# Címtárak kezelése

Gyakorlati útmutató Készítette: Micskei Zoltán Utolsó módosítás: v1.6, 2015.03.14..

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	z LDAP-ról általánosan	2
2	Li	nux: openLDAP	4
	2.1	Ismerkedés az LDAP címtárral	4
	2.2	Az LDAP címtár kezelése parancssori eszközökkel	
3	W	indows: Active Directory	
	3.1	Active Directory Users and Computers	
	3.2	AD Explorer	20
	3.3	Lekérdezés PowerShellből	
	3.4	Csoportházirendek	27
4	Ös	sszefoglalás	
	4.1	További információ	29
5	Fü	iggelék	
	5.1	DIGEST-MD5 hitelesítés használata openLDAP esetén	

# 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 *sémá*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 bejegyzést RDN-jének és a szülője DN-jének összefűzésével kapjuk.

Egy címtár szerveren belül a címtár csúcsa az úgynevezett *root DSE*<sup>1</sup>, 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<sup>2</sup>. Egy naming contextet az úgynevezett *root DN*-jével azonosítják<sup>3</sup>, 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 cn a common name attribútum neve, a leggyakrabban ezt használjuk egy elem nevének a megadására. A dc a domain component rövidítése, a gyökérelem neve konvenció szerint a DNS nevet követ, ennek a részeit vesszük fel. 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

<sup>&</sup>lt;sup>1</sup> A DSE a *DSA-specific entry* rövidítése, ahol a DSA a *Directory System Agent* rövidítése, ami a címtárat tároló szervert jelöli.

<sup>&</sup>lt;sup>2</sup> Az LDAP továbbá lehetővé teszi, hogy részfák kezelését és tárolását delegáljuk másik szervereknek.

<sup>&</sup>lt;sup>3</sup> Pontosabban a szabvány ezt *context prefix*nek hívja, de a gyakorlatban erre root DN néven hivatkoznak.

alatta levő 5 elem. A cn=joe testvére a 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<sup>4</sup> (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

<sup>&</sup>lt;sup>4</sup> Az LDAP nem érzékeny a kis- és nagybetű közötti különbségre.

## 2 Linux: openLDAP

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

- openLDAP<sup>5</sup> 2.4.40 LDAP címtár,
- Apache Directory Studio<sup>6</sup> 2.0 LDAP böngésző,
- PyLDAP<sup>7</sup> modul LDAP címtár elérése Pythonból,
- Példa elemek a címtárban<sup>8</sup>.

## 2.1 Kapcsolódás a címtárhoz Apache Directory Studio programmal

Az openLDAP kiszolgálónak nincs grafikus felülete, így az ismerkedéshez érdemes az Apache Direcotry Studio programot használni.

1. Indítsuk el a virtuális gépet!

A gyakorlati anyagban az Apache Directory Studio programot a virtuális gépen futtatjuk, így indítsuk el a grafikus felületét. De lehetne akár távolról is csatlakozni a szerverhez, ilyenkor értelemszerűen majd a virtuális gép IP-címét kell megadni csatlakozáskor.

2. Indítsuk el az Apache Directory Studio programot.



2. ábra: Az Apache Directory Studio indítóképernyője

3. A Directory Studio lehetőségei közül mi most az LDAP Browser funkciót fogjuk használni. Hozzunk létre egy új LDAP kapcsolatot (*LDAP* menü/*New Connection…*).

A helyi kiszolgálóhoz csatlakozunk, így a gépnév localhost legyen (3. ábra). A virtuális gép tűzfalán nyitva vannak az LDAP portok, így akár távolról is tudnánk csatlakozni.

<sup>&</sup>lt;sup>5</sup> openLDAP szerver, URL: <u>http://www.openldap.org/</u>

<sup>&</sup>lt;sup>6</sup> Apache Directory Studio, URL: <u>http://directory.apache.org/studio/</u>

<sup>&</sup>lt;sup>7</sup> pyLDAP modul, URL: <u>https://github.com/Noirello/PyLDAP/</u>

<sup>&</sup>lt;sup>8</sup> Hasonló jellegű tesztadatok generálásáról lehet itt olvasni: Darvas Dániel. "Active Directory tesztadatok generálása" URL: <u>http://blog.inf.mit.bme.hu/?p=394</u>

A gyakorlat és a házi feladat során egyszerűsítésként nem használunk titkosított csatornát, de ez éles környezetben nem javasolt!

~	New LDAP Connection	<b>^ 0</b>	+ 😣
Network Paramete	F		
Please enter connec	tion name and network parameters.	LDA	P
Connection name: i	fserver		
Network Parameter-			
Hostname:	localhost		~
Port:	389		~
Encryption method:	No encryption		~
	Server certificates for LDAP connections ' <u>Certificate Validation</u> ' preference page.	can be managed in the	
Provider:	Apache Directory LDAP Client API		~
		Check Network Paramete	er
🗆 Read-Only (preve	nts any add, delete, modify or rename op	eration)	

3. ábra: LDAP kapcsolat beállításai

4. Hitelesítési adatok megadása

Hogy hozzáférjünk a címtár minden részéhez, és, hogy módosítani is tudjuk később, adjunk meg hitelesítési adatokat is (4. ábra).

A *Simple Authentication* mód esetén felhasználónevet és jelszót vár (a felhasználót már a DN-jével kell megadni!). A szerver támogat más hitelesítési módokat is egyébként.

Csatlakozáshoz használjuk a cn=Manager,dc=irf,dc=local felhasználót. A címtárat úgy állítottuk be, hogy ez a felhasználó mindenhez hozzáférjen. Figyeljük meg, hogy ez már nem egy operációs rendszer szintű felhasználó (mint a root vagy a meres), hanem az LDAP egy saját felhasználója.

<b>1</b>	New LDAP Connection	↑ □ X				
Authentication Please select an authentication method and input authentication data.						
Authentication Method Simple Authentication						
Authentication Par	ameter					
Bind DN or user: cn=Manager,dc=irf,dc=local						
Bind password:						
Save password Check Authentication						
SASL Settings						
▸ Kerberos Settin	gs					

4. ábra: LDAP hitelesítési adatok megadása

5. Base DN megadása

Megadhatjuk, hogy a címtár melyik részfájához akarunk csatlakozni. A példa virtuális gépen csak egy ilyen base DN van, így a *Fetch Base DNs* megnyomása után automatikusan ez lesz kijelölve.

Ezen a képernyőn még a kapcsolat további beállításait lehet szabályozni (pl. letöltse-e a működési attribútumokat is, amik nem felhasználói, hanem a címtár működéséhez szükséges adatokat tárolnak).

	n ^ o + 😣			
Browser Options You can specify additional parameters for browsing th	e directory.			
Base DN Get base DNs from Root DSE Base DN: dc=irf,dc=local				
Limits Aliases Dereferencing Referrals Handling Count Limit: 1000 @ Follow Referrals manu Time Limit (s): 0 @ Search @ Follow Referrals auton Ignore Referrals				
Controls Use ManageDsalT control while browsing Fetch subentries while browsing (requires addition Paged Search Page Size: 100 Scroll Mo	nal search request) de			
Features Fetch operational attributes while browsing				

#### 5. ábra: LDAP kapcsolat beállításai

#### 6. Kapcsolat megnyitása

A Finish gombra kattintva meg is nyílik a kapcsolat, és a bal oldali menüben a címtár gyökerét lehet majd látni.

😫 LDAP Browser 🗖 🗖	🔳 dc=irf,dc=local 🛿	
Q   🗞   🗖 🔄 🔻	DN: dc=irf,dc=local	
· - · · ♪ »	Attribute Description	Value
	objectClass	dc0bject (auxiliary)
Root DSE (2)	objectClass	organization (structural)
	dc	irf
Searches	ο	irf
Dookmarks		

6. ábra: Megnyitott kapcsolat a Directory Studio programban

Ezzel sikeresen csatlakoztunk a címtárunkhoz.

#### 2.2 Ismerkedés az LDAP címtárral

Kezdésnek megvizsgáljuk a címtár felépítését, majd elvégzünk néhány alapfeladatot, mint például felhasználók létrehozása vagy csoportokhoz adása.

1. A címtár struktúrája

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



7. ábra: A példa címtár felépítése

A címtár gyökérelemének neve dc=irf,dc=local. Ez alatt találhatóak felhasználók, szervezeti egységek (*organizational unit* – OU) és csoportok. Az Apache Directory Studio kiírja az egy csomóponthoz tartozó gyerekelemek számát is, például a dc=irf,dc=local bejegyzésnek 4 darab gyerekeleme van (a többinél ez a szám még azért nem látszik, mert azoknak a gyerekeit még nem kértük le – a Directory Studio alapértelmezés szerint mindig csak a legszükségesebb információt kéri le).

2. Egy elem részletes tulajdonságai

Nézzük meg a Partners nevű szervezeti egység attribútumait (8. ábra).

😫 LDAP Browser 📃 🗖	🔳 ou=Partners,dc=irf,dc=loca	8
Q   🚸   🗖 🔄 🔻	DN: ou=Partners,dc=irf,dc=loc	al
▼ = ▼ ▼ ▲	Attribute Description	Value
	objectClass	organizationalUnit (structural)
Root DSE (2)	objectClass	top (abstract)
□	ou	Partners
¢ cn=nobody	description	Partners Organizational Unit
🗄 🏯 ou=Partners (11)		
🛨 🖧 ou=Projects (26)		
🕀 🔒 ou=University (3)		

8. ábra: Szervezeti egység attribútumai

Az ábrán látszik, hogy a bejegyzés DN-je ou=Partners,dc=irf,dc=local. Az OU nevű attribútuma az RDN-je is egyben (*relative distinguished name* – az adott hierarchia szinten belül egyedi, megkülönböztető név). Az ábrán ezen kívül a *description* és az *objectClass* attribútuma látszik. Figyeljük meg, hogy az objectClass többértékű attribútum.

Módosítsuk a bejegyzést, például írjuk át a leírását (jobb gomb az attribútumon, majd *Edit value* menüpont).

3. Válasszunk most ki egy felhasználót, például a cn=nobody nevűt (*cn: common name*).

Az egész bejegyzést könnyedén megkaphatjuk LDIF formátumban az összes attribútumának értékével (jelöljük ki a bejegyzést, jobb gomb / *Advanced / Copy entry as LDIF* menüpont). A következő eredményt kapjuk:

```
dn: cn=nobody,dc=irf,dc=local
objectClass: inetOrgPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: nobody
gidNumber: 1000
homeDirectory: /home/users/nobody
sn: Nobody
uid: nobody
uidNumber: 1999
description: Dummy user for empty groups
displayName: Nobody
givenName: Nobody
loginShell: /bin/sh
mail: nobody@nomail.no
```

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, ezek alapján áll össze, hogy milyen attribútumai is vannak az adott bejegyzésnek. A *posixAccount* miatt van például *uid* és *uidNumber* ennél a bejegyzésnél.

4. Új elem létrehozása

Az egyik szervezeti egység jobb gombos menüjéből válasszuk ki a *New / New entry* menüpontot. A megjelenő képernyőn válasszuk a *Create entry from scratch* lehetőséget. Ez után nekünk kell megadni, hogy milyen osztályok legyenek a típusai az új elemnek (9. ábra). Adjuk hozzá a person osztályt.

⊽	New Entry		∧ o + ⊗
Object Classes Please select object classes of th class.	e entry. Select at least or	ne structural object	
Available object classes	Add Remove	Selected object classes	5

9. ábra: objectClass kiválasztása

A következő lépés annak a meghatározása, hogy mi legyen az RDN attribútum (10. ábra).

~	New Entry	∧ o + ⊗
Distinguish Please sele	<b>ned Name</b> ct the parent of the new entry and enter the RDN.	
Parent:	ou=Partners,dc=irf,dc=local	Browse
RDN:		+ -
DN Preview:	RDN is invalid	

10. ábra: RDN megadása

RDN-nek választhatjuk bármelyik attribútumot (vagy akár több kombinációját), de érdemes valami alapvető, garantálhatóan egyedit megjelölni. Tehát ne a description attribútumra essen most a választásunk, hanem inkább a *cn*-re. Adjuk meg az RDN-ként használt attribútum értékét is, így már a DN Preview résznél láthatjuk is az új elem majdani DN-jét. Figyeljük meg, hogy hogyan épül fel a DN!

A person osztálynak kötelező attribútuma még az *sn* (*surname*), így a következő, Attributes lapon ki kell legalább azt tölteni. A *New Attribute…* gomb segítségével további, a bejegyzés típusaiban definiált attribútumokat lehetne hozzáadni.

Más típusú elemet is hasonlóan lehet létrehozni.

5. Csoportok kezelése

Válasszuk ki a cn=LexCorpstaff,ou=LexCorp,ou=Partners,dc=irf,dc=local csoportot. 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 (*New Value* link), és adjuk hozzá az újonnan létrehozott felhasználónkat.

DN: cn=LexCorpstaff,ou=LexCorp,ou=Partners,dc=irf,dc=local 🛛 🖻 🖹 🗙 🍇					
Attribute Description	Value				
objectClass	group0fNames (structural)				
cn	LexCorpstaff				
😑 member (42 values)					
member	cn=abiggar,ou=LexCorp,ou=Partners,dc=irf,dc=local				
member	cn=achatsworth1,ou=LexCorp,ou=Partners,dc=irf,dc=local				
member	cn=adaggett3,ou=LexCorp,ou=Partners,dc=irf,dc=local				

11. ábra: Csoporttagság tárolása

6. Keresés a címtárban

Az *LDAP / New Search* menüpont segítségével tudunk a címtárban keresni. Kereséshez a következőket kell megadni:

- Search Base: melyik csomóponttól kezdve akarunk keresni,
- *Search Scope*: csak az adott elemben (*Object*), az adott elem közvetlen gyerekelemei között (*One level*) vagy az összes leszármazottja (*Subtree*) között akarunk keresni,
- *Search Filter*: a keresési kifejezés az LDAP saját prefix nyelvén.

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

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

Ezt felhasználva keressük meg az ilyen nevű személyeket a Partners szervezeti egység teljes részfájában.

#### 2.3 Az LDAP címtár kezelése parancssori eszközökkel

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

- Idapadd: új elem hozzáadása (a háttérben az Idapmodify parancsot hívja meg a -a kapcsolót megadva),
- ldapmodify: meglévő elem vagy elemek módosítása és hozzáadása,
- Idapsearch: 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,
  - o GSSAPI: Kerberos V5 hitelesítés,
  - o EXTERNAL: külső forrás használata, például Linux IPC hitelesítés,
  - o ...
- *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 grafikus 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=Partners,dc=irf,dc=local" -s sub "(&(objectclass=person)(sn=b\*))" cn sn

Az eredmény valami hasonló lesz:

```
# extended LDIF
#
# LDAPv3
# base <ou=Partners,dc=irf,dc=local> with scope subtree
# filter: (&(objectclass=person)(sn=b*))
# requesting: cn sn
#
# cburgoyne, Daily Star, Partners, irf.local
dn: cn=cburgoyne,ou=Daily Star,ou=Partners,dc=irf,dc=local
cn: cburgoyne
sn: Burgoyne
...
```

A keresés itt is 73 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 1dapsearch.

2. Új elem hozzáadása konzolról

Az 1dapadd 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=Manager,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=Partners,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=Partners,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=Partners,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=Manager,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<sup>9</sup>). 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=Partners,dc=irf,dc=local
changeType: delete
# modify an entry
dn: cn=test1,ou=Partners,dc=irf,dc=local
changeType: modify
add: telephonenumber
telephonenumber: 555-1111
-
# different operators are separated by a -
replace: mail
mail: test@irf.local
-
```

<sup>&</sup>lt;sup>9</sup> Ezen kívül vannak még a DN és RDN módosítására szolgáló changetype típusok is, amikkel átnevezni vagy áthelyezni lehet bejegyzéseket.

delete: description

Ezt a következő paranccsal tudjuk végrehajtani:

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

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

A segédlet eddigi része áttekintette az alapokat. További információt az 1dap\* parancsok manual oldalán találhatunk, ezt érdemes most átfutni (előbb-utóbb úgyis meg kell tenni, nem fogjuk tudni megúszni, hogy megnézzük a teljes referenciát).

#### 2.4 LDAP címtár lekérdezése Pythonból

2014-től kezdve kísérleti jelleggel használjuk a PyLDAP modult, aminek a segítségével Python3 kódból lehet LDAP címtárat elérni.

1. Csatlakozás a címtárhoz

A következő rövid kóddal lehet a helyi LDAP kiszolgálóhoz csatlakozni.

```
from pyldap import LDAPClient
client = LDAPClient("ldap://localhost")
conn = client.connect()
```

(Megjegyzés: az ldaps nem működik a kiadott virtuális gépen.)

2. Hajtsunk végre egy egyszerű keresést

```
conn.search("ou=Partners,dc=irf,dc=local", 2, "(&(objectClass=person)(sn=bev*))")
```

A search() első paramétere a base DN, ahonnan keresni akarunk. A második a search scope (0 – csak adott elem, 1 – csak egy szinttel lentebb, 2 – teljes részfában keresés). A harmadik pedig a kereső-kifejezés a már megszokott formában.

Az eredményeket egy listában kapjuk vissza.

További példákat a modul leírásában találhatunk.

## 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 R2* 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.

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



12. 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<sup>10</sup>, 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 tartomány nevét a felhasználónév elé kell írni, egy \ jel előtt megadva (pl. IRHF\Administrator, lásd 12. ábra).

<sup>&</sup>lt;sup>10</sup> Egy számítógép legfeljebb egy tartománynak lehet tagja, ha nem tartományi tag, akkor pedig egy munkacsoportba (workgroup) tartozik.

*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.

A belépéshez szükséges jelszót a virtuális gép mellett lévő README fájl tartalmazza.

3. Ismerkedés a címtárral

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

			Active D	irectory Users and Computers
File Action View Help				
🗢 🤿 🙍 🗊 📋 🖾 🤷 😫	7 🗾 🍇			
Active Directory Users and Computers [irfserver.irfhf.local]	Name	Туре	Description	
Saved Queries	🛅 Builtin	builtinDomain		
⊿ 🙀 irfhf.local	Computers	Container	Default container for up	
Builtin	🖻 Domain Controllers	Organizational	Default container for do	
Computers	📔 ForeignSecurityPrincipals	Container	Default container for sec	
Domain Controllers	Managed Service Accounts	Container	Default container for ma	
ForeignSecurityPrincipals	Partners	Organizational		
Managed Service Accounts	Projects	Organizational		
Partners	University	Organizational		
Projects		Container	Default container for un	
Iniversity		container	belaute container for up	
Users				

13. 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 *Partners, Projects, University* csomópontokat 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 *Partners* már egy *szervezeti egység* (organizational unit, OU), ezt a másfajta ikon is jelzi.

4. A címtár hierarchiája

Bontsuk ki a University tárolót, hogy lássuk a hierarchia egy részét (14. ábra).

FIGYELEM: a University tároló tartalma csak egy példa, hogy milyen jellegű felépítéseket lehet tárolni egy címtárban.

Hozzunk létre további hierarchiaszinteket a címtárban a gyökértől kiindulva (15. 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).

⊿

📓 University	
⊿ 道 Faculti	es
⊿ 🛅 Fac	ulty of Architecture
Þ 🖬	Department of Design
Þ 🖬	Department of Energetics
Þ 🖬	Department of Infrastructure
⊿ 🛅 Fac	ulty of Engineering
Þ 🖬	Department of Electronics
Þ 🖬	Department of Mechanics
Þ 🖬	Department of Vehicles
þ 道 Fac	ulty of Informatics
þ 🖬 Fac	ulty of Natural Sciences
⊿ 道 Person	nel
📑 Aca	ademic
📑 Ace	count
🖬 IT	
🛅 Leg	Jal





15. ábra: Új szervezeti egység létrehozása

1azer Rackham Properties	? ×	Ma	zer Rackham Prope	rties		?
Dial-in Environment Sessions Remote Desktop Services Profile Personal Virtual De General Address Account Profile Telephones Orga	Remote control   sktop   COM+ nization   Member Of		Member Of Remote control General Address	Dial-in │ Termi Account │	Environment nal Services Profile Profile Telephones	Sessions COM+ Organization
Mazer Rackham Erst name: Mazer initials: Last name: Rackham Digplay name: Mazer Rackham			Gosen logun maine.     mazer     User logon name (pre-)     IRFHF\     Logon Hours	<u>M</u> indows 2000 Log On <u>T</u> a	@irfhf.local ):  mazer	
Description:         Orlief Strategist           Offige:	Qther		Account options:	e password at nge password expires using reversible	next logon	* 
Web page:	Other		Account expires	012. március	s 10.	<b>X</b>

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

5. Felhasználók tulajdonságai

Válasszuk ki a címtárban szereplő egyik tetszőleges felhasználót, és nézzük meg a tulajdonságait (16. 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!

TIPP: az alapértelmezett jelszóházirend szerint a jelszónak legalább 8 karakter hosszúnak kell lennie, és tartalmaznia kell kis- és nagybetűt, valamint számot vagy speciális karaktert.

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 (17. ábra). A kiadott virtuális gépen például a Projects OU alatt találunk csoportokat.

esearch Properties	<u>? ×</u>	research Properties	
General Members Member Of Managed By		General Members Member Of	Managed By
😡 research		Members:	
		Name	Active Directory Domain Services
		S Felix Hoenikker	irfhf.local/People/Research
Group name (pre-Windows 2000): research		👗 Joao Figueira Alvarez	intht.local/People/Research
		Management	innr.iocai/People/Management
Description: All members of the Research division		Morris Zapp	infinitiocal/reopie/Research
E eret	[]	Randall Petersen Amstr	iffhf local/People/Research
		Sheldon Cooper	ifhf.local/People/Research
Group scope			
O Domain local			
Universal			
Notes:			
	<u> </u>		1
		Add <u>B</u> emove	
	▼		
OK Cancel	Apply		OK Cancel

17. 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 (18. ábra).

Find Users, Contacts, and File Edit View	Groups		<u> </u>
Find: Users, Contacts, and Gro	oups 💌 I <u>n</u> :	ifhf.local	Browse
Users, Contacts, and Groups	Advanced		
Field 🔻	Condition:	Value:	Find Now
			Stop
, Condition List:	,	Add <u>R</u> emove	<u>C</u> lear All
Name Starts with	re		<i>Ş</i>
Description Present			
Search results:			-
Name Type		Description	
Research Group		All members of the Research	division
Read-only Domai Group		Members of this group are Re	ead-Only Domain Contr
Remote Desktop Group		Members in this group are gra	anted the right to logor
Replicator Group		Supports file replication in a c	lomain
•			Þ
4 item(s) found			1.

18. ábra: Egy összetett keresés

Keressük meg az olyan felhasználókat, akiknek a telefonszáma 777-tel kezdődik, és ki van töltve 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 (ez megtalálható a virtuális gépen a C:\Program Files (x86)\sysinternals könyvtárban, de elérhető a tálcáról is).

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 (19. ábra), mint az ADUC GUI-ban.

th: DC=irfhf,DC=local,irfserver.irfhf.local [irfserver.irfhf.local]						
I Active Directory Explorer	Attribute	Syntax	Count	Value(s)		
🖃 🗍 irfserver.irfhf.local [irfserver.irfhf.local]	auditingPolicy	OctetString	1	0 1		
⊡ <u>∰</u> DC=irfhf,DC=local	creationTime	Integer8	1	2014.03.11. 15:29:27		
·  ·  CN=Configuration,DC=irfhf,DC=local	🔊 dc	DirectoryString	1	irfhf		
CN=Schema,CN=Configuration,DC=irfhf,DC=local	aistinguishedName	DN	1	DC=irfhf,DC=local		
DC=DomainDnsZones,DC=irfhf,DC=local	dSASignature	OctetString	1	10004000000000000		
	dSCorePropagationData	GeneralizedTime	1	1601.01.01. 1:00:00		
	forceLogoff	Integer8	1	0x8000000000000000		
	fSMORoleOwner	DN	1	CN=NTDS Settings,CN=IRFSI		
	gPLink	DirectoryString	1	[LDAP://CN={31B2F340-016[		
	instanceType	Integer	1	5		
	isCriticalSystemObject	Boolean	1	TRUE		
	lockoutDuration	Integer8	1	0xFFFFFFFBCF1DCC00		
	lockOutObservationWin	Integer8	1	0xFFFFFFFBCF1DCC00		
	lockoutThreshold	Integer	1	0		
	masteredBy	DN	1	CN=NTDS Settings,CN=IRFSI		
	🔊 maxPwdAge	Integer8	1	0xFFFFDEFF0AA68000		
	🔊 minPwdAge	Integer8	1	0xFFFFFF36D5964000		
	iminPwdLength	Integer	1	7		

19. 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 szervezeti egységeket itt is (20. ábra).

Path: OU=Faculties,OU=University,DC=irfhf,DC=local,irfserver.irfhf.local [irfserver.irfhf.local]								
Active Directory Explorer Active Directory Explorer infserver.infh.local [infserver.infh.local] CN=Builtin CN=Computers CN=	Attribute a cn a distinguishedName a distinguishedName a distinguishedName a distinguishedName a nTSecurityDescriptor a objectCategory a objectCategory a objectClass a objectClass a objectGUID a ou a uSNChanged a uSNCreated a whenChanged a whenCreated	Syntax DirectoryString DN GeneralizedTime Integer DirectoryString NTSecurityDescriptor DN OID OctetString DirectoryString Integer8 Integer8 GeneralizedTime GeneralizedTime	Count 1 1 1 1 1 1 1 1 1 1 1 1 1	Value(s) Faculties OU=Faculties,OU=University,DC=irfhf,DC=local 1601.01.01. 1:00:00 4 Faculties D:AI(OA;;CCDC;4828cc14-1437-45bc-9b07-ad6fC CN=Organizational-Unit,CN=Schema,CN=Configu top;organizational-Unit {0ABFA2B9-1176-42FD-A0E1-179419E572BD} Faculties 0x31F8 0x31F8 2014.03.11. 16:09:12 2014.03.11. 16:09:12				

20. ábra: Egy szervezeti egység adatai az AD belső megjelenítésében

- a. Mi a szervezeti egység *megkülönböztetett neve* (distinguished name, DN)? Vizsgáljuk meg, hogyan épül ez fel.
- b. Nézzük végig a szervezeti egység attribútumait!
- 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

#### 21. 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 (21. 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.

A PowerShell második verziójában jelent meg az ActiveDirectory nevű új modul, amely a legújabb verzióban már 147 darab cmdletet biztosít az AD kényelmes kezelésére.

1. Az ActiveDirectory modul betöltése

A következő paranccsal tudjuk betölteni a modult (erre 3-as PowerShelltől kezdve 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) [12] 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 (22. ábra). Az *Active Directory Web Services* alapértelmezetten a 9389-es porton figyel, és a cmdletek ehhez csatlakoznak.



22. ábra: Az Active Directory Web Service architektúrája [13]

Amikor betöltjük az ActiveDirectory modult, akkor az megpróbál automatikusan csatlakozni az aktuális tartományhoz. A kiadott virtuális gépen ez elvileg sikerrel is jár, úgyhogy ilyenkor nincs több előkészítésre szükség.

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 (23. ábra), ez egy jó kiindulópont lehet egy-egy feladat megoldása során.

	Act	ive Di	rectory Powersi	nell		
		http://blo	gs.msdn.com/adpowershell			
Account Management			1			
	Account	Settings N	lanagement	Group Membership Mar	agement	
Account Lifecycle Management	Search-AD	Account		Add-ADGroupMember		
	Disable-A	DAccount		Remove-ADGroupMember		
New-ADUser	Enable-AD	Account		Action of Apple apple		
Set-ADUser	Unlock-AD	Account		Add-ADPrincipalGroupMem	pership	
Set-ADUser	Set-ADAcc	ountPasswo	ord	Get-ADPrincipalGroupMem	pership	
Remove-ADUser	Set-ADAcc	ountContro	51	Remove-ADPrincipalGroup	Tembership	
New-ADGroup	Clear-ADA	ccountExp	Iration	Get-ADAccountAuthorizat:	lonGroup	
Set-ADGroup	Set-ADAcc	ountExpira	ation			
Set-ADGroup						
Remove - ADGroup						
conste rasin sup						
New-ADComputer	1			Password Policy Manage	ement	
Set-ADComputer				New ADE instant and Party and Policy		
Set-ADComputer						
Remove-ADComputer	Managed	Service A	ccount Management	Get-ADFineGrainedParcuo	delicy	
vellove-Abcollpucer				Set ADEineGrainedPasswordPolicy		
New ADCanuicalcount	Add-ADCom	puterServi	ceAccount	Persue ADEineGrainadDace	upolicy	
Get ADServiceAccount	Get-ADCom	puterServi	ceAccount	Remove-Aprilledrainedrass	wordPolicy	
Set ADServiceAccount	Remove-AD	ComputerSe	rviceAccount	Add ADEinsfesiesdDasses	deal i auf ub i ach	
Set-ADServiceAccount	A CONTRACTOR OF CONTRACTOR	2002000000000000		Add-ADFInedrainedPasswor	dPolicySubject	
KENDVE-ADSELVICEACCOUNC	Install-A	DServiceAd	count	Bergue ADEineGrainedPasswor	upolicySubject	
New ADOresedentionslikett	Uninstall	-ADService	Account	Remove-AprineGraineGPass	wordPolicySubject	
Set ADOrganizationalUnit	Reset-ADS	erviceAcco	untPassword		and Dall day	
Set ADOrganizationalUnit				det-AbuserkesuitantPassi	ordpolicy	
Sec-Aborganizacionalonic				Get-ADDefaultDomainPasswordPolicy Set-ADDefaultDomainPasswordPolicy		
Remove-Abor Bautractonatonic						
opology Management		Outin		Directory	Provider cmdle	
		Option	al Feature Management	Object		
		Option	al Feature Management	Object	Get-PSProvider	
Domain Controller Management		Get-ADC	al Feature Management	Object	Get-PSProvider New-PSDrive	
Domain Controller Management		Get-ADC Enable-	al Feature Management OptionalFeature ADOptionalFeature	Object Management	Get-PSProvider New-PSDrive Get-PSDrive	
Domain Controller Management		Get-ADC Enable- Disable	al Feature Management OptionalFeature - ADOptionalFeature - ADOptionalFeature	Object Management	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer		Get-ADC Enable- Disable	al Feature Management OptionalFeature -ADOptionalFeature -ADOptionalFeature	Object Management	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive	
Domain Controller Management Get-ADDomainController Nove-ADDirectoryServer Nove-ADDirectoryServerOperationNast	erRole	Get-ADC Enable- Disable	al Feature Management OptionalFeature -ADOptionalFeature e-ADOptionalFeature	Object Management New-ADObject Get-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item	
Domain Controller Management Set-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast	erRole	Get-ADC Enable- Disable	al Feature Management OptionalFeature -ADOptionalFeature ADOptionalFeature	Object Management New-ADObject Get-ADObject Set-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast	erRole	Get-ADC Enable- Disable	al Feature Management OptionalFeature ADOptionalFeature PADOptionalFeature Domain and Forest	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast	erRole	Get-ADX Enable- Disable	al Feature Management OptionalFeature -ADOptionalFeature -ADOptionalFeature Domain and Forest	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast	erRole	Get-ADX Enable Disable	al Feature Management OptionalFeature ADOptionalFeature ADOptionalFeature Domain and Forest Management	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast Password Replication Policy Manage	ement	Get-ADX Enable Disable	al Feature Management OptionalFeature ADOptionalFeature PADOptionalFeature Domain and Forest Management	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Bename-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Move-Item	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast Password Replication Policy Manage	erRole	Get-ADX Enable- Disable	al Feature Management OptionalFeature -ADOptionalFeature -ADOptionalFeature -Domain and Forest Management Get-ADRootDSE	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Rename-ADObject Restare-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Renome-Item	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast Password Replication Policy Manage	ement	Get-ADX Enable Disable	al Feature Management PrionalFeature -ADOptionalFeature -ADOptionalFeature Domain and Forest Management Get-ADRootDSE	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Rename-ADObject Restore-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Rename-Item Get-ItemProperty	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast Password Replication Policy Manage Add-ADDomainControllerPasswordRepli	errRole ement cationPolicy	Get-ADX Enable- Disable	al Feature Management ADOptionalFeature ADOptionalFeature Domain and Forest Management Get-ADRootDSE Get-ADDomain	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Rename-ADObject Restore-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Rename-Item Get-ItemProperty Set-ItemProperty	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast Password Replication Policy Manage Add-ADDomainControllerPasswordRepli Get-ADDomainControllerPasswordRepli	erRole ement cationPolicy cationPolicy	Get-ADC Enable- Disable	al Feature Management ADOptionalFeature ADOptionalFeature Domain and Forest Management Get-ADRootDSE Get-ADDomain Set-ADDomain	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Rename-ADObject Restore-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Rename-Item Get-ItemProperty Set-ItemProperty Set-ItemProperty	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast Password Replication Policy Manage Add-ADDomainControllerPasswordRepli Get-ADDomainControllerPasswordRepli Remove-ADDomainControllerPasswordRepli	ement cationPolicy cationPolicy plicationPolicy	Get-ADC Enable Disable	al Feature Management ADOptionalFeature ADOptionalFeature Domain and Forest Management Get-ADRootDSE Get-ADDomain Set-ADDomain Set-ADDomain	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Rename-ADObject Restore-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Rename-Item Get-ItemProperty Set-ItemProperty Remove-ItemProperty	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServerOperationMast Password Replication Policy Manage Add-ADDomainControllerPasswordRepli Get-ADDomainControllerPasswordRepli	ement cationPolicy cationPolicy plicationPolicy	Get-ADX Enable Disable	al Feature Management ADOptionalFeature ADOptionalFeature -ADOptionalFeature Domain and Forest Management Get-ADRootDSE Get-ADDomain Set-ADDomain Set-ADDomainMode	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Remove-ADObject Restore-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Rename-Item Get-ItemProperty Set-ItemProperty Set-ChildItem	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServer Move-ADDirectoryServerOperationMast Password Replication Policy Manage Add-ADDomainControllerPasswordRepli Get-ADDomainControllerPasswordRepli Remove-ADDomainControllerPasswordRepli	erRole ement cationPolicy cationPolicy plicationPolicy cationPolicyUs	Get-ADX Enable Disable	al Feature Management ADOptionalFeature ADOptionalFeature -ADOptionalFeature Domain and Forest Management Get-ADRootDSE Get-ADDomain Set-ADDomain Set-ADDomain Set-ADDomainYode Get-ADForest	Object Management New-ADObject Get-ADObject Set-ADObject Remove-ADObject Rename-ADObject Restore-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Remove-Item Move-Item Rename-Item Get-ItemProperty Set-ItemProperty Remove-ItemProperty Get-ChildItem	
Domain Controller Management Get-ADDomainController Move-ADDirectoryServerOperationMast Password Replication Policy Manage Add-ADDomainControllerPasswordRepli Remove-ADDomainControllerPasswordRepli Get-ADDomainControllerPasswordRepli Get-ADDomainControllerPasswordRepli	ement cationPolicy cationPolicy plicationPolicy cationPolicyUs	Get-ADX Enable- Disable	al Feature Management ADOptionalFeature ADOptionalFeature Domain and Forest Management Get-ADRootDSE Get-ADDomain Set-ADDomain Set-ADDomain Set-ADDomain Set-ADForest Set-ADForest	Object Management New-ADObject Get-ADObject Remove-ADObject Remove-ADObject Rename-ADObject Restore-ADObject	Get-PSProvider New-PSDrive Get-PSDrive Remove-PSDrive New-Item Get-Item Renowe-Item Move-Item Renome-Item Get-ItemProperty Set-ItemProperty Remove-ItemProperty Get-ChildItem Get-ACL	

23. ábra: PowerShell AD cmdletek listája [11]

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<sup>11</sup> 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 (24. ábra).

<sup>&</sup>lt;sup>11</sup> Active Directory for Windows PowerShell About Help Topics, URL: <u>http://technet.microsoft.com/en-us/library/hh531525(v=ws.10).aspx</u>



24. 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
	demoi »DNC	DC inflet DC local
Inthe	configuration	DU=10TAT, DU=10CA1
Schema		CN=Configuration DC=iocal
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=Projects
PS AD:\OU=Projects,DC=irfhf,DC=local> cd c:
PS C:\> cd "AD:\OU=Partners,DC=irfhf,DC=local"
```

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

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

a. Keressük meg a Partners 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 rkeith

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=rkeith,OU=Academic,OU=Personnel,OU=University,
Enabled	:	False
GivenName	:	Rachel
Name	:	rkeith
ObjectClass	:	user
ObjectGUID	:	62c2e964-a493-44b9-a622-c18d4b4c9014
SamAccountName	:	rkeith
SID	:	S-1-5-21-3265894680-3469142855-917753721-1109
Surname	:	Keith
UserPrincipalName	:	rkeith@irfhf.local

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

Get-ADUser rkeith -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=Partners,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=Partners,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 [10] 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 (25. ábra).

Ξ 🙀	irfhf.local	Links					
	🛒 Default Domain Policy	Display links in this location:	irfhf local				
+	🛾 📔 Domain Controllers		Jiminiocar				
+	Groups	The following sites, domains, and OUs	are linked to this (	GPO:			
+	B 🖬 Hotels	Location 🔺	E	Inforced	Link Enabled	Path	
+	B 🖬 HQ	iffef loopl	N	lo.	Vee	iffef loopl	
+	📑 Partners	in in iocai	IN .	10	Tes	innitiocal	
+	📔 People						
+	🛾 📑 Group Policy Objects						
+	🛯 📑 WMI Filters						
+	🛯 🛅 Starter GPOs						
🛨 📑 Sit	tes						
👸 Gr	oup Policy Modeling						
💼 Gr	oup Policy Results						

25. 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. Készítsünk a *Partners* OU-hoz egy új házirendet (26. 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?

Group Policy Management Editor		
<u>File Action View H</u> elp		
🗢 🔿 🖄 🖬 🗟 🖬 🝸		
PeopleGPO [IRFSERVER.IRFHF.LOCAL] Policy	hll Settings	
Policies     Software Settings     Windows Settings	6to4 Relay Name Edit <u>policy setting</u>	Setting A A General Setting A Setting Setting A Setting
<ul> <li>Administrative I emplates: Policy defi</li> <li></li></ul>	Requirements: At least Windows 7 or Windows Server 2008 R2	E:       6to4 State         E:       Access data sources across domains         E:       Access data sources across domains
	Description: This policy setting allows you to specify a 6to4 relay name for a 6to4 host. A 6to4 relay is used as a default gateway for IPv6 network traffic sent by the 6to4 host. The 6to4 relay name setting has no	Access data sources across domains
Policies     Preferences	effect if 6to4 connectivity is not available on the host. If you enable this policy setting, you can	Access data sources across domains     Access data sources across domains     Access data sources across domains     Action on server disronnect
	If you disable or do not configure this policy setting, the local host setting is used, and you cannot specify a relay name for a 6to4 host.	Activate Shutdown Event Tracker System State Data feat     ActiveX installation policy for sites in Trusted zones     Add a specific list of search providers to the user's search     Add Printer wizard - Network can page (Managed network)
		Advanced Administrators security group to reaming user pro     Advanced Administrators security group to reaming user pro     Advanced Administrators     Admin-approved behaviors     Administratively sectioned offine files
	Extended Standard	
1671 setting(s)		

26. 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 [10] 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", 25 Januaray 2014, elérhető online: <u>http://www.openldap.org/doc/</u>
- [8] Zytrax.com. "LDAP for Rocket Scientists", Open Source Guide, version 0.1.15, elérhető online: http://www.zytrax.com/books/ldap/

#### Windows

- [9] Gál Tamás, Szabó Levente, Szerényi László. "Rendszerfelügyelet rendszergazdáknak". Szak Kiadó, 2007., elérhető online: <u>https://technetklub.hu/Downloads/Browser.aspx?shareid=1&path=PDF</u>
- [10] Soós Tibor, "Microsoft PowerShell 2.0 rendszergazdáknak elmélet és gyakorlat", Microsoft Magyarország, 2010., elérhető online: <u>https://technetklub.hu/Downloads/Browser.aspx?shareid=1&path=PDF</u>

- [11] 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-powershelloverview.aspx
- [12] Active Directory PowerShell Blog. "Active Directory Powershell: Installation using RSAT on Windows 7", 24 Mar 2009, elérhető online: <u>http://blogs.msdn.com/b/adpowershell/archive/2009/03/24/active-directory-powershell-installation-using-rsat-on-windows-7.aspx</u>
- [13] 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-servicesoverview.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<sup>12</sup>). 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.

3. Felhasználó leképezés megadása

<sup>&</sup>lt;sup>12</sup> 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.

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:

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<sup>13</sup> segítségével, ami egy jól használható grafikus felületet biztosít az LDAP címtár elérésére.

LDAP - Root DSE - 192.168.160.130 - Apache Directory Studio							
<u>F</u> ile <u>E</u> dit <u>N</u> avigate LDAP <u>W</u> indow <u>H</u> elp							
😫 LDAP Browser 🛛 🖓 📓 Root DSE 🕱							
Q   Image And							
▼ = ▼ ▼ №	Attribute Description	Value					
	objectClass	OpenLDAProotDSE (structural)					
A Root DSE (2)	objectClass	top (abstract)					
A desirf deslocal	configContext	cn=config					
Searches	entryDN						
Bookmarks	monitorContext	cn=Monitor					
	namingContexts	dc=irf,dc=local					
	namingContexts	dc=my-domain,dc=com					
G Connections Servers -	structuralObjectClass	OpenLDAProotDSE					
	subschemaSubentry	cn=Subschema					
	supportedControl	1.2.826.0.1.3344810.2.3 (Matched Values Control)					
Lap 192.168.160.130	supportedControl	1.2.840.113556.1.4.319 (Simple Paged Results)					
	supportedControl	1.3.6.1.1.12 (Assertion Control)					
	supportedControl	1.3.6.1.1.13.1 (LDAP Pre-read Control)					

27. 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)

Ezek után kapcsolódjunk (*Open connection*), és a jelszó megadása után tudjuk is böngészni a címtárat (27. ábra).

<sup>&</sup>lt;sup>13</sup> <u>http://directory.apache.org/studio/</u>

Azt érdemes még megnézni, hogy a háttérben milyen kommunikáció zajlik, ezt például Wiresharkban tudjuk megfigyelni (28. 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.

No	. Time	Source	Destination	Protocol	Length Info
	1 0.000000	192.168.160.1	192.168.160.130	ТСР	66 23087 > ldap [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
	2 0.008000	192.168.160.1	192.168.160.130	тср	54 23087 > ldap [ACK] Seq=1 Ack=1 Win=65700 Len=0
	3 0.008000	192.168.160.130	192.168.160.1	TCP	66 ldap > 23087 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=64
	4 2.832000	192.168.160.1	192.168.160.130	LDAP	80 bindRequest(1) " <root>" sas]</root>
	5 2.844000	192.168.160.130	192.168.160.1	TCP	54 ldap > 23087 [ACK] seq=1 Ack=27 win=14656 Len=0
	6 2.846000	192.168.160.130	192.168.160.1	LDAP	283 bindResponse(1) saslBindInProgress (SASL(0): successful result: )
	7 2.849000	192.168.160.1	192.168.160.130	LDAP	350 bindRequest(2) " <root>" sas]</root>
	8 2.853000	192.168.160.130	192.168.160.1	LDAP	110 bindResponse(2) success
	9 2.856000	192.168.160.1	192.168.160.130	LDAP	112 searchRequest(3) " <root>" baseObject</root>
	10 2.866000	192.168.160.130	192.168.160.1	LDAP	102 searchResEntry(3) " <root>"</root>
	11 2.876000	192.168.160.1	192.168.160.130	TCP	54 [TCP ACKed lost segment] 23087 > ldap [ACK] Seq=381 Ack=348 Win=65352 Len=0
	12 2.877000	192.168.160.130	192.168.160.1	LDAP	68 [TCP Retransmission] searchResDone(3) success [1 result]
	13 2.877000	192.168.160.1	192.168.160.130	LDAP	152 searchRequest(4) "cn=Subschema" baseObject
	14 2.883000	192.168.160.130	192.168.160.1	LDAP	153 searchResEntry(4) "cn=Subschema"
*				III	
	Framo 7: 250 b	the on wine (2000 k	vite) 250 bytes can	turod (	2800 bits)
	Ethorpot TT S	CES 01 WHE (2800 L	(00.50.56.c0.00.08)	Det · )	2000 D1 (3) 2000 D1 (3) 2000 D1 (3)
	Internet Drote	c. viiware_c0.00.08	102 168 160 1 (102	, DSL. 160 160	VIIIWale_19.34.60 (00.00.29.19.34.60)
*	Thernet Protoc	petrol protocol Src	192.108.100.1 (192.)	100.100	.1), USL 192.100.100.150 (192.108.100.150)
	Lightwoight Di	actory Accoss Proto	col	), DSC I	Polt. Tuap (309), Seq. 27, Ack. 230, Lett. 290
		ectory Access Proce	To " encl		
	EDAPMessage i	2	II> Sasi		
	messagerD.	2 histopast (0)			
		: Dinakequest (0)			
	🖻 binakeque	250			
	Version	1: 3			
	name:	d			
	auchen	incation: sasi (3)			
	⊟ SaST	handen, protot upt			
	mee	Indirials: DIGESI-MD5	2657424757466242826	7572657	2666166652422
		S-APT Ceneric Socuri	ty Service Applicat	ion Pro	
	⊟ G5:	inknown header (clas	s=1 nc=1 tag=2)	TOIL PLO	gram interrate
			3-1, pc-1, tag-3)		
00	50 53 54 2d 4d	44 35 04 82 01 04	63 68 61 72 73 65	ST-MD5	5Charse
00	60 74 3d 75 74	66 2d 38 2c 75 73	65 72 6e 61 6d 65	t=utf-	-8, username
00	70 3d 22 72 6f	61 74 22 2c 72 65	61 6c 6d 3d 22 69	="root	r, realm="1
00	00 72 00 20 60 00 22 26 72 51	33 47 71 26 38 41	44 43 56 69 6b 7a	rt.100	
00	a0 75 6f 43 39	76 33 33 77 44 63	4f 66 32 69 68 74		BW pccf2ht
00	b0 57 46 56 4a	4a 55 72 73 4a 53	57 73 3d 22 2c 6e	WEVJJI	Ins JSWs=".n

28. ábra: LDAP kapcsolódás hálózati forgalma