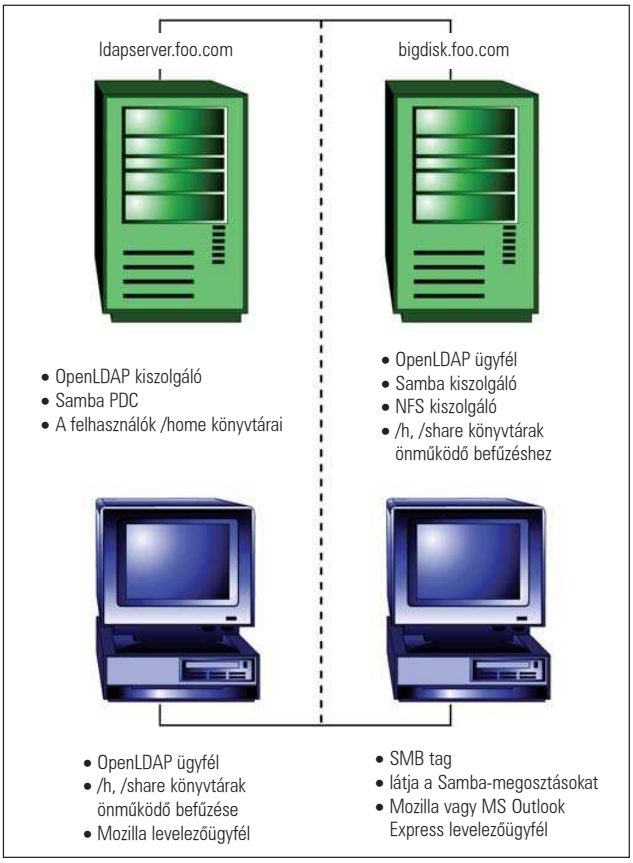
OpenLDAP mindenütt

Elektronikus leveleket tartalmazó könyvtárak megosztása, egységesített beléptetés és kevert környezetű fájlmegosztás – lépésről lépésre.

Írásom célja bemutatni, hogyan lehet az OpenLDAP-ot nem egységes környezetben működő könyvtári alapszolgáltatásként felhasználni. Az LDAP-kiszolgáló adhat osztott levélkönyvtár-szolgáltatást, egységes bejelentkezési lehetőséget a Linux- és Windows-felhasználóknak, elvégezheti a saját könyvtárak önműködő befűzését, illetve a fájlmegosztást linuxos és windowsos ügyfeleken egyaránt.
A Midwest Tool & Die immár három éve használja az OpenLDAP-ot, ami eddig kifogástalan teljesítményt nyújtott.
A könyvtárak esetében százszázalékos rendelkezésreállást tapasztaltunk. A cég vezetése szemében az első nagy előny a levélkapcsolatok könyvtárának megosztási lehetősége volt. Mára minden hálózati számítógépen egységesített beléptetéssel rendelkezünk. Számítógép-felhasználóink ugyanazt a fájltárhelyet érhetik el Windows/Samba, illetve Linux/NFS/önműködő befűzés segítségével. Eredményül végső soron a hálózati források zökkenőmentes elérését kaptuk.
A cikkben bemutatott egyszerű kevert környezet az *1. ábrán* látható. Az itt tárgyalt beállítások nem térnek ki az SSL használatára. Elképzelhető, hogy az általunk használt `ldapsync.pl` program felfedheti az LDAP üzemeltetői jelszót. A Windows-ügyfelek a felhasználói jelszavakat gyorstárazhatják, ezzel újabb linuxos biztonsági kockázatot teremtenek. Figyelmesen és megfontoltan vizsgálják meg biztonsági igényeiket és a leírt beállítást csak a saját felelősségükre használják! Sem a szerzők, sem munkáltatónk nem vállal semmilyen felelősséget az esetleg felmerülő biztonsági gondokért!



1. ábra Kevert OpenLDAP-környezet

Az LDAP-kiszolgáló telepítése és beállítása

Az itt tárgyalt LDAP-kiszolgálót RPM bináris csomagként (`openldap-2.0.11-8`) telepítettük Red Hat 7.1-es rendszeren. E csomagon kívül szükségünk lesz még az `auth_ldap` és az `nss_ldap` csomagokra is. A cikkben feltételezzük, hogy az általunk használt tartomány neve ***foo.com***. Ha a legfrissebb forrást szeretnénk használni, kövessük a
➲ http://www.openldap.org/doc/admin/quickstart.html oldalon olvasható utasításokat, töltsük le és telepítsük az OpenLDAP-ot. Javítsuk át az OpenLDAP-kiszolgáló beállítófájlját (***/etc/openldap/slapd.conf***) a következők szerint:

```
# Schemas to use
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/redhat/
          ➥rfc822-MailMember.schema
include
/etc/openldap/schema/redhat/autofs.schema
include   /etc/openldap/schema/redhat/
          ➥kerberosobject.schema
database        ldbm
suffix          "dc=foo,dc=com"
rootdn          "cn=Manager,  dc=foo,dc=com"
rootpw          {crypt}sadtCr0CILzv2
directory       /var/lib/ldap

index default                                   eq
index objectClass,uid,uidNumber,gidNumber    eq
index   cn,mail,surname,givenname          eq,sub

# Access Control
access to attr=userPassword
   by self          write
   by anonymous     auth
   by dn="cn=manager,dc=foo,dc=com"      write
   by *     compare
access to *
   by self write
   by dn="cn=manager,dc=foo,dc=com"      write
   by * read
```

A bejegyzések csoportosításához használt ou eljárás

ou	bejegyzéstípus
ou=people	személyek
ou=contacts,ou=people	levélkapcsolatok
ou=group	csoportok a Linux-rendszeren
ou=auto.master	az automount /etc/auto.master parancsot helyettesíti
ou=auto.home	az automount /etc/auto.home parancsot helyettesíti
ou=auto.misc	az automount /etc/auto.misc parancsot helyettesíti

Az LDAP-sémák könyvtárbejegyzéseket alkotó objektumosztályokat és jellemzőket határoznak meg. A fenti változtatások elvégzésével az igényeinket leíró sémameghatározások nehezét már el is végeztük. A szükséges sémák, amelyeket a ***slapd.conf*** első része sorol fel, RPM-telepítésünkbe csomagolva már eleve meg vannak adva.
Amennyiben új `objectClass`-t vagy jellemzőt kellene hozzáadnunk a könyvtárhoz, olvassuk el az OpenLDAP felügyeleti útmutatót a ➲ http://www.openldap.org/doc/admin20/schema.html címen. Mi most az alapértelmezett adatbázistípust, az ldbm-et használjuk, példáink pedig az LDAP tartomány-összetevőket használják. Így aztán a ***foo.com***-ból ***dc=foo,dc=com*** válik. Továbbá a felügyelőnek (manager) teljes írási joga lesz az LDAP-bejegyzésekre.
A Red Hat 7.3 kézikönyv javaslata szerint felügyelő jelszavát érdemes a crypttel titkosítani:

```
perl -e "print crypt('jelsz ',
➥'s _karakterek',);"
```

Az előző Perl-sorban a „só_karakterek”-et cseréljük le valamilyen két karakteres sóra (eredetileg a salt: kriptográfiai kifejezés, a jelszavak kódolásakor felhasznált tetszőleges karaktereket jelenti, amelyek a kódolás „véletlenségét” biztosítják – a ford.), a jelszót pedig a jelszó egyszerű karakteres változatával. Az eredményül kapott kódolt jelszót a fentieknek megfelelő módon másoljuk a ***slapd.conf*** fájlba.
Az indexsorok a gyakran lekért jellemzők esetében növelik a teljesítményt. Az ***Access control*** (eléréskorlátozás) az `userPassword` bejegyzés hozzáférhetőségét szabályozza, de a felhasználó és a kezelő ezt a bejegyzést is módosíthatja. Az összes egyéb könyvtár esetében csak a kezelőnek van írási joga, mindenki más csak olvasási joggal rendelkezik.

A könyvtárszerkezet létrehozása

Az LDAP-ot faszerkezetként képzelhetjük el, amelynek a ***foo.com*** a törzse. Az ágakat szervezeti egységekként (`ou`, azaz organizational units) hozhatjuk létre, ahogyan azt a *2. ábrán* bemutatjuk.
A könyvtár minden egyes bejegyzését egyedileg azonosítja a megkülönböztető név (`dn`, vagyis distinguished name). Az LDAP-felügyelő `dn`-je tehát a következőképpen nézne ki: ***dn: cn=manager, dc=foo, dc=com.***
Az `ou` lehetőséget nyújt a bejegyzések csoportosítására, ahogy azt *táblázatunkban* megfigyelhetjük.
Az egyes bejegyzéseket LDIF-ben (LDAP Interchange Format, azaz LDAP csereformátum) készítettük el, majd a ***top.ldif*** fájlba mentettük:

```
dn: dc=foo, dc=com
objectclass: dcObject
objectclass: organization
o: Foo Company
dc: foo

dn: cn=manager, dc=foo, dc=com
objectclass: organizationalRole
cn: manager

dn: ou=people, dc=foo, dc=com
ou: people
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: foo.com

dn: ou=contacts, ou=people, dc=foo, dc=com
ou: contacts
ou: people
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: foo.com

dn: ou=group, dc=foo, dc=com
ou: group
objectclass: organizationalUnit
objectclass: domainRelatedObject
```

Az `ldapadd` segítségével legfelső szintű bejegyzéseinket adjuk a könyvtárhoz:

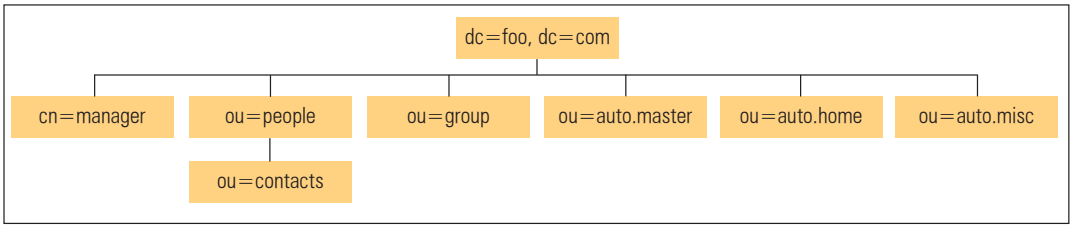
```
ldapadd -x -D 'cn=manager,dc=foo,dc=com'
➥-W -f top.ldif
```

Majd munkánkat az összes bejegyzés lekérésével próbáljuk ki:

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

Levélkapcsolatok megosztása

Immár elegendő LDAP-szerkezetet építettünk fel ahhoz, hogy ténylegesen használatba vehessük őket. Kezdetnek osszuk meg levélkapcsolatainkat, amelyeknek szintén LDIF formátumban kell lenniük.
A folyamat egyszerűsítése érdekében jó, ha címlistánkat LDIF formátumban exportálni tudjuk. Mozilla 1.0 alatt például az



2. ábra A szervezeti egységek mint az LDAP-fa ágai

Addressbook (címlista) ablak *Tools* menüjéből exportálhatunk LDIF formátumban. A Microsoft Outlook Express úgyszintén lehetővé teszi a címlisták ilyen formátumú mentését. Az eredményfájlt majd fel kell dolgoznunk, hogy úgy nézzen ki, mint az alábbi kapcsolatok példánk; e feladat megoldásához a Perlt tudnám ajánlani.
A kapcsolatokat címük egyedileg azonosítja. Íme egy példa kapcsolat dn-je:

```
dn: uid=someone@somewhere.com,ou=contacts,
    ou=people, dc=foo,dc=com
```

Az összes jellemzővel a teljes kapcsolatbejegyzés a következőképpen néz ki:

```
dn: uid=valaki@valahol.hu,ou=contacts,
    ou=people, dc=foo,dc=com
cn: Valaki Akit Ismer nk
mail: valaki@valahol.hu
uid: valaki@valahol.com
givenname: Valaki
sn: AkitIsmer nk
objectclass: person
objectClass: top
objectClass: inetOrgPerson
```

Minden egyes kapcsolatbejegyzést egy üres sorral válasszunk el egymástól, majd a fájlt ***contacts.ldif*** néven mentsük. A kapcsolatokat az `ldapadd`-dal adhatjuk a könyvtárhoz:

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

Ismét ellenőrizzük a műveletet egy `ldapsearch`-csel, ami az összes bejegyzést visszakéri:

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

Levélügyfelek beállítása

Ideje beállítani a Mozillát, hogy az új LDAP-kiszolgálónkat használja (lásd a *3. ábrát*). A Mozilla ***Mail and News*** ablakából válasszuk az ***Edit*** menüpontot, és kattintsunk a ***Mail & Newsgroup Account Setting***-re. Az ***Addressing*** fülön válasszuk az ***Use a different LDAP server***-t, kattintsunk az ***Edit Directories***-re, majd az ***Add***-ra. Töltsük ki a ***Directory Server Properties*** űrlapot:

```
Name: FOO
Server: ldapserver.foo.com
base DN: ou=people,dc=foo,dc=com
```

Ezt követően meg kell mondanunk a Mozillának, hogy a címeket a mi könyvtárunkban keresse. A ***Mail and Newsgroups preferences*** alatt válasszuk az ***Address Autocompletion***-t, a ***Directory Server***-hez pedig írjuk be: `FOO`.
Próbáljuk ki beállításainkat; írjunk levelet egy olyan személynek, aki LDAP könyvtárunkban szerepel. A címnek a gépelés során önműködően ki kell egészülnie. A másik kipróbálási lehetőség, ha LDAP könyvtárunkban a ***Mozilla Mail Address Book***-ból keresni kezdünk. Egy olyan keresésnek, ami a ***Name*** (név) vagy az ***E-mail*** mezőben *-t (csillagot) tartalmaz, az összes kapcsolatbejegyzést vissza kell adnia. A Microsoft Outlook Express alatt az LDAP könyvtár használatát hasonlóképpen be tudjuk állítani.

Egységesített Linux-bejelentkezés LDAP-val

Ha felhasználóink bejelentkezési adatait LDAP alatt tároljuk, ugyanazt a felhasználónevet és jelszót bármely linuxos gépen használhatjuk. Első lépésben el kell döntenünk, hogy milyen felhasználóneveket akarunk bevinni az LDAP-ba. A mi felhasználói UID/GID-sémánk a következő volt:

- Rendszerazonosítók: UID < 500
- Valós emberek LDAP alatt: 499 < UID < 10 000
- Helyi felhasználók, csoportok (akik nincsenek az LDAP-ban) > 10 000

Ez a felhasználói séma 9500 LDAP-felhasználót és csoportbejegyzést engedélyez, ugyanakkor lehetővé teszi, hogy helyi, rendszerenkénti felhasználók és csoportok is létezzenek, amelyek nem kavarodnak össze az LDAP UID/GID-bejegyzésekkel.

Felhasználói bejegyzések készítése a helyi gépen

A helyi számítógép-felhasználók bejegyzéseit az `uid`-ként megadott felhasználói név azonosítja. A helyi gépfelhasználók az ***ou=people*** tagjai lesznek:

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

A teljes bejegyzés az azonosítók elérésvezérléséhez szükséges jellemzőket is tartalmazza:

```
dn: uid=gomerp,ou=people,dc=foo,dc=com
uid: gomerp
cn: Gomer Pyle
givenname: Gomer
sn: Pyle
mail: gomer.pyle@foo.com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: kerberosSecurityObject
objectClass: shadowAccount
userPassword: useradd_ldap_flag
shadowLastChange: 11547
shadowMax: 99999
shadowFlag: 0
krbname: gomerp@FOO.COM
loginShell: /bin/bash
uidNumber: 531
gidNumber: 531
homeDirectory: /h/gomerp
gecos: Gomer Pyle
```

Az átállás megkönnyítése érdekében az OpenLDAP egy átalakítóeszközt tartalmaz, ami képes kikeresni a felhasználói adatokat – olvassuk el a ***/usr/share/openldap/migration***-t.
Először is szerkesszük át a `migrate_common.pe`-t:

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "foo.com";

# Default base
$DEFAULT_BASE = "dc=foo,dc=com";

# turn this on to support more general object
```

```
# classes such as person.
$EXTENDED_SCHEMA = 1;
```

Majd gyűjtsük ki a felhasználói azonosítókhoz tartozó adatokat:

```
/usr/share/openldap/migration/
➥migrate_passwd.pl /etc/passwod >people.ldif
```

Ha ez megvan, ellenőrizzük az eredményül kapott LDIF állományt. A rendszergazdához és a helyi rendszerfelhasználókhoz tartozó azonosítókat érdemes eltávolítani, hiszen ezeknek nem kell megjelenniük az LDAP alatt. Végül a felhasználói bejegyzéseket adjuk az LDAP-hoz:

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

Mint mindig, most is ellenőrizzük munkánkat az összes bejegyzést visszaadó `ldapsearch`-csel:

```
ldapsearch -x -b "dc=foo,dc=com" "(objectclass=*)"
```

Minthogy a számítógép-felhasználók az `ou=people`-höz tartoznak, levelezőprogramunkból egyúttal a címeiket is elérhetjük.

Csoportbejegyzések készítése

Minden egyes olyan csoporthoz, ami több linuxos gép közt oszlik meg, egy-egy csoportbejegyzést kell létrehoznunk. Minden felhasználónak szüksége lesz továbbá a felhasználó saját csoportjához tartozó csoportbejegyzésre is. A csoportbejegyzéseket a `cn` azonosítja, és valamennyi csoport az ***ou=group*** alá tartozik, például:

```
dn: cn=gomerp,ou=group,dc=foo,dc=com
```

A felhasználó saját csoportja a következőképpen néz ki:

```
dn: cn=gomerp,ou=group,dc=foo,dc=com
objectClass: posixGroup
objectClass: top
cn: gomerp
userPassword: {crypt}x
gidNumber: 531*

VØg l  gy fest egy osztott csoport:

dn: cn=web_dev,ou=group,dc=foo,dc=com
objectClass: posixGroup
objectClass: top
cn: web_dev
gidNumber: 502
memberUid: gomerp
memberUid: goober
memberUid: barneyf
```

A csoportbejegyzések létrehozása után gyűjtsük ki a csoportadatokat:

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

Ellenőrizzük az eredményül kapott LDIF állományt, távolítsuk el belőle azokat a rendszercsoportokat és helyi felhasználókat, akiknek nem kell megjelenniük az LDAP-ban. Ezt követően a csoportbejegyzéseket adjuk az LDAP-hoz:

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

Ellenőrizzük munkánkat az összes csoportbejegyzést lekérdező `ldapsearch` kéréssel:

```
ldapsearch -x -b 'dc=foo,cd=com'
```

Automount beállítása a saját könyvtárak megosztásához (és az NFS-megosztásokhoz)

Az egységesített beléptetés keretében felhasználóink egyetlen saját könyvtárral rendelkeznek, amelyet NFS-sel osztunk meg. A dolgokat egyszerűsítendő a saját könyvtárakat az ***ldapserver.foo.com***-on tároljuk, és a ***/home*** könyvtárat NFS-sel osztjuk meg. Az NFS rendszer ismertetése meghaladja e cikk kereteit, de segítségül megadunk egy rendkívül egyszerű de működőképes ***/etc/exports*** sort:

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

A Linux LDAP-ügyfél a bejelentkezés során az `automount` és az NFS segítségével befűzi a felhasználó saját könyvtárát. Az LDAP alatti `automount` a NIS (Network Information Service) `automount` befűzési listákat váltja fel. Az ***auto.master, auto.home*** és ***auto.misc*** `automount` listákat fogjuk helyettesíteni. Az ***auto.master***-hez egy új szervezeti egységet is létrehozunk:

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

Az ***auto.master*** bejegyzést a `cn` határozza meg. Az `automountInformation` kapcsoló utasítja az ***automount***-ot, hogy a listát az LDAP-ból vegye:

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

Ha már itt vagyunk, készítsünk egy ***auto.master*** bejegyzést mindjárt a másik NFS osztott könyvtárhoz is:

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

Az ***automount*** bejegyzéseket LDIF formátumban hoztuk létre, azután ***auto.master.ldif*** néven mentjük:

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

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

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

Az ***auto.master*** bejegyzéseket adjuk az LDAP-hoz:

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

Következő lépésben új szervezeti egységet készítünk az ***auto.home*** számára: ***ou=auto.home*** A saját könyvtárat a `cn` adja meg:

```
dn: cn=gomerp,ou=auto.home,dc=foo,dc=com
```

Készítsünk LDIF formátumú ***auto.home*** bejegyzéseket minden egyes felhasználóhoz, és ***auto.home.ldif*** néven mentsük őket:

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

dn: cn=gomerp,ou=auto.home,dc=foo,dc=com
objectClass: automount
automountInformation:
    ldapserver.foo.com:/home/gomerp
cn: super3
```

Az ***auto.home*** bejegyzéseket adjuk az LDAP-hoz:

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

Amikor a Linux LDAP-ügyfél önműködően befűzi a saját könyvtárunkat (***ldapserver.foo.com:/home/gomerp***), a ***/h/gomerp*** alá fog kerülni. Más NFS-megosztásokat is beírhatunk az LDAP-ba, amelyek aztán szükség szerint önműködően befűződnek. Ezeket az `automount` térképeket az ***ou=auto.misc*** formátumú ***auto.misc*** szervezeti egység tárolja.
A korábbiakban már elkészítettük a ***/share***-hez tartozó ***auto.master***-bejegyzést. Most az NFS-megosztásokhoz készítsük bejegyzéseket az ***auto.misc*** alatt, és ***auto.misc.ldif*** néven mentsük őket:

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

dn: cn=redhat,ou=auto.misc,dc=foo,dc=com
objectClass: automount
automountInformation:
    bigdisk.foo.com:/pub/redhat
cn: redhat

dn: cn=engineering,ou=auto.misc,dc=foo,dc=com
objectClass: automount
automountInformation:
    bigdisk.foo.com:/data/engineering
cn: engineering
```

Az ***auto.misc*** bejegyzéseket adjuk az LDAP-hoz:

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

Amikor a Linux LDAP-ügyfél osztott könyvtárunkat önműködően befűzi, a ***bigdisk.foo.com:/data/engineering*** a ***/share/engineering*** alá kerül.

Az LDAP-ügyfél beállítása a linuxos gépeken

Először is fel kell telepítenünk az `auth_ldap` azonosításkezelő csomagot, és az `nss_ldap` névváltás-szolgáltatás csomagot. A Red Hat `/usr/bin/authconfig` eszköze nagyon hasznos lehet az ügyfél beállítása során. Válasszuk ki a ***Use LDAP→Server: ldapserver.foo.com, base DN: dc=foo,dc=com*** bejegyzést. Az `authconfig` ezekbe a fájlokba fog írni: ***/etc/ldap.conf***, ***/etc/openldap/ldap.conf*** és ***/etc/nsswitch.conf***.

Ellenőrizzük, hogy a ***/etc/nsswitch.conf*** az alábbiakban látható bejegyzésekhez hasonlókat tartalmaz-e:

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

Nézzük meg, hogy a ***/etc/ldap.conf***-ban ilyen bejegyzéseket látunk-e:

```
host ldapserver.foo.com
base dc=foo,dc=com
```

illetve szerepel-e a ***/etc/openldap/ldap.conf***-ban az alábbiakhoz hasonlót

```
HOST ldapserver.foo.com
BASE dc=foo,dc=com
```

A Linux-kiszolgáló végső beállításai

Az LDAP-kiszolgáló egyben LDAP-ügyfél. Az LDAP-kiszolgálón ki kellene kapcsolnunk a ***/home*** önműködő befűzését ***/h***-ként. Az `nsswitch`-et úgy állítottuk be, hogy először a fájlokat ellenőrizze, és az önműködő befűzés adataiért csak ezután forduljon az LDAP-hoz. Ezért az ***ldapserver.foo.com:/etc/auto.master*** alatt egy álbejegyzést hozunk létre:

```
/h /etc/auto.null
```

A sajátkönyvtár-kiszolgálón a felhasználók jelszó- és csoportbejegyzéseit el kell távolítani a ***passwd*** és ***group*** fájlokból. Készítsünk mentéseket, majd szerkesszük át a ***/etc/passwd***, ***/etc/shadow***, ***/etc/group*** és ***/etc/gshadow*** fájlokat, eltávolítva az LDAP valós embereihez tartozó bejegyzéseket. Próbaképpen jelentkezzünk be a Linux LDAP-ügyfélre egy LDAP felhasználónévvel. A megfelelő felhasználóhoz tartozó bejelentkezési héjprogramot és a saját könyvtárat kell látnunk. Az ***auto.misc***-megosztások kipróbálásához a megosztást név

szerint kell elérnünk:

```
cd /share/redhat
```

Az `automount` az NFS-megosztásokat csak akkor fűzi be, amikor valaki használni akarja őket, így a */share/redhat* mindaddig nem látható, ameddig senki sem akarja elérni.

Egységesített Microsoft Windows-beléptetés Samba és LDAP segítségével

Ha egységes beléptetést szeretnénk Windowshoz és Linuxhoz, először is állítsuk be a Samba Primary Domain Controllert (PDC). A felhasználók saját könyvtárait SMB-ügyfeleken keresztül osztjuk meg. A Samba beállításainak részletei sajnos már túlmutatnak e cikk keretein.

Az ldapsync.pl és a Samba beállítása

A felhasználói jelszavakat MS Windows alól is meg lehet változtatni a Samba és a `ldapsync.pl` Perl-program segítségével, amelyet a ➲ http://www.mami.net/univr/tng-ldap/howto/#how_to_change_password címen érhetünk el.
Az `ldapsync.pl` parancsfájl a `/bin/passwd` program helyettesítésére használható, amelyet a Samba hív meg, amikor a felhasználók jelszavát megváltoztatjuk, és összehangolja őket a Samba-jelszavakkal. Az `ldapsync.pl` parancsfájlt a Samba hívja meg, amikor a felhasználó Windowsból változtatja meg a jelszavát, és ugyanúgy rendszergazdai jogosultság alatt fut, akárcsak a `/bin/passwd`, amelyet a módosítatlan Samba használ. Az LDAP által kezelt felhasználókhoz szükség lesz az `ldapsync.pl` parancsfájlra. Minthogy a felhasználók jelszavait az LDAP-ban tároljuk, és nem helyileg a */etc/passwd* fájlban, az LDAP könyvtárat és módosítókat az `ldapsync.pl` parancsfájl fogja összekapcsolni a felhasználó LDAP-beli jelszó bejegyzésével.
Könnyebben áttekinthető formában a folyamat így áll össze:

1. A felhasználó Windows alól meghívja a jelszóváltoztató programot.
2. A felhasználó rákattint a jelszóváltoztatás elfogadására, és adatot küld a Samba-kiszolgálónak.
3. A Samba megnézi a beállításfájlját, és tudja, hogy az `ldapsync.pl`-t kell az LDAP-jelszavak megváltoztatásához meghívnia.
4. Az `ldapsync.pl` a `-o %u` kapcsolóval hívódik meg, ami azt eredményezi, hogy a program nem kérdez rá a régi jelszóra. Futás közben a felhasználó nevét átadja a parancsfájlnak (ez fontos, ha a rendszergazdai jelszót nem akarjuk anélkül megváltoztatni, hogy tudnánk róla).
5. A Samba az új jelszót átadja az `ldapsync.pl`-nek, anélkül, hogy a régivel bármit is törődne.
6. Az `ldapsync.pl` beszélgetni kezd a Sambával, az új jelszót tartalmazó helyes választ várva.
7. Ha az üzenetváltás sikeres volt, a jelszót az `ldapsync.pl` kódolja.
8. Az `ldapsync.pl` ezután a felhasználó helyes dn-jéhez köti az LDAP-ot, és a felhasználó LDAP-bejegyzésén végrehajt egy ***ldapmodify***-t, lecserélve az LDAP-ban tárolt ***userPassword*** mezőt.
9. Az LDAP és a Samba még utoljára üzenetet vált, meghallgatva az LDAP sikerességének jelentését, ahol is a folyamat a végéhez ér.

A Samba ilyen beállításához a következő ***Smb.conf*** bejegyzésekre lesz szükségünk:

```
passwd program = /etc/samba/ldapsync.pl -o %u
passwd chat = *New*password*
➥%n\n*Retype*new*password* %n\n *modifying*
```

Amikor a felhasználó Windows alatt megváltoztatja a jelszavát, először meg kell adnia a régi jelszót, majd az újat, végül ellenőrzésképpen újfent be kell gépelnie az új jelszót. Mivel az `ldapsync.pl` meghívásakor nem törődtünk a régi jelszóval, csak a két új bejegyzést vizsgáljuk meg. Itt a * (csillag) arra utasítja, hogy bármit megtaláljon, amit a pontos meghatározás követ. Tehát a `*New*password*%n\n` jelentése: minden, amit a `New` szó követ, ami után bármi állhat, ezt a `password` szó követi, azután ismét akármi, végül a felhasználó által begépelt új jelszó (`%n`). A `modifying` azt jelenti, hogyha az LDAP ezt adja vissza, akkor módosította a bejegyzést, azaz a folyamat sikeres volt.
Az `ldapsync.pl`-t is át kell szerkesztenünk, hogy az LDAP kapcsolási adatokat bevihessük:

```
$binddn = "cn=manager,dc=foo,dc=com";
$passwd = "passwd";
```

Végül az `ldapsync.pl` elérését kizárólag a rendszergazdára korlátozzuk (0700).

NFS-megosztások Sambán keresztüli megosztása

Az NFS-megosztásokat is megoszthatjuk a windowsos ügyfelekkel, ha az NFS-gazdagépen Samba kiszolgálót futtatunk. A Samba-kiszolgálónak fel kell csatlakoznia a ***FOO SMB*** tartományra. Az SMB-tartományhoz való csatlakozáshoz a következő parancsot futtassuk rajta:

```
smbbpasswd -j [FOO] -r [PDC]
```

Karbantartás

Gratulálunk! Az LDAP-kiszolgáló immár működőképes az osztott levélkapcsolatokkal, egységes beléptetéssel és osztott fájltárolással rendelkezik, amelyet bármelyik ügyfélről elérhetünk. Esetleg írhatunk néhány karbantartói parancsfájlt, ami megkönnyíti a felhasználók és csoportok azonosítóinak kezelését. E feladatra ismét csak a Perlt ajánljuk.

Köszönetnyilvánítás

Az `ldapsync.pl`-t eredetileg ***Jody Haynes*** készítette a Samba-Tng-hez.

A Kapcsolódó címek a 43. CD Magazin/openLDAP könyvtárában találhatók.

Linux Journal 2002. december, 104. szám

Craig Swanson (craig.swanson@midwest-tool.com)
A Midwest Tool & Die résztulajdonosa, 1993 óta használ Linuxot. Saját kezűleg tervezte a cég hálózatát, és a programfejlesztés, illetve a termelési mérnökség (manufacturing engineering) felett atyáskodik.

Matt Lung (matt.lung@midwest-tool.com)
Hálózati mérnökként dolgozik a Midwest Tool & Die-nál. Májusban szerzett diplomát a Purdue Egyetemen. Ő állította be a cég virtuális belső hálózatát. Szeret robotokat építeni.