# Biztonságos levelezés LDAP és IMAP segítségével (2. rész)

Ha sikerül egy IMAP-levélkiszolgálót egy LDAP-címtárral házasítanunk, akkor minden egyszerűbbé és biztonságosabbá lesz, és a felhasználók is könnyebben tudnak levelezni. Mick ezúttal a rázósabb témákról szól, amelyeken keresztülrágva magunkat a cég elektronikus levélügyi szakértőjévé képezhetjük magunkat.

Az LDAP és a Cyrus IMAP-kiszolgáló együttes használatáról szóló cikksorozat első részében telepítettük és beállítottuk a Cyrus IMAP-ot és a Cyrus SASL-t. Ez alkalommal felhasználókat adunk a Cyrus IMAP adatbázisához, majd olyan módon állítjuk be a Postfixet, hogy a Cyrus IMAP-kiszolgálónak továbbítsa a leveleket.

## A Cyrus IMAP leírása

Mielőtt elmerülnénk a Cyrus IMAP beállításának és felügyeletének részleteiben, egy megjegyzés a leírásokkal kapcsolatban. A Cyrus IMAP-hoz html-formátumú rendszergazdai útmutató jár. A SuSE-terjesztésekben a kézikönyv a */usr/share/doc/packages/cyrus-imapd/doc*, *Simon Matter* Red Hat SRPM terjesztésében (lásd a cikksorozat első részét) pedig a */usr/share/doc/cyrus-imapd-2.1.12* útvonalon érhető el. A megtévesztő ***Installation*** (telepítés) névvel ellátott hivatkozás egy olyan oldalra vezet, amely nemcsak a telepítéssel, de a beállítással és a felügyeleti teendőkkel kapcsolatos tudnivalókat is tartalmazza. A kézikönyv mellett számos súgóoldal is tartozik a Cyrus IMAP-hoz, a legfontosabbak az ***imapd.conf(5)***, az imapd(8) és a cyradm(1). A Cyrus IMAP elektronikus leírása mellett érdemes tanulmányozni ***Dianna*** és ***Kevin Mullet*** „Managing IMAP" című könyvét is. Amennyire én tudom, ez az egyetlen kizárólag IMAP-pal foglalkozó könyv. A Cyrus IMAP kapcsán az LDAP használatára ugyan már nem tér ki, de rendkívül jól megírt könyv, amely tisztán és érthetően magyarázza el az IMAP-pal kapcsolatos fogalmakat és a Cyrus IMAP felügyeletét, továbbá az UW-IMAP-pal is foglalkozik.

## A cyradm használata

A Cyrus IMAP-hoz tartozik egy Perl parancsfájl, a `cyradm`, ezzel lehet a legkényelmesebben létrehozni és kezelni a felhasználók postaládáit. A `cyradm` használatba vétele előtt jó néhány dologgal kell tisztában lennünk. Először is a `cyradm`-ot olyan fiókkal kell futtatni, amit elektronikus levelek olvasására nem használunk. Másként fogalmazva, elektronikus levelezésre soha ne használjunk felügyeleti IMAP-fiókot. A szokatlantól eltérő írási–olvasási engedélyek miatt az ilyen fiókot levélolvasásra és -küldésre használva kedvezőtlenül befolyásolhatjuk a kiszolgáló működését. Amint a múltkori alkalommal megtanultuk, a Cyrus felügyeleti fiókjainak nevét a */etc/imapd.conf* fájlban szereplő `admins` változó adja meg.

Másodszor a `cyradm` ugyanazt a hitelesítési eljárást használja, mint a Cyrus IMAP egyéb részei. Előző írásomban ezt úgy határoztuk meg, hogy a */etc/imapd.conf* fájl `sasl_pwcheck_method` változóját `saslauthd` értékre állítottuk, a */etc/sysconfig/saslauthd* fájl módosításával pedig LDAP, illetve SuSE-terjesztésnél PAM használatát írtuk elő. A PAM ezt követően a */etc/pam.d/imap* és a */etc/openldap/ldap.conf* fájl segítségével vehető rá arra, hogy az IMAP-tranzakciók hitelesítéséhez LDAP-ot használjon. Magyarul, a `cyradm` a rendszergazdákat is LDAP-on keresztül azonosítja és hitelesíti, feltéve, hogy az előző alkalommal leírtak alapján helyesen állítottuk be a Cyrus IMAP LDAP-támogatását. Végül a hitelesítés elvégzéséhez a `cyradm` egy LDAP `auth` keresést végez a megadott felhasználónévvel és jelszóval, keresési szempontként az UID LDAP-jellemzőt használva. Ha tehát egy fiókot fel szeretnénk hatalmazni a `cyradm` futtatására, akkor a hozzá tartozó LDAP-bejegyzésnek UID és `userPassword` jellemzőt egyaránt tartalmaznia kell. Az UID kötelező jellemző, a `userPassword` pedig megengedett, mint a `posixAccount` objektumosztály része. Minden IMAP-felhasználó fiókját hozzá kell tehát rendelni a `posixAccount` osztályhoz.

Az utolsó dolog: az OpenLDAP-kiszolgáló */etc/openldap/slapd.conf* fájljában olyan hozzáférési lista (ACL) beállításokat kell megadnunk, amelyek a `userPassword` jellemzőhöz hozzáférést engednek az IMAP-kiszolgáló (illetve a hozzá tartozó `saslauthd` folyamat) által az LDAP-kiszolgálóhoz való csatlakozáshoz, vagyis a hitelesítésekhez használt LDAP-felhasználó számára. Az LDAP ACL-utasítások leírása a ***slapd.conf(5)*** súgóoldalon található, illetve korábbi, „Hitelesítés LDAP használatával (3. rész)" című cikkemben (Linuxvilág, 2003. szeptembere) is ismertettem őket.

A `cyradm` jellemzően felügyeleti parancssorként fut, nem normál parancsként. Elindítása után a `cyradm` bekéri felhasználónevünket és a felügyelni kívánt gép nevét, majd

a megfelelő jelszót is. Sikeres hitelesítés esetén felhasználói beavatkozást igénylő (interaktív) munkamenetet indít, ennek saját parancsai és beépített súgója van. A `cyradm` felhasználói beavatkozást nem igénylő módon is futtatható, a parancsfájlok írásával kapcsolatban pedig a cyradm(1) súgóoldalon találunk útmutatást.
A `cyradm` meghívásának legegyszerűbb módja:

```
bash-$> cyradm --user felhasználónév gépnév
```

Ha a `cyradm`-et ugyanazon az állomáson futtatjuk, mint amelyen a Cyrus IMAP-ot, akkor a localhost gépnevet adjuk meg, ha viszont távoli gépet szeretnénk felügyelni, akkor annak nevére vagy IP-címére lesz szükség. Alapbeállítás szerint a `cyradm` a 143-as TCP-kapun keresztül próbál csatlakozni. Mivel a Cyrus IMAP ezt a kaput csak nyílt, szöveg alapú kapcsolattartásra használja, a `--port` kapcsolóval kell jeleznünk a programnak, hogy a TLS titkosítású adatkapcsolathoz a 993-as számú TCP-kaput szeretnénk igénybe venni: `--port 993`. Szerintem ilyen esetben az a legegyszerűbb, ha a távoli IMAP-kiszolgálóra SSH-n keresztül lépünk be, majd helyben futtatjuk a `cyradm`-ot.
Tegyük fel, hogy az IMAP-kiszolgálómon helyben akarom futtatni a `cyradm`-et, és felügyeleti fiókom neve `mick_admin`. A kiadandó parancs a következőképpen fest:

```
bash-$ cyradm -u mick_admin localhost
IMAP Password: **********

   localhost>
```

A `localhost>` parancssor megjelenése jelzi, hogy a `cyradm` parancssori munkamenetét sikeresen elindítottuk. Ha a rendelkezésre álló parancsok teljes listáját meg szeretnénk jeleníteni, adjuk ki a `help` parancsot vagy gépeljünk be egy kérdőjelet. Összesen húsz parancs létezik, mindegyiket rövidíteni lehet, sokszor kétféle módon is. A súgó képernyőjén a parancsok összes változata megjelenik.

## Postaládák létrehozása a cyradm segítségével

Postaládát a `createmailbox` paranccsal tudunk létrehozni, illetve használhatjuk a parancs `create` vagy `cm` rövidítését is:

```
localhost> cm user.bwooster
localhost>
```

Ennél hatékonyabb nem is lehetne a parancssor használata. Egy apróságot megjegyeznék, a postaládához tartozó felhasználónév nem ***user.bwooster***, hanem egyszerűen ***bwooster***. A ***user.*** előtagot a Cyrus IMAP-postaládák létrehozásakor mindig meg kell adni. Ha tehát a Bubba felhasználónak postaládát szeretnénk adni, a `cm user.bubba` parancsot kell kiadnunk. Ezt követően a postaládán belül a `cm user.bubba.sent`, a cm `user.bubba.drafts` stb. parancsokkal hozhatunk létre alkönyvtárakat.
A ***user.*** előtag csak a Cyrus és a felügyeletét végzők számára látható. Amikor Bubba az Evolution vagy valamely más IMAP-ügyfél segítségével csatlakozik a kiszolgálóhoz, akkor csak egy ***Inbox*** nevű könyvtárat fog látni, függetlenül attól, hogy felhasználóneve ***user.bubba***. Az alkönyvtárak is ***sent***, ***drafts*** stb. névvel jelennek meg, az Inbox alatt.
Érdemes még megemlíteni, hogy a postaládák létrehozásakor a Cyrus semmilyen visszajelzést nem ad arról, hogy a műveletet sikeresen végrehajtotta-e. Akit ez – hozzám hasonlóan – idegesít, az a `listmailbox`, röviden az `lm` paranccsal ellenőrizheti, hogy éppen milyen postaládák vannak a rendszerben:

```
localhost> lm
   user.bwooster (\HasNoChildren)
```

Hisszük vagy sem, a Cyrus IMAP ezt követően készen áll arra, hogy fogadja a ***bwooster*** felhasználó leveleit, illetve levélolvasási lehetőséget adjon számára. Feltéve, hogy létezik egy bwooster UID jellemzőt tartalmazó LDAP-bejegyzésünk. Cyrus IMAP alatt az új postaláda létrehozásával egyben a megadott felhasználó IMAP-fiókja is létrejön. Mielőtt azonban áttérnénk arra, hogy a Postfix MTA-t hogyan kell rávenni a levelek Cyrus IMAP-nak való továbbítására, néhány szó a Cyrus IMAP ACL-jeiről, vagyis hozzáférés-vezérlési listáiról.

## A Cyrus IMAP hozzáférés-vezérlési listái

Egy Cyrus IMAP alapú rendszer minden postaládájához egy vagy több hozzáférés-vezérlési lista (ACL) tartozhat, ezek azt határozzák meg, hogy az egyes felhasználók milyen műveleteket hajthatnak végre az adott postaládán vagy könyvtáron. Alapesetben egy új postaládához csak egyetlen ACL tartozik, ez teljes felügyeleti jogot ad a postaláda gazdájának a ládára.
Érdekes, hogy a rendszergazdák alapesetben csak keresési és felügyeleti jogosultsággal rendelkeznek a postaládákra, vagyis a `listmailbox` paranccsal megtekinthetik a ládák nevét, illetve módosíthatják a rájuk vonatkozó ACL-ek tartalmát. Ebből fakadóan, ha törölni akarunk egy postaládát, akkor először létre kell hoznunk egy olyan ACL-t, amely felügyeleti jogot ad felügyeleti fiókunk számára. Nem hibáról, hanem biztonsági szolgáltatásról van szó, amely segít megelőzni a véletlen törléseket.
Példánknál maradva, az imént létrehozott postaládát a `mick_admin` felügyeleti fiók használatával az alábbi parancsokat kiadva törölhetjük:

```
$ cyradm -u mick_admin localhost
IMAP Password: *****

localhost> setaclmailbox user.bwooster mick_admin
➥all
localhost> deletemailbox user.bwooster
```

A második parancsot talán nem nagyon kell magyarázni, az első elemein viszont érdemes végigmenni. Itt a `cyadm setaclmailbox` parancsát adtuk ki, ezt `sam` vagy `setacl` formában rövidíthettük volna. A parancsot a kérdéses postaláda neve követi (***user.bwooster***), majd annak a fióknak a neve következik, amelynek jogot szeretnénk adni (szükség esetén a jogok megvonását is hasonló módon végezhetjük el), ebben az esetben `mick_admin`. Utolsó elemként engedélykódok csoportját vagy egy különleges karakterláncot kell megadnunk. A példában az `all` karakterláncot látjuk,

ennek segítségével az összes engedélyt megadhatjuk vagy elvehetjük. A ***user.bwooster*** postaládát úgy is tudtuk volna törölni, hogy a parancs végére c betűt írunk be, vagyis postaláda és alpostaládák létrehozására és törlésére adunk jogosultságot. Az ACL-ekben szereplő további engedélyek összefoglalása az *táblázatunkban* szerepel (60. CD Magazin/MAP könyvtárban).
Az ACL-ekről a cyradm(1) súgóoldal és a Cyrus IMAP html-formátumú leírásában olvashatunk részletesebben. Mindenkinek javaslom, hogy miután a `cyradm` segítségével létrehozta a postaládákat, minden alkalommal legalább ellenőrizze az ACL-ek tartalmát, ha nem is változtatja meg őket. Sok helyen nincs szükség arra, hogy a felhasználók alapértelmezett c (létrehozási és törlési) joga megmaradjon.
Ha például minden alpostaládát (***user.felhasznalo.sent***, ***user.felhasznalo.saved*** stb.) saját kezűleg hozunk létre, akkor előfordulhat, hogy a felhasználók számára nem akarjuk engedélyezni újabbak létrehozását vagy a meglévők törlését.

## A Postfix beállítása a levelek Cyrus IMAP-nak történő továbbítására

Az első részben már volt szó a levélszállító ügynökök (Mail Delivery Agent, MDA) szerepéről: ezek juttatják el a leveleket a postaládákba. Mint MDA, a Cyrus IMAP képes a levelek postaládákba juttatására, ám ehhez előbb meg kell kapnia őket valamilyen levéltovábbító ügynöktől (Message Transfer Agent, MTA). A legnépszerűbb MTA a Sendmail, de ha egyszerűbb és biztonságosabb megoldásra vágyunk, válasszuk ***Wietse Venema*** kiváló programját, a Postfixet (➲ http://www.postfix.org). Mivel én is a Postfixet használom MTA-ként, és a legtöbb Linux-terjesztésben vagy alapértelmezett, vagy választható MTA-ként megtalálható, a továbbiakban csak vele foglalkozom részletesebben.
Vajon az IMAP-kiszolgálónak a helyi szervezet SMTP-továbbító gépén kell futnia? Lehetőség nyílik rá, de nem muszáj így lennie. Biztonság és teljesítmény szempontjából ellenben előnyösebb, ha az SMTP-továbbító kizárólag ezt az egy feladatot látja el. Ekkor az IMAP-kiszolgáló saját Postfix-példányt futtathat, amely a kinevezett (dedicated) SMTP-továbbítótól fogadja a leveleket, és nem közvetlenül más hálózatok MTA-itól. Bármilyen hálózati felépítést is választottunk, a továbbiakban feltételezzük, hogy az az MTA, amelytől az IMAP-kiszolgáló a leveleket kapja, ugyanazon a gépen fut, mint a Cyrus IMAP.
Ahhoz, hogy a Postfix a Cyrusnak továbbítsa a leveleket, három állományt kell átszerkeszteni. Az első a ***/etc/postfix/main.cf***, ebben az alábbi sort kell a megjegyzésből kivenni, vagy ha hiányzik, begépelni:

```
mailbox_transport = cyrus
```

A második fájl a ***/etc/postfix/master.cf***, ebben két sort kell hasonló módon élesítenünk:

```
cyrus unix - n n - - pipe
user=cyrus argv=/usr/libexec/cyrus/deliver -r
➥${sender} ${user}
```

Lehet, hogy a saját rendszerünkön a második sor más lesz, a Cyrus deliver program meghívásának módja az idők során módosult. Ha a Cyrus IMAP és a Postfix telepítését egyaránt saját Linux-terjesztésünk legújabb változatának CD-éjéről vagy letöltési helyéről végeztük, akkor az abban talált ***/etc/postfix/master.cf*** fájlnak módosítás nélkül működnie kell. Ha viszont a Cyrus IMAP vagy a Postfix akár csak egyikét is forrásból tettük fel, akkor szükségünk lehet némi barkácsolásra, ekkor a Google segítségével deríthetjük ki a második sor helyes formátumát és tartalmát. Erről egyébként annyit érdemes leírni, hogy az `argv=/usr/libexec/cyrus/deliver` átadott értékben szereplő elérési útnak a helyi rendszer Cyrus `deliver` parancsára kell mutatnia.
A harmadik és egyben utolsó Postfix fájl a ***/etc/aliases***. Egyes rendszereken a ***/etc/postfix/aliases*** név alatt szerepel. Hacsak nem LDAP-ot használunk az álnevek kikeresésére – ennek tárgyalása meghaladná írásom kereteit, de a széljegyzetben kitérek rá –, akkor az ***aliases*** fájlban minden Cyrus postaládához léteznie kell legalább egy bejegyzésnek, továbbá a postaládákhoz igényelt álneveket is fel kell sorolni. Például a Bubba felhasználó számára az alábbi sorral kell bővíteni a ***/etc/aliases*** állományt:

```
bubba:      bubba
```

Egyszerű, igaz? Elmarad a ***user.*** előtag, és a Cyrus postaládákra felhasználónév alapján hivatkozunk. Ha a Cyrus-, vagyis LDAP-felhasználónevek egyeznek a helyi rendszerben szereplő felhasználónevekkel, akkor ezekhez a felhasználókhoz nem kell álnév-bejegyzéseket létrehoznunk.
A Cyrus egyik szépsége, hogy használatakor a felhasználóknak nem kell héjhozzáférést adnunk.
Ha Bubba az adott cég marketingelemzője, akkor hozzáadhatjuk az alábbi sort is:

```
marketing_zseni: bubba
```

Az ***aliases*** fájl szerkesztése után ne feledjük el kiadni a `postalias` parancsot, amely létrehozza az új álnév-adatbázist:

```
bash-$> postalias hash:/etc/aliases
```

## Összegzés

Természetesen még sok mindennel tisztában kell lennünk, hogy Cyrus IMAP rendszergazdának vallhassuk magunkat, ám az eddigiek alapján bele tudunk kezdeni egy LDAP-képes Cyrus IMAP-kiszolgáló üzemeltetésébe. A két írásom alapján elsajátított tudásanyag elegendő ahhoz, hogy bonyolultabb kérdésekkel is foglalkozhassunk, mint például az LDAP-jelszavak módosításának lehetővé tétele a felhasználók számára, az LDAP-kiszolgáló beüzemelése telefonkönyvként, megosztott IMAP-könyvtárak biztonságos beállítása, biztonságos webes levelezőfelület létrehozása, például a SquirrelMail telepítésével és így tovább.

*Linux Journal 2004. január, 117. szám*

***Mick Bauer*** (mick@visi.com)
Biztonsági szakember, a Linux Journal biztonsági témákkal foglalkozó szerkesztője, biztonsági tanácsadó a Minnesota állambeli Minneapolisban található Upstream Solutions LLC Inc.-nél.