Biztonságos levelezés az LDAP segítségével (1. rész)

Célunk egy biztonságos, méretezhető levélkiszolgáló üzembe helyezése, amely a meglévő LDAP-kiszolgálónk segítségével hitelesíteni tudja az IMAP-felhasználókat.

Nemrég végeztünk egy OpenLDAP-kiszolgáló építésével. Mostani és következő írásomban az LDAP egyik leghasznosabb alkalmazási területével, a hitelesítéssel és a telefonkönyv-szolgáltatással foglalkozom. Természetesen nem az LDAP témát fogom továbbvinni. A központi téma az IMAP (Cyrus) lesz, illetve az, hogy miként tudunk a tudására és az LDAP szolgáltatásaira támaszkodva biztonságos távoli levelezési lehetőséget nyújtani. Értelemszerűen feltételezzük, hogy már üzembe helyeztünk egy LDAP-kiszolgálót – vagy legalábbis ismerjük ennek módját –, és feltöltöttük a szükséges felhasználóadatokkal.

Szállító és továbbító ügynökök

Elsőként tekintsük át az IMAP szerepét az elektronikus táplálékláncon belül. Az IMAP, vagyis az Internet Message Access Protocol (internetes üzenet-hozzáférési protokoll, leírása az RFC 3501 dokumentumban található) a levélszállító ügynökök (Mail Delivery Agent, MDA) egyik protokollja. Míg a levéltovábbító ügynökök (Mail Transport Agent, MTA) – például a Postfix és a Sendmail – hálózatok között továbbítják a leveleket, addig az MDA-k az MTA-k és a megcímzett levelesládák közötti szállításáért felelősek. A „Building secure servers with Linux” című könyvemből kiragadva a példát, az MTA a postahivatalok között ingázó teherautóhoz, az MDA pedig a küldeményeket a hivatalból az otthonunkba hozó levélkihordóhoz hasonlítható. Egy IMAP alapú MDA-rendszer két részből áll: egy IMAP-kiszolgálóból, amely a felhasználók levelesládáinak ad helyet és valamilyen MTA-tól fogadja a leveleket, valamint az IMAP-ügyfélprogramot futtató felhasználók csoportjaiból. A három legnépszerűbb nyílt forrású IMAP-kiszolgáló a University of Washington IMAP (UW IMAP), a Carnegie Mellon Egyetem háza tájáról származó Cyrus IMAP, illetve az Inter7 Internet Technologies által fejlesztett Courier IMAP. A legelterjedtebb IMAP-ügyfélprogramok a Netscape/Mozilla Communicator, a Ximian Evolution, a Microsoft Outlook Express, a KMail, a `mutt`, a `pine` és az Apple Mac OS X Mail. Az IMAP-ügyfelekkel e helyen nem foglalkozunk, ami viszonylag könnyű beállításuk és használatuk miatt talán megbocsátható. Ráadásul mivel a legtöbb IMAP-ügyfél az IMAP-kiszolgálók túlnyomó részével gond nélkül működik, a dolognak ezen a részén kár lenne túl sokat rágódni.

Melyik IMAP-kiszolgálót válasszuk?

Az IMAP-rendszer építésekor a rendszergazda első döntése a megfelelő kiszolgáló kiválasztása. Milyen fontosabb különbségek fedezhetők fel az UW IMAP, a Courier IMAP és a Cyrus IMAP között? Mivel az utóbbi kettő szolgáltatásai elég gyakran bővülnek, a kérdés részletes megválaszolása alól kimenteném magam. Amit mondhatok:

1. A három megoldás közül az UW IMAP a legkevésbé rugalmas, mivel csak helyi felhasználói fiókokon alapuló levélszállítást támogat. Minden felhasználó bejövő leveleit egyetlen fájlban, a */var/mail/felhasználónév* név alatt tárolja. Ennek a megoldásnak két hátránya van: egyrészt minden levelező személynek rendszerfelhasználót kell létrehozni, másrészt egy-egy felhasználó postaládáját egyszerre csak egy folyamat tudja írni, s ez fájlzárolási hibákat okozhat.
2. A Courier IMAP-ot, amely jelenleg a Courier Mail Server része, a `qmail` levélkönyvtár rendszerének támogatására tervezték. Esetében a felhasználók saját levélkönyvtárakkal rendelkeznek, ezek a leveleket a teljesítmény és a fájlzárolási hibák elkerülése szempontjából egyaránt a kedvezőbb módon: külön fájlokban tárolják. A Courier adatbázisban is tárolni tudja a leveleket (lásd a 3. pontot), és az újabb változatai már támogatják az LDAP alapú hitelesítést.
3. A Cyrus IMAP telepítése a másik kettőjénél bonyolultabb, nagyrészt a működéséhez szükséges Cyrus SASL hitelesítő könyvtáraknak köszönhetően. A Cyrus IMAP viszont saját felhasználó- és levéladatbázist használ, mindkettő teljesen független az operációs rendszertől, így rendszerfelhasználók hozzáadása nélkül bővíthetjük a levelezéshez hozzáféréssel rendelkezők körét. A levelek egyszerű fájlok helyett adatbázisban való tárolásából fakadó teljesítménynövekedése magától értetődő.

Én legtöbbet a Cyrus IMAP-ot használtam, így a továbbiakban erről fogok bővebben szólni. Az UW IMAP, a Courier IMAP és a Cyrus IMAP weblapjára ellátogatva – lásd a *Kapcsolódó címeket* –, majd a szolgáltatások listáját áttekintve mindenki maga döntse el, hogy melyik program felel meg a leginkább az igényeinek. Írásom hátralévő részeiben remélhetőleg a tőlem eltérően döntők is találnak hasznos tudnivalókat, legalább az elgondolások szintjén.

A Cyrus IMAP letöltése és telepítése

Jómagam a jobb csomagkezelők nyújtotta változat- és javításkezelő szolgáltatások végett nagyon szeretem a futtatható állományokból álló csomagokat. Mielőtt valaki rosszra gondolna, a nagyobb terjesztések csomagkezelőit kivétel nélkül a jobbak közé sorolom. Azt javaslom mindenkinek, hogy a Cyrus IMAP telepítését saját terjesztésének frissítőszolgáltatása segítségével vagy valamilyen adathordozóról végezze el, ha ez lehetséges. A Cyrus SASL-csomagra is szükség lesz, ez adja a Cyrus IMAP számára a hitelesítő háttérrendszert. Az `SMTP AUTH` úgyszintén ezt használja, ezért lehetséges, hogy már fel is van telepítve.

A SuSE 8.2-es rendszerhez a `cyrus-imapd` és a `cyrus-sasl2` RPM-ekre lesz szükség, míg például Debian 3.0-s alatt a `packages cyrus-common`, a `cyrus-imapd`, a `libsasl2` és a `sasl2-bin` csomagokat kell beszerezni. SuSE és Debian futtatásakor egyaránt figyelembe kell venni, hogy a korábbi rendszereken régebbi – 2.0-s változat előtti – Cyrus SASL-csomagok lehetnek feltelepítve; a Cyrus IMAP által végzett, a későbbiekben ismertetett LDAP alapú hitelesítéshez viszont a SASL 2.0-s vagy újabb változat szükséges. Ha a futó terjesztésre 2.0-s előtti SASL-csomag van telepítve, akkor Cyrus SASL forráskódját le kell tölteni és le kell fordítani (ez az ➲ ftp.andrew.cmu.edu/pub/cyrus-mail címen érhető el).

A Red Hat 9.0-s rendszer alatt picivel több munkára lesz szükség, mint a legújabb SuSE- vagy Debian-terjesztések esetében, mivel a 7.1-es változat óta a Cyrus IMAP-csomagok kikerültek a Red Hat-terjesztésből. Elsőként a `cyrus-sasl`, a `cyrus-sasl-plain` és a `cyrus-sasl-md5` csomagot kell telepíteni, ezek a normál Red Hat 9.0-s terjesztés részei. Ezt követően egy SRPM-csomag formájában le kell tölteni magát a Cyrus IMAP-ot, amit a ***home.teleport.ch/simix*** címről tehetünk meg. (Az oldal karbantartásáért köszönet illeti a svájci ***Simon Matter***-t.)

Ha még sosem akadt dolgunk forrás-RPM-mel, vagyis SRPM-mel, ne essünk kétségbe; futtatható RPM-et az SRPM-ből a következő paranccsal készíthetünk:

```
rpm --rebuild [--target geptipus] srpm.nev.src.rpm
```

Ebben az ***srpm.nev.src.rpm*** az SRPM fájl neve, a „geptipus" pedig a gép típusát adja meg (például i386, i586, i686). Nekem például egy Pentium III alapú kiszolgálóm van, ezen az `rpm --rebuild --target i686 cyrus-imapd-2.1.12-7.src.rpm` utasítást kellett kiadnom. Ugyan a `--target` átadott érték elhagyható, de ha nagyobb IMAP-felhasználó adatbázist fogunk kezelni, akkor a Cyrus IMAP-ot érdemes a saját gépünk processzortípusának megfelelően fordítani, mert így az alapértelmezett i386 fordításhoz képest érzékelhető sebességnövekedést fogunk tapasztalni. Az `rpm` ezt követően önműködően több új futtatható RPM-et is elkészít, kifejezetten a helyi rendszerhez testreszabva. Ezek az RPM-ek a ***/usr/src/redhat/RPMS/*** könyvtárba kerülnek, amelyben az alkönyvtár pontos neve a `--target` átadott értékétől függ; az i386/ az alapértelmezett. A keletkező RPM-ek a következők: `cyrus-imapd`, `cyrus-imapd-utils`, `cyrus-imapd-devel` és `perl-Cyrus`. Telepítésüket az *`rpm -Uvh fájlnév`* paranccsal végezhetjük el.

A SASL beállítása

A továbbiakban még két dolgot végzünk el: egyrészt az IMAP-felhasználók hitelesítése terén kiaknázzuk meglévő LDAP-kiszolgálónk képességeit, másrészt Cyrus IMAP-kiszolgálónkat úgy állítjuk be, hogy csak SSL feletti, titkosított kapcsolatokat fogadjon a végfelhasználóktól. Korábbi írásaimban kellően felmagasztaltam a központi hitelesítést, így az LDAP által kínált értékes lehetőségek remélhetőleg senkinek nem jelentenek újdonságot. Korábban már ejtettem szót arról, hogy az elektronikus levelek nyílt szövegben folytatott lekérése milyen veszélyeket rejt magában. Normál POP3- és IMAP-kapcsolatoknál a felhasználónév, a jelszó és a levelekben található adatok egyaránt titkosítatlanul haladnak keresztül a hálózaton. Minden hallgatózás jellegű támadásnak ki vannak téve, ami különösen a vezeték nélküli hálózaton vagy az interneten – amely a világ legmegbízhatatlanabb hálózataként kezelhető – keresztül végzett lekérdezésekre igaz. Térjünk vissza a SASL témájához! Mivel a Cyrus IMAP és a Cyrus SASL egyaránt a Carnegie Mellon Egyetemről származik, és a Cyrus fejlesztői nyilván nem akartak valami teljesen újat alkotni, a Cyrus IMAP a hitelesítés tekintetében a Cyrus SASL szolgáltatásaira támaszkodik. Álljunk csak meg! Nem éppen erre a célra akarunk LDAP-ot használni? De igen. A SASL abból a szempontból is feleslegesnek tekinthető, hogy saját felhasználó-adatbázis használatára tervezték.

A SASL azonban nemcsak saját adatbázisát tudja használni, de a hitelesítési műveleteket más hitelesítési források – például PAM vagy LDAP – felé is tovább tudja adni. A legegyszerűbb eljárás a `saslauthd`, a SASL hitelesítési démon beállításainak módosítása, ezt a ***/etc/saslauthd.conf*** fájl tartalmának átírásával tehetjük meg. Az *1. kódrészletben* egy ***saslauthd.conf*** mintafájl tartalma látható.

Az `ldap_servers` kulcsszó után szóközzel elválasztva az LDAP-kiszolgálók URI-jait kell felsorolni. Az 1. kódrészletben nyílt szövegalapú LDAP-kapcsolatot adtam meg a helyi LDAP-folyamathoz. Természetesen az `ldap` helyett titkosított kapcsolatokkal dolgozó `ldaps` protokollt is választ-

1. kódrészlet A /etc/saslauthd.conf mintafájl

```
ldap_servers: ldap://localhost/
ldap_search_base: dc=proba,dc=org
ldap_bind_dn: cn=kiszolgalok,dc=proba,dc=org
ldap_bind_pw: ide_kell_irni_a_jelszot
```

2. kódrészlet A /etc/imapd.conf példafájl

```
configdirectory: /var/lib/imap
partition-default: /var/spool/imap
admins: cyrus bauer
sievedir: /var/lib/imap/sieve
sendmail: /usr/sbin/sendmail
hashimapspool: true
sasl_pwcheck_method: saslauthd
sasl_mech_list: PLAIN
tls_cert_file: /var/lib/imap/slapd3.pem
tls_key_file: /var/lib/imap/slapd3key.pem
tls_cipher_list: HIGH:MEDIUM:+SSLv2
```

hattam volna, illetve távoli gép teljesen minősített tartománynevét vagy IP-címét is megadhattam volna, mint például ➲ ldaps://ldap.proba.org.
Az `ldap_search_base` a felhasználók megkülönböztető neveinek (DN) az alapja, vagyis a közös része. Az `ldap_bind_dn` és az `ldap_bind_pw` az a DN és jelszó, amelyet a `saslauthd` az LDAP-kiszolgáló elérésekor fog használni. Erre a célra mindenkinek egy külön LDAP-bejegyzés létrehozását javaslom. Az 1. kódrészletben a „kiszolgalok” egy különleges LDAP-fiók neve, ennek `objectClass` jellemzője `simpleSecurity` `Object`, vagyis a DN és az `objectClass` mellett egyetlen további jellemzővel rendelkezik, és ez a `userPassword`.
A kifejezetten a kiszolgálók számára létrehozott LDAP-fiók segítségével az LDAP naplóiban könnyen meg lehet különböztetni a kiszolgálófolyamatok és a felhasználók által indított lekérdezéseket. Mindezt sokkal nehezebb volna elvégezni, ha az IMAP például személyes LDAP-fiókok azonosító adatait használná. Ha még kifinomultabb naplózást szeretnénk végezni, akkor minden LDAP-lekérdezéseket végző kiszolgálófolyamat számára külön LDAP-fiókot hozhatunk létre, mint például Cyrus és Postfix.
Jómagam ezekkel a lehetőségekkel éltem a saját */etc/saslauthd.conf* fájlom megírásakor, de természetesen továbbiak is léteznek. A Cyrus SASL csomagban található egy `LDAP_SASLAUTHD` fájl, ami a *saslauthd.conf* fájlban használható beállítások leírását tartalmazza. Ez a fájl a forráskódcsomag *saslauthd* könyvtárában található, ha pedig a SASL telepítését futtatható csomagból végezzük, akkor oda kerül, ahová az adott terjesztés a leírásokat helyezi; valószínűleg a */usr/share/doc* könyvtár valamely alkönyvtárába.
A */etc/saslauthd.conf* átírásán túl arról is meg kell győződni, hogy a `saslauthd` indítása a `-a ldap` kapcsolóval történik-e. Red Hat alatt ehhez a */etc/sysconfig/saslauthd* fájlt kell módosítani úgy, hogy a MECH átadott érték `ldap` legyen.
A SuSE-terjesztésnél ugyanezt a fájlt kell átírni, de az átadott érték neve `SASLAUTHD_AUTHMECH`. Ismétlem, a kívánt végeredmény az, hogy a `saslauthd` a `-a ldap` kapcsolóval induljon.
Ha végeztünk a `saslauthd` beállításainak módosításával és újraindítottuk a démont, akkor készen állunk az IMAP-szolgáltatás üzembe helyezésére. Ezzel már nem lesz gond.

A Cyrus IMAP beállítása

A Cyrus IMAP működését befolyásoló beállítások túlnyomó része a */etc/imapd.conf* fájlban található. A *2. kódrészlet* egy *imapd.conf* mintafájl tartalmát szemlélteti.
Mint valószínűleg feltűnt, az *imapd.conf* beállításainak jelentős része a Cyrus IMAP által igényelt programok és egyebek elérési útját adja meg. Nem fogok részletesebben foglalkozni velük, leírásuk az ***imapd.conf(5)*** súgóoldalon található meg –, de a 2. kódrészlet nem alapértelmezett értékkel ellátott beállításain gyorsan végigszaladnék:
`admins` – az IMAP-rendszernek a `cyradm` segédeszközzel való felügyeletére meghatalmazott Cyrus IMAP-felhasználók listája. (A `cyradm` használatáról egy későbbi írásban lesz szó.) Ha a `sasl_pwcheck_method` beállításnak a `saslauthd` értéket adjuk, és ha a `saslauthd` már be van állítva az LDAP használatára, akkor már rá is vettük a Cyrus IMAP-ot az LDAP alapú hitelesítésre. Ilyenkor hiába létezik `cyrus` felhasználó a helyi Linux-rendszeren, vagyis a */etc/passwd* fájlban, a `cyrus` egy külön LDAP-bejegyzést is igényel.
A `cyradmin` futtatásakor meg kell adni a `cyrus` jelszavát, ekkor az adatbázisban lévő Cyrus jelszavára és nem a linuxos `cyrus`-éra van szükség. Másként fogalmazva, az `admins` kulcsszó után felsorolt fiókoknak mindig abban az adatbázisban kell jelen lenniük, amelyet a `sasl_pwcheck_method` beállításnál kiválasztottunk.
Amikor a Cyrus IMAP-ot – akár forrásból, akár futtatható csomagból – telepítettük, egy új felhasználót (`cyrus`) kellett létrehoznunk, és átadni neki a legtöbb Cyrus IMAP-fájl tulajdonjogát. Mint a jobb szolgáltató démonok, a Cyrus IMAP is külön felhasználóként fut, és feladatainak túlnyomó részét nem rendszergazdaként látja el.
A 2. kódrészletben további három általam testreszabott beállítás látható, ez a `tls_cert_file`, a `tls_key_file` és a `tls_cipher_list`. Szerepük rendre megegyezik az OpenLDAP *slapd.conf* fájljában található `TLSCertificateFile`, `TLSCertificateKeyFile` és `TLSCipherSuite` beállításokéval. Azért akartam erre külön felhívni a figyelmet, mert az itt megadott tanúsítvány- és kulcsfájl megegyezik a rendszer OpenLDAP-kiszolgálója által használttal. Ennek az az oka, hogy rendszeremben a Cyrus IMAP és az OpenLDAP ugyanazon a kiszolgálón fut, nincs tehát semmi okom arra, hogy mindkét szolgáltatás külön kiszolgáló-tanúsítványokat használjon. A */etc/openldap* könyvtárból viszont – a tulajdonlások és az engedélyek kezelésének egyszerűsítése végett – mindkét fájlt a */var/lib/imap* könyvtárba másoltam.
Ha az LDAP-szolgáltatás külön állomáson futna, akkor a 2003. augusztusi cikkemben ismertetett eljárást követve az alábbi parancsokkal külön TLS-tanúsítvány – kulcspárost kellett volna létrehoznom az LDAP-kiszolgáló számára:

```
openssl req -new -x509 -nodes -out
slapdtanusitvany.pem
➥-keyout slapdkulcs.pem -days 365
```

Bármelyik megoldást választjuk is, a tanúsítvány- és a kulcsfájlt egyaránt a cyrus tulajdonába kell adnunk, és csak a tulajdonosuk kaphat rájuk olvasási jogot.
Ha a Cyrus IMAP telepítését forrásból végezzük el, akkor alapértelmezett SSL-kulcsokat fog használni, ebből viszont hiba származik, ha egy IMAP-ügyfél TLS- és nem SSL-titkosítás használatával próbál csatlakozni. Nemcsak megbízhatósági, de minden egyéb szempontból is rossz ötlet az alapértelmezett tanúsítványt vagy kulcsokat használni, bármihez is. Mindig használjuk a meglévő kiszolgálótanúsítvány – kulcspárosunkat, vagy hozzunk létre újat. Így az IMAP-kiszolgálónk megbízhatóbb és biztonságosabb lesz.
Nincs más hátra, mint a Cyrus IMAP újraindítása (`/etc/init.d/cyrus-imapd restart`), és a felhasználók hozzáadása a cyradm segítségével. Ezt a részt azonban, akárcsak a helyi MTA beállítását a levelek átadására az IMAP-nak, hagyjuk a következő alkalomra.

Mick Bauer

Linux Journal 2003. november 115. szám