Az LDAP és a biztonság (1. rész)

Az OpenLDAP segítségével az összes alkalmazás kényelmes közös címtárat használhat. Helyes beállításával a hálózat biztonsága nemhogy csökken, hanem nőni fog.

Tegyük fel, hogy IMAP-kiszolgálót üzemeltetünk rengeteg felhasználóval, de nem szeretnénk minden felhasználónak teljes értékű fiókot létrehozni a kiszolgálón. Inkább valamiféle központi felhasználóhitelesítő szolgáltatást kellene használni, ami más célokra is jó lehet. Ha már itt tartunk, szükség lesz egy állandó elérésű (online) címjegyzékre szervezetünk levelező- és csoportmunkaprogramjai számára. Ezenkívül tegyük fel, a felhasználóknak titkosítóeszközökre is szükségük van, amelyek X.509-es tanúsítványokat használnak, valamint az egész szervezet számára kezelik a digitális tanúsítványokat. Elképzelhető, hogy létezik egyetlen szolgáltatás, ami mind a négy igényt ki tudja elégíteni? Az LDAP képes erre, sőt többre is. A nyílt forrás közössége abban a szerencsés helyzetben van, hogy rendelkezésére áll egy szabad, megbízható és teljes értékű LDAP-kiszolgáló és -ügyfél, ami a legtöbb Linux-terjesztésnek része: ez az OpenLDAP.

Az egyetlen hátrány, hogy az OpenLDAP egy bonyolult szörny. Értelmes használatához még több rövidítést és elvont elképzelést kell megismernünk a szokásos Unix-trükkökön kívül. Felszerelkezve a következő néhány hónapban megjelenő folytatással és egy kis elhatározással, nagyhatalmú LDAP-istenek lehetünk, akik egyszerre több vasat tartanak a tűzben, és a hálózatunk egyszerre lesz biztonságosabb és könnyebben használható. Tapasztalataim szerint a „biztonságosabb” és az „egyszerűbben használható” rendszer ritkán valósítható meg egyszerre, ezért is lelkesedem azért, hogy ebben a rovatban végre bemutathatom az OpenLDAP-t.

Az LDAP alapjai

Dióhéjban összegezve: az LDAP címtárszolgáltatást nyújt, azaz egy központi adatbázisban érhetők el az emberek, csoportok és a szervezetet alkotó más elemek adatai. Mivel minden szervezet különböző lehet, és nem feltétlenül ugyanazokat az adatokat tartják lényegesnek, a címtárszolgáltatásnak rugalmasnak és testreszabhatónak kell lennie. A megoldás ezért a feladat jellegéből adódóan bonyolult.

A címtárszolgáltatásra létezik egy protokoll, az X.500. Az X.500-at nagy és összetett szervezetek nagy léptékű címtárszolgáltatásaira tervezték. Ennek megfelelően az X.500 önmagában annyira nagy és bonyolult protokoll, hogy pehelysúlyú változata, az LDAP, amit az RFC 1777 ír le – és gyakorlatilag az X.500 protokoll részhalmaza –, sokkal inkább elterjedt, mint az eredeti X.500.

Az X.500 és az LDAP nyílt protokollok, miként a TPC/IP; egyik sem önálló termék. A protokollt valamilyen programnak kell megvalósítani, ez lehet magmodul, kiszolgálódémon vagy ügyfélprogram. A TCP/IP-hez hasonlóan nem minden LDAP-megvalósítás egyforma, még csak nem is feltétlenül képesek együttműködni egymással (módosítás nélkül). Most egy bizonyos LDAP-megvalósításról lesz szó, az OpenLDAP-ról, de tudnunk kell, hogy léteznek más programok is, amelyek szintén megvalósítják az LDAP-t. Például ilyen a Netscape Directory Server, a Sun ONE Directory Server és bizonyos korlátokkal a Microsoft Active Directory a Windows 2000 Serverben.

Szerencsére az LDAP-t bővíthetőre tervezték. Ha az egyik környezetben létrehozunk egy LDAP-adatbázist, az cseresza-batos lesz más LDAP-megvalósításokkal is, egyszerűen csak be kell állítanunk az adatbázis rekordformátumát vagy sémáját. Ez a téma a következő hónapban kerül sorra. Ennek köszönhetően gond nélkül futtathatjuk az OpenLDAP-kiszolgálót Linuxon, és a címjegyzéket elérhetővé tehetjük, mondjuk egy Netscape Communicatort futtató Mac-felhasználó számára is.

Az OpenLDAP beszerzése és telepítése

Az OpenLDAP hasznos és fontos eszköz, ennek következtében minden jelentős Linux-terjesztésnek része. Általában több csomagra bontják szét: az egyik a kiszolgálódémont, a másik az ügyfélprogramokat, a harmadik a fejlesztéshez szükséges programkönyvtárakat tartalmazza. Ez a cikk az LDAP-kiszolgáló felállítását tárgyalja, így magától értetődő, hogy terjesztésünk OpenLDAP-kiszolgáló csomagját telepíteni kell. Ezenkívül telepítsük az OpenLDAP futásidejű programkönyvtárait, ha azok nem részei a kiszolgáló csomagjának. Azt gondolhatnánk, hogy az OpenLDAP ügyfélprogramjainak telepítése kihagyható egy olyan kiszolgálón, ahol nincsenek helyi felhasználók, és az LDAP-műveletek a hálózaton keresztül fognak zajlani. Ez sajnos nem így van, kimondottan javasolt az ügyfélprogramokat is feltelepíteni, mert sokat segíthetnek a rendszer kipróbálásában és a hibakeresésben.

Red Hat alatt az OpenLDAP a következő csomagokból áll: openldap (OpenLDAP-programkönyvtárak, -beállítóállományok és a leírás); openldap-clients (OpenLDAP-ügyfélprogramok és -parancsok); openldap-servers (OpenLDAP-kiszolgálóprogramok); valamint az openldap-devel (fejlécállományok és programkönyvtárak fejlesztők számára). Bár a csomagok legtöbb függősége teljesen érthető (például glibc), két szükséges csomag talán még nincs telepítve: a cyrus-sasl és cyrus-sasl-md5, ezek az LDAP hitelesítő műveleteit hivatottak közvetíteni.

SuSE alatt a következő RPM-ekben helyezkedik el az OpenLDAP: openldap2-client (az ***n1*** könyvtárban a SuSE 7.3 és 8.0 esetén); openldap2 (ebben az OpenLDAP-programkönyvtárak és a kiszolgálódémonok csücsülnek, és az ***n2*** könyvtár részét képezik); openldap2-devel (a SuSE 7.3-ban az ***n2***-ben található, a SuSE 8.0-ban az ***n4***-ben érhető el). A Red Hatnél a már említett cyrus-sasl csomagot mindenképpen telepítsük fel, ami a ***sec1*** könyvtárban helyezkedik el.

A 7.3-as és 8.0-s terjesztésekben a SuSE az OpenLDAP 1.2-es változatát is közreadta a 2.0-s mellett. Mindenképpen a 2.0-s csomagokat telepítsük, hacsak nincs különleges okunk az OpenLDAP 1.2 futtatására. Ez a tanács nem vonatkozik a Red Hat- és a Debian-terjesztésekre, mert ezek kizárólag az OpenLDAP 2.0-t használják.

A Debian 3.0-s (Woody-) terjesztésben a megfelelő deb-csomagok a következők: libldap2 (OpenLDAP programkönyvtárak a Debian ***libs*** könyvtárából); `slapd` (az OpenLDAP-kiszolgáló a ***net*** könyvtárból); és az ldap-utils (OpenLDAP-ügyfélparancsok szintén a ***net*** könyvtárból). Ezenkívül még a ***libsasl7***

1. lista A /etc/openldap/slapd.conf testreszabott része

```
database        ldbm
suffix          "dc=wiremonkeys,dc=org"
rootdn          "cn=ldapguy,dc=wiremonkeys,
                 ➥dc=org"
rootpw          {SSHA}zRsCkoVvVDXObE3ewn19/
                 ➥Imf3yDoH9XC
directory       /var/lib/ldap
```

2. lista A slappasswd parancs

```
[root@mydirserver openldap]
# slappasswd -h {SSHA}
New password: *********
Re-enter new password: *********
{SSHA}16JhhIDajRc1cDwwa1t6o0ske8goj8Od
```

programkönyvtárra is szükség van a Debian ***libs*** könyvtárából. Amennyiben kedvenc terjesztésünk nem tartalmazza az OpenLDAP bináris csomagjait, vagy a legújabb OpenLDAP-ból szükségünk van egy adott tulajdonságra, amelyik nincs benne terjesztés OpenLDAP-csomagjában, vagy testreszabott OpenLDAP-csomagot szeretnénk, még mindig lefordíthatjuk az OpenLDAP hivatalos honlapjáról (➲ http://www.openldap.org) letölthető forrást.

A slapd beállítása és elindítása

Az OpenLDAP fő kiszolgálódémonjának a neve `slapd`, és az OpenLDAP telepítése után az első feladatunk ennek beállítása. A beállítások elsősorban a */etc/openldap/slapd.conf* állomány szerkesztésével végezhetők el.
A ➲ http://www.openldap.org/doc/admin20/guide.html címen megtalálható „OpenLDAP 2.0 Administrator's Guide” kitűnően elmagyarázza a `slapd` elindításának és futtatásának kezdőlépéseit a 2. fejezet 8. pontjától kezdve. A dokumentum a címtárszolgáltatásokat és az LDAP fogalmait írásunknál nagyobb mélységben tárgyalja.
Menjünk végig a lépéseken, hogy biztosan jól sikerüljön a kezdés. Az első teendő a ***slapd.conf*** szerkesztése – szemléltetésül tekintsük meg az *1. listát*. Láthatjuk, hogy a ***slapd.conf*** jellegzetes Linux-beállítóállomány: minden sora egy kapcsolónevet tartalmaz, amit egy érték követ. Az 1. listán szereplő első kapcsoló, a `database` azt adja meg, hogy milyen adatbázisháttérrel kívánjuk az OpenLDAP-t használni. Általában a legjobb az `ldbm`-et választani, ami a gyors `dbm` adatbázis-formátumot használja, de a `shell` (egyéni héjprogramhátterek) és a `passwd` (a */etc/passwd* használata háttérként) szintén érvényes beállítás.
Az 1. listán a következő kapcsoló a `suffix`, amely meghatározza, hogy milyen lekérdezések illenek erre az adatbázis-meghatározásra. Az itt megadott végződés a ***wiremonkeys.org***, amelyet az LDAP nyelvén balról jobbra értelmezett tartományelem- (`dc`) kifejezések sorozataként adunk meg. Más szavakkal, ha egy LDAP-ügyfél a `cn=bubba,dc=wiremonkeys,dc=org` megkülönböztető nevű (`dn`) gépet keresve lekérdezi a példakiszolgálónkat, akkor mivel a `dn` vége `dc=wiremonkeys,dc=org`, ez az adatbázis fog ráilleni. A megkülönböztető nevekről többet tudhatunk meg a „Gyorstalpaló az X.500-as nevezéktanról” című írásból (az 51. CD Magazin/LDAP könyvtárában található).
Az 1. lista következő két bejegyzése az LDAP-adatbázis felügyeletével kapcsolatos; a `rootdn` és a `rootpw` azt a felhasználónév és jelszópárost adja meg, amelyet a helyi vagy távoli parancsoknak kell megadniuk, ha felügyeleti műveletet akarnak végrehajtani az LDAP-adatbázison. Érdekes módon ez a bejegyzés csak erre a célra használatos. Nem jelenik meg a szabályos LDAP-adatbázis lekérdezésekben.
Ez felveti azt az ellentmondást, hogy akkor milyen módon lehet hitelesíteni azokat a műveleteket, amelyek a hitelesítési (LDAP) adatbázis feltöltéséhez szükségesek. Később, ha már feltöltöttük az LDAP-adatbázist valódi adatokkal, az egyik rekordot a ***slapd.conf*** hozzáférési listáit használva nevezzük ki felügyeleti fióknak, és töröljük a `rootdn` és `rootpw` bejegyzést. Ezt a lépést egy későbbi írásban tárgyalni fogjuk; pillanatnyilag a `rootdn` és a `rootpw` is megfelel.
Nagyon rossz ötlet a `rootpw` értékét egyszerű szövegben tárolni. Ehelyett a `slappasswd` parancsot kell használni, ami a jelszó kódolt formáját állítja elő, miként a *2. lista* is mutatja. Láthatjuk, hogy a `slappasswd` bekéri a jelszót, és a kódolt jelszót a `-h` kapcsolóval megadott algoritmus szerint előállítja és kiírja a képernyőre. A `-h` után kapcsos zárójelben kell megadni a kívánt algoritmus nevét. A lehetséges választék a slappasswd(8) súgóoldalon fel van sorolva. A `slappasswd` kimenetét közvetlenül bemásolhatjuk a ***slapd.conf*** állományba, én is pontosan ezt tettem az 1. lista `rootpw` értékének létrehozásakor.
Visszatérve az 1. listához, a következő érték a címtár meghatározásában a könyvtár. Nem meglepő módon ez azt adja meg, hogy a helyi állományrendszerben melyik könyvtárban legyen az LDAP-címtár létrehozva. Mivel a */var* a megszokott helye a növekvő állományoknak, mint a naplók vagy az adatbázisok, az 1. lista a */var/lib/ldap* értéket tartalmazza. Létező könyvtárat kell megadni, és az OpenLDAP felhasználójának és csoportjának – általában `ldep` és `ldap` – tulajdonában kell lennie. A jogosultságokat állítsuk a `0700 (-rwx------)` értékre.
Műszaki értelemben ennyi elég az elinduláshoz: az `ldap` indító-parancsfájljával próbáljuk meg elindítani a `slapd` démont. Ez leggyakrabban a */etc/init.d/ldap*, de terjesztésenként különböző lehet. Nyugodtan adjunk hozzá bejegyzéseket az LDAP-adatbázishoz az `ldapadd` parancs használatával – a korábban említett eljárás megmutatja, hogyan.
Mielőtt a hálózaton keresztül kezdenénk el kezelni és lekérdezni az LDAP-adatbázist, be kell állítani a TLS-titkosítást. Ez fontos, mert az OpenLDAP által használt egyszerű hitelesítési eljárás a hitelesítési adatokat titkosítás nélkül küldi át a hálózaton. Sajnos elfogyott a rendelkezésemre álló hely, ezért ez a téma a jövő hónapra marad. Aki nem tud addig várni, az olvassa el ***Vincent Danen*** Using OpenLDAP for Authentication írását a ➲ http://www.mandrakesecure.net/en/docs/ldap-auth.php címen, bár ez bizonyos tekintetben a Mandrake-et helyezi középpontba. Szintén tárgyalni fogom az LDAP-adatbázis szerkezetének meghatározásával kapcsolatos megfontolásokat, és az LDAP-adatbázis létrehozásának a módját.
Addig is sok szerencsét!

Linux Journal 2003. július, 111. 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.