény valami hasonló lesz:

   ```
   # extended LDIF
   #
   # LDAPv3
   # base <ou=HQ,dc=irf,dc=local> with scope oneLevel
   # filter: (&(objectclass=person)(sn=b*))
   # requesting: cn sn
   #

   # aburbeck, HQ, irf.local
   dn: cn=aburbeck,ou=HQ,dc=irf,dc=local
   cn: aburbeck
   sn: Burbeck

   # abrodt, HQ, irf.local
   dn: cn=abrodt,ou=HQ,dc=irf,dc=local
   ```

```
...
```

A keresés itt is 5 elemet ad vissza. Ahogy a kérésben is látszik, a `-s` és `-b` kapcsoló segítségével tudjuk szabályozni, hogy hol és milyen mélyen keressen.

Figyeljük meg, hogy egyszerű hitelesítést használtunk, és nem adtunk meg felhasználónevet, így anonim lekérdezést hajtott végre az `ldapsearch`.

2. Új elem hozzáadása konzolról

   Az `ldapadd` segítségével tudunk új elemet hozzáadni, ilyenkor az új elemet LDIF formátumban kell leírni.

   *LDIF alapok*: Az LDIF-ben a sor eleji # a komment jele. Ha több elem szerepel egy LDIF fájlban, akkor azokat egy üres sorral kell elválasztani. Egy sort meg lehet törni, ilyenkor a következő sor kezdete elé egy darab szóközt kell rakni. Egy elemhez először a DN-jét kell megadni, `dn: <DN>` formában, majd utána az attribútumait felsorolni. Az attribútumoknál az attribútum nevét, egy kettőspontot, egy szóközt majd az attribútum értékét kell megadni.

   Nézzünk egy egyszerű példát egy elem hozzáadására:

   ```
   ldapadd -H ldap://localhost:389 -x -D "cn=root,dc=irf,dc=local" -W
   ```

   Itt most már megadtunk nevet is a hitelesítéshez (`-D`), és a `-W` hatására a jelszót az indulás után be fogja kérni egy *Enter LDAP Password:* felszólítással. A `-w` kapcsoló után a jelszót meg lehetne adni közvetlenül a parancsnak.

   ```
   Ezek után a standard inputon kell megadni az LDIF adatokat, írjuk be most például a következőket:

   dn: ou=TestOU,ou=HQ,dc=irf,dc=local
   objectClass: organizationalUnit
   objectClass: top
   description: Test OU from ldapadd
   ```

   Az elem megadását egy üres sorral kell lezárni. Ha minden jól ment, akkor az *adding new entry* üzenetnek kell megjelennie. Ezután hozzáadhatunk további elemeket, vagy kiléphetünk a `Ctrl+D` segítségével.

3. Új elemek hozzáadása fájlból

   Próbáljuk ki most több elem hozzáadását, másoljuk át a következőket egy `useradd.ldif` fájlba.

   ```
   dn: cn=test1,ou=HQ,dc=irf,dc=local
   objectclass: inetOrgPerson
   cn: test1
   sn: Test
   givenName: User
   uid: test1
   userpassword: password
   ```

```
mail: test1@irf.local
description: LDIF test

dn: cn=Gipsz Jakab,ou=HQ,dc=irf,dc=local
objectclass: inetOrgPerson
cn: Gipsz Jakab
sn: Gipsz
givenName: Jakab
uid: gipszj
userpassword: password
mail: gipsz.jakab@irf.local
```

Ezt utána a következő paranccsal tudjuk betölteni az LDAP-ba:

```
ldapadd -H ldap://localhost:389 -x -D "cn=root,dc=irf,dc=local" -w <jelszo> -f
useradd.ldif
```

4. Meglévő elem módosítása

Módosítás esetén kicsit máshogy néz ki az LDIF fájl, meg kell azt is adni benne, hogy mit akarunk módosítani. A `dn:` sor után meg kell adni egy `changetype:` direktívában a módosítás fajtáját (modify, add, delete[8]). Módosítás esetén attribútumokat lehet hozzáadni, lecserélni vagy törölni (add, replace, delete) úgynevezett műveletekkel.

Nézzük egy példát, ami szemlélteti a fentieket. Mentsük ezt el `modify.ldif` néven:

```
# delete an entry
dn: cn=Gipsz Jakab,ou=HQ,dc=irf,dc=local
changeType: delete

# modify an entry
dn: cn=test1,ou=HQ,dc=irf,dc=local
changeType: modify
add: telephonenumber
telephonenumber: 555-1111
-
# different operators are separated by a -
replace: mail
mail: test@irf.local
-
delete: description
```

Ezt a következő paranccsal tudjuk végrehajtani:

```
ldapmodify -H ldap://localhost:389 -x -D "cn=root,dc=irf,dc=local" -w LaborImage
-f modify.ldif
```

Ennek hatására töröltük Gipsz Jakabot a címtárból és módosítottuk a test1 felhasználót.

[8] Ezen kívül vannak még a DN és RDN módosítására szolgáló changetype típusok is, amikkel átnevezni vagy áthelyezni lehet bejegyzéseket.

A segédlet eddigi része áttekintette az alapokat. További információt az `ldap*` parancsok manual oldalán találhatunk, ezt érdemes most átfutni (előbb-utóbb úgyis meg kell tenni, nem fogjuk tudni megúszni, hogy megnézzük a teljes referenciát).

# 3 Windows: Active Directory

A feladatokat egy Windows Servert futtató virtuális gépen fogjuk végrehajtani, amely letölthető a tárgy weboldaláról. A Microsoft legújabb kiszolgálókra szánt operációs rendszere, a *Windows Server 2012* csak 64 bites számítógépen fut, így ez egy 64 bites virtuális gép, aminek a futtatásához hardveres virtualizáció támogatásra (Intel VT-x, AMD-V) van szükség a fizikai gépben. A tárgyban már ezt a verziót használjuk, mert a régi 32 bites kiszolgálókra már nem érhető el az *Active Directory PowerShell* modul. Egyébként a címtár szerkezete és a grafikus felülete nagyon hasonló mindkét változat esetén.

A segédlet a következő lépéseken keresztül segít megismerkedni az Active Directory címtárral.

1. Először kipróbáljuk az *Active Directory Users and Computers* konzolt: megnézzük a címtár szerkezetét és meglévő elemeit, létrehozunk új elemeket.
2. Ha nagyjából eligazodunk már a címtárban, akkor a *Sysinternals AD Explorer* eszköz segítségével megnézzük a címtár belső felépítését (az egyes elemek LDAP neveit és attribútumait, az LDAP sémát stb.)
3. Ezután egyszerű lekérdezéseket hajtunk végre PowerShellből.
4. Végül kitekintünk kicsit a *csoportházirend*ek (group policy) világába.

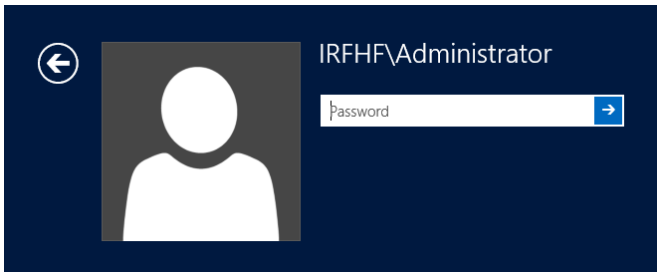
## *3.1 Active Directory Users and Computers*

Első lépésként megnézzük a címtár tartalmát, majd létrehozunk és módosítunk elemeket.

1. A virtuális gép indítása

   A virtuális gép indításakor az **I moved it** opciót válasszuk!

2. Belépés a szerverre




**8. ábra: Belépő képernyő tartományi környezetben**

Active Directory használata esetén az alapegység a *tartomány* (domain), az egy tartományba tartozó számítógépeket és egyéb elemeket tudjuk központilag kezelni, ezeknek az adatai tárolódnak a címtárban. Ha egy számítógép tagja egy tartománynak[9], akkor a belépésnél már nem csak azt kell megadni, hogy milyen felhasználóval akarunk belépni, hanem hogy a tartományi vagy helyi felhasználóval akarunk-e belépni. A

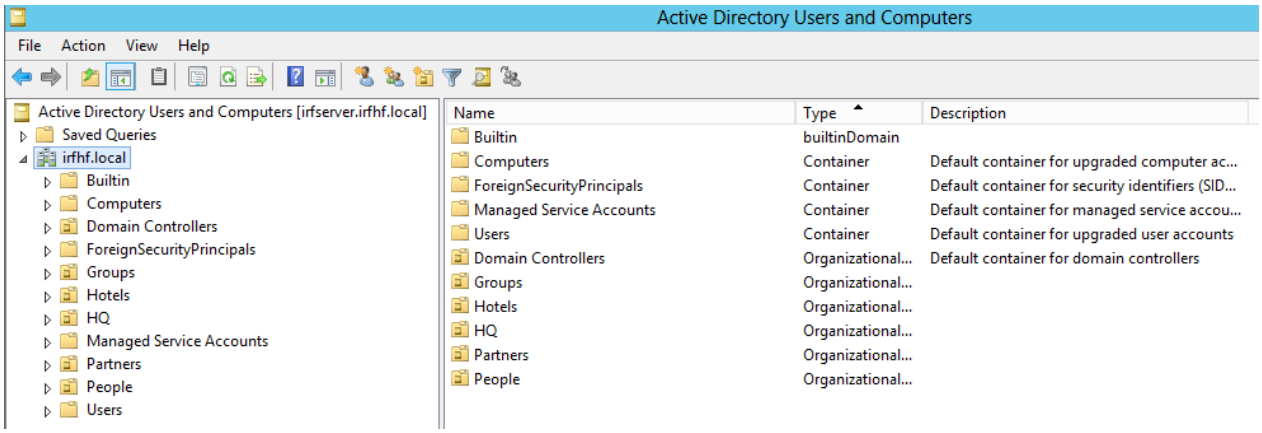
[9] Egy számítógép legfeljebb egy tartománynak lehet tagja, ha nem tartományi tag, akkor pedig egy munkacsoportba (workgroup) tartozik.

tartomány nevét a felhasználónév elé kell írni, egy \ jel előtt megadva (pl. IRHF\Administrator, lásd 8. ábra).

*Tartományvezérlő* (domain controller) esetén (olyan számítógép, ami az Active Directory címtár egy példányát tárolja) viszont nincsenek helyi felhasználók, így ez esetben egyértelmű a helyzet. Mivel a virtuális gépünk tartományvezérlő, ezért itt ilyenkor az `IRFHF` nevű tartományhoz tartozó Administrator felhasználóval lépünk be.

3. Ismerkedés a címtárral

   Az *Active Directory Users and Computers* konzol elindítása után a következőt látjuk.




**9. ábra: Az Active Directory Users and Computers konzol**

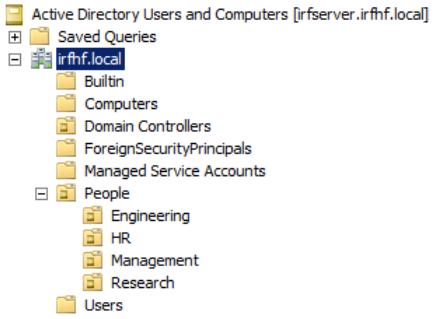
A bal oldali faszerkezet csúcsában láthatjuk, hogy jelenleg az `irfserver.irfhf.local` tartományvezérlőhöz csatlakoztunk.

A címtárunk gyökéreleme az `irfhf.local` csomópont, ennek jelenleg a közvetlen gyerekeit látjuk. Ezek a *Groups, Hotels, HQ, People* csomópontot kivéve a beépített gyári elemek, amik megtalálhatóak minden Active Directoryban. A jobb oldalon az elemek listájában láthatjuk, hogy nagy részük *Container* típusú, míg például a *People* már egy *szervezeti egység* (organizational unit), ezt a másfajta ikon is jelzi.

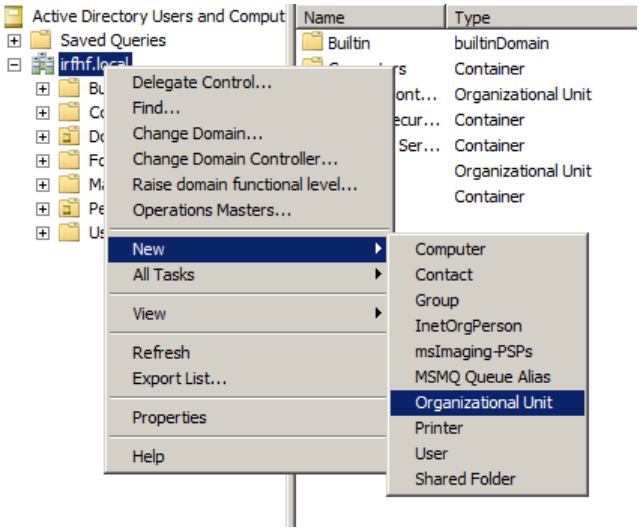
4. A címtár hierarchiája

   Bontsuk ki *People* tárolót, hogy lássuk teljes hierarchiáját (10. ábra).

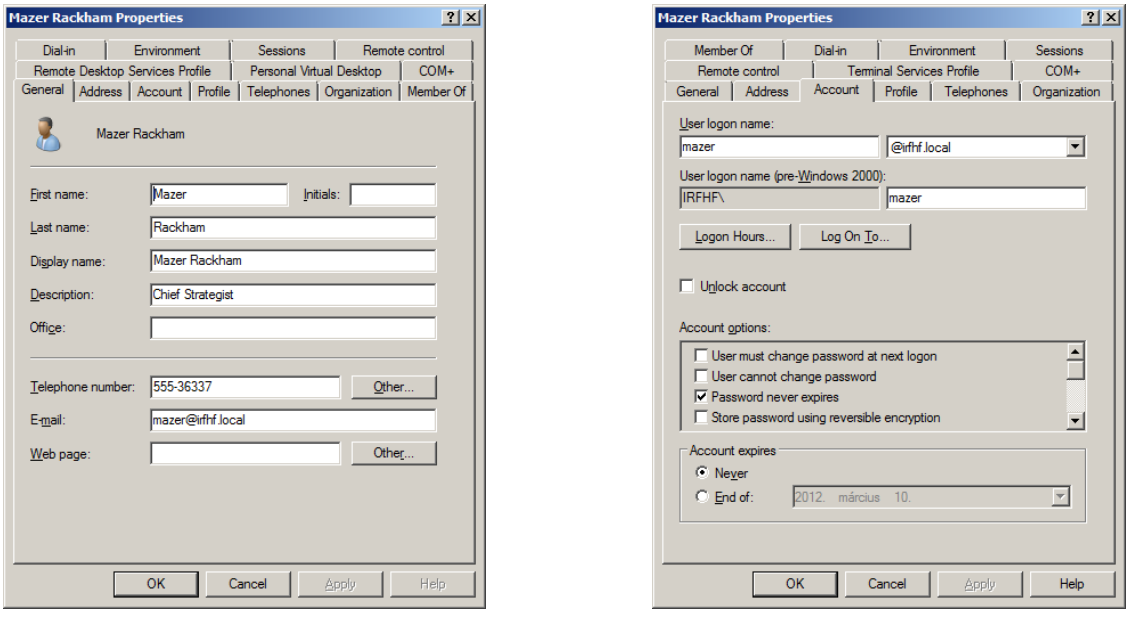
   Hozzunk létre további hierarchiaszinteket a címtárban a gyökértől kiindulva (11. ábra)! (LDAP címtár esetén elvileg megengedett, hogy tetszőleges típusú elemnek legyen gyereke, így mást is lehetne tárolónak használni, de az AD GUI-ja csak szervezeti egységet enged).




**10. ábra: A címtár jelenlegi hierarchiája**




**11. ábra: Új szervezeti egység létrehozása**




**12. ábra: Felhasználó általános tulajdonságai (bal) és bejelentkezési adatai (jobb)**

5. Felhasználók tulajdonságai

   Válasszuk ki a címtárban szereplő egyik felhasználót, és nézzük meg a tulajdonságait (12. ábra).

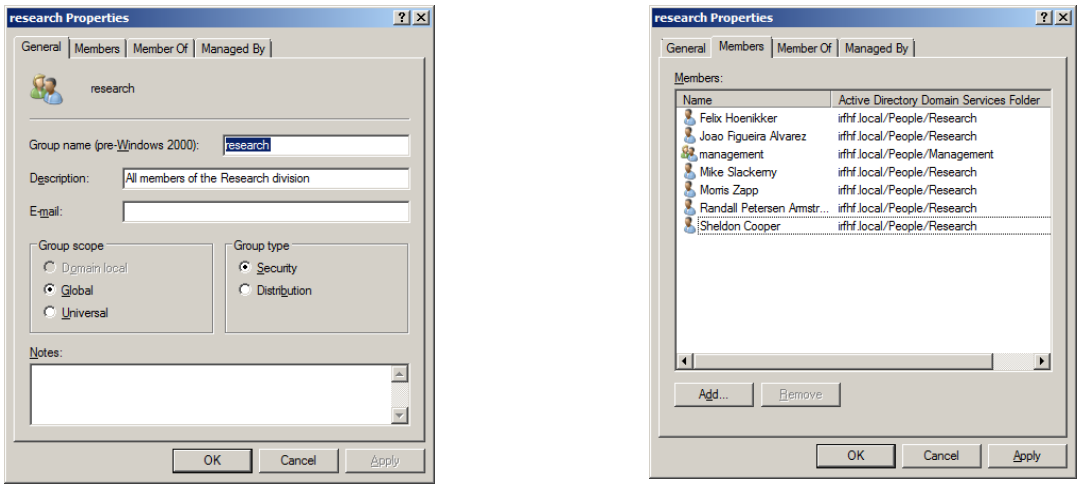
   a. Írjuk át valamelyik tulajdonságát!
   b. Keressük ki, hogy milyen csoportoknak a tagja!
   c. Hol tárolhatjuk a címtárban egy felhasználóról, hogy ki a felettese?
   d. Hozzunk létre egy új felhasználót, és állítsuk be az alaptulajdonságait!

   Most nézzük meg, hogyan lehet csoportokba foglalni a felhasználókat.

6. Csoportok kezelése

   *Csoport*okat (group) azért hozunk főleg létre Active Directory környezetben, hogy később felhasználók egy halmazának valamilyen közös jogosultságokat osszunk az operációs rendszerben vagy valamilyen más alkalmazásban (tehát csoportok segítségével valósítjuk meg a *Role Based Access Control* módszert).

   Válasszunk ki egy meglévő csoportot, és nézzük meg a tulajdonságait (13. ábra).




**13. ábra: Egy csoport általános tulajdonságai (bal) és tagjai (jobb)**

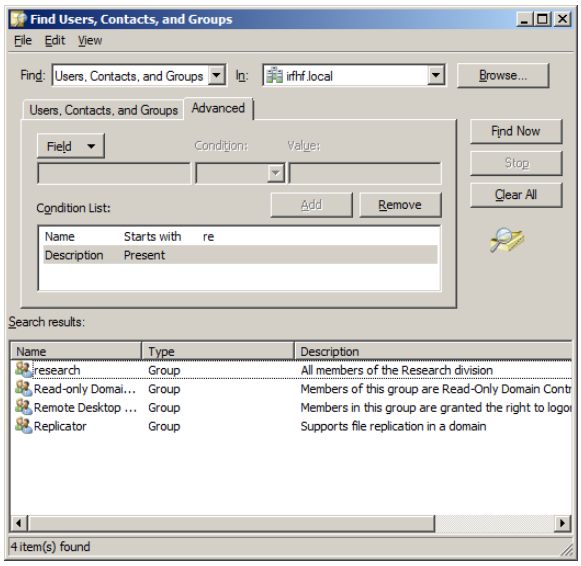
   Egy csoport esetén viszonylag kevés attribútumot lehet megadni (név, leírás, email…). Figyeljük meg viszont az ábrán, hogy csoportnak lehetnek más csoportok is a tagjai.

   a. Hozzunk létre egy új csoportot!
   b. Rakjunk bele meglévő felhasználókat és csoportokat az új csoportba!

   Most, hogy hozzáadtunk saját elemeket is a címtárhoz, próbáljunk meg keresni benne.

7. Keresés a címtárban

   Nyissuk meg a keresés ablakot (*Find…* a jobb gombos menüben). Alapesetben a név és leírás alapján lehet keresni, de az összetett nézetben egész bonyolult lekérdezéseket is meg lehet adni (14. ábra).




**14. ábra: Egy összetett keresés**

Keressük meg az olyan felhasználókat, akiknek a telefonszáma 555-tel kezdődik, és nincsen kitöltve az email címük!

Ezzel áttekintettük az Active Directory legalapvetőbb elemeit. További információért lásd a [9] magyar nyelvű könyvet.

## *3.2 AD Explorer*

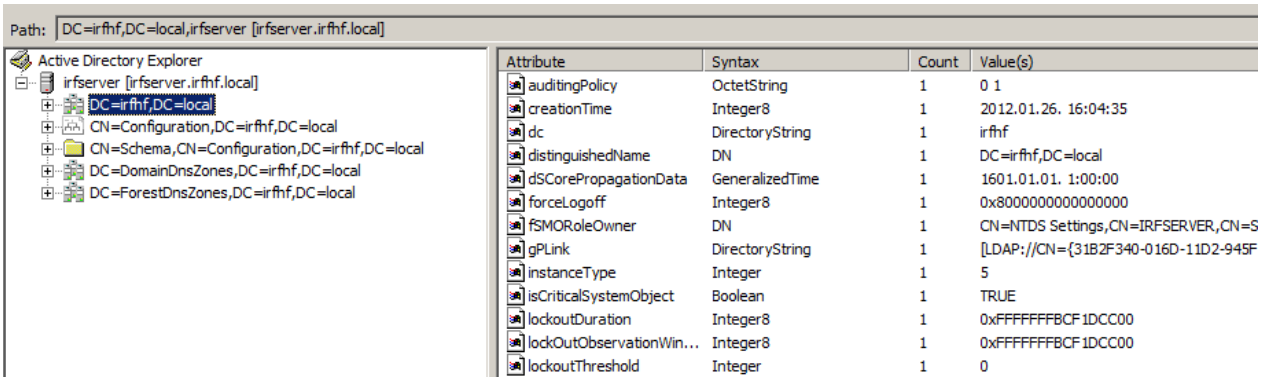
Most nézzünk be a „motorháztető alá", lássuk, hogy hogyan tárolja a címtár az elemeit. Ehhez a *Sysinternals AD Explorer* eszközt fogjuk használni.

1. Csatlakozás a címtárhoz

   Miután elindítottuk az AD Explorert, csatlakozzunk a tartományvezérlőhöz (*Connect to Active Directory* menüpont) az *Administrator* felhasználóval.

2. A címtár partíciói

   A csatlakozás után már egy más kép fogad minket (15. ábra), mint az ADUC GUI-ban.



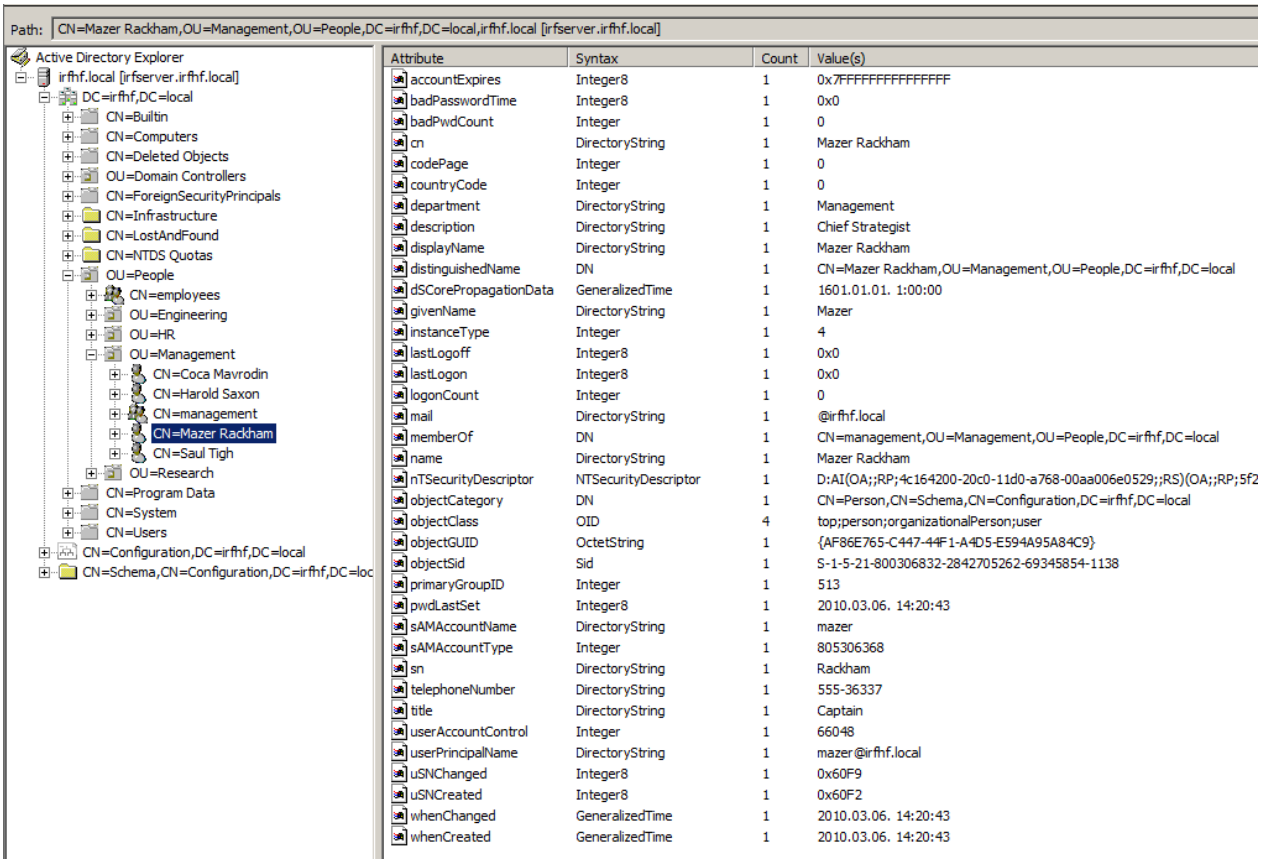

**15. ábra: A címtár partíciói az AD Explorer eszközből**

A címtárat itt is egy fa elemeiként látjuk, azonban itt már az elemek belső neve szerepel (pontosabban a DN-jük). Egy elem kijelölése esetén a jobb oldalon látjuk az attribútumai nevét, típusát és értékét is.

3. Tartományi partíció (Domain Directory Partition)

   A tartomány elemeit (felhasználók, számítógépek, csoportok, …) a tartományi partíció tárolja. Ezt jeleníti meg az *Active Directory Users and Computers* eszköz is, csak az egy egyszerűbben használható felhasználói felületet nyújt.

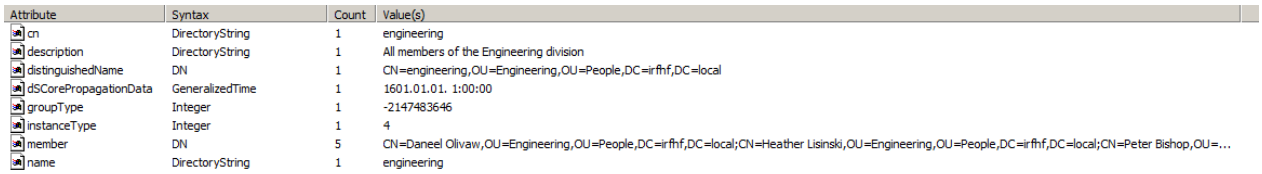
   Keressük ki az előző részben megtekintett felhasználónkat itt is (16. ábra).




**16. ábra: Egy felhasználó adatai az AD belső megjelenítésében**

   a. Mi a felhasználó *megkülönböztetett neve* (distinguished name, DN)? Vizsgáljuk meg, hogyan épül ez fel.
   b. Nézzük végig a felhasználó attribútumait! Melyik tárolja a login nevét?
   c. Azt, hogy milyen attribútumai vannak egy elemnek, az határozza meg, hogy milyen osztályoknak a példánya. Ezt az *objectClass* attribútum tárolja. Jelen esetben milyen osztályokat jelent ez?

**Feladat**: A DN fogalmának jobb megértése érdekében rajzoljuk fel a címtár egy részének a neveit (válasszunk ki két másik, különböző OU-ban lévő felhasználót, és rajzoljuk fel az ő és őseik viszonyát, valamint RDN és DN neveiket).



| Attribute | Syntax | Count | Value(s) |
|---|---|---|---|
| cn | DirectoryString | 1 | engineering |
| description | DirectoryString | 1 | All members of the Engineering division |
| distinguishedName | DN | 1 | CN=engineering,OU=Engineering,OU=People,DC=irfhf,DC=local |
| dSCorePropagationData | GeneralizedTime | 1 | 1601.01.01. 1:00:00 |
| groupType | Integer | 1 | -2147483646 |
| instanceType | Integer | 1 | 4 |
| member | DN | 5 | CN=Daneel Olivaw,OU=Engineering,OU=People,DC=irfhf,DC=local;CN=Heather Lisinski,OU=Engineering,OU=People,DC=irfhf,DC=local;CN=Peter Bishop,OU=... |
| name | DirectoryString | 1 | engineering |

**17. ábra: Csoporttagság – többértékű attribútumok**

Azt érdemes még megfigyelni, hogy hogyan tárolja a csoporttagságot a címtár. A felhasználónak van egy *memberOf* tulajdonsága, míg a csoportnak pedig egy *member* attribútuma (17. ábra). Mindkét attribútum lehet többértékű, ilyenkor az AD Explorer pontosvesszővel összefűzve jeleníti meg az egyes elemeket.

d. Próbáljuk meg módosítani a csoport tagjait úgy, hogy egy nem létező elemet adunk meg. Mi történik ilyenkor?
e. Mozgassunk át egy felhasználót egy másik szervezeti egységbe. Mi történik ilyenkor azoknál a csoportoknál, amiknek tagja?

Végezetül nézzük meg, hogy egy szervezeti egységnek milyen attribútumai vannak.

4. Séma partíció (Schema Directory Partition)

   A séma partícióban (`CN=Schema,CN=Configuration`) tárolja a címtár, hogy az egyes osztályokhoz milyen attribútumok tartoznak. Az osztály egy része általános (pl. *inetOrgPerson*), másik része pedig erősen Microsoft specifikus (pl. *ms-DFS-Link-v2*).

   Nézzük meg pár ismert osztály (pl. organizationalUnit, User) tulajdonságait.

## *3.3 Lekérdezés PowerShellből*

Két fő módon kérdezhetünk le PowerShellből AD címtárat. Az *AD Service Interface* (ADSI) általánosabb és elérhető a régebbi Windows Servereken is. Az *Active Directory Module for Windows PowerShell* pedig kifejezetten AD elérésére szolgáló célorientált cmdletek gyűjteménye, ami a Windows Server 2008 R2-ben bevezetett *AD Web Services* felületet használja a háttérben. A gyakorlaton ezt fogjuk használni (az ADSI-ról egy bemutató megtalálható a függelékben, de a házi feladatban erre nem lesz szükség).

A PowerShell második verziójában jelent meg az `ActiveDirectory` nevű új modul, mely 76 darab cmdletet biztosít az AD kényelmes kezelésére.

1. Az `ActiveDirectory` modul betöltése

   A következő paranccsal tudjuk betölteni a modult (erre 3-as PowerShellben nincs is szükség, ott automatikus modulbetöltés van már):

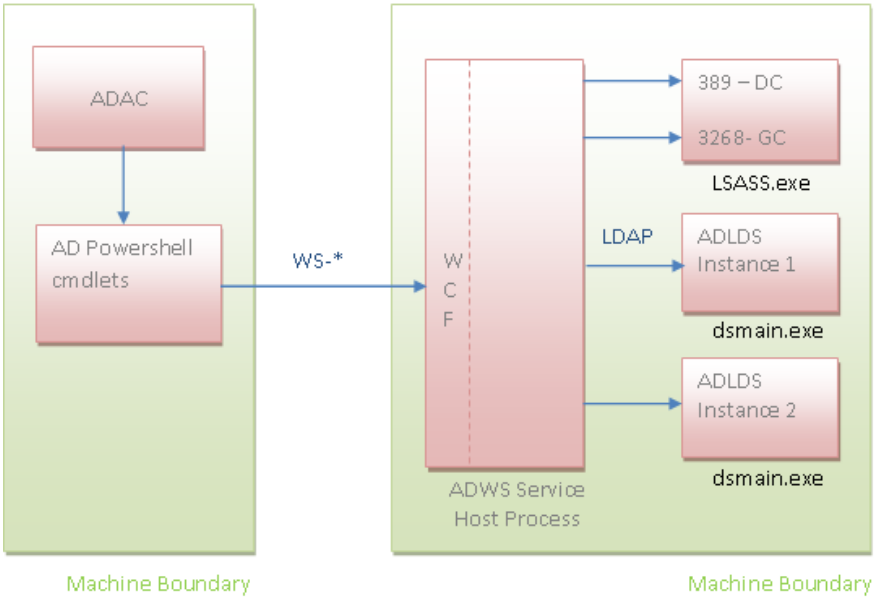
   ```
   Import-Module ActiveDirectory
   ```

   Kliens Windowsokon nem elérhető alapesetben ez a modul, azt a Remote Server Administration Toolkit (RSAT) [13] részeként lehet telepíteni.

2. Csatlakozás a címtárhoz

   A modul a háttérben nem az LDAP-protokollt, hanem egy új, webszolgáltatás alapú felületét használja az AD-nek. A rendszer architektúráját mutatja be a következő ábra

(18. ábra). Az *Active Directory Web Services* alapértelmezetten a 9389-es porton figyel, és a cmdletek ehhez csatlakoznak.




**18. ábra: Az Active Directory Web Service architektúrája [14]**

Amikor betöltjük az `ActiveDirectory` modult, akkor az megpróbál automatikusan csatlakozni az aktuális tartományhoz. Ha ez nem sikerülne (mert például a gépünk nem tagja a tartománynak), akkor a következő hibaüzenet kapjuk:

```
WARNING: Error initializing default drive: 'Unable to find a default server with
Active Directory Web Services running.'.
```

Ha tudjuk, hogy melyik tartományhoz akarunk kapcsolódni, akkor ennek a legegyszerűbb módja az, ha egy új PSDrive meghajtót hozunk létre:

```
New-PSDrive -Name AD -PSProvider ActiveDirectory -Root "" -Server "10.90.1.10"
-Credential irfhf\administrator
```

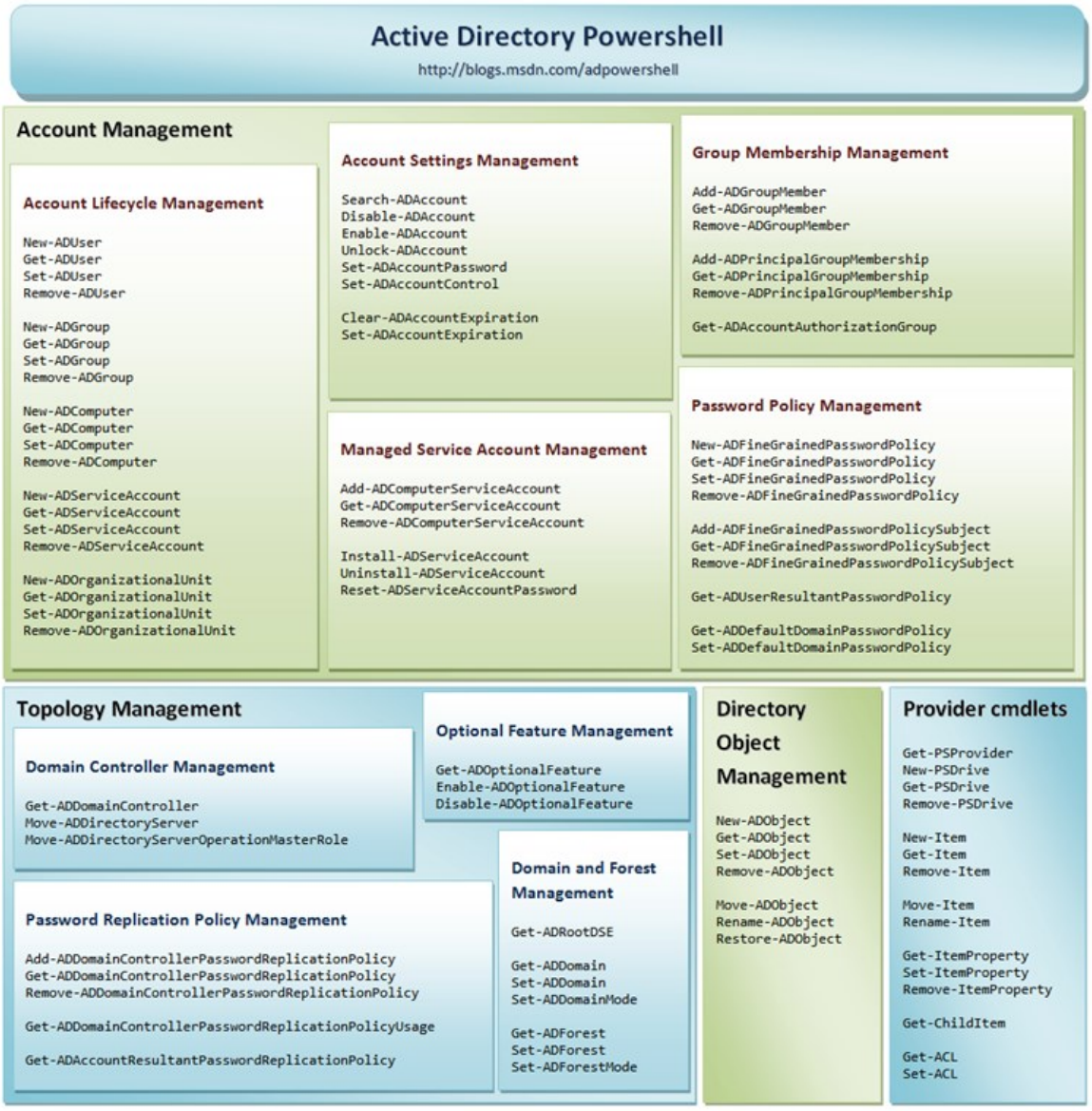
Itt most az egyik tartományvezérlő IP-címét adtuk meg közvetlenül, de az ActiveDirectory modul számos más módszert is biztosít a címtár megcímzésére.

3. Az elérhető cmdletek kilistázása

Gyors áttekintést kaphatunk az elérhető funkciókról, ha kilistázzuk az ActiveDirectory modulban lévő cmdleteket:

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

A könnyebb eligazodás kedvéért az alábbi ábra tematikusan csoportosítja az elérthető cmdleteket (19. ábra), ez egy jó kiindulópont lehet egy-egy feladat megoldása során.

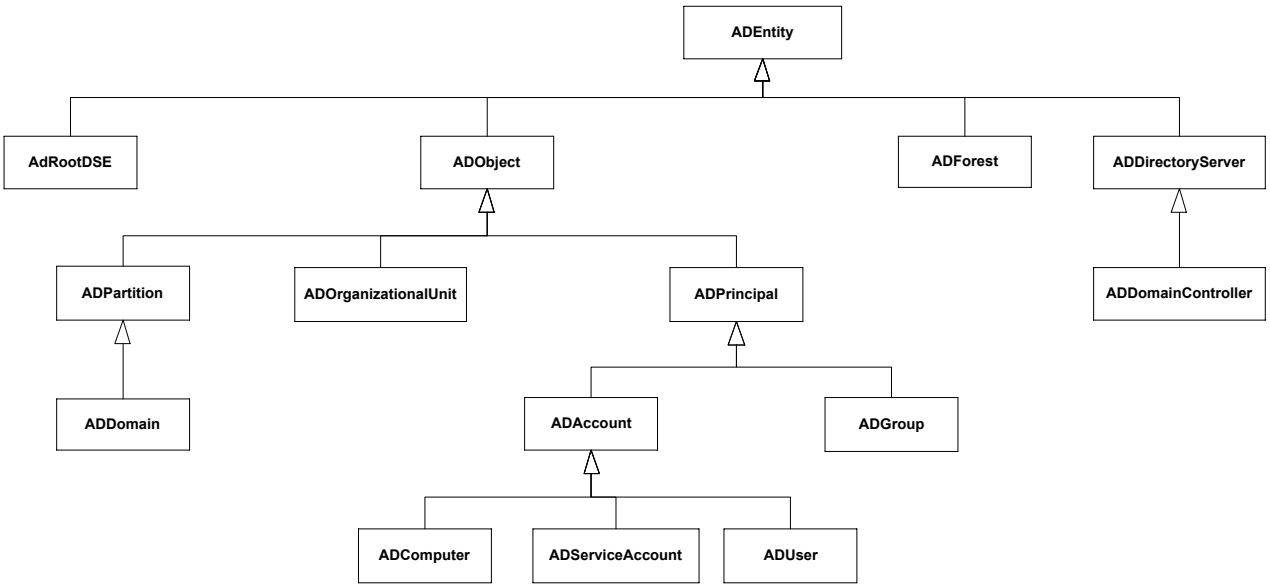



**19. ábra: PowerShell AD cmdletek listája [12]**

Tanulmányozzuk az ábrát, próbáljuk kitalálni, hogy mire szolgálnak az egyes főbb dobozok és a bennük lévő cmdletek! (A Topology Management tartalmára első körben valószínűleg nem lesz szükségünk.)

4. Az ActiveDirectory modul objektumainak modellje

   Az `about_ActiveDirectory_ObjectModel` súgó téma részletes leírást tartalmaz arról, hogy az egyes objektumok milyen típusú információt tárolnak. A közöttük lévő öröklési kapcsolat ott szövegesen van ismertetve, az alábbi ábra a legfontosabb elemeket grafikus formában jeleníti meg (20. ábra).




**20. ábra: Az ActiveDirectory modul fontosabb osztályai**

5. Navigálás az AD: meghajtóban

   Az AD: meghajtó látszólag ugyanolyan meghajtó, mint a többi, a megszokott parancsokkal tudunk navigálni benne, pl. `cd` (`Set-Location`), `ls` (`Get-ChildItem`):

```
PS C:\> cd AD:
PS AD:\> dir

Name                ObjectClass     DistinguishedName
----                -----------     -----------------
irfhf               domainDNS       DC=irfhf,DC=local
Configuration       configuration   CN=Configuration,DC=irfhf,DC=local
Schema              dMD             CN=Schema,CN=Configuration,DC=irfhf,DC=local
DomainDnsZones      domainDNS       DC=DomainDnsZones,DC=irfhf,DC=local
ForestDnsZones      domainDNS       DC=ForestDnsZones,DC=irfhf,DC=local
```

   (A példakódokban most szerepel majd a prompt is, és nem csak a végrehajtandó utasítás, hogy lássuk, hogy mi az aktuális könyvtár éppen.)

   Arra figyeljünk csak, hogy az elemekre a DN-jükkel vagy az RDN-jükkel kell hivatkozni, és nem a sima nevükkel:

```
PS AD:\> cd '.\DC=irfhf,DC=local'
```

   Működik az automatikus kiegészítés is (`TAB`), csak itt is a DN-t vagy RDN-t kell elkezdeni beírni. DN megadása esetén figyeljünk, hogy idézőjelek közé kell rakni, hisz egyéb esetben a vesszőt a PowerShell tömboperátorként értelmezné.

```
PS AD:\DC=irfhf,DC=local> cd .\OU=People
PS AD:\OU=People,DC=irfhf,DC=local> cd c:
PS C:\> cd "AD:\OU=People,DC=irfhf,DC=local"
```

Az AD: meghajtóban navigálva egyszerűbb kereséseket és szűréseket is el tudunk végezni:

```
PS AD:\OU=People,DC=irfhf,DC=local> ls -Recurse | ? {$_.ObjectClass -eq "group"}
```

a. Keressük meg a People OU-ban lévő olyan felhasználókat, akiknek J-vel kezdődik a neve!

Az AD elemek kezelésére a másik lehetőség, hogy a dedikált cmdleteket használjuk.

6. Felhasználó lekérdezése

Kiindulásképpen kérdezzünk le egy konkrét felhasználót:

```
PS C:\> Get-ADUser sheldon
```

TIPP: a Get-AD* cmdletek használához már nem kell az AD: meghajtót használni, az bármilyen könyvtárból működik.

Válaszként visszakapunk egy `Microsoft.ActiveDirectory.Management.ADUser` típusú objektumot, valamint a képernyőn megjelennek a legfontosabb tulajdonságai:

```
DistinguishedName : CN=Sheldon Cooper,OU=Research,OU=People,DC=irfhf,DC=local
Enabled           : True
GivenName         : Sheldon
Name              : Sheldon Cooper
ObjectClass       : user
ObjectGUID        : 277903d8-860f-4c08-9362-905b93b280b9
SamAccountName    : sheldon
SID               : S-1-5-21-2841431523-2606397889-4261208849-1112
Surname           : Cooper
UserPrincipalName : sheldon@irfhf.local
```

Ha le akarjuk kérdezni az összes tulajdonságát, akkor azt a következő módon tudjuk megtenni:

```
Get-ADUser sheldon -Properties *
```

Felhasználót létrehozni a `New-ADUser` segítségével lehet. Próbáljuk is ki, hozzunk létre egy új felhasználót!

7. Keresés a címtárban

Keresni az egyes cmdletek `-Filter` paraméterével lehet, ilyenkor a feltételt a PowerShell saját *PowerShell Expression Language* nyelvén lehet megfogalmazni. Az `LDAPFilter` paraméter segítségével pedig a megszokott LDAP keresési szintaxist lehet használni.

A keresés mélységét és irányát az LDAP-ból ismert `SearchBase` és `SearchScope` paraméterekkel lehet befolyásolni.

Ha nem egy specifikus elemtípusra akarunk keresni (pl. csoport, felhasználó), akkor használhatjuk a `Get-ADObject` cmdletet:

```
Get-ADObject -Filter 'CN -like "m*"' -SearchBase "OU=People,DC=irfhf,DC=local" `
-SearchScope Subtree
```

A fenti parancs például megkeresi az összes objektumot, akinek *m* betűvel kezdődik a CN attribútuma a megadott szervezeti egységben. A keresés hasonlóan működik a specifikusabb cmdletekkel is.

Nézzünk most egy összetettebb lekérdezést:

```
Get-ADuser -Filter 'name -like "m*" -and mail -like "m*"' -SearchBase
"OU=People,DC=irfhf,DC=local"
```

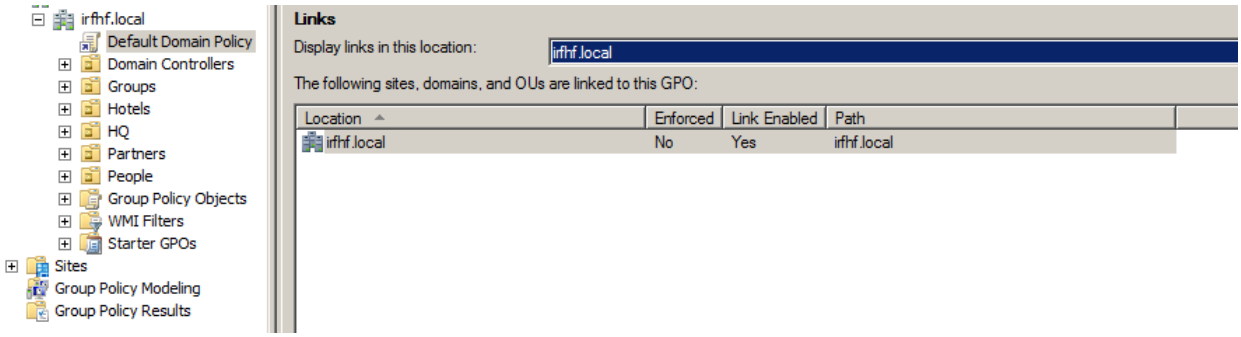
Itt lekérdeztük az olyan felhasználókat, akik az adott OU-ban vannak, és *m*-mel kezdődik a nevük és az e-mail címük is. Figyeljük meg, hogy a keresési kifejezésben itt is használhatjuk az LDAP attribútumok nevét.

További példákat az `about_ActiveDirectory_filter` súgó témában találunk.

Az ActiveDirectory modul részletes leírása megtalálható a PowerShell könyv [11] 2.13. fejezetében.

## 3.4 Csoportházirendek

Zárásként nézzük meg egy picit a csoportházirendeket, mely az AD környezetben a központi menedzsment és jogosultságosztás legfontosabb eleme. A csoportházirendek kezelését a *Group Policy Management Console* felületről végezhetjük el (21. ábra).




**21. ábra: Group Policy Management Console felülete**

1. Ismerkedés a konzollal

   Nyissuk meg a Group Policy Management Console felületet.

   Legalább egy házirendnek minden tartományban kell léteznie, ez pedig a *Default Domain Policy*. Nézzük meg a tulajdonságait (*Scope*, *Details* fül).

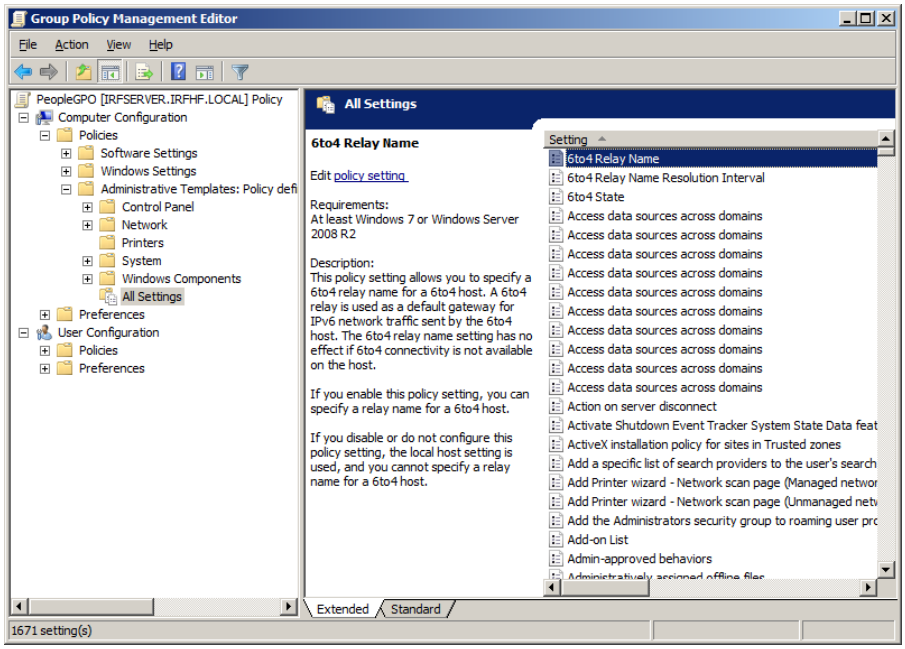
   Nézzük meg, hogy milyen beállítások vannak megadva rá (*Settings* fül). Miket szabályoznak ezek a beállítások?

2. Házirend szerkesztése

   Minden szervezeti egységhez (OU) lehet külön házirendet készíteni vagy csatolni. Szerkesszük a *People* OU-hoz rendelt házirendet (22. ábra).

A házirendben külön lehet megadni számítógép és felhasználó specifikus beállításokat, valamint kötelezően érvényre jutó (policy) és ajánlott beállításokat (preferences).

a. A számítógéphez tartozó *Windows Settings* résznél keressük ki a *Security* eseménynapló maximális méretét szabályozó beállítást, és állítsuk be 32 MB-ra!
b. Az Administrative Templates részben szereplő házirendek között a Filter opcióval (Action menü) lehet részletesen keresni. Keressük ki azokat a beállításokat, amikben a DHCP kulcsszó szerepel! (Vigyázat: a keresési kifejezés beírásakor legyen angol a billentyűzetkiosztás, különben nem talál semmit.)
c. Nézzük meg a felhasználói beállításokat is! Hol lehet szabályozni, hogy a felhasználók Asztalán megjelenjen-e a Lomtár ikon?




**22. ábra: Csoportházirend szerkesztése**

Az itt bemutatottak csak a csoportházirendek legalapvetőbb funkciói. Az újabb szerververziókban 3000-nél is több beállítást lehet megadni házirendekkel. Bővebb információ a [9] könyvben található.

# 4 Összefoglalás

A gyakorlat során áttekintettük az LDAP-hoz kapcsolódó ajánlások alapjait. Megismerkedtünk az LDAP címtár felépítésével, az LDAP-protokollal és a hozzá kapcsolódó hitelesítési módszerekkel. Néhány egyszerűbb példán keresztül megnéztük az LDIF formátumot. Ha valamelyik fogalomban még nem vagyunk biztosak, akkor az „LDAP for Rocket Scientists" online könyvben [8] érdemes utánakeresni (a Concepts és a Glossary része nagyon jó) vagy megnézni a kapcsolódó RFC-ben.

Az első gyakorlati példánk az openLDAP és a kapcsolódó linuxos eszközök voltak. Itt a parancssori eszközökhöz az LDIF formátumot kell alaposabban tanulmányozni. Ha valahol elakadunk, és az ldap* parancsok manual oldala nem segít (sajnos elég szűkszavúak), akkor szintén a [8] könyvben találunk segítséget (8. és 14. fejezet).

Windows esetén az Active Directoryt vizsgáltuk meg, a gyakorlati anyag bemutatta mind a grafikus felületét, mind a kezeléséhez szükséges PowerShell cmdleteket. Itt ha elakadunk, akkor a magyar nyelvű PowerShell könyvet [11] érdemes fellapozni.

## *4.1 További információ*

LDAP (általános)

[1] Internet Engineering Task Force. „Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006

[2] Internet Engineering Task Force. „Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006

[3] Internet Engineering Task Force. „Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006

[4] Internet Engineering Task Force. „Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters", RFC 4515, June 2006

[5] Internet Engineering Task Force. „Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms", RFC 4513, June 2006

[6] Internet Engineering Task Force. „The LDAP Data Interchange Format (LDIF) - Technical Specification", RFC 2849, June 2000

Linux

[7] The OpenLDAP Project. „OpenLDAP Software 2.4 Administrator's Guide", 12 February 2012, elérhető online: http://www.openldap.org/doc/

[8] Zytrax.com. „LDAP for Rocket Scientists", Open Source Guide, version 0.1.14, elérhető online: http://www.zytrax.com/books/ldap/

Windows

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

[10] PowerShell Pro blog. „Managing Active Directory with Windows PowerShell", PowerShell Tutorial, elérhető online: http://www.powershellpro.com/powershell-tutorial-introduction/powershell-tutorial-active-directory/

[11] 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

[12] 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

[13] Active Directory PowerShell Blog. „Active Directory Powershell: Installation using RSAT on Windows 7”, 24 Mar 2009, elérhető online: http://blogs.msdn.com/b/adpowershell/archive/2009/03/24/active-directory-powershell-installation-using-rsat-on-windows-7.aspx

[14] 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

# 5 Függelék

A függelék az érdeklődőknek tartogat némi kiegészítő információkat, ami segít kicsit jobban megismerni az openLDAP-ot.

## *5.1 DIGEST-MD5 hitelesítés használata openLDAP esetén*

A következő rövid leírás bemutatja, hogy hogyan lehet DIGEST-MD5 hitelesítést használni az LDAP-hoz kapcsolódás során. A főbb lépések a következők:

- DIGEST-MD5 mechanizmus engedélyezése,
- az operációs rendszer SASL komponensében a felhasználó(k) DIGEST jelszavának megadása,
- az úgynevezett Identity mapping, azaz a hitelesítés során megadott külső felhasználónevet kell egy LDAP DN-re leképezni.

CentOS 6.2 és openLDAP 2.4.24 esetén ezeket a következő módon lehet végrehajtani.

1. DIGEST-MD5 mechanizmus engedélyezése

   Az LDAP szervertől le lehet kérdezni, hogy milyen mechanizmusokat támogat jelenleg, ezt az információt az LDAP legfelső bejegyzésétől le lehet kérdezni (az az úgynevezett root DSE[10]). A root DSE-t alapesetben a kliensekben nem látjuk, a következő módon kérdezhetőek le az attribútumai:

   ```
   ldapsearch -x -H ldap://localhost:389 -b "" -LLL -s base +
   ```

   (A -LLL hatására a megjegyzések nem jelennek meg, a + pedig megjeleníti az úgynevezett operational attribútumokat is.)

   A kimenetből a `supportedSASLMechanisms` attribútum érdekes most számunkra. Ha a DIGEST-MD5 nem szerepel értékként, akkor a SASL komponensben telepíteni kell azt is. CentOS esetén ezt a következő paranccsal lehet telepíteni:

   ```
   yum install cyrus-sasl-md5
   ```

2. DIGEST jelszó megadása

   Az SASL komponens egy külön adatbázist tárol a jelszavakról, ebbe a következő paranccsal lehet beírni a jelszavunkat:

   ```
   [root@irf ~]# saslpasswd2 root
   ```

   Ezen kívül feltétel még, hogy az LDAP felhasználónak, akinek majd megfeleltetjük ezt a felhasználót, a jelszavát nyílt szöveggént kell tárolni a `userPassword` attribútumában.

[10] Nem összetévesztendő az úgynevezett naming contextek gyökérelemével (pl. dc=irf,dc=local), ez annál eggyel magasabb szintű elem. Ez tárolja például azt is, hogy a szerveren milyen naming contextek érhetőek el.

3. Felhasználó leképezés megadása

   DIGEST-MD5 esetén a SASL komponens a felhasználó nevét `uid=<username>,cn=digest-md5,cn=auth` formában adja át majd az LDAP-nak. Ezért meg kell valahol mondani, hogy ehhez melyik, az LDAP-ban definiált DN tartozik. Ezt tipikusan az LDAP beállításainál az `authz-regexp` attribútummal tudjuk szabályozni.

   Az openLDAP 2.4-es verziójától a korábbi `sldap.conf` szöveges konfigurációfájlról áttértek futási idejű konfigurációra, azaz az LDAP szerver a saját beállításait is LDAP-ban tárolja, a `cn=config` naming contextben. (Ami egy jó ötlet lenne, a gond csak az, hogy a dokumentációk nagy része még sokszor a régi módszert írja le, ezen kívül nem is olyan egyszerű szerkeszteni ezt.)

   A konfigurációs beállítások definíciót a következő manualban tudjuk megnézni:

   ```
   man slapd-config
   ```

   Nézzük meg, ki férhet hozzá a cn=config adatbázishoz! Ezt az olcAccess attribútuma tárolja:

   ```
   slapcat -n 0 -H ldap:///olcDatabase={0}config,cn=config
   ```

   (Az `slapcat` közvetlenül az adatokat tároló adatbázis tartalmát listázza, nem használja az LDAP protokollt az elérésre. A 0-s adatbázis mindig a konfigurációt tároló adatbázis. Az `slapcat` és egyéb `slap*` parancsokkal óvatosan bánjunk, mert akár inkonzisztens állapotot is elő lehet vele idézni.)

   A kimenetben a kiadott virtuális gépen használt openLDAP-ban a következő beállítás szerepel:

   ```
   olcAccess: {0}to *  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,
    cn=auth" manage  by * none
   ```

   Tehát a konfigurációs részt csak az operációs rendszer root felhasználója tudja elérni (korábbi dokumentációk egy `cn=admin,cn=config` felhasználót feltételeznek, de az most itt nem létezik).

   Adjunk hozzá egy leképezést, ami egyelőre csak a root felhasználóról gondoskodik. A következő LDIF fájl tartalmazza a módosításokat:

   ```
   dn: cn=config
   changetype: modify
   add: olcAuthzRegexp
   olcAuthzRegexp: uid=root,cn=[^,]*,cn=auth cn=admin,dc=meinedomain,dc=local
   ```

   Ezt a következő módon tudjuk betölteni (a fenti részletet auth.ldif néven elmentve):

   ```
   ldapadd -Y EXTERNAL -H ldapi:/// -f auth.ldif
   ```

   (Itt most az EXTERNAL mechanizmust használtuk a hitelesítésre, az `ldapi:///` pedig azt jelzi, hogy a parancsot végrehajtó felhasználó adatait használja fel.)

4. Hitelesítés kipróbálása

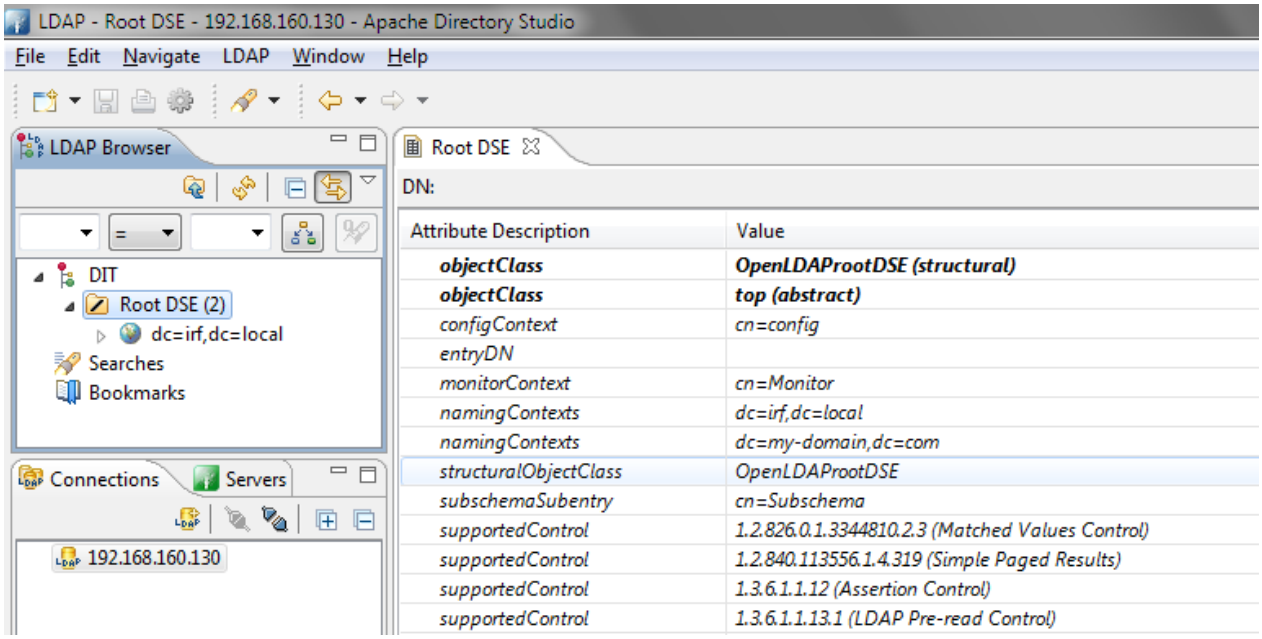
   A hitelesítés kipróbálására jó módszer az `ldapwhoami` parancs:

```
[root@irf ~]# ldapwhoami -Y DIGEST-MD5
SASL/DIGEST-MD5 authentication started
Please enter your password:
SASL username: root
SASL SSF: 128
SASL data security layer installed.
dn:cn=root,dc=irf,dc=local
```

   Látszik, hogy sikeres volt a hitelesítés, és a root linuxos felhasználó a `cn=root,dc=irf,dc=local` felhasználóra képződött le.

5. Csatlakozás kipróbálása másik gépről

   A hitelesítés beállításának igazából akkor van haszna, ha távoli gépről csatlakozunk a címtárhoz. Ezt könnyen ki is próbálhatjuk például az Apache Directory Studio[11] segítségével, ami egy jól használható grafikus felületet biztosít az LDAP címtár elérésére.




**23. ábra: Az Apache Directory Studio felülete**

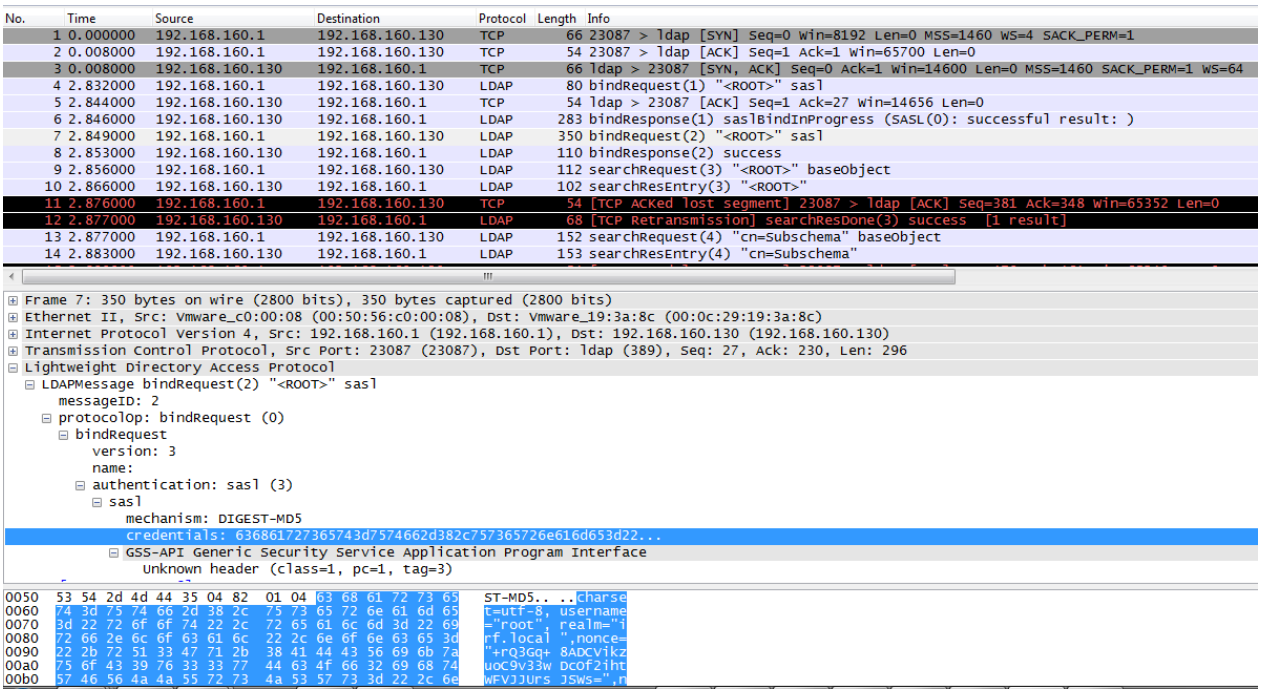
   A kapcsolat létrehozásánál az eddig ismertetett biztonsági beállításokat mind megadhatjuk. A legegyszerűbb teszthez adjuk meg a következőket:

   - Network parameters: hostname (VM IP-címe), port (389), No encryption
   - Authentication: authentication method (DIGEST-MD5), Bind DN or user (root)

[11] http://directory.apache.org/studio/

Ezek után kapcsolódjunk (*Open connection*), és a jelszó megadása után tudjuk is böngészni a címtárat (23. ábra).

Azt érdemes még megnézni, hogy a háttérben milyen kommunikáció zajlik, ezt például Wiresharkban tudjuk megfigyelni (24. ábra). Az ábrán látható, hogy a TCP kapcsolat felépítése után a kliens egy `bindRequest` üzenetet küld, a kiszolgáló a `bindResponse` üzenetben jelzi, hogy további adatokat vár az SASL hitelesítéshez, majd a kliens a 7-es számú keretben átadja a DIGEST-MD5 mechanizmushoz tartozó adatokat (legalul látszik a Credentials mező tartalma is). A jelszó tehát titkosítva megy át, de az is látszik, hogy a további forgalom titkosítás nélkül halad.




**24. ábra: LDAP kapcsolódás hálózati forgalma**

## *5.2 ADSI használata*

Az ADSI segítségével LDAP címtárakhoz vagy a Windows helyi felhasználói adatbázisához lehet csatlakozni, ott keresni és elemeket manipulálni. Az ADSI használatának folyamata:

- csatlakozás a címtár gyökeréhez vagy egy konkrét elemhez,
- a címtár eleméhez tartozó attribútumok módosítása,
- változtatások visszamentése.

1. Csatlakozás a címtárhoz.

   ADSI használata esetén az [ADSI] típus adaptert (type adapter) kell használni egy LDAP nevet tartalmazó sztringgel együtt. Több lehetőségünk is van:

   ```
   $root=[ADSI]""
   ```

Így az alapértelmezett tartomány (aminek a számítógép a tagja) gyökéreleméhez csatlakozunk. Hasonló eredményt érünk akkor is, ha explicit megnevezzük a tartományt:

```
$r = [ADSI]"LDAP://dc=irfhf,dc=local"
```

FIGYELEM: az ADSI ennél a sztringnél az LDAP szó esetén érzékeny a nagybetűkre, ha nem így írjuk, akkor `"Unknown error (0x80005000)"` hibát kaphatunk.

Lekérhetünk közvetlenül egy felhasználót, szervezeti egységet vagy csoportot is:

```
$e = [ADSI] "LDAP://cn=engineering,OU=engineering,OU=People,DC=irfhf,DC=local"
```

Egy LDAP objektum nevét könnyedén átmásolhatjuk az AD Explorerből az elem jobb gombos menüjében található *Copy Object Name* paranccsal.

Az így visszakapott objektum rendelkezik az összes, az LDAP-ban megadott attribútumával, tehát például a

```
$e.member
```

változó visszaadja a csoport tagjait.

a. Próbáljuk meg lekérdezni a csoport leírását valamint a SID-jét is!

Az ADSI nem tölti be mindegyik attribútumot automatikusan az objektum mezőibe. Ha valamit nem talál, pedig a címtárban benne van, akkor érdemes a `Get()` metódushívással próbálkozni:

```
$e.Get("mail")
```

Ha elírjuk az objektum nevét az ADSI kérésben, akkor a következő hibát kaphatjuk, amikor először megpróbáljuk elérni az objektumot:

```
"There is no such object on the server."
```

2. Objektum módosítása

Egy visszakapott objektumot könnyen módosíthatunk: csak új értéket kell adni a megfelelő attribútumának, majd meghívni a `SetInfo()` metódust rajta. (A metódushívás nélkül a változtatás nem látszik a címtárban!)

```
$e.description = "New description"
$e.SetInfo()
```

3. Objektumok létrehozása

Új elem létrehozásához a majdani szülőjét kell először lekérni, majd annak a `Create()` metódusát kell meghívni. Ez a metódus első paraméterként az új elem típusát várja (egy LDAP sémabeli osztály), másodikként pedig az új elem RDN-jét.

Nézzünk egy példát egy új szervezeti egység létrehozására:

```
$ou = [ADSI] "LDAP://OU=engineering,OU=People,DC=irfhf,DC=local"
$newOu = $ou.Create("organizationalUnit", "ou=maintenance")
$newOu.SetInfo()
```

Figyeljük meg, hogy a változtatások itt is csak a `SetInfo` hívás után lépnek életbe.

Egy felhasználó létrehozásakor érdemes még legalább pár másik értéket is megadni:

```
$ou = [ADSI] "LDAP://OU=engineering,OU=People,DC=irfhf,DC=local"
$newUser = $ou.Create("user", "cn=Montgomery Scott")
$newUser.put("sAMAccountName", "scotty")
$newUser.put("userPrincipalName", "scotty@irfhf.local")
$newUser.SetInfo()
```

Most megadtuk a bejelentkezési nevét (user logon name) két formában, de ezen kívül valós környezetben természetesen a vezeték és keresztnevét, e-mail címét stb. is hasznos lenne kitölteni.

4. Keresés

   Az AD-ben való kereséshez a .NET keretrendszer `DirectorySearcher` osztályát lehet segítségül hívni. Lássunk egy egyszerű keresést:

```
$objDomain = [ADSI]"LDAP://DC=irfhf,DC=local"
$objSearcher = New-Object System.DirectoryServices.DirectorySearcher
$objSearcher.SearchRoot = $objDomain
$objSearcher.Filter = "(&(cn=i*)(objectClass=group))"
$objSearcher.SearchScope = "Subtree"
$colResults = $objSearcher.FindAll()
$colResults | % {echo "Name: $($_.Properties.name)" }
```

   Ez a teljes címtárban megkeresi azokat a csoportokat, amiknek a neve i betűvel kezdődik. A keresés mélysége, a visszaadott elemek száma és tulajdonságai mind-mind beállíthatóak.

Bővebb leírást a [10] cikkben vagy a PowerShell könyv [11] 3.5 fejezetében találhatunk az ADSI használatáról.