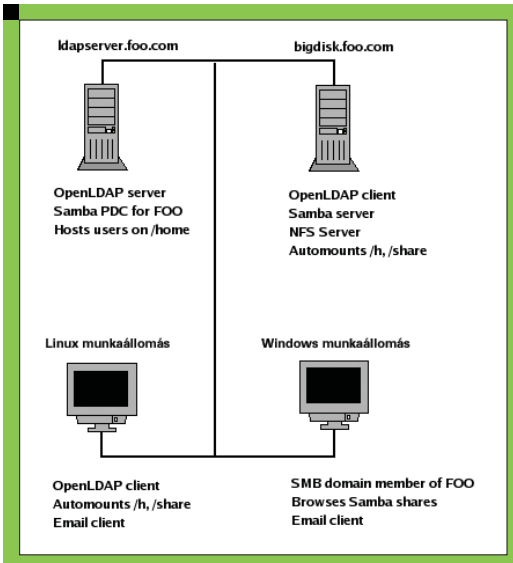
OpenLDAP mindenütt – újra

A Samba 3 új szolgáltatásként képes egységes címtárat biztosítani az összes ügyfél számára. Az új program közös alapot szolgáltat a levelezéshez, a fájlmegosztáshoz és a többi szolgáltatáshoz.

2003 januárjában megjelent, *„OpenLDAP mindenütt”* című írásunk alapján több olvasónk is sikeresen épített egységesített vállalati bejelentkezési rendszert. Azóta az *OpenLDAP* és a *Linux* egyaránt sokat fejlődött. Az alábbiakban szeretnénk bemutatni, hogyan használható az *OpenLDAP* vegyes környezet központi címtárszolgáltatásaként. Az *LDAP* kiszolgáló az összes ügyfél számára megosztott elektronikus levelező címtárat biztosít, valamint támogatja a *Linux* és a *Microsoft Windows* alapú ügyfelek bejelentkezését, a kezdőkönyvtárak önműködő befűzését és a fájlmegosztást. Az írásunk alapjául szolgáló, egyszerű, vegyes környezetet az *1. ábrán* szemléltettük.

LDAP-kiszolgáló telepítése és beállítása

Az írásunk tárgyát adó *LDAP* kiszolgálót bináris *RPM* csomagokból és az *openldap-2.2.13-2* segítségével telepítettük, *Fedora Core 3* rendszerre. Az *nss_ldap* csomagot szintén telepítenünk kellett. A legújabb források az *openldap.org* webhelyről érhetők el (lásd a forrásokat). Telepítés után az *1. kódrészletben* látható módon írjuk át a */etc/openldap/slapd.conf* beállító fájlt. Az üres karakterrel kezdődő sorok értelmezése az előző sor folytatásaként történik, vagyis a hosszabb sorok végére nem kell visszaperjelet írni.
Az *LDAP* séma a címtárbejegyzéseket alkotó objektumosztályokat és jellemzőket határozza meg. Az *RPM* csomagban is megtalálható *Red Hat*-féle *autofs* séma pont megfelel az igényeinknek. Ha hozzá szeretnénk adni a címtárhoz egy *objektumosztályt* (`objectClass`) vagy *jellemzőt* (`attribute`), tanulmányozzuk át az *OpenLDAP* felügyeleti útmutatóját.
Az adatbázis típusa az alapértelmezett *ldbm* lett. Példánkban az *LDAP* tartomány összetevőjét használjuk, így a `pelda.com` `dc=pelda,dc=com` formát nyert.
A *kezelő (manager)* teljes írási jogot kapott az *LDAP* bejegyzésekhez. A kezelő jelszavát a /usr/sbin/slappasswd segítségével hozhatjuk létre, majd a titkosított jelszót a *slapd.conf* `rootpw` bejegyzésébe kell bemásolnunk.
Az indexsorok révén gyorsítható a gyakrabban lekérdezett jellemzők elérése. A hozzáférés-vezérlés korlátozza a `userPassword` *(felhasználói jelszó)* bejegyzés elérését, ezt csak a felhasználó és a kezelő módosíthatja. Minden más bejegyzésre a kezelő írási, mások pedig olvasási jogot kaptak.



1. ábra Vegyes környezetben a Linux és a Windows alapú ügyfelek közös LDAP-infrastruktúrát használnak

A címtárszerkezet létrehozása

A címtár minden elemét egyértelműen azonosítja a *megkülönböztető neve (distinguished name,* `dn`*)*. A `pelda.com` megkülönböztető neve például: `dc=pelda, dc=com`.
Az `organizationalUnit` *(szervezeti egység,* `ou`*)* a bejegyzések csoportosítására biztosít lehetőséget. A címtár szerkezete a *2. kódrészlet* alapján követhető.
A legfelsőbb szintű bejegyzéseket *LDAP adatcsere formátumban (LDAP Interchange Format, LDIF)* hozzuk létre, majd a *3. kódrészletben* látható formában elmentjük őket a `top.ldif`-be.
A legfelsőbb szintű bejegyzéseket az `ldapadd` paranccsal adjuk hozzá a címtárhoz:

```
ldapadd -x -D 'cn=manager,dc=pelda,dc=com' \
-W -f top.ldif
```

Ezután egy az összes bejegyzést lekérdező `ldapsearch` paranccsal ellenőrizzük munkánkat:

```
ldapsearch -x -b 'dc=pelda,dc=com'
```

1. kódrészlet A slapd.conf fájl fontos, az LDAP biztonságos futtatásához szükséges beállításokat tartalmaz

```
# slapd.conf
# a használni kívánt sémák
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/
            ➥inetorgperson.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/samba.schema
include     /etc/openldap/schema/redhat/autofs.schema
# az adatbázis megadása
database    ldbm
suffix      "dc=pelda,dc=com"
rootdn      "cn=Manager,dc=pelda,dc=com"
# A nyílt jelszavakat, különösen a rootdn esetében
# kerülni kell. Használjunk erős hitelesítést.
# root jelszó
rootpw      {SSHA}xxxxxxxxxxxxxxxxxxxx
directory   /var/lib/ldap
# Az adatbázishoz fenntartott indexek
index       objectClass,uid,uidNumber,gidNumber,
            ➥memberUid eq
index       cn,mail,surname,givenname eq,subinitial
index       sambaSID eq
index       sambaPrimaryGroupSID eq
index       sambaDomainName eq
# A felhasználók hitelesítést végezhetnek, illetve
# megváltoztathatják jelszavukat.
access to attrs=userPassword,sambaNTPassword,
       sambaLMPassword
       by dn="cn=Manager,dc=pelda,dc=com" write
       by self write
       by anonymous auth
       by * none
# A többi jellemző mindenki számára olvasható.
access to *
       by self write
       by dn="cn=Manager,dc=pelda,dc=com" write
       by * read
```

Az e-mail címek megosztása

Ezen a ponton már elegendően bonyolult *LDAP*-szerkezetet alkottunk ahhoz, hogy valós használatba vehessük. Kezdjük az e-mail címek megosztásával. Az eljárás egyszerűbb, ha a névjegyalbumunkat ki tudjuk menteni *LDIF* formátumban, erre például a *Mozilla Thunderbird* az *Address Book (Címjegyzék)* ablak *Tools (Eszközök)* menüjéből biztosít lehetőséget. A kapott fájlt további műveletek végrehajtásával az alábbi példához hasonló formátumúra kell hozni, ez a legjobban talán *Perlben* oldható meg.

A névjegyeket a hozzájuk tartozó e-mail címek azonosítják egyedileg. Például egy névjegy megkülönböztető neve: `dn: uid=valaki@valahol.com,ou=contacts,?ou=people,dc=pelda,dc=com`.

2. kódrészlet Az LDAP megkülönböztető nevei a szervezeti egységek szerint faszerkezetbe rendeződnek

```
+ dc=pelda,dc=com
|- ou=People                  Személyek
|  |- ou=contacts,ou=people   E-mail címek
|- ou=Groups                  Rendszercsoportok
|- ou=auto.master             Automount mester térkép
|- ou=auto.home               Automount térkép
|- ou=auto.misc               Automount térkép
|- ou=Computers               Samba tartománytagok
|- cn=NextFreeUnixId          Következő szabad
                              Samba-azonosító
|- SambaDomainName            Samba tartományi
                              információs
                              objektumosztály
```

A névjegy teljes bejegyzése az összes adattal így alakul:

```
dn: uid=valaki@valahol.com,ou=contacts,
?ou=people,dc=pelda,dc=com
mail: valaki@valahol.com
uid: valaki@valahol.com
givenName: Valaki
sn: Kitudja
cn: Valaki Kitudja
objectClass: person
objectClass: top
objectClass: inetOrgPerson
```

Az egyes névjegyeket egy-egy üres sorral válasszuk el egymástól, majd mentsük el őket egy *contacts.ldif* nevű fájlba. A címtárhoz az `ldapadd` paranccsal adhatjuk hozzá a névjegyeket:

```
ldapadd -x -D 'cn=manager,dc=pelda,dc=com' \
-W -f contacts.ldif
```

Az utána következő ellenőrzést az előbbihez hasonlóan, az `ldapsearch` paranccsal végezhetjük el.

A levelezőügyfelek beállítása

A következő lépésünk a *Mozilla Thunderbird* beállítása az új *LDAP* kiszolgáló használatára (2. *ábra*). A *Thunderbird Tools (Eszközök)* menüjéből válasszuk az *Options (Beállítások)* parancsot. A *Composition (Összeállítás)* lapon válasszuk a *Directory Server (Címtárkiszolgáló)*, az *Edit Directories (Címtárak szerkesztése)*, majd az *Add (Hozzáadás)* parancsot. A *Directory Server Properties (Címtárkiszolgáló tulajdonságai)* panelen a következő adatokat kell beírnunk:

```
Name: PELDA
Server: ldapkiszolgalo.pelda.com
base DN: ou=people,dc=pelda,dc=com
```

Az *Advanced (Speciális)* lapon a címtár méretének megfelelően növeljük meg a kapott találatok számát. A `pelda.com` esetében mi 1000 találatot állítottunk be.

A beállításokat úgy ellenőrizhetjük, hogy írunk egy üzenetet egy az *LDAP* címtár névjegyalbumában szereplő személynek. Gépelés közben a programnak magától ki kell egészítenie a címet. Szintén alkalmas az ellenőrzésre, ha a ***Thunderbird Mail Address Bookjából (E-mail címjegyzék)*** indítunk egy *LDAP* keresést. A keresést a `PELDA` címjegyzékben végezzük, és keresési feltételként a ***Name or Email contains (Név vagy e-mail tartalmazza a következőt)*** mezőbe írjunk be egy csillagot; ekkor eredményként az összes névjegyet meg kell kapnunk.

Egységesített, LDAP alapú bejelentkezés Linux alatt

Ha a felhasználói fiókok adatait *LDAP* alatt tároljuk, akkor ugyanazt a felhasználónevet és jelszót tetszőleges linuxos konzolon használhatjuk. Először el kell döntenünk, hogy mely felhasználóneveket szeretnénk bevinni *LDAP* alá. Az *1. táblázat* a saját felhasználói sémánk ***UID/GID (felhasználóazonosító/csoportazonosító)*** kiosztását szemlélteti. A fenti felhasználói sémával 9000 egységesített, *LDAP* alatti bejelentkezési bejegyzést tudunk létrehozni, valamint az *LDAP* alatti *UID*-kkal és *GID*-kkel nem ütköző helyi felhasználókat és csoportokat is meg tudunk adni. A felhasználói séma szerint a *Samba* elsődleges tartományvezérlője számára szükséges fiókokat is el tudjuk különíteni.

A felhasználói bejelentkezési bejegyzések létrehozása LDAP alatt

A felhasználói bejelentkezési bejegyzéseket `uid`-ként a bejelentkezési név azonosítja. A bejelentkezési felhasználók az `ou=people` tagjai, vagyis a megkülönböztető név a következő lesz:

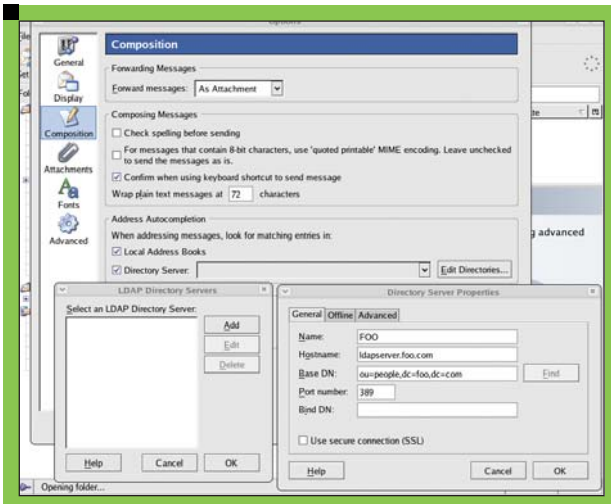
```
dn: uid=gomerp,ou=people,dc=pelda,dc=com
```

A teljes bejegyzés a fiók elérésének szabályozásához szükséges jellemzőket is tartalmazza, amint az a *4. kódrészletben* is látható, továbbá a *Samba* által igényelt beállításokat is felöleli; ezekről később lesz szó.
Az *OpenLDAP*-hoz áttérést segítő programok is tartoznak, ezekkel ki tudjuk nyerni a felhasználói fiókok adatait; minderről részletesebb tájékoztatást a */usr/share/openldap/migration* könyvtárban lehet találni. Ha meglévő */etc/passwd* fájlt szeretnénk *LDIF* formátumúvá alakítani, akkor először ismerkedjünk meg a ***migrate_common.ph*** fájllal. A fájlt át kell írnunk, megadva tartományunk nevét és az alapértelmezett alapsémát, illetve engedélyezve a kiterjesztett sémát:

```
# Alapértelmezett DNS-tartomány
$DEFAULT_MAIL_DOMAIN = "pelda.com";
# Alapértelmezett alap
$DEFAULT_BASE = "dc=pelda,dc=com";
# Bekapcsolásával általánosabb objektumosztályokat
# is támogathatunk,
# mint például a person (személy).
$EXTENDED_SCHEMA = 1;
```

Nyerjük ki a fiókok adatait a */etc/passwd* fájlból:

```
/usr/share/openldap/migration/migrate_passwd.pl \
/etc/passwd > people.ldif
```



2. ábra A vállalati címtár használatához adjuk meg a kiszolgáló adatait a Thunderbird Directory Server Properties (Címtárkiszolgáló tulajdonságai) párbeszédpanelén

1. táblázat *A felhasználói sémánk UID/GID-kiosztása*

Fiók típusa	UID
Rendszerfiókok	UID < 500
Különleges Samba fiókok	499 < UID < 1000
Egységesített fiókok	999 < UID < 10000
Helyi felhasználók, melyek nem szerepelnek az LDAP-ban	> 10000

Ellenőrizzük a kapott *LDIF* fájlt. A rendszerfiókokhoz – mint a root – és a helyi felhasználók saját, az *LDAP*-ban szükségtelen csoportjaihoz tartozó bejegyzéseket távolítsuk el. Adjuk hozzá a felhasználói bejegyzéseket a címtárhoz, majd az `ldapsearch` paranccsal a már ismert módon ellenőrizzük az eredményt:

```
ldapadd -x -D 'cn=manager,dc=pelda,dc=com' -W \
-f people.ldif
```

Mivel a bejelentkezési felhasználók az `ou=people` szervezet tagjai, ettől kezdve elektronikus levélcímüket a levelező-programunkból is elő tudjuk keresni.

Csoportbejegyzések létrehozása

Minden több linuxos számítógép között megosztani kívánt csoporthoz létre kell hoznunk egy csoportbejegyzést. Emellett minden felhasználót be kell sorolnunk egy saját csoportba. A csoportbejegyzéseket a cn azonosítja, és minden csoport az `ou=Groups` (csoportok) szervezethez tartozik. Például:

```
dn: cn=gomerp,ou=Groups,dc=pelda,dc=com
```

Egy felhasználó saját csoportja a következőképpen néz ki:

```
dn: cn=gomerp,ou=Groups,dc=pelda,dc=com
objectclass: posixGroup
objectclass: top
```

3. kódrészlet Az LDAP-fa csúcsát (top.ldif) kézzel hozzuk létre, egyszerű, kulcs: érték formátumban

```
dn: dc=pelda,dc=com
objectClass: dcObject
objectClass: organization
o: Példa Vállalat
dc: pelda
dn:ou=People,dc=pelda,dc=com
objectClass: organizationalUnit
ou: People
dn:ou=Groups,dc=pelda,dc=com
objectClass: organizationalUnit
ou: Groups
dn:ou=contacts,ou=people,dc=pelda,dc=com
associatedDomain: pelda.com
ou: contacts
ou: people
objectClass: organizationalUnit
objectClass: domainRelatedObject
```

```
cn: gomerp
userPassword: {crypt}x
gidNumber: 5223
```

Egy megosztott csoport pedig így:

```
dn: cn=web_dev,ou=Groups,dc=pelda,dc=com
objectclass: posixGroup
objectclass: top
cn: web_dev
gidNumber: 5019
memberUid: gomerp
memberUid: goober
memberUid: barneyf
```

Másoljuk ki a csoportadatokat a */etc/group* fájlból:

```
/usr/share/openldap/migration/migrate_passwd.pl \
/etc/group > group.ldif
```

Ellenőrizzük a kapott ***LDIF*** fájlt. A rendszercsoportokhoz és a helyi rendszerfelhasználókhoz tartozó, az ***LDAP***-ban szükségtelen adatokat töröljük belőle.
Adjuk hozzá a csoportbejegyzéseket a címtárhoz, majd az `ldapsearch` paranccsal végezzük el az ellenőrzést:

```
ldapadd -x -D 'cn=manager,dc=pelda,dc=com' -W \
-f group.ldif
```

Az ***automount*** beállítása a kezdőkönyvtárak megosztására és az ***NFS*** megosztások elérhetővé tételére.
Egységesített bejelentkezésnél a felhasználók központi, ***NFS***-en ***(Network File System, hálózati fájlrendszer)*** keresztül megosztott kezdőkönyvtárral rendelkeznek. Bár mi a kezdőkönyvtárakat az ***ldapkiszolgalo.pelda.com***-on helyeztük el, majd megosztottuk a */home* könyvtárat, a fájlkiszolgálónak és az ***OpenLDAP***-nak nem muszáj azonos gépen futnia. Az ***NFS*** tárgyalása túlmutatna témakörünkön, mégis idézzük be azt az egy sort a */etc/exports* fájlból, mely a kezdőkönyvtárak elérhetővé tételéért felelős:

4. kódrészlet Egy felhasználói bejelentkezési bejegyzés a bejelentkezéshez szükséges adatok mellett a Samba bizonyos beállításait is tartalmazza

```
dn:uid=gomerp,ou=People,dc=pelda,dc=com
uid: gomerp
cn: Gomer Pyle
sn: Pyle
givenname: Gomer
mail: gomer.pyle@pelda.com
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSAMAccount
uidNumber: 5000
homeDirectory: /h/gomerp
loginShell: /bin/bash
description: Gomer Pyle
displayName: Gomer Pyle
gecos: Gomer Pyle
gidNumber: 513
userPassword: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaSID: S-1-5-21-1400792368-3813960858
➥-1703501993-11000
sambaPrimaryGroupSID: S-1-5-21-1400792368
➥-3813960858-1703501993-513
sambaLogonScript: gomerp.cmd
sambaHomeDrive: H:
sambaHomePath: \\LDAPKISZOLGALO\gomerp
sambaLMPassword: XXXXXXXXXX
sambaAcctFlags: [U]
sambaNTPassword: XXXXXXXXXX
sambaPwdLastSet: 1097240543
sambaPwdMustChange: 1105016543
```

```
/home *.pelda.com(rw)
```

A linuxos ***LDAP***-ügyfelek az ***automount*** és az ***NFS*** segítségével bejelentkezéskor befűzik a felhasználó kezdőkönyvtárát.
Az ***LDAP*** az ***automount*** szemszögéből a ***NIS (network information service, hálózati információs szolgáltatás) automount*** térképek helyettesítője. Az ***auto.master***, az ***auto.home*** és az ***auto.misc automount*** térképét kell helyettesítenünk, amihez új szervezeti egységet kell létrehoznunk az ***auto.master*** számára:

```
dn: ou=auto.master,dc=pelda,dc=com
objectClass: top
objectClass: automountMap
ou: auto.master
```

Az `auto.master` bejegyzést a `cn` azonosítja. Az `automountInformation` jellemző arra utasítja az automountot, hogy a térképet ***LDAP*** alatt keresse:

```
dn: cn=/h,ou=auto.master,dc=pelda,dc=com
objectClass: automount
automountInformation: ldap:ou=auto.home,
➥dc=pelda,dc=com
cn: /h
```

Ha már itt vagyunk, hozzuk létre a többi ***NFS***-en keresztül megosztott könyvtár `auto.master` bejegyzését is:

```
dn: cn=/share,ou=auto.master,dc=pelda,dc=com
objectClass: automount
automountInformation: ldap:ou=auto.misc,
➥dc=pelda,dc=com
cn: /share
```

Az `automount` bejegyzéseket ***LDIF*** formátumban készítsük elő, mentsük el őket ***auto.master.ldif*** névvel, majd adjuk hozzá a bejegyzéseket az ***LDAP***-hoz:

```
ldapadd -x -D 'cn=manager,dc=pelda,dc=com' -W -f
auto.master.ldif
```

Ez után hozzunk létre egy új szervezeti egységet az `sauto.home` számára:

```
dn:ou=auto.home,dc=pelda,dc=com
objectClass: top
objectClass: automountMap
ou: auto.home
```

A kezdőkönyvtár-bejegyzéseket a `cn` azonosítja:

```
dn: cn=gomerp,ou=auto.home,dc=pelda,dc=com
objectClass: automount
automountInformation:
➥ldapkiszolgalo.pelda.com:/home/gomerp
cn: gomerp
```

Hozzuk létre az összes felhasználó `auto.home` bejegyzését ***LDIF*** formátumban, mentsük el ***auto.home.ldif*** névvel, majd adjuk hozzá a bejegyzéseket az ***LDAP***-hoz:

```
ldapadd -x -D 'cn=manager,dc=pelda,dc=com' -W \
-f auto.home.ldif
```

Linux alapú ***LDAP*** ügyfélről automatikusan befűzve az `ldapkiszolgalo.pelda.com:/home/gomerp` kezdőkönyvtár a */h/gomerp* útvonalon lesz elérhető. Szükség esetén további ***NFS***-megosztásokat is megadhatunk ***LDAP*** alatt, illetve befűzhetünk automatikusan. Az `auto.misc` szervezeti egység ezeket az automatikus befűzést segítő térképeket tartalmazza, formátumuk `ou=auto.misc`.
A */share auto.master* bejegyzését a fentiek szerint már létrehoztuk, most következzen az `ou=auto.misc` bejegyzés:

5. kódrészlet Részletek az OpenLDAP címtárral való együttműködésre beállított Samba smb.conf fájljából

```
[global]
...
  obey pam restrictions = No
  ldap passwd sync = Yes
  ldap passwd sync = Yes
...
  passdb backend = ldapsam:ldap://
  ➥ldapkiszolgalo.pelda.com/
  ldap admin dn = cn=Manager,dc=pelda,dc=com
  ldap suffix = dc=pelda,dc=com
  ldap group suffix = ou=Groups
  ldap user suffix = ou=People
  ldap machine suffix = ou=Computers
  ldap idmap suffix = ou=People
  ldap ssl = no
  add user script = \
    /usr/local/sbin/smbldap-useradd -m "%u"
  ldap delete dn = Yes
  delete user script = \
    /usr/local/sbin/smbldap-userdel "%u"
  add machine script = \
    /usr/local/sbin/smbldap-useradd -w "%u"
  add group script = \
    /usr/local/sbin/smbldap-groupadd -p "%g"
  delete group script = \
    /usr/local/sbin/smbldap-groupdel "%g"
  add user to group script = \
    /usr/local/sbin/smbldap-groupmod -m "%u" "% g"
  delete user from group script = \
    /usr/local/sbin/smbldap-groupmod -x "% u" "%g"
  set primary group script = \
    /usr/local/sbin/smbldap-usermod -g "%g" "%u "
```

```
dn:ou=auto.misc,dc=pelda,dc=com
ou: auto.misc
objectClass: top
objectClass: automountMap
```

Az ***NFS***-megosztások bejegyzéseit az `ou=auto.misc` alatt kell létrehozni:

```
dn:cn=redhat,ou=auto.misc,dc=pelda,dc=com
objectClass: automount
automountInformation:
nagymeghajto.pelda.com:/pub/redhat
cn: redhat
dn:cn=engineering,ou=auto.misc,dc=pelda,dc=com
objectClass: automount
automountInformation:
nagymeghajto.pelda.com:/data/engineering
cn: engineering
```

A bejegyzéseket mentsük el ***auto.misc.ldif*** névvel majd adjuk hozzá őket az ***LDAP***-hoz:

```
ldapadd -x -D 'cn=manager,dc=pelda,dc=com' -W -f
➥auto.misc.ldif
```

Linux alapú *LDAP* ügyfélről automatikusan befűzve a `nagymeghajto.pelda.com:/data/engineering` megosztott könyvtár */share/engineering* névvel fog látszani.

A linuxos LDAP-ügyfél beállítása

A linuxos *LDAP* ügyfél beállításának megkezdése előtt telepíteni kell a ***névszolgáltatás-kapcsoló (name service switch)*** csomagot, az *nss_ldap*-t. A *Red Hat* */usr/bin/authconfig* segédeszköze kényelmesen alkalmazható az ügyfél beállítására. Válasszuk a ***Use LDAP (LDAP használata)*** beállítást, majd a ***Server (Kiszolgáló)*** mezőbe írjuk be a következőt: ***ldapkiszolgalo.pelda.com***, a ***Base DN (Alap DN)*** mezőbe pedig a következőt: `dc=pelda,dc=com`. Az *authconfig* a következő fájlokba írja az adatokat: */etc/ldap.conf*, */etc/openldap/ldap.conf* és */etc/nsswitch.conf*.

Ellenőrizzük, hogy a */etc/nsswitch.conf* fájlban szerepelnek-e a következő bejegyzések:

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
automount:  files ldap
```

Ellenőrizzük, hogy a */etc/ldap.conf* fájl tartalmazza-e a következő bejegyzéseket:

```
host ldapkiszolgalo.pelda.com
base dc=pelda,dc=com
```

Ellenőrizzük, hogy a */etc/openldap/ldap.conf* tartalmazza-e a következő sorokat:

```
HOST ldapkiszolgalo.pelda.com
BASE dc=pelda,dc=com
```

A linuxos kiszolgáló további beállításai

Azon az *NFS*-kiszolgálón, amelyen a kezdőkönyvtárak találhatók, el kell távolítani a felhasználók jelszó- és csoportbejegyzéseit a *password* és a *group* fájlból. Készítsünk biztonsági mentéseket, majd írjuk át a */etc/passwd*, a */etc/shadow*, a */etc/group* és a */etc/gshadow* fájlt, törölve az *LDAP* alatt is szereplő személyek bejegyzéseit. Esetünkben a */etc/passwd* fájlban nem maradhat 1000 és 9999 közötti *UID*. Ellenőrzésképpen jelentkezzünk be egy *Linux* alapú *LDAP* ügyfélre egy *LDAP* felhasználónév használatával. A felhasználó bejelentkezési héját és kezdőkönyvtárát kell látnunk. Az *auto.misc* megosztásokat a megosztási név alapján történő eléréssel ellenőrizhetjük, például:

```
cd /share/redhat
```

Az *automount* csak tényleges használatukkor fűzi be az *NFS* megosztásokat, tehát a */share/redhat* könyvtár csak használata után lesz látható.

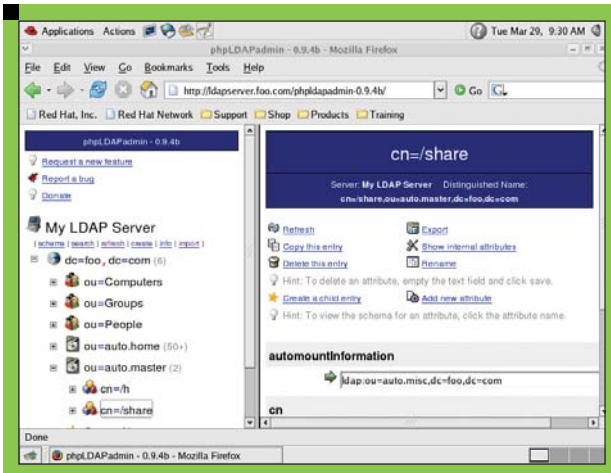
Egységesített bejelentkezés Samba és LDAP használatával

A *Samba* és az *LDAP* együttes használatának célja az, hogy egységes bejelentkezést tegyünk lehetővé a *Microsoft Windows* alapú ügyfelek számára. A gyakorlatban ez azt jelenti, hogy a felhasználók bármelyik munkaállomásról bejelentkezhetnek a hálózatra, illetve hozzáférést nyerhetnek a megosztott mappákhoz, fájlokhoz és nyomtatókhoz. Az egységesített bejelentkezés felé az első lépés a *Samba* beállítása ***elsődleges tartományvezérlőnek (primary domain controller, PDC)***. Ennek részletes tárgyalása túlmutatna írásunk keretein, ám a témáról kiváló *HOGYAN* található az *Idealx* webhelyén (lásd a forrásokat). Az *Idealx* munkatársai nagyszerű kiegészítéseket készítettek a *Samba Projecthez*, és aki komolyan akar foglalkozni a *Sambával*, annak érdemes megismerkednie segédeszközeikkel. Feltételezve, hogy már szereztünk tapasztalatot a *Samba* tartományvezérlők kezelésében, az *5. kódrészletben* részben megadott beállító fájl megfelelő alapot szolgáltathat a példánkban szereplőhöz hasonló környezet üzembe helyezéséhez. A teljes fájl a *Linux Journal FTP*-helyéről tölthető le. (Lásd a forrásokat.)

Mindezek után már csak annyi dolgunk maradt, hogy az *LDAP*-ot rávegyük a *Samba* az elmúlt évek során megjelent újdonságaiból fakadó lehetőségek kihasználására. Az eljárás hasonló a fentiekhez, de a *Samba* újabb szolgáltatásait is érdemes kihasználni. A *Samba 3*-as változatánál már lehetőség van arra, hogy az összes *Samba* fiókadatot az *LDAP* címtárban tároljuk, aminek az az előnye, hogy minden adat egyetlen központi helyre kerül.

6. kódrészlet Az smbldap-populate eszköz automatikusan hozzáadja az OpenLDAP-kiszolgáló és a Samba együttműködéséhez szükséges fiókokat

```
[root]# smbldap-populate
Using builtin directory structure
adding new entry: dc=pelda,dc=com
adding new entry: ou=Users,dc=pelda,dc=com
adding new entry: ou=Groups,dc=pelda,dc=com
adding new entry: ou=Computers,dc=pelda,dc=com
adding new entry: ou=Idmap,dc=pelda,dc=org
adding new entry:
➥cn=NextFreeUnixId,dc=pelda,dc=org
adding new entry:
➥uid=Administrator,ou=Users,dc=pelda,dc=com
adding new entry:
➥uid=nobody,ou=Users,dc=pelda,dc=com
adding new entry: cn=Domain
➥Admins,ou=Groups,dc=pelda,dc=com
adding new entry: cn=Domain
➥Users,ou=Groups,dc=pelda,dc=com
adding new entry: cn=Domain
➥Guests,ou=Groups,dc=pelda,dc=com
adding new entry: cn=Print
➥Operators,ou=Groups,dc=pelda,dc=com
adding new entry: cn=Backup
➥Operators,ou=Groups,dc=pelda,dc=com
adding new entry:
➥cn=Replicator,ou=Groups,dc=pelda,dc=com
adding new entry: cn=Domain
➥Computers,ou=Groups,dc=pelda,dc=com
```



3. ábra A címtár webes megjelenítése a phpLDAPadminnal

A Samba és az LDAP együttműködése

Az *LDAP* és a *Samba* együttes használatának fontos elemét képezik a tényleges együttműködéshez szükséges további fiókok és *LDAP* bejegyzések. Az egységesített bejelentkezési kiszolgáló működéséhez több jól ismert windowsos tartományi felhasználói és csoportfiókra is szükség van. A tartományi fiókok adatainak tárolásához különleges OU bejegyzéseket is létre kell hoznunk. Szerencsére létezik egy *smbldap-populate* nevű parancsfájl, mely az összes szükséges bejegyzést hozzáadja a rendszerhez. A parancsfájl része az *Idealx smbldap-tools* csomagjának, mely a *PDC* és a *Sambával* együttműködő *LDAP* címtár üzembe helyezésében egyaránt fontos segítséget jelent. A *6. kódrészlet* példa arra, hogy mit kell látnunk az *smbldap-populate* parancsfájl futtatásakor.

Ha megvizsgáljuk a parancsfájl kimenetét, láthatjuk, hogy jó néhány új felhasználót, csoportot és szervezeti egységet adott hozzá a címtárhoz, ilyen például a jól ismert *Domain Admins (Tartományi rendszergazdák)* és *Domain Users (Tartományi felhasználók)* csoport. A *Microsoft Windows NT* alapú változatai alapesetben is tartalmazzák ezeket a csoportbejegyzéseket. Mindegyikhez tartozik egy *viszonylagos azonosító (relative identifier, RID)* is, tehát az *LDAP* alatti felhasználói és csoportbejegyzésekhez a megfelelő windowsos felhasználók vagy csoportok *Windows* alatti *RID*-it kell rendelni. Az *smbldap-populate* parancsfájl ezekre a részletekre is ügyel. A szükséges jól ismert felhasználói és csoport *RID*-k a következők:

```
Név             RID
-----------------
Domain Admins 512
Domain Users  513
Domain Guests 514
```

A fenti felhasználói és csoportbejegyzések mellett további *OU* bejegyzésekkel egyéb tartományi szolgáltatásokat is elérhetővé tehetünk. Az első ilyen az `ou=Computers`, mely a tagkiszolgálók és a tartományi munkaállomások gépfiókjainak tárolására szolgál. A második az `ou=Idmap`, erre a *Samba Windows*-kiszolgáló által ellenőrzött tartomány tagkiszolgálójaként történő használatakor van szükség. Az utolsó új bejegyzés az `ou=NextFreeUnixId`, ez az új felhasználók és csoportok létrehozásakor következőként felhasználható *UID*-t és *GID*-t adja meg.

A címtár felügyelete

Az *LDAP* címtár kezdeti feltöltése és a *Samba* üzembe helyezése után készen állunk a felhasználók és a csoportok címtárhoz való hozzáadására. Az *Idealx* parancssori segédprogramjaival ezt a feladatot is könnyedén elintézhetjük, de léteznek *PHP* alapú címtárkezelők is, melyekkel szintén megkönnyíthetjük munkánkat, mi például a *phpLDAPadmint* és az *LDAP Account Managert (LAM)* ajánljuk. Mindkettő könnyen használható, a címtárat és a bejegyzéseket grafikus formában jeleníti meg, illetve módot ad az *LDAP* bejegyzések szerkesztésére is (*3. ábra*). A *Java* alapú *LDAP* böngésző egy további eszköz a címtár tartalmának megtekintésére és szerkesztésére.

A 2002 decemberében megjelent cikk óta a *Samba 3.x* kiadásai rengeteg fejlesztést hoztak. Az új változatokra áttérve komolyabb ellenőrzést valósíthatunk meg a fiókok felett, valamint továbbfejlesztett csoportmegfeleltetési szolgáltatásokat érhetünk el – mindent összefoglalva magasabb szintű felügyeletet valósíthatunk meg a tartomány felett.

Karbantartás

Mindenkinek javasoljuk, hogy új *LDAP* címtárát az *egyszerű hitelesítés és biztonsági réteg (simple authentication and security layer, SASL)* és a *szállítási rétegbeli biztonság (transport layer security, TLS)* alkalmazásával védje. Erről bővebben az internetes anyagokban lehet olvasni. Gratulálunk! *LDAP* kiszolgálónkat sikeresen üzembe helyeztük, és készen állunk az elektronikus levélcímek megosztására, az egységesített bejelentkezés, valamint a bármely ügyfélről elérhető, szintén egységesített fájltárolási szolgáltatások biztosítására.

Linux Journal 2005. július, 135. szám

Craig Swanson
(craig.swanson@slssolutions.net) hálózatervezéssel és Linux tanácsadással foglalkozik az SLS Solutionsnél. A Midwest Tool & Die cégnél linuxos programok fejlesztésében is részt vesz. Craig 1993 óta használ Linuxot.

Matt Lung
(matt.lung@slssolutions.net) hálózatokkal és számítógéprendszerekkel kapcsolatos tanácsadást végez az SLS Solutionsnél, illetve a Midwest Tool & Die hálózati mérnöke.

KAPCSOLÓDÓ CÍMEK

A cikkhez tartozó források elérhetősége:
➲ www.linuxjournal.com/article/8267