LDAP azonosítás a gyakorlatban – egy esettanulmány

A kliensek beállítása (2. rész)

Ha az előző részben leírtak alapján sikerült telepíteni a kiszolgálót, már csak a kliensek beállítása van hátra. Ebben a részben mellesleg valamennyi olyan kiszolgáló beállítását is bemutatom, amelyek rendszerünkben LDAP azonosítást használnak majd.

Névfeloldó szolgáltatás beállítása

Ezt minden gépen el kell végezni, amelyiken az *LDAP* adatbázisból azonosít. Először is telepítettem a ***libnss-ldap*** csomagot:

```
apt-get install libnss-ldap
```

A telepítéskor megkérdezi a következőket és a válaszoknak megfelelően létrehozza az */etc/libnss-ldap.conf* fájlt:

- Mi az *IP* címe az *LDAP* kiszolgálót futtató gépnek
- *LDAP search base*: adatbázis alap (*dc=cegnev,dc=hu*)
- *LDAP* kiszolgáló verziója
- Igényel bejelentkezést az *LDAP* adatbázis (nem)
- Csak a tulajdonos számára legyen-e írható/olvasható a beállító fájl (nem)

Módosítottam az */etc/nsswitch.conf* fájlt a következőképpen:

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
hosts:          files dns
networks:       files
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       files
```

Csak a *Linux* újraindítása után fog működni, de éppen ezért előbb célszerű a *PAM*-ot is beállítani, mert az is újraindítást igényel. A beállítást úgy lehet ellenőriztem, hogy létrehoztam egy ideiglenes fájlt, egy olyan felhasználó tulajdonába adtam amelyik csak az *LDAP* adatbázisban létezik, majd ellenőriztem. Ha például a ***nagypeter*** felhasználó már létezik az adatbázisban:

```
touch /tmp/fajlnev
chown nagypeter /tmp/fajlnev
ls -l /tmp/fajlnev
```

A PAM rendszer beállítása

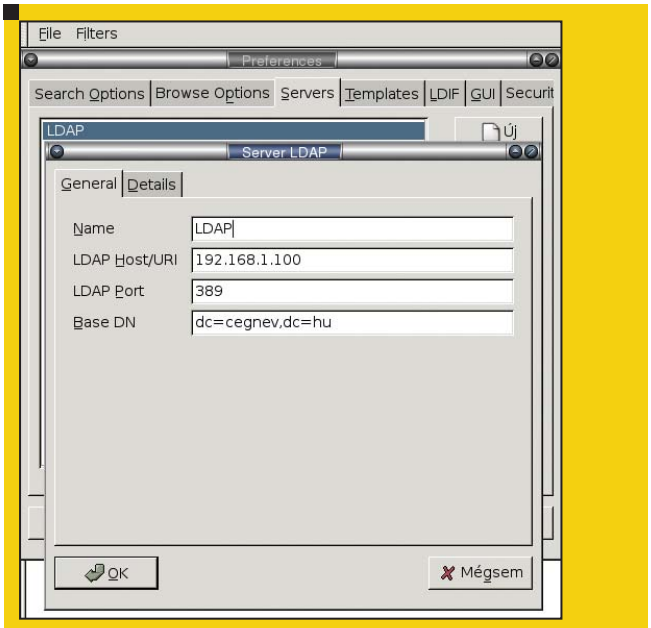
Ezt is minden gépen el kell végezni, melyen az *LDAP* adatbázisból szeretnénk azonosítani. Először telepítettem a *PAM LDAP* modulját:

```
apt-get install libpam-ldap
```

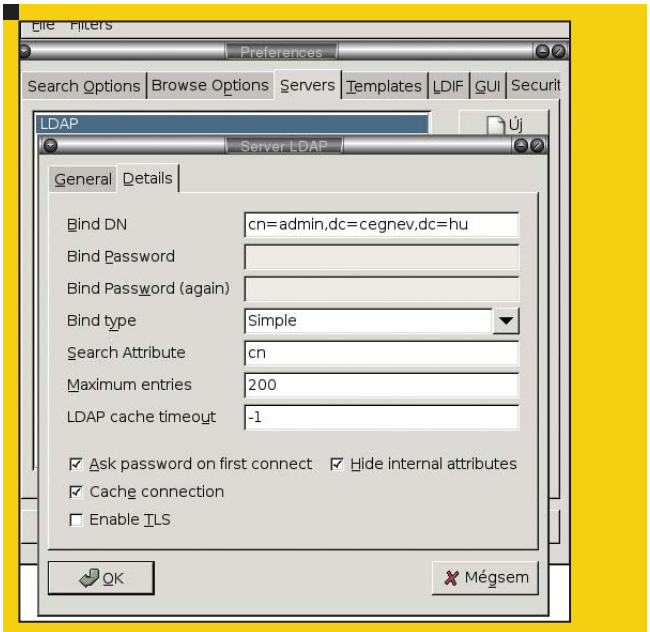
Ha a telepítés a fenti módon parancssorral történik, akkor az */etc/pam_ldap.conf* fájban kell a beállításokat elvégezni. Egyszerűbb azonban a ***libpam-ldap*** és a ***libnss-ldap*** csomagokat egyszerre a ***dselect*** segítségével telepíteni, mert ekkor a feltett kérdésekre adott válaszok alapján az */etc/pam_ldap.conf* tartalma is módosul.
Az */etc/pam_ldap.conf* fájl következő sorait kellett módosítanom:

```
host 127.0.0.1
base dc=cegnev,dc=hu
ldap_version 3
scope sub
pam_password md5
```

Módosítottam a következő fájlokat az eredeti sorok kikommentezésével és új sorok beírásával. A módosítás



1. ábra GQ beállítása: LDAP kiszolgáló adatainak megadása



2. ábra GQ beállítása: adminisztrátor megadása

után először az *LDAP* kiszolgálóról próbál azonosítani, ha ez nem lehetséges, akkor pedig a rendszerfájlokból:

/etc/pam.d/common_account fájl:

```
# account       required        pam_unix.so
account         sufficient      pam_ldap.so
account         required        pam_unix.so
```

/etc/pam.d/common_auth fájl:

```
# auth    required      pam_unix.so nullok_secure
auth      sufficient    pam_ldap.so
auth      required      pam_unix.so try_first_pass
```

/etc/pam.d/common_password fájl:

```
# password  required      pam_unix.so nullok
                          ➥obscure min=4 max=8 md5
password    sufficient    pam_ldap.so
password    required      pam_unix.so nullok
                          ➥obscure min=4 max=8 md5
```

/etc/pam.d/common_session fájl:

```
# session       required        pam_unix.so
session         sufficient      pam_ldap.so
session         required        pam_unix.so
```

A beállítás a *Linux* újraindítása után fog működni. Kipróbálni legegyszerűbben egy csak *LDAP* adatbázisban lévő felhasználó nevében történő bejelentkezéssel lehet.

Meglévő Linux csoportok és fiókok átvitele

Amennyiben a rendszerfiókokon és rendszercsoportokon kívül csak *Samba* fiókokra és csoportokra van szükségünk, úgy ez a lépés természetesen kimarad.

Az átvitelre (migrációra) a *migrationtools* csomagot kell telepíteni:

```
apt-get install migrationtools
```

Módosítani kell az */etc/migrationtools/migrate_common.ph* fájlban a következőket:

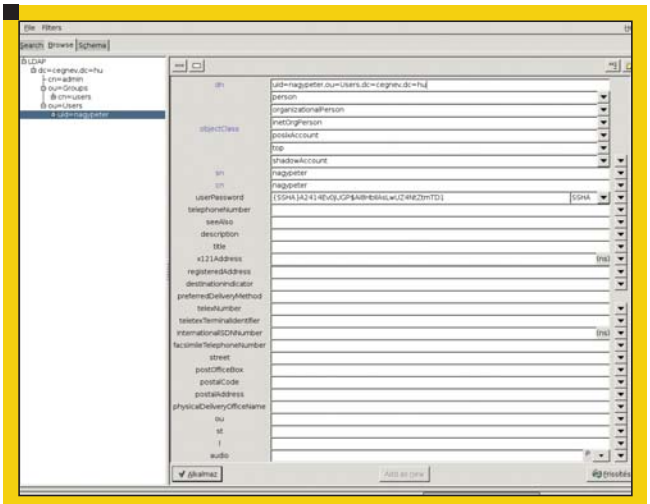
```
$DEFAULT_BASE = "dc=cegnev,dc=hu";
$EXTENDED_SCHEMA = 1;

# A következő sorokat pedig ki kell
# kommentezni:
#$DEFAULT_MAIL_DOMAIN = "padl.com";
#$DEFAULT_MAIL_HOST = "mail.padl.com";
```

Az */usr/share/migrationtools* könyvtárban lévő programokkal lehet a szükséges *.ldif* fájlokat létrehozni, a következő módon:

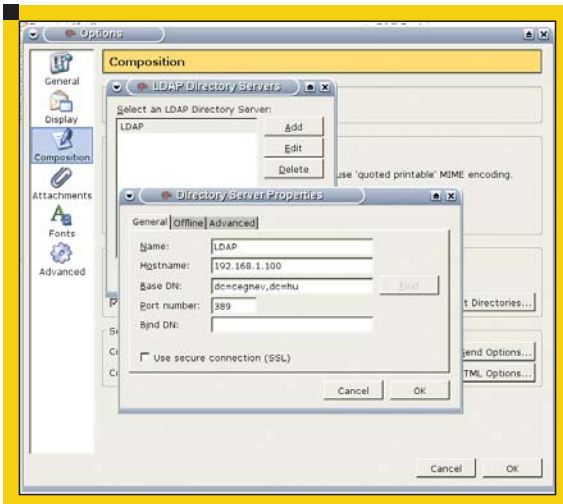
```
cd /usr/share/migrationtools
./migrate_base.pl  > ./base.ldiff
./migrate_hosts.pl  /etc/hosts > ./hosts.ldiff
./migrate_passwd.pl /etc/passwd > ./passwd.ldiff
./migrate_group.pl /etc/group > ./group.ldiff
```

A létrejött *.ldif* fájlok tartalmát a következő parancsokkal lehet az *LDAP* adatbázishoz adni:

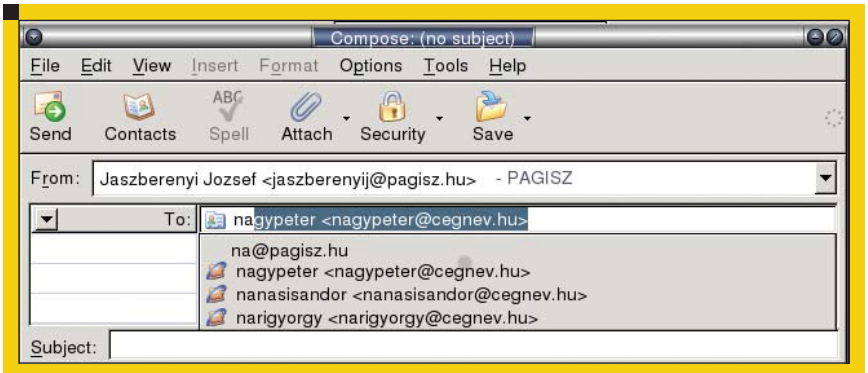
```
ldpadd -x -D "cn=admin,dc=cegnev,dc=hu" -W -f
➥./base.ldiff
ldpadd -x -D "cn=admin,dc=cegnev,dc=hu" -W -f
➥./hosts.ldiff
ldpadd -x -D "cn=admin,dc=cegnev,dc=hu" -W -f
➥./passwd.ldiff
ldpadd -x -D "cn=admin,dc=cegnev,dc=hu" -W -f
➥./group.ldiff
```



3. ábra Adatbázis böngészése GQ-val



4. ábra Mozilla Thunderbird beállítása LDAP kiszolgálóhoz



5. ábra E-mail cím keresése címzett megadásához

Bind DN:
(cn=admin,dc=cegnev,dc=hu)

Az *Ask password on first connect* kapcsolót bekapcsolva hagytam, így nem lehet megadni az adminisztrátori jelszót ebben az ablakban, hanem az adatbázis első elérésekor bekéri a program.
A *Browse* fülre kattintással lehet az adatbázist megnézni és szükség szerint módosítani. A *Search* fülre kattintás után az adatbázisban keresni lehet.

Grafikus LDAP adatbázis-kezelő program telepítése

Az eddigiekben minden esetben parancssorból mutattam be az adatbázis műveleteket. Számos grafikus felületű program áll rendelkezésre (például *GQ*, *Directory Assistant*, *Webmin LDAP* kezelő moduljai, *php4-ldap*, stb.) ezeknek a műveleteknek a kényelmesebbé tételére. Én a *GQ*-t használom a saját gépemen *KDE* alatt, de kiválóan működik más ablak kezelőkkel is.

Telepítettem *gq* csomagot:

```
apt-get install gq
```

Elindítása után először beállítottam az adatbázis elérésének adatait, a következő módon:

```
File -> Preferences -> Servers -> New
Name: beállítás tetszőleges neve (LDAP)
LDAP Host/Uri: LDAP kiszolgáló IP címe, vagy DNS
neve (192.168.1.100)
LDAP port: LDAP kiszolgáló portja (389)
Base DN: adatbázis alap (dc=cegnev,dc=hu)
```

Mivel az adatokat nem csak megnézni hanem módosítani is akartam, a *Details* fülre kattintás után beállítottam az adminisztrátort:

Levelezőkliens beállítása

A fejlettebb levelezőprogramok képesek az *LDAP* kiszolgálóban nevek, illetve e-mail címek keresésére. A *Mozilla Thunderbird* beállítását mutatom be, de természetesen más programok (pl. *MS Outlook Express*) is tudják használni, csak a beállításuk másképpen történik.
Megjelenítettem az *Edit: szerkesztés -> Preferences: beállítások -> Composition: Levél írása* ablakot. *Directory Server: címtár kiszolgáló* kapcsolót bekapcsoltam, majd az *Edit Directories...: címtárak szerkesztése* gombra kattintottam.
A megjelenő ablakban *Add: hozzáadás* gombra kattintottam, majd a mezőket kitöltöttem a következő módon:

NAME: beállítás tetszőleges neve (*LDAP*)
Hostname: kiszolgáló *DNS* neve, vagy *IP* címe (*192.168.1.100*)
Base DN: adatbázis kezdőpont (*dc=cegnev,dc=hu*)
Port (*389*)

Megfelelő beállítást követően levél írásakor a címzett mezőbe elég begépelni a címzett nevének, vagy e-mail címének néhány kezdőbetűjét és megjelenik az összes olyan név és cím, ami az adott betűkkel kezdődik.
A keresést szűkíteni több betű begépelésével lehet.
MS Outlook Express használata esetén kicsit bonyolultabb ez a művelet: új levél írásánál a címzett

1. Lista /etc/ldap/slapd.conf módosítása Samba azonosításhoz

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/
                ➥inetorgperson.schema
# Hozzáírtam a SAMBA schema fájlt:
include         /etc/ldap/schema/samba.schema

#  Módosítottam, hogy milyen index állományok
#  legyenek:
# index           objectClass eq
index           uid,uidNumber,gidNumber,
                ➥memberUid   eq
index           cn,mail,surname,givenname
                ➥eq,subinitial
index           sambaSID                    eq
index           sambaPrimaryGroupSID        eq
index           sambaDomainName             eq

# Módosítottam a hozzáférési jogosultságokat,
# hogy a SAMBA jelszavakat
# is tudja módosítani az LDAP adminisztrátor és
# a tulajdonos:
# access to attrs=userPassword
access to attrs=userPassword,sambaNTPassword,
➥sambaLMPassword
  by dn="cn=admin,dc=cegnev,dc=hu" write
  by dn="cn=replicator,dc=cegnev,dc=hu" read
  by anonymous auth
  by self write
  by * none

access to *
        by dn="cn=admin,dc=cegnev,dc=hu" write
        by * read
```

megadása ablakban az *LDAP* kiszolgáló kiválasztása után a keresés funkcióval végezhető el.

LDAP kiszolgáló beállítása Samba kiszolgálóhoz

Munkahelyemen a munkaállomásokon *MS Windows* működik, ezért van szükség *Samba* kiszolgálóra. Természetesen az *LDAP* kiválóan működik *Samba* nélkül is, így ha valakinek nincs szüksége rá, akkor ezek a lépések értelem szerűen elhagyhatók.
Az *LDAP* kiszolgáló részére a *schema* fájlok írják le, milyen mezőket tud tárolni. Ezek helye a */etc/ldap/schema* könyvtárban van. Ha *Samba* azonosítást kívánunk használni, akkor ki kell egészíteni a könyvtár tartalmát a *Samba* részére készített *schema* fájlal. Telepítettem ehhez a *samba-doc* csomagot, a tömörített *schema* fájlt bemásoltam kicsomagolva az */etc/ldap/schema* könyvtárba és beállítottam a tulajdonost, illetve a jogosultságot:

```
apt-get install samba-doc
zcat /usr/share/doc/samba-doc/examples/LDAP/
➥samba.schema.gz > /etc/ldap/schema/samba.schema
chown slapd.slapd /etc/ldap/schema/samba.schema
chmod 640 /etc/ldap/schema/samba.schema
```

LDAP kiszolgálót leállítottam, majd módosítottam az */etc/ldap/slapd.conf* fájlt (itt most csak a *master* kiszolgálón végzett módosításokat mutatom be; *1. Lista*).
Ellenőriztem a */etc/slapd.conf* fájlt:

```
slaptest
```

LDAP kiszolgálót elindítottam, majd működését ellenőriztem.

Samba fiókok kezelése

Az *smbldap-tools* csomag *Perl* nyelven íródott programjaival kényelmesen lehet a *Samba* fiókokat kezelni.
Ezek a parancsok megtalálhatók a *samba-doc* csomag telepítése után, az */usr/share/doc/samba-doc/examples/LDAP/smbldap-tools-x.x.x* könyvtárban is. A csomagot az elsődleges *Samba* tartományvezérlőre (*PDC*) telepítettem:

```
apt-get install smbldap-tools
```

A függőségek miatt nálam 14 csomagot telepített. Parancsai a */usr/sbin* könyvtárba kerülnek, de használatuk előtt be kell állítani. Átmásoltam először a */usr/share/doc/smbldap-tools/examples* könyvtárból az *smbldap.conf.gz* fájlt kitömörítve és az *smbldap_bind.conf* fájlt az */etc/smbldap-tools* könyvtárba:

```
zcat /usr/share/doc/smbldap-tools/examples/
➥smbldap.conf.gz > /etc/smbldap-tools/
➥smbldap.conf
cp /usr/share/doc/smbldap-tools/examples/
➥smbldap_bind.conf /etc/smbldap-tools/
➥smbldap_bind.conf
```

Munkahelyemen eddig is működött *Samba* tartományvezérlő. Mivel a tartomány azonosítónak (*SID*) nem szabad megváltozni, lekérdeztem a régi *Samba* kiszolgálónkon az értékét és egy fájlba írattam, ahonnan szövegszerkesztővel másoltam át:

```
net getlocalsid tartomanynev > SID
```

Módosítottam az */etc/smbldap-tools/smbldap.conf* fájlt a *2. Listának* megfelelően.
Az */etc/smbldap-tools/smbldap_bind.conf* fájlban beállítottam a master kiszolgáló adminisztrátort és jelszavát:

```
masterDN="cn=admin,dc=cegnev,dc=hu"
masterPw="adminjelszo"
```

A titkosítás nélkül megadott jelszó miatt veszélyes lenne ha ehhez idegen hozzáférne, ezért módosítottam a jogosultságát:

```
chmod 600  /etc/smbldap-tools/smbldap_bind.conf
```

2. Lista /etc/smbldap-tools/smbldap.conf fájl

```
# Mentett tartomány azonosító (SID) érték
SID="S-1-5-21-2139989288-483860436-2398042574"

# Ha van szolga LDAP kiszolgáló, akkor a címe
# és a portja
slaveLDAP="127.0.0.1"
slavePort="389"

# LDAP kiszolgáló címe és portja
masterLDAP="127.0.0.1"
masterPort="389"

# A TLS bejegyzéseket csak titkosított
# kapcsolat esetén kell beállítani

# Adatbázis kiindulási pontja
suffix="dc=cegnev,dc=hu"

# Felhasználófiókok, csoportok, gépek, stb.
➥tárolóegységeinek neve
usersdn="ou=Users,${suffix}"
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Groups,${suffix}"
idmapdn="ou=Idmap,${suffix}"

# SAMBA Domain neve
sambaUnixIdPooldn="sambaDomainName=CEGNEV,
➥${suffix}"

# Keresési hatókör az adatbázisban
scope="sub"

# Milyen titkosítást használjon a jelszavakhoz
hash_encrypt="SSHA"

# A továbbiakban a fájlban UNIX és a SAMBA fiók
# alapbeállítások vannak
#  shell beállítás, home könyvtár, login
# script, stb. ezeket értelem szerint
# módosítottam
```

A beállítások elvégzése után először létrehoztam a ***Samba*** számára szükséges alap adatbázis-szerkezetet a következő paranccsal:

```
smbldap-populate
```

A csomag további parancsait az *1. Táblázat* tartalmazza. A parancsok alkalmasak ***UNIX*** és ***Samba*** csoportok és fiókok kezelésére egyaránt. Valamennyi parancsról segítséget lehet kiíratni a parancs után gépelt `-h` kapcsolóval. Az ***smbldap*** parancsok használatára a *2. Táblázatban* találunk néhány példát.
Samba gépfiókot létrehozni én csak 2 egymás után kiadott paranccsal tudtam.

1. táblázat *Az smbldap parancsai*

`smbldap-useradd`	fiók létrehozása
`smbldap-userdel`	fiók törlése
`smbldap-usermod`	fiók módosítása
`smbldap-usershow`	fiók megjelenítése
`smbldap-userinfo`	alapértelmezett héj, teljes név, stb. módosítása
`smbldap-passwd`	jelszó módosítása
`smbldap-groupadd`	csoport létrehozása
`smbldap-groupdel`	csoport törlése
`smbldap-groupmod`	csoport módosítása, csoporttagok hozzáadása és törlése
`smbldap-groupshow`	csoport adatainak és tagjainak megjelenítése

2. táblázat *Néhány példa az smbldap parancsainak használatára*

`Smbldap-groupadd csoport`	Létrehoz megadott nevű UNIX csoportot
`smbldap-groupadd -a csoport`	Létrehoz megadott nevű Samba csoportot
`smbldap-groupmod -m fiok csoport`	Hozzáadja a megadott fiókot a csoporthoz
`smbldap-useradd fiok`	Létrehoz megadott nevű UNIX fiókot
`smbldap-useradd -a fiok`	Létrehoz megadott nevű Samba fiókot
`smbldap-passwd fiok`	Módosítja a fiók jelszavát

Előbb az

```
smbldap-useradd -w -d /dev/null -s /bin/false
gepnev
```

paranccsal létrehozom a megadott nevű gépfiókot, majd a

```
smbldap-usermod -a gepnev$
```

művelettel hozzáadom a fiókhoz a ***Samba*** mezőket.

Elsődleges tartományvezérlő Samba kiszolgáló beállítása LDAP azonosításhoz

A ***Samba*** leállítása után módosítottam az */etc/samba/smb.conf* fájlt az *3. Listának* megfelelően. Itt most csak az ***LDAP*** kiszolgálóval való együttműködés miatti fontos részeket mutatom be:
Minden ***Samba*** kiszolgálóra telepítettem ***LDAP slave*** kiszolgálót a gyorsabb működés érdekében, ezért van a ***localhost*** megadva a kiszolgáló nevénél. Az `add machine script` kezdetű sor biztosítja, ha egy munkaállomást újratelepítés

3. Lista /etc/samba/smb.conf fájl LDAP azonosításhoz

```
[global]
  workgroup = DOMAIN_NEV
  netbios name = SERVER_NEVE
  server string = %h Linux (Samba %v)
  browseable = yes

  security = user
  local master = yes
  os level = 255
  domain master = yes
  preferred master = yes
  domain logons = yes

  log file = /var/log/samba/log.%m
  max log size = 1000
  syslog only = no
  syslog = 0

  passdb backend = ldapsam:"ldap://localhost"
  ldap timeout = 10
  ldap admin dn = cn=admin,dc=cegnev,dc=hu
  ldap suffix = dc=cegnev,dc=hu
  ldap group suffix = ou=Groups
  ldap user suffix = ou=Users
  ldap machine suffix = ou=Computers
  ldap idmap suffix = ou=Idmap

  add machine script = /usr/sbin/smbldap-useradd
  ➥-w "%u"
  # add user script = /usr/sbin/smbldap-useradd
  ➥-m "%u"
  # ldap delete dn = Yes
  # delete user script = /usr/sbin/smbldap-
  ➥userdel "%u"
  # add group script = /usr/sbin/smbldap-
  ➥groupadd -p "%g"
  # delete group script = /usr/sbin/smbldap-
  ➥groupdel "%g"
  # add user to group script = /usr/sbin/
  ➥smbldap-groupmod -m "%u" "%g"
  # delete user from group script = /usr/sbin/
  ➥smbldap-groupmod -x "%u" "%g"
  # set primary group script = /usr/sbin/
  ➥smbldap-usermod -g '%g' '%u'

  encrypt passwords = true
  ldap passwd sync = Yes
  # unix password sync = Yes
  passwd program = /usr/sbin/smbldap-passwd
  ➥-u %u
  passwd chat = "Changing password for*\nNew
  ➥password*" %n\n "*Retype new password*"
  ➥%n\n"
  obey pam restrictions = no

  admin users = administrator
  invalid users = root
  guest account = nobody

  logon script = scripts\%U.bat
  logon path =
  logon home =
```

után vissza kell tenni a tartományba, automatikusan frissüljön a fiókja. A `logon path =` és `logon home =` paraméter nélküli sorokra azért van szükség, hogy alapértelmezés szerint helyi profilja legyen a felhasználóknak. Ha ez a két sor hiányzik, akkor az alapértelmezés a központi vándor profil, még akkor is, ha a felhasználó fiókjában törölve van a profil elérési útja.
A *Samba*-nak megadtam az *LDAP* adminisztrátor jelszavát, amit a */var/lib/samba/secrets.tdb* fájlban tárol:

```
smbpasswd -w adminjelszo
```

Elindítottam a *Samba* kiszolgálót:

```
/etc/init.d/samba start
```

Ellenőriztem a *Samba* működését a felhasználófiókok kiíratásával. Mivel még más fiókot nem hoztam létre, csak az *administartor* és a *nobody* felhasználó jelenik meg, melyeket az `smbldap-populate` parancs hozott létre:

```
pdbedit -L
```

Egy fiókról részletes információt a következő paranccsal lehet megjeleníteni:

```
pdbedit -Lv fioknev
```

Meglévő Samba fiókok és csoportok átvitele (migráció)

Ez az egyik legnagyobb probléma, mert az átvitt fiókok nevének, azonosítójának, jelszavának, stb. meg kell egyezni, máskülönben használhatatlanok lesznek. Erre a problémára nem találtam igazán jól használható megoldást, így magam írtam meg a szükséges programot *Perl* nyelven. A program futtatásához 4 fájlra volt szükségem az eredeti kiszolgálókról. Ezek közül az első kettő az a */etc/passwd* és */etc/shadow* (melyek a felhasználókat és a gépfiókokat is tartalmazták) az eddigi *NIS master* kiszolgálónkról másoltam le.
A másik két fájlt az eredeti *Samba* kiszolgálón állítottam elő, a következő parancsokkal:

```
pdbedit -Lv > smbfiokok
pdbedit -Lw > smbpasswd
```

Valamennyi fájlt átmásoltam a *master LDAP* kiszolgáló egy könyvtárába. Szövegszerkesztővel átnéztem a *Samba* kiszolgálón előállított fájlokat és eltávolítottam a zavaró üzeneteket az elejükről és végükről. Az „*smbfiokok*” fájlnak a művelet után „----------” karaktersorozattal kell kezdődni (a fiókokat ez választja el egymástól), az *smbpasswd* fájlban pedig minden egyes sornak egy fiókadatot kell tartalmazni. Az *smbfiokok* fájlból eltávolítottam azokat a fiókokat, melyeket nem kívántam átvinni az *LDAP* adatbázisba. A *passwd* és *shadow* állományokat nem módosítottam, mivel a program csak azokat a fiókokat olvassa ezekből az állományokból, melyek az *smbfiokok* fájlban megtalálhatók. Elindítottam az általam készített *smbuserldif* programot, ami elkészítette a felhasználó- és gép-fiókok hozzáadására alkalmas *smbldap.ldif* fájlt. Ennek tartalmát a szokásos módon az adatbázishoz adtam:

```
smbldap -x -D "cn=admin,dc=cegnev,dc=hu" -W -f
smbldap.ldif
```

A csoportok átvitelére a fenti program nem alkalmas, ezért egy másik kis programot készítettem, amelyik ezt a feladatot elvégzi. A *NIS* kiszolgálóról lemásoltam az */etc/group* fájlt és szövegszerkesztővel eltávolítottam azokat a csoportokat, melyeket nem kívántam átvinni. Az általam készített *migrategroup* program futtatásával létrehoztam a *UNIX* csoportokat és felvettem azokba a szükséges felhasználókat. Ha valaki *Samba* csoportot kíván átvinni, akkor hasonlóan járhat el, de a programban az `smbldap-groupadd` parancs után egy `-a` kapcsolót kell elhelyezni. A program nem fogja helyesen beállítani azonban a *Samba* csoport azonosítóját, ezért azt le kell kérdezni az eredeti *Samba* kiszolgálón és az adatbázisban módosítani (például *GQ*). *Samba* kiszolgálón a *Samba* csoportokat és azonosítójukat a következő paranccsal lehet lekérdezni:

```
net groupmap list
```

Postfix levelező kiszolgáló beállítása LDAP azonosításhoz

Telepítettem a *postfix LDAP* azonosító modulját:

```
apt-get install postfix-ldap
```

Létrehoztam egy */etc/postfix/ldap-aliases.cf* fájlt a következő tartalommal:

```
version = 3
server_host = localhost
search_base = dc=cegnev,dc=hu
```

A */etc/postfix/main.cf* fájlt a következőképpen módosítottam:

```
alias_maps = hash:/etc/aliases,
ldap:/etc/postfix/ldap-aliases.cf
```

Postfix konfigurációját újra beolvastattam

```
/etc/init.d/postfix reload
```

Courier-POP3 és Courier-IMAP beállítása LDAP azonosításhoz

Munkahelyemen a *Courier POP3* és *IMAP* kiszolgálók titkosítás nélküli és titkosított változata is telepítve van, mivel a hálózaton kívülről csak titkosítottan érhető el a levelezés. Az azonosítás a *PAM*-on keresztül történik. Módosítani kell az */etc/pam.d/pop3* és */etc/pam.d/imap* fájlok tartalmát, mivel azokban nem a *Debian „sarge”*-ban szokásos common-* fájlokra történő hivatkozás van. Mind a két fájlban „kikommenteztem” az eredeti sorokat és beírtam a következőket:

```
@include common-auth
@include common-account
@include common-password
@include common-session
```

Azonosítást használó squid proxy beállítása LDAP kiszolgálóhoz

Intézményünkben az internetezés csak *proxy* kiszolgálón keresztül, azonosítás után lehetséges. Ezzel szűrni tudjuk a tanulók által megjeleníthető tartalmat és a *proxy* használat lehetővé teszi a sávszélesség korlátozást is, amire a szűkös internet sávszélességünk miatt nagy szükség van.
A */etc/squid/squid.conf* fájlba a következő sorokat írtam:

```
# "basic" az azonositas tetszoleges neve
# -h utan kell megadni az LDAP kiszolgalo IP
cimet
auth_param basic program /usr/lib/squid/ldap_auth
-b "dc=cegnev,dc=hu" -v 3 -h 192.168.1.100

# Az acl.dolgozok es acl.tanulok fajlokban vannak
a felhasznalonevek (soronkent egy nev)
# Az acl-ek ezután már szokás szerint
használhatók
acl dolgozok proxy_auth "/etc/squid/
➥acl.dolgozok"
acl tanulok  proxy_auth "/etc/squid/
➥acl.tanulok"
```

Az *LDAP* azonosítás nálunk több hete hibátlanul működik. Miután minden olyan kiszolgálóra telepítettem *slave* kiszolgálót, mely gyakran igényel azonosítást, a sebességgel sem volt semmi probléma. A kiszolgálók erőforrásainak terheltségét csak minimális mértékben növelte a *NIS*-hez képest.
A kedvező tapasztalataim miatt minden közepes és nagyobb hálózatban ajánlani tudom kipróbálását.

Jászberényi József
(jaszberenyij@pattantyus-gyor.sulinet.hu)

Szeret biciklizni, kirándulni, olvasni, sörözni és szabadban főzni. A stratégiai játékoktól a műszaki CAD programokig sok minden érdekli. Legtöbbet szerverprogramokkal foglalkozik és néha mérgelődik.


Linuxvilág
www.linuxvilag.hu