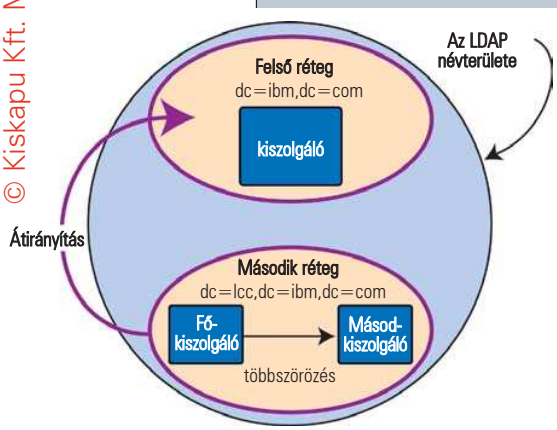
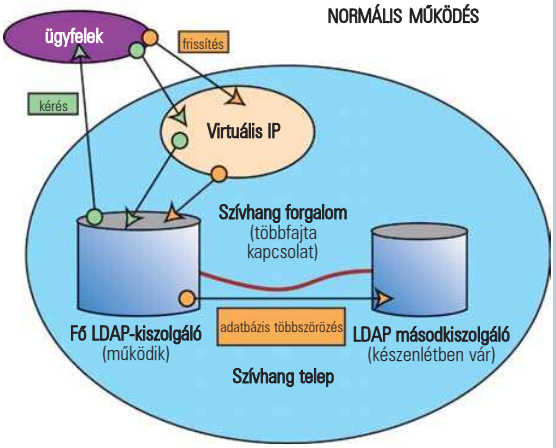
Magas rendelkezésre állású LDAP

Vegyünk egy LDAP-kiszolgálót, majd adjunk hozzá pár evőkanálnyi fejlesztést a Linux-HA projektből, és máris kész egy magas rendelkezésre állású azonosítótelep.



1. ábra
Az LDAP névterenként egyetlen mestert engedélyez

Minél több programot és szolgáltatást használ egy vállalat, annál nagyobb segítséget jelent a rendszergazdák számára a központosított azonosítás. Ráadásul egy központi adatbázis használatával a biztonság is nagymértékben növelhető. Gondot jelenthet viszont, ha minden hitelesítést egyetlen gépre helyezünk. Ebben az esetben egyetlen gép meghibásodása esetén az egész vállalat leállhat. Itt kerülnek a képbe a hibatűrő telepek. Ebben a cikkben azt tárgyaljuk, hogyan hozhatunk létre felhasználók azonosítására szolgáló megbízható kiszolgálótelepet. Példánkban egy LDAP-kiszolgáló (Lightweight Directory Access Protocol, vagyis pehelysúlyú könyvtárhozzáférési/címtárhozzáférési protokoll) látja el a központosított felhasználóazonosítást, melyre a különböző alkalmazások feliratkozhatnak. A szolgáltatást két gépre bízzuk, ehhez a Linux-HA kezdeményezés (➲ http://www.linux-ha.org) heartbeat csomagját használjuk fel.



2. ábra
A slurpd küldi ki az LDAP adatbázis változásait a mesterről a segédre

Az LDAP háttere

Munkánk során az OpenLDAP kiszolgálót használjuk fel, mely sok különféle Linux-terjesztésben megtalálható. A Red Hat Linux 7.1-es változata a 2.0.9-es OpenLDAP-t tartalmazza. Ezen cikk írásának idején az alkalmazás legfrissebb változata a 2.0.11-es. Az OpenLDAP Alapítvány azért jött létre, hogy megalkossanak egy nagy teherbírású, kereskedelmi minőségű, nyílt forráskódú LDAP-csomagot, amely különböző LDAP-alkalmazásokat, fejlesztőeszközöket tartalmaz. Az OpenLDAP 1.0-s változata 1998 augusztusában jelent meg, jelenleg pedig már a 2.0-s sorozatnál tartanak, melyet 2000 augusztusában kezdtek el, és ami már támogatja az LDAPv3-at is.

Az LDAP, mint bármely más jól működő hálózati szolgáltatás, képes egyszerre több kiszolgálón futni. Ezt adatbázis-többszörözéssel (replication) és átirányítással (referral) valósítja meg. Az átirányítások segítségével válik lehetségessé, hogy az LDAP-névterület több kiszolgáló között legyen szétosztva, és hogy több LDAP-kiszolgálót egyetlen többszintű rendszerbe szervezzük. Az LDAP egy névtérhez (namespace) csak egyetlen főkiszolgálót enged hozzárendelni (*1. ábra*).

A többszörözést az OpenLDAP többszörözője végzi, a `slurpd`, mely meghatározott időközönként felébred, és ellenőrzi a főkiszolgálón a naplófájlt, hogy megtudja, történt-e változás. A módosítások ezt követően a másodkiszolgálókra is átkerülnek. Az olvasási kéréseket bármely kiszolgáló megválaszolhatja, frissítéseket azonban csak a főkiszolgálón lehet elvégezni. Ha egy alárendelt kiszolgálón próbálunk meg frissíteni, akkor egy olyan átirányítást kapunk vissza, amelyből megtudhatjuk a főkiszolgáló címét. Ezt követően az ügyfél feladata, hogy megtalálja a főkiszolgálót és elvégezze rajta a frissítést.

Az OpenLDAP-csomagban nincs terhelésmegosztásra alkalmas eszköz, erre a célra valamilyen IP-szintű kérelemszóró programot használhatunk, mint amilyen például a `balance`.

Feladatunk tehát egy hibatűrő rendszer kialakítása. Ehhez két kiszolgálót kapcsoltunk össze. Használhattunk volna osztott tárolóegységet is a két gép között, így az adatokból csak egyetlen másolatot kellene kezelni, mi azonban a „megosztott-semmi" elméletet követtük, ezért minden kiszolgáló saját tárolóeszközzel rendelkezik. Az LDAP-adatbázisok alapesetben kisméretűek, és csak ritkán frissülnek (tanács: ha *tényleg* nagy LDAP-adatbázissal kell dolgoznod, gondold végig, hogy névteredet átirányításokkal feloszthatod-e kisebb egységekre).

A megosztott-semmi elrendezés némi odafigyelést igényel, mikor egy korábban leállított csomópontot indítunk újra: minden időközben történt változást hozzá kell adni az adatbázishoz, még mielőtt a kiesett csomópontot újra elindítjuk. Erre az esetre láthatsz majd példát a későbbiekben.

A géptelep kiépítése

Mielőtt belekezdenénk, oszlassunk el egy félreértést. A legtöbb HA (high availability – magas rendelkezésre állású) géptelep kiépítésének alapja egy üzemelésfigyelő („létfenntartó") szolgáltatás, amelyet szívhangnak (heartbeat) hívunk. Ezt a szívhangot használjuk, hogy a géptelepben található csomópontok egészségi állapotát ellenőrizzük. A Linux-HA (➲ http://www.linux-ha.org) kínál alkalmazást erre a célra, melyet – mily meglepő – Hearbeatnek hívnak. A hasonló elnevezések itt olykor félreértéshez vezethetnek, ezért a cikkben a Linux-HA csomagjára Heartbeatként hivatkozunk, az általános fogalomra pedig szívhangként.

A Linux-HA projekt 1998-ban a Linux-HA HOGYAN-ból

kifejlődve indult útjára, amit *Harald Milz* készített. A munkát jelenleg *Alan Robertso* irányítja, de a csapatnak még megannyi résztvevője van. A Hearbeat 0.4.9-es változata 2001 elején jelent meg. A Heartbeat a csomópontok állapotát vizsgálja valamilyen hálózati közvetítőn keresztül, mely leggyakrabban soros vonal vagy hálózat. Hasznos több egymástól független közvetítővel („szívhangvezetékkel") is ellátni a rendszert. A csomópontok mindegyikén fut egy Heartbeat nevű program. A főprogram olvasó és író alprogramot hoz létre minden egyes közvetítőhöz, valamint elindít egy ellenőrző alprogramot is. Ha egy csomópont kiesik, akkor a Heartbeat az indító és leállító parancsfájlokat lefuttatja a megfelelő csomóponton. A programterveknek megfelelően ezek a parancsfájlok ugyanazokat a kapcsolókat használják, mint a rendszerindító parancsfájlok (amelyek alapesetben a */etc/init.d/* könyvtárban találhatók). A mintafájlokban a fájlrendszer, a webkiszolgáló és az IP-beállítások kezelésére találunk példát.

Két LDAP-kiszolgálóval sokféle különböző kiépítés használható. Először is létrehozhatunk egy úgynevezett „készenléti" rendszert, ahol a mester (a főcsomópont) egy látszólagos IP-cím, ami egy futó kiszolgálóra mutat. Ilyenkor a másodkiszolgáló csak várakozik. Ha a főkiszolgálón hiba lép fel, a virtuális IP és a szolgáltatás átköltözik a várakozó („cold", „hideg") csomópontra. Ez egy viszonylag egyszerű kiépítés, de az adatok elosztása, és egyeztetése gondot okozhat a két csomópont között.

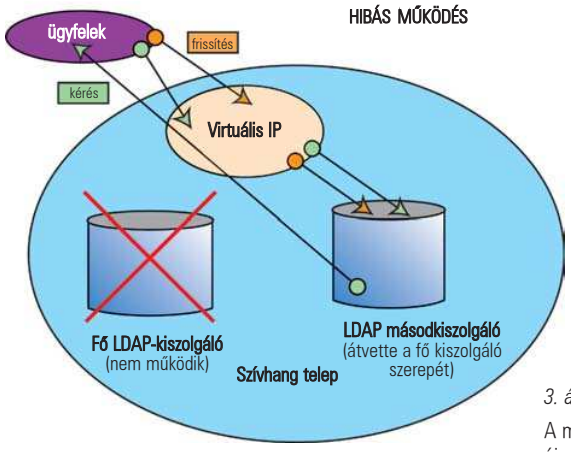
A másik lehetőség, hogy mindkét kiszolgáló „él". Ebben az esetben a főcsomópont futtatja az LDAP-kiszolgáló mesterpéldányát, míg a másodcsomópont csak egy segédpéldányt (egy „szolgát"). A mesteren elvégzett frissítések ennél a felállásnál a `slurpd` segítségével azonnal továbbítódnak a másodkiszolgálóra (*2. ábra*).

A mestergép (főcsomópont) hibája esetén a szolga teljes egészében átveheti kérések kiszolgálását, de mivel a szolgán nem végezhetünk adatfelvitelt, csak lekérdezni tudunk. Hogy teljes értékű szolgáltatásunk legyen, a másodkiszolgálón mesterpéldányként újraindítjuk az LDAP-szolgáltatást (*3. ábra*).

Ez a második felállás teljes körű LDAP-szolgáltatásokat biztosít, azonban egyetlen dologgal még mindig számolnunk kell. Ha a másodkiszolgáló adatbázisa frissül, a főkiszolgáló adatbázisát a hiba elhárítása után, még szolgálatba állítás előtt frissíteni kell.

A Hearbeat rendelkezik egy nagyszerű hibavédelmi lehetőséggel (failback), mely megakadályozza, hogy a kiesett csomópont engedély nélkül ismét erőforrásokat foglaljon le egy leállást követően. Ezt a beállítást érdemes bekapcsolni, és az újraindítást kézzel elvégezni.

A mi kiépítésünk emellett a Heartbeat által biztosított látszólagos IP (Virtual IP) szolgáltatást is használja. Ha erős terhelésre kell felkészülnünk, a látszólagos IP helyett egy IP-szórót vagy terheléselosztó rendszert is használhatunk, ami szétosztja a kéréseket a kiszolgálók között. Ebben az esetben, ha egy másodkiszolgáló adatbázisát próbáljuk módosítani, egy átirányítást (referral) kapunk vissza. Az átirányítások követése nem történik meg önműködően, azt az ügyfélprogramnak kell megvalósítania. Az elsődleges és másodlagos csomópontok ugyanúgy vannak beállítva, eltekintve a többszörözésért felelős kapcsolóktól (a Linuxvilág honlapján ➲ http://www.linuxvilag.hu/HA-LDAP – és a Linux Journal FTP-kiszolgálóján – ftp.ssc.com/pub/lj/listings/issue104/5505.tgz fájlban – elérhető). A főkiszolgáló beállításait tartalmazó állományban találjuk meg a



3. ábra
A másodkiszolgáló újraindul mesterként

többszörözés naplójának a helyét, és a másodkiszolgálók listáját, vagyis azokat a címeket, melyeknek az azonosítási adatokat tartalmazniuk kell:

```
replica host=slave5:389
binddn="cn=Manager,dc=lcc,dc=ibm,
➥dc=com";
bindmethod=simple credentials=secret
```

A másodkiszolgálók beállításai között nincs utalás a főkiszolgálóra. Ehelyett felsorolja a sokszorosításhoz szükséges követelményeket:

```
updatedn
➥"cn=Manager,dc=lcc,dc=ibm,dc=com"
```

A következő részben a Hartbeat beállításával folytatjuk cikkünket.

Linux Journal 2002. december, 104. szám

Cliff White (cliffw@osdl.org)
Az OSDL műszaki munkatársa (www.osdl.org). 1989 óta dolgozik különböző Unix- és Linux-változatokkal. Hogy biztos legyen a dolgában, minden reggel azonosítja önmagát.

Jay D. Allen (allen5@us.ibm.com)
Nappal a legújabb IT-megoldásokon dolgozik programfejlesztőként az IBM Linux for Service Providers Labnél (LSPL), ahol Linuxot használ Intelen és RS/6000-en. Éjszakánként elmaradott megoldásokkal foglalatoskodik, főként a DEC PDP-11-ével, és egyéb régiségekkel.