Központosított hitelesítés és vállalati címtár megvalósítása (2. rész)

Ti Leggett folytatja sorozatát a biztonságos testületi címtár építéséről.

Múlt hónapban átvereked-tük magunkat az egyszeri bejelentkezés és a testületi címtár infrastruktúra elindításán. Ebben a cikkben eddigi kemény munkánk eredményét használjuk fel a *Linux* és *Mac OS X* kliensgépek csatlakoztatásához, ezek megfelelő konfigurálásával. Bár ez alkalommal nem lesz annyi megvizsgálandó részlet, mint a múltkor, de most is sok mindenről szót kell ejtenünk, úgyhogy álljunk is neki! A konfigurációs fájlokat ez alkalommal is megtalálják a cikkhez tartozó források között.

Ebben a részben arról lesz szó, hogy hogyan lehet csatlakoztatni a *Gentoo Linuxot* és a *Red Hat Enterprise Linux (RHEL) 3.* és *4.* kiadását; értelemszerűen a legtöbb más *Linux* terjesztést is többékevésbé hasonlóan kell konfigurálni. Szót ejtünk a *Mac OS X 10.4*-es *„Tigris"* (*Tiger*) kiadásának kliensgépként történő integrálásáról is. A következő rész számol be majd arról, hogy miként lehet rávenni a *Microsoft Windows* kliensgépeket az általunk elkészített hitelesítési és engedélyezési rendszer használatára; ez lényegében a *Samba* csomag konfigurálását és beállítását jelenti.

Az egyszeri bejelentkezés lehetővé tételéhez a *Linux* és a *Tigris* kliensgépek számára meg kell adnunk a kulcsokat tartalmazó *Kerberos keytab* fájlt. Ez ugyanúgy történik, mint ahogy az eddigi *keytab* fájlok esetén. Mind a *Linux*, mind a *Tigris* kliensgépek számára a */etc/krb5.keytab* fájlban adhatjuk meg a kulcstáblázatot.

Linux kliensek beállítása

Nem minden felhasználó szeretné/tudja megoldani, hogy a gépe teljes mértékben beépüljön a *Kerberos* tartományba (*realm*), különösen a hordozható gépeknél. Ha nincs teljes körű jogosultságunk az összes gép fölött, melyekről a felhasználók csatlakozni akarnak, kénytelenek vagyunk megengedni a hagyományos jelszavas hitelesítést is. Bár a jelszavak hálózaton át történő küldözgetése a *Kerberos* több biztonsági célkitűzését meghiúsítja, mindaddig, amíg rendszergazdaként ennek tudatában vagyunk, és csak megfelelő korlátok között tesszük lehetővé a használatát, nem követünk el nagyobb hibát, mintha nem is használnánk a *Kerberost*. A *Kerberosnak* még mindig számos előnye van olyan eljárásokkal szemben, melyek például a */etc/password*-re, *NIS*-re vagy a jelszavak *LDAP* tárolására épülnek. Jóval egyszerűbben lehet kikényszeríteni bizonyos jelszószabályokat a *Kerberos*-szal, mint más módszerekkel, és a jelszavak tárolása is biztonságosabb egy *Kerberos* adatbázisban.

Érdemes elolvasni a *Linuxvilágból* Alf *Wachsmann: „Központosított hitelesítés Kerberos 5-tel"* című cikksorozatának első részét, főleg azt a bekezdést, mely a kerberos *PAM* hitelesítés lehetővé tételéről szól. ➲ *linuxvilag.hu/node/3002370*

Craig Swanson és *Matt Lung* az *„OpenLDAP mindenütt"* című cikkben érintik a */etc/nsswitch.conf*, a */etc/ldap.conf* és a */etc/openldap/ldap.conf* beállítását ➲ *linuxvilag.hu/node/3001551*. Ezeket a fájlokat mi is fogjuk fésülgetni, hogy a sebesség és biztonság tekintetében még kifinomultabb hatást érjünk el. Először is nézzük a */etc/openldap/ldap.conf*-ot. Ez a fájl határozza meg az *OpenLDAP* parancssori eszközeinek (mint az *ldapdadd* és az *ldapsearch*) alapértelmezett beállításait. A mi */etc/openldap/ldap.conf* fájlunkat az *1. Lista* mutatja. További információk és opciók az *ldap.conf(5)* kézikönyv (*man*) oldalakon találhatóak. Mivel nincs mód arra, hogy a */etc/openldap/ldap.conf*-ban megadjuk, hogy a *StartTLS*-t szeretnénk használni, kifejezetten meg kell adnunk egy *ldaps://URL*-t. Ezek után adjunk ki egy egyszerű `ldapsearch` parancsot, amely alapértelmezetten *SASL* hitelesítést használ, és így a */etc/openldap/ldap.conf*-ban kell keresnie az alapértelmezett gazdagépet és hálózati faszerkezet gyökerét (*base*). Most állítsuk munkába a névkiszolgáló kapcsolót (*Name Service Switch, NSS*). Természetesen ehhez az *nss_ldap* csomagot telepíteni kell, mégpedig lehetőleg a legújabb verzióját, mert a régebbiek nem kezelik bizonyos szolgáltatásoknak, pl. a hálózati csoportoknak (*netgroups*) az *LDAP* alapú tárolását. Először is magát az *nss_ldap* csomagot kell beállítanunk a */etc/ldap.conf* szerkesztésével. Ez nem ugyanaz, mint a */etc/openldap/ldap.conf* – ez utóbbi ugyanis csak az *OpenLDAP* eszközök számára érvényes, míg az előbbi kifejezetten az

1. Lista /etc/openldap/ldap.conf

```
BASE "o=ci,dc=example,dc=com"
URI ldaps://ldap.example.com
➥ldaps://kdc.example.com
TLS_CACERTDIR /etc/ssl/certs
TLS_REQCERT allow
```

2. Lista /etc/ldap.conf

```
host ldap.example.com
➥kdc.example.com
base o=ci,dc=example,dc=com
ssl start_tls
tls_checkpeer no
tls_cacertfile /etc/ssl/
➥certs/ci-cert.pem
nss_base_passwd ou=people,
➥o=ci,dc=example,dc=com
nss_base_group ou=group,
➥o=ci,dc=example,dc=com
nss_base_hosts ou=hosts,
➥o=ci,dc=example,dc=com
nss_base_services
➥ou=services,o=ci,
➥dc=example,dc=com
nss_base_netgroup
➥ou=netgroups,o=ci,
➥dc=example,dc=com
```

nss_ldap konfigurációs fájlja. A *2. Listában* láthatjuk, hogy hogyan kell a ***/etc/ldap.conf***-nak kinéznie. Érdemes alaposabban megvizsgálnunk, hogy mit állítanak be ezek a sorok; annál is inkább, mert erre a fájlra vonatkozóan nincs kézikönyv oldal (***bár jó magyar nyelvű segítség található itt: ➲ http://panther.inf.elte.hu/linux/postfix-ldap-kerberos.html – a ford.***). Az első sor adja meg az LDAP gazdagépeket, amikhez kapcsolódni lehet, a második pedig a hálózati faszerkezet gyökerét, ahonnan a keresés indul (***base***). A következő három sor a ***TLS*** kapcsolat létrehozásáról szól. Mint látható, az ***nss_ldap*** ismeri a ***StartTLS***-t, így használhatjuk ezt a módszert a ***TLS*** kapcsolat felhúzására. Az utolsó sorok a kereséskezdő gyökereket írják le a különböző ***nss*** által vezérelt attribútumok számára. Ezeket a teljesítmény-optimalizáció miatt kell beállítanunk. Ha egy felhasználónevet keresünk, amely a faszerkezet egy adott ágában található, akkor nincs értelme a teljes címtárat bejárnunk. Például az `nss_base_passwd` adja meg azon információk keresési kezdőpontját, amelyek egy klasszikus rendszerben a ***/etc/passwd***-ben voltak eltárolva. De ha úri kedvünk úgy diktálja, lehet akár több ágban is tárolni felhasználóneveket, csak akkor ezt az opciót nem lehet használni. Egy sereg egyéb opció is megadható ebben a fájlban; ezek megtalálhatóak az ***nss_ldap*** csomaghoz tartozó ***ldap.conf*** példafájlban. Győződjünk meg arról, hogy megvan-e a CA tanúsítvány a ***/etc/ssl/certs***-ben, és futtassuk le a ***c_rehash***-t. Ugyanezt a műveletsort kell elvégezni ***mindazokon*** a gépeken, amelyek SSL kapcsolaton keresztül fordulnak az LDAP kiszolgálóhoz valamilyen információért. Most a ***/etc/nsswitch.conf*** fájl szerkesztése következik – itt adható meg az ***LDAP*** számára, hogy hol keresse az információkat. Ne tegyük az elejére az ***LDAP***-t, mert így nem leszünk képesek feloldani az ***LDAP***-kiszolgáló nevét. Ha van olyan felhasználó, akit a helyi gépen a ***/etc/passwd*** vagy ***/etc/shadow*** fájlhoz adtunk, hogy az ***LDAP***-től függetlenül hitelesítse magát, töröljük vagy tegyük megjegyzésbe. Ezután már ki lehet próbálni, működik-e minden:

```
# getent passwd leggett
leggett:x:1001:100:Ti Leggett:/
➥home/leggett:/bin/bash
# id leggett
uid=1001(leggett)
➥gid=100(users)
```

Ha mindkét parancs működik, továbbléphetünk. Néhány program újraindítást igényel a ***/etc/nsswitch.conf***-ban történt változások érzékeléséhez; például az ***OpenSSH*** is ilyen. Indítsuk tehát újra az ***sshd***-t, és kíséreljük meg az ***slogin*** futtatását.
Eddigi tevékenységünk eredményeként már lehetséges a kapcsolódás ***Gentoo*** és ***RHEL*** kliensgépekről, de nézzük még át, miket kell ezeken a gépeken helyileg beállítani.
A ***Kerberos*** hitelesítéshez szükséges fájlok:

- ***/etc/krb5.conf***
- ***/etc/krb5.keytab***
- ***/etc/pam.d/system-auth***

Az ***OpenLDAP*** rendszerű felhasználókezelést az alábbi fájlok teszik lehetővé:

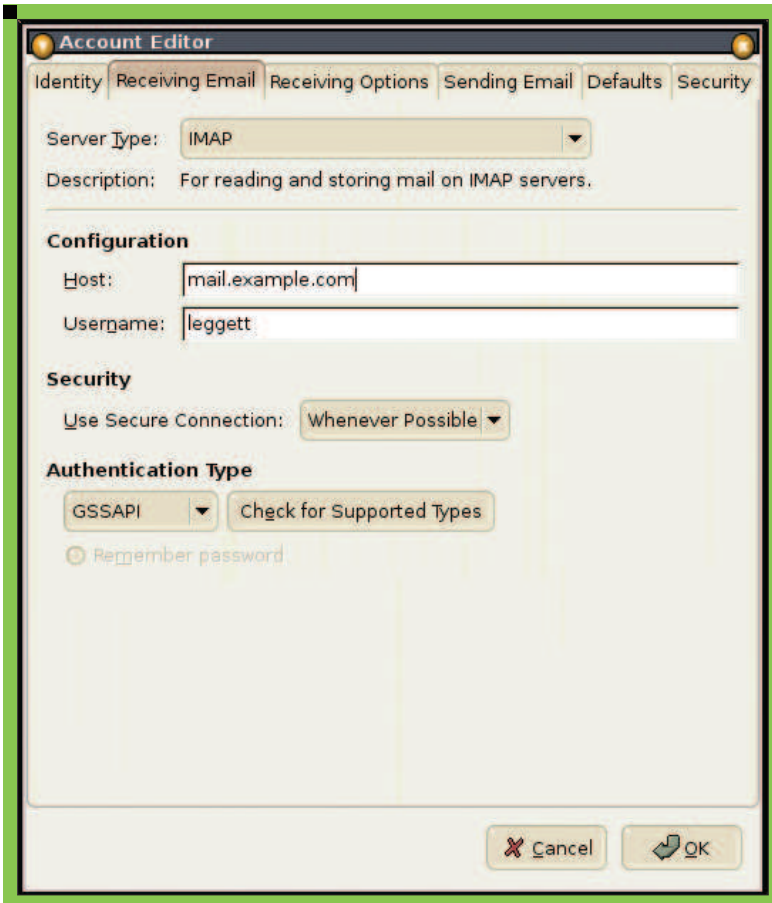
- ***/etc/openldap/ldap.conf***
- ***/etc/ldap.conf***
- ***/etc/nsswitch.conf***
- ***/etc/ssl/certs/ci-cert.pem (Gentoo)***
- ***/usr/share/ssl/certs/ci-cert.pem (RHEL)***

E sorok írásakor az ***RHEL 4*** használatára vonatkozóan van egy megszorítás. Ha a ***/etc/ldap.conf***-ban gépneveket használunk ***IP***-címek helyett, hiba lép fel. Emiatt az a javaslatom, hogy használjuk az ***LDAP***-ot a ***/etc/nsswitch.conf***-beli gépnevek felkutatására, és használjunk ***DHCP***-t a kliensgépek ***IP***-címeinek felderítésére. Ha azt tapasztaljuk, hogy a hálózat lábra állítása laphibát (***segfault***) okoz a ***dhclient***-ben, változtassuk meg a gépneveket ***IP***-címekre a ***/etc/ldap.conf***-ban.
A ***Gentoo*** és az ***RHEL 4*** alatt pillanatok alatt rávehető az ***sshd*** az egyszeri bejelentkezés használatára. Mindössze ennyit kell beállítani a ***/etc/ssh/sshd_config*** fájlban:

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
UsePAM yes
```

Ezen sorok beírása után újraindítható az ***sshd***.
Sajnos az ***RHEL 3***-ban található ***sshd*** egy régi ***GSSAPI (GSS: General Security Service, Általános Biztonsági Szolgáltatás)*** mechanizmust támogat, amely érzékeny a beékelődéses (***man-in-the-middle*** típusú) támadásra. Ezt a ***gssapi*** programot később lecserélték a ***gssapi-with-mic*** nevűre – ezt használja már az ***RHEL 4*** és a ***Gentoo*** is. Úgy győződhetünk meg arról, hogy az aktuális ***sshd***-nk melyik mechanizmust támogatja, hogy tegyük lehetővé a ***GSSAPI*** hitelesítést az ***sshd_config*** fájlban, majd próbáljunk meg SSH-kapcsolatot létrehozni a `-v` (***verbose,*** bőbeszédű) kapcsolóval. Ekkor részletes jelentést kapunk arról, hogy milyen kapcsolódási mechanizmusokat támogat az adott ***sshd***. Ha a kliens és a szerver egymástól eltérő mechanizmust támogat, akkor jelszót fog kérni a program. Ilyenkor ugyanis az igazolványok átküldése kissé eltérően és egymás mechanizmusaival összeegyeztethetetlenül történik.
Célunk, hogy a felhasználóknak csak naponta egyszer kelljen beírniuk a jelszavukat, és hogy ez a jelszó ne közlekedjen a hálózat kábelein. Miért verekednénk át magunkat megannyi problémán, ha a felhasználóink minden e-mail ellenőrzéskor elküldenék a hálózaton a jelszavukat? Szerencsére egyre több e-mail kliensprogram

támogatja a *GSSAPI* mechanizmust. A *Mozilla Thunderbird* használóknak nincs szerencséjük (e sorok írásakor), azonban van néhány más alternatíva, például a *KDE KMail 1.8*-as változata vagy az *Ximian Evolution 2.2*-es verziója is rendelkezik *GSSAPI* támogatással. (*Ma már a Thunderbird is – a ford.*) Sosem használtam *KMailt*, így inkább arra szorítkozom, amit ismerek. Az *Evolutiont* nem nehéz rávenni a *GSSAPI* használatára. Csak ki kell választani a *GSSAPI*-t, mint hitelesítési módot, mind a *„levelek küldése”*, mind a *„levelek fogadása”* fülön (*1. ábra*). Ha a *„biztonságos kapcsolat használata”* (*„Use Secure Connection”*) opciót az *„amikor csak lehetséges”* (*„Whenever Possible”*) állapotba kapcsoljuk, akkor az *Evolution* a *StartTLS*-t használja a biztonságos adatátvitelhez.



1. ábra Evolution 2.2 – Postafiók beállítások

Mac OS X kliensgépek

A *Tigrissel* kezdődően az *Apple* az operációs rendszer szinte minden összetevőjét kerberizálta. Ha *Panther 10.3*-at futtató kliensgép hálózatba kapcsolására lenne szükség, keressen fel e-mailben; jó adag tudnivalóra lesz szükség. A *Tigris* beillesztése azonban viszonylag egyszerű. Kezdjük a */Library/Preferences/edu.mit.Kerberos* fájl szerkesztésével. Ez meglehetősen hasonlít linuxos megfelelőjéhez, a */etc/krb5.conf*-hoz, néhány egészen apró különbségtől eltekintve, ami a *3. Listában* látható.

Ha már be van állítva a *Kerberos*, akkor a *következő* lépés az, hogy gépünk számára előállítjuk a megfelelő kulcsokat tartalmazó */etc/krb5.keytab* fájlt. Futtathatjuk a *kadmin*-t az *OS X* kliensgépen, de a *10.4*-es változattal érkező program apró hibái miatt érdemes odaírni a `-o` kapcsolót:

```
#/usr/sbin/kadmin -p <admin
#princ> -o
```

Ezzel készen is vagyunk a *Kerberos alapú* hitelesítéssel Tigris gépeken. E cikk írásakor sajnos van egy olyan hiba, amely a gép hitelesítő rendszerének leállásához vezet. Ez abban az esetben lép fel, amikor egy hálózati felhasználó akkor próbál *sudo*-val futtatni egy parancsot, amikor már érvényes *Kerberos* igazolvánnyal rendelkezik. Az *Apple*-lel együttműködve keressük ennek a megoldását, így azt javaslom, hogy amennyiben ez a hiba megmarad, vegyék fel velem a kapcsolatot.

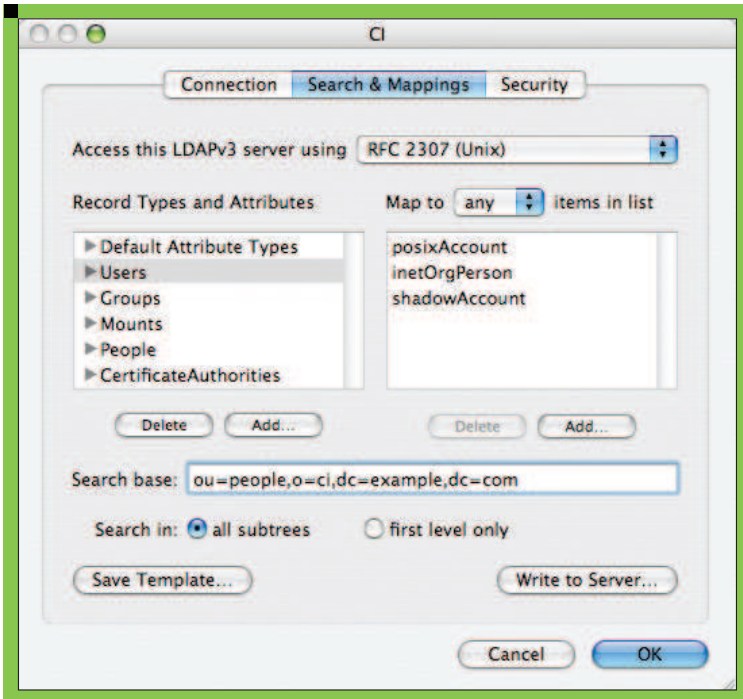
A *Mac OS X* nem használ *nsswitch*-et a névszolgáltatáshoz. Ehelyett egy *„Címtár Szolgáltatás”*-nak (*Directory Services*) nevezett rendszert használ e célra. Elmagyarázom, hogy hogyan kell beállítani a címtár szolgáltatásokat egy grafikus felületű eszközzel, melynek neve: *„Belépés a címtárba”* (*„Directory Access”*). Jó tudni azonban, hogy ez az eszköz végül is csak ezt a két fájlt módosítja: a */Library/Preferences/DirectoryService/DSLDAPv3PlugInConfig.plist*-et és a */Library/Preferences/DirectoryService/SearchNodeConfig.plist*-et.

A grafikus felület az *Alkalmazások/Eszközök* alatt található (*Applications/Utilities*). Először is kapcsoljuk be az *LDAPv3* beépülőt, majd válasszuk ki és kattintsunk a *„Beállít”* gombra

3. Lista /Library/Preferences/edu.mit.Kerberos

```
[libdefaults]
 ticket_lifetime = 600
 default_realm =
 ➥CI.EXAMPLE.COM
 default_tkt_enctypes = des3-
 ➥hmac-sha1 des-cbc-crc
 default_tgs_enctypes = des3-
 ➥hmac-sha1 des-cbc-crc
 dnsfallback = no
[realms]
 CI.EXAMPLE.COM = {
  kdc = kdc.example.com:88
  kdc = ldap.example.com:88
  admin_server =
  ➥kdc.example.com:749
 }
[domain_realm]
 .example.com =
 ➥CI.EXAMPLE.COM
 example.com = CI.EXAMPLE.COM
```

2. ábra Új „LDAP Címtárhoz kapcsolódás" megadása OS X alatt



3. ábra LDAP keresés finomítása OS X alatt

(*Configure*). Ha bent vagyunk, kattintsunk az *„Opciók"* legördülő menüre (*„Show Options"*), majd az *„Új"*-ra (*„New"*), hogy megadhassunk egy új *LDAP* kiszolgálót. Írjuk be az *LDAP* szerver nevét, és mindhárom jelölőnégyzetet jelöljük be (2. *ábra*), majd a *„Folytat" („Continue")* gomb következik. Ezek után válasszuk az *RFC 2307 (Unix)* sablont, írjuk be az *LDAP* gyökereket, *„Folytat"* gomb, végül adjuk meg a konfiguráció nevét (*„Configuration Name"*). Készen is vagyunk!
Részletesen megadható, hogy a *Címtár Szolgáltatások* keresőfunkciója mely könyvtárakban pásztázzon, csak úgy, mint Linux alatt a */etc/ldap.conf*-ban. Ha kiválasztunk egy megfelelő címtár szolgáltatást és rákattintunk a *„Szerkeszt" („Edit")* gombra, megjelennek a kifinomultabb opciók. Kattintsunk a *„Keresés és megfeleltetés" („Search & Mappings")* fülre. Itt látható egy *„Bejegyzéstípusok és tulajdonságok" („Record Types and Attributes")* fejléccel ellátott lista. Bármelyik sor kiválasztásával megadható egy részletesebben megfogalmazott kereséskezdő gyökér (3. *ábra*). Két kattintás az *OK*-ra, majd az *„Alkalmaz"*-ra (*„Apply"*) – és már életbe is léptek és mentésre kerültek a friss beállítások. Természetesen ilyenkor szeretnénk ellenőrizni, hogy a címtárban végbevitt változtatások helyesen működnek-e. Az *OS X*-ben van egy parancssori eszköz, a ***dscl***, amely többféle címtárban való keresésre szolgál: az *LDAP*-on kívül lehet vele *NetInfoban*, *NIS*-ben is keresni, és az összes olyan helyen, amit a *„Belépés a címtárba" („Directory Access")* megjelenít.
Először arról győződjünk meg, hogy tudunk-e az *LDAP* kiszolgálón közvetlenül keresni:

```
# dscl localhost list \
 /LDAPv3/ldap.example.com/Users
```

Ha a `dscl`-t kapcsolók nélkül futtatjuk, kapunk egy használati útmutatót és egy parancssort. Álljon itt még két példa a `dscl` használatára:

```
# dscl localhost list
# /Search/Users
# dscl localhost read
# /Search/Users/leggett
```

Itt a */Search*-et (*keresés*) használjuk, amely minden bekapcsolt címtáron keres. Vagyis, ha van helyi felhasználó a *NetInfo* címtárban, valamint *LDAP* felhasználóink is vannak, a */Search* mindkét címtárban fog keresni, és az egyesített listát fogja megjeleníteni.
A második példában az olvasási műveletet (*read*) használjuk; ez mutatja meg az adott ág (konkrétan a */Search/Users/leggett*) végpontjaihoz tartozó részletes információkat.
A `dscl` igen hasznos, ha csak konzol elérésünk van egy *OS X*-et futtató géphez.
Miután ellenőriztük, hogy az *LDAP* felhasználóink elérhetőek, meg kell gyártanunk a helyi home könyvtárakat a frissen készült *LDAP* felhasználók számára:

```
# install -d -o leggett
# /Users/leggett
# ln -sf /Users /home
```

Az *OS X 10.4*-es verziójának finomabb házirend-beállítási lehetőségei vannak, mint amit a standard *POSIX* nyújt az operációs rendszer bizonyos összetevőinek elérését illetően. Alapértelmezésben az *admin* csoport tagjainak van adminisztrátori jogosultsága. Ez a csoport azonban helyileg van eltárolva az egyes gépek *NetInfo* címtárában. Állítólag igen nagy meggondolatlanság lenne törölni vagy átnevezni ezt a csoportot. Sajnos még csak felül

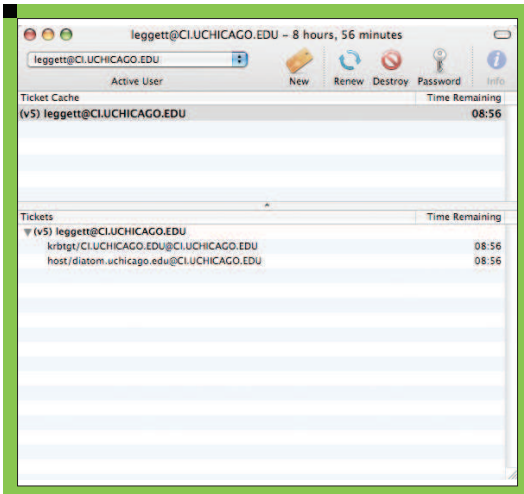
sem bírálható egy másik, hasonló nevű *LDAP* csoporttal, mert a keresési sorrendben elsőbbsége van a helyi *NetInfo* címtárnak.
A */etc/authorization* fájl szerkesztésével azonban megoldható, hogy valamely helyi csoport szerepét egy *LDAP* csoport vegye át. Ez egy egyszerű *Apple plist*-formázott fájl (*plist: Property List*, tulajdonságlistát leíró fájlformátum). Ezzel a rendszer különböző összetevőihez adhatunk meg szerepeket. Ha a különböző jogosultságok megadásánál megváltoztatjuk a sorokat erről:

```
<key>group</key>
<string>admin</string>
```

erre:

```
<key>group</key>
<string>ldap-admins</string>
```

akkor ezáltal az *ldap-admins* csoport tagjainak adjuk át az adminisztrátori jogosultságot az adott a gépen.
Ez eltér a */etc/sudoers*-ben megadott *sudo* jogosultságtól; a programok telepítésére és rendszerbeállítások módosítására vonatkozik.
Ezen a ponton be kell tudnunk lépni *legett* felhasználóként. A Tigris *sshd*-je minden *GSSAPI* mechanizmust támogat, a *gssapi*t és a *gssapi-with-mic*-et is. A korábbi *OS X* változatok csak a *gssapi*t támogatták, így csak jelszóval lehetett bejelentkezni *OS X* kliensre (vagy onnan máshova). Az egyszeri bejelentkezés támogatása az *sshd*-től teljesen független, így ezzel kapcsolatban nem kell konfigurációs fájlokat szerkesztenünk.
Ahogy korábban megállapítottam, a 10.4-es verziótól kezdve az *OS X* szinte minden beépített szolgáltatása és alkalmazása kerberizált – így az levelezést lehetővé tevő *Mail.app* is az. Ha saját *CA*-t futtatunk vagy önaláírt tanúsítványokat használunk, akkor először importálni kell a *CA*-nk tanúsítványát a rendszer-kulcslánca-ba, hogy a *Mail.app* ne panaszkodjon, amikor önaláírt, *SSL*-re épülő szolgáltatáshoz kapcsolódik, mint amilyen az *IMAP* és az *SMTP*.
Másoljuk a *CA* tanúsítványt az *OS X* kliensre, majd futtassuk *sudo*-val a *certtool*-t:



4. ábra OS X Kerberos alkalmazás

```
sudo certtool i ci-cert.pem v \
k=/System/Library/Keychains/
➥X509Anchors
```

Most már el lehet indítani a *Mail.app*-t. Van egy apró trükk, amivel a felhasználói fiókok legyártásakor már be tudjuk kapcsolni a *GSSAPI*-t. Töltsük ki a felhasználói nevet, és hagyjuk üresen a jelszót. Ha nincs érvényes igazolványunk, akkor a *Kerberos* jelszót fog kérni. Mihelyt elkészült a felhasználói fiók, térjünk vissza és kapcsoljuk be az *IMAP SSL* támogatását. Alapértelmezetten nincs bekapcsolva, és a *Mail.app* nem teszi lehetővé a választást a felhasználói fiók létrehozásakor.
Az *OS X* különböző változatai (a 10.3-as verziótól kezdve) rendelkeznek egy Kerberos.app nevű grafikus alkalmazással (*4. ábra*), ami lehetővé teszi a *Kerberos* igazolványok egyszerű kezelését. Ez azonban jól el van temetve a */System/Library/CoreServices* mélyére. Ezt a hasznos alkalmazást érdemes felvenni a panelra és a betöltéskor elindítandó programok közé. Ez automatikusan megújítja a lejárt tanúsítványokat, és több más hasznos funkciója mellett kijelzi például a hátralevő érvényességi időtartamot. Az *Apple* számos szolgáltatása és alkalmazása teljesen kerberizált, például a *Safari*, a *VPN*, az *Xgrid* és *AFP*, melyek által az *Apple* felhasználók és rendszergazdák teljes értékű polgárai lesznek hálózatunknak.

Sínre tétel

Most már valószínűleg mindenki látja, micsoda lehetőségek rejlenek az *LDAP* címtárakban és a *Kerberos* hitelesítésben. Hatékony és skálázható infrastruktúránk van, valamint ezt teljes mértékben használó kliensgépeink. A következő cikkben a *Microsoft Windows* kliensgépek integrálásáról lesz szó. Addig is élvezzük munkánk gyümölcsét!

Köszönetnyilvánítás

Munkámban segítséget nyújtottak: Matematikai, Információtechnológiai és *Számítástudományi tanszék* (*Office of Advanced Scientific Computing Research, Office of Science*), az *Amerikai Energiaügyi Minisztérium* a *W-31-109-ENG-38* számú szerződés szerint. További támogatást kaptam a Chicagoi Egyetem Számítástudományi Intézetétől és a Nemzeti Tudományos Alaptól.

Linux Journal 2006., 141. szám

Ti Leggett
(leggett@mcs.anl.gov) a Futures Laboratory of the Mathematics and Computer Science Division rendszergazdája az Argonne National Laboratory-ban; emellett a Chicagoi Egyetem Számítástudományi Intézetében is dolgozik.

KAPCSOLÓDÓ CÍMEK

➲ www.linuxjournal.com/article/8636