

## Központi, címtárszolgáltatás alapú jogosultságkezelés (2. rész)

Ki és hova jelentkezhet be? Megbízható, központi címtárral ennek szabályozása nem okozhat gondot.

**A** jogosultságkezelés az a folyamat, amelynek során eldöntjük, hogy X entitás, jellemzően egy személy, jogosult-e az Y erőforrás használatára. X vizsgálata meghatározása a hitelesítési folyamat feladata. A számítógépes hálózatokban a jogkezelés egyik lépése annak meghatározása és ellenőrzése, hogy az egyes felhasználók a hálózat mely számítógépeihez kaphatnak hozzáférést. Egyszerű példaként a számítógép `/etc/passwd` fájljában lévő `janos:x:1234:56:/home/janos:/bin/bash` sor említhető, amely a `janos` nevű felhasználónak hozzáférést ad a helyi géphez. Ha a `janos` nevű felhasználónak több számítógép használatára szeretnénk jogot adni, akkor az összes gép `/etc/passwd` fájljához hozzá kell adnunk a fenti sort.

**Linux** alatt jellemzően minden olyan felhasználó, aki jogot kap a helyi számítógépre való bejelentkezésre, helyi fiókkal rendelkezik. Ez arra is visszavezethető, hogy a felhasználóknak nemcsak bejelentkezési jogot kell kapniuk, de munkájuk elvégzéséhez további erőforrásokhoz, például a kez-dőkönyvtárakhoz is hozzá kell férniük. Ha minden számítógépen létrehozunk a megfelelő helyi fiókokat, akkor ez a kérdés megoldottnak tekinthető.

A helyi fiókokra épülő megoldással az a baj, hogy a fiókok egységessége nem biztosított. Azonos felhasználó-névhez egy másik gépen másik felhasználóazonosító és/vagy csoportazonosító tartozhat. Ennél is nagyobb gondot jelent, ha különböző gépeken két különböző fiókhöz azonos felhasználóazonosító és csoportazonosító tartozik. Lehetséges például, hogy a `janos` nevű felhasználó az 1-es számítógépen az 1234 felhasználóazonosítót és az 56 csoportazonosítót kapja, míg a `ju1ia` nevű felhasználóhoz a 2-es számítógépen ugyancsak az 1234 felhasználó- és az 56 csoportazonosító tartozik. Ez a felállás megosztott erőforrások használatakor komoly biztonsági kockázatot jelent. Például egy NFS-kiszolgáló számára a két fiók azonosnak látszik, tehát a két felhasználó akadálytalanul törölheti egymás fájljait.

A egységesség problémáján úgy lehetünk úrrá, hogy minden szükséges információt egyetlen központi hitelesítési adatforrásból veszünk, természetesen biztosítva a számítógépeknek a hozzáférést ehhez a forráshoz. A címtárszol-

gáltatások pontosan ezt a célt szolgálják. Napjainkban a két legelterjedtebb, központi hitelesítésre használt címtárszolgáltatás a **NIS** (*hálózati információk szolgáltatás, network information service*, korábban *yellow pages*, azaz *sárga oldalak*, röviden **YP** névvel futott) és az **LDAP** (*lightweight directory access protocol, egyszerű címtárelérési protokoll*).

### A NIS és az LDAP összehasonlítása

Amikor arra a kerül a sor, hogy ki kell választanunk, címtárszolgáltatásként a **NIS**-t vagy az **LDAP**-t használjuk, nem árt néhány tényezőt figyelembe vennünk. Ha cégünk már rendelkezik **LDAP**-kiszolgálóval, akkor egyszerűnek tűnik a megoldás: bővíteni kell a hitelesítési és jogkezelési adatokkal. Csakhogy a vállalati **LDAP**-kiszolgálókat általában névjegyek tárolására és hasonló, valóban egyszerű feladatokra használják. A jogkezelési adatok hozzáadása komoly terhelést róna a kiszolgálóra, hiszen a programok által indított, felhasználónév, felhasználóazonosító, csoportazonosító stb. lekérdezésére irányuló kéréseket mind meg kell válaszolnia. Általában érdemesebb egy további, kizárólag a jogkezeléssel foglalkozó **LDAP**-kiszolgálót üzembe állítani. A címtár felé irányuló lekérdezések sokszínűsége miatt a teljesítmény hangolása is rendkívül nehéz. A gyakoribb lekérdezéseket úgy gyorsíthatjuk fel, hogy az összes szükséges **LDAP** indexmegadást hozzáadjuk a `slapd.conf` fájlhoz, ám túlságosan sok indexmegadást sem célszerű hozzáadni, mert ezzel az **LDAP** adatbázisfájljainak növekedését okozzuk, ami miatt viszont újfent csökkenni fog a sebesség.

Az **LDAP** azokban a hálózatokban nyújt jobb megoldást, ahol sok **UDP**-csomag vész el, ugyanis **TCP/IP** alapú, vagyis az újraküldések elvégzését a hálózati rétegre bízta. A **NIS** ezzel szemben **UDP** feletti *távoli eljárás-hívást* (*remote procedure call, RPC*) alkalmaz. Esetében minden eldobott csomag egy válasz nélkül maradt **NIS**-lekérdezést jelent, amelyet az ügyfélnek meg kell ismételnie. Azt, hogy hálózatunkra mennyire jellemző a csomagvesztés, a `netstat -s` -u parancsot különböző gépeken, különböző időpontokban kiadva vizsgálhatjuk meg. Jó esetben a parancs csak elenyésző számú hibát jelez.

Írásomban elsősorban a *NIS*-sel foglalkozom, mivel üzembe helyezése rendkívül egyszerű, és ha elégedetlenség vagyunk vele, akkor rendkívül könnyen áttérhetünk róla az *LDAP* használatára. A *PADL Software Pty, Ltd.* több nyílt forrású, a *NIS* adatfájlok *LDAP* fájlkká alakítására alkalmas programot is készített. (Lásd az internetes forrásokat.) A teljesítményhangolás természetesen mindenképpen ránk marad. Ha *LDAP*-ról akarunk *NIS* használatára áttérni, akkor az átalakítást magunknak kell megoldanunk.

### A *NIS*-kiszolgálók beállítása

A *NIS*-kiszolgálók nem igényelnek komolyabb hardveres erőforrásokat. Gyakorlatilag bármilyen átlagos gépen futtathatók. Ugyanakkor a szolgáltatást érdemes lehet külön gépre telepíteni. Nálunk, a *Stanford Linear Accelerator Centerben (SLAC)* 500 *Linux*ot és *Solaris*ot futtató ügyfélgépet szolgálunk ki egyetlen régi *Sun Netra T1* géppel. Négy *NIS*-kiszolgáló szolgálja ki 700 *Solaris* és *Linux* alapú asztali számítógépünket, és további hat a körülbelül 2500 darab, szintén *Solaris* és *Linux* alapú számítási kiszolgálót. Az ügyfelek nem teljesen egyenletesen oszlanak el a kiszolgálók között.

### A mester kiszolgáló beállításai

Jelentkezzünk be arra a gépre, amelyre telepíteni szeretnénk a mester *NIS*-kiszolgálót, majd ellenőrizzük, hogy a legújabb portmap, ypserv és yp-tools *RPM*-ek telepítve vannak-e. Ha nem, töltsük le és telepítsük őket. Az alábbi parancsokat kivétel nélkül rootként kell kiadni. Indítsuk el a portmapper démont:

```
# service portmap start
```

A következő lépés új *NIS*-tartományunk nevének megadása. A név tetszőleges, de nyilván érdemes olyat választani, ami tükrözi cégen belüli szervezetünk, részlegünk nevét. Ha például *nis.pelda.com* a teljes *pelda.com* *NIS*-tartománya, akkor a tervezési részleghez választhatjuk a *terv.pelda.com*-ot.

A mester kiszolgálón a *NIS*-tartománynevet a következő paranccsal állíthatjuk be:

```
# domainname nis.pelda.com
```

A következő sort:

```
NISDOMAIN=nis.pelda.com
```

pedig a */etc/sysconfig/network* fájlhoz kell hozzáírunk.

A *NIS*-kiszolgáló elérhetőségét egy */var/yp/securenets* nevű, alábbi tartalmú fájl létrehozásával korlátozhatjuk:

```
# netmask      # network
255.255.255.0  192.168.0.0
```

Ez egy fontos biztonsági lépés, ne feledkezzünk meg róla! Ha ezt a fájlt nem hozzuk létre, bárki képes lesz lekérdezéseket intézni *NIS*-kiszolgálónkhoz.

Haladjunk tovább: meg kell határoznunk, milyen adatokat akarunk *NIS* alatt tárolni. Jogosultságkezelési célokra a */etc/group* és a */etc/passwd* fájl, továbbá egy netgroup nevű dolog elegendő lesz. Ennél azonban sokkal többre is van lehetőség. Ötleteket a *NIS*-kiszolgáló */var/yp/Makefile* fájljából lophatunk.

Az alábbiakban bemutatom, hogyan történik az említett három fájl *NIS* segítségével végzett terjesztésének beállítása. Módosítsuk a *NIS*-térkép adatbázisfájljait létrehozó *Makefile*-t:

```
# cp /var/yp/Makefile /var/yp/Makefile.save
# vi /var/yp/Makefile
```

Az alábbi két beállítás értékét true-ról false-ra változtatva megakadályozhatjuk a *passwd* és a *shadow*, illetve a *group* és a *gshadow* fájlok egyesítését:

```
MERGE_PASSWD=false
MERGE_GROUP=false
```

Módosítsuk a *NIS* adatforrásait tartalmazó könyvtárak nevét:

```
YPSRCDIR = /etc/NIS
YPPWDDIR = /etc/NIS
```

Azokat a fájlokat, amelyekből nem akarunk *NIS* adatbázisokat készíteni, tegyük megjegyzésbe. Én csak az alábbi hármat hagytam meg:

```
GROUP      = $(YPPWDDIR)/group
PASSWD     = $(YPPWDDIR)/passwd
NETGROUP   = $(YPSRCDIR)/netgroup
```

Az *all*: kezdetű, az összes lehetséges *NIS*-térkép listáját tartalmazó bejegyzést tegyük megjegyzésbe. Adjuk hozzá az alábbi új sort:

```
all:      passwd group netgroup
```

Ügyeljünk a tabulátorokra! A *Makefile* fájlokban a parancsok igazítására kizárólag tabulátorokat használjunk, szóközöket ne.

Hozzuk létre a *Makefile*-ban megadott adatforrás könyvtárat:

```
# mkdir /etc/NIS/
# chmod 700 /etc/NIS
```

majd helyezzünk bele egy *passwd* fájlt:

```
# grep -v '^root' /etc/passwd > /etc/NIS/passwd
```

A fájlból vegyük ki a root fiókot, valamint az összes egyéb rendszerfiókot; kizárólag a valódi felhasználói fiókokat hagyjuk meg benne.

Ha a */etc/passwd*-t még mindig használjuk titkosított jelszavakkal, akkor itt az ideje, hogy az előző cikkben (*Linuxvilág, 2005. március*) ismertetett módon áttelepít-

sük őket *Kerberos 5* alá. Ha ezt nem tesszük meg, akkor a titkosított jelszavak hozzáférhetőkké válnak, amikor a *passwd* fájlt továbbadjuk a szolga *NIS*-kiszolgálónak vagy a *NIS*-ügyfelek felé.

Gyűjtjük össze a helyi */etc/passwd* fájlokat az összes olyan gépről, mely az új *NIS*-tartomány része lesz. Távoltítsuk el belőlük a rendszerfiókokat, majd az összes fájlt másoljuk egybe:

```
% cat jelszo_1 jelszo_2 jelszo_3 ... >
↳ osszegyujtott_jelszavak
```

Az alábbi paranccsal távolítsuk el a kettős bejegyzéseket:

```
% sort osszegyujtott_jelszavak | uniq >
↳ egyedi_jelszavak
```

Ellenőrizzük a fennmaradt bejegyzések egységességét:

```
% cut -d':' -f1 egyedi_jelszavak | sort | uniq -c
↳ | \
egrep -v "\s*1"
```

Ha a parancs bármit is ad kimenetként, akkor van két különböző, de azonos fióknévvel rendelkező bejegyzésünk. Ha az eltérés nem az *UID* vagy a *GID* mezőben jelentkezik, akkor egyszerűen válasszuk ki az egyik bejegyzést, és töröljük a másikat. Ha az *UID* vagy a *GID* mező tér el, akkor fel kell oldanunk az ütközést, ami akár egészen bonyolult feladat is lehet. Végezzünk újabb ellenőrzést; van-e két azonos *UID*-vel rendelkező fiók?

Ha a:

```
% cut -d':' -f3 egyedi_jelszavak | sort | uniq -c
↳ | \
egrep -v "\s*1"
```

parancs bármilyen kimenetet is ad, akkor igen. A második kapott szám a kettős *UID*. Az ütközés feloldása ebben az esetben is fárasztó feladat lehet. Hasonló módon az összes */etc/group* fájlt is egyesítenünk kell.

A kapott fájlokat másoljuk a */etc/NIS/passwd* és a */etc/NIS/group* elérési út alá. A *netgroup* fájlt egyelőre hagyjuk ki, majd később foglalkozunk vele.

Indítsuk el a mester *NIS*-kiszolgálót:

```
# service ypserv start
```

A *NIS*-térképeket az alábbi paranccsal:

```
# /usr/lib/yp/ypinit -m
```

illetve a megjelenő utasításokat követve vehetjük használatba.

Ha a mester *NIS*-kiszolgáló számára az összes *NIS*-térkép elérhetővé akarjuk tenni, akkor ezt a gépet *NIS*-ügyfélnek is be kell állítanunk. Ellenőrizzük, hogy ez a *NIS*-ügyfél csak a mester *NIS*-kiszolgálóhoz tud-e kötni, ezzel megelőzhetjük, hogy például egy áramkimaradás után az induló gépek között körkörös függés alakuljon ki.

## A szolga kiszolgáló beállítása

A szolga *NIS*-kiszolgálók olyan *NIS*-ügyfelek, melyek a mester *NIS*-kiszolgálótól kapott térképeket továbbterjesztik a többi *NIS*-ügyfél felé. Ellenőrizzük, hogy a legújabb portmap, ypserv, ypbind és yp-tools *RPM*-ek az összes szolga kiszolgáló gépre telepítve vannak-e. Egy szolga *NIS*-kiszolgáló üzembe helyezésének első lépése az, hogy *NIS*-ügyfélként állítjuk be. Ennek módjáról a következő részben lesz szó.

Ha a *NIS*-ügyfél beállítása megtörtént, indítsuk el:

```
# service ypbind start
```

A mester *NIS*-kiszolgálón adjuk hozzá az új szolga *NIS*-kiszolgáló nevét a */var/yp/ypservers* fájlhoz, majd futtassuk le az alábbi parancsokat:

```
# cd /var/yp
# /usr/lib/yp/makedbm ypservers
/var/yp/nis.example.com/ypservers
```

A mester *NIS*-kiszolgálón a */etc/YP/Makefile* fájlban a *NOPUSH* megadást is meg kell változtatnunk, true értékről false-ra, a frissített *NIS*-térképek ugyanis csak ekkor kerülnek át a mester kiszolgálóról a szolgára vagy szolgákra.

Visszatérve az új szolga *NIS*-kiszolgálóra, elindításához a következő parancsot kell kiadnunk:

```
# /usr/lib/yp/ypinit -s nismester
```

Itt a *nismester* a mester *NIS*-kiszolgáló neve. Ennek egy teljesen minősített tartománynévnek kel lennie, feltéve, hogy *DNS*-kiszolgálónk a névkeresésekre ilyet ad vissza. A mester *NIS*-kiszolgálóról másoljuk a */var/yp/securenets* fájlt az új szolga kiszolgálóra, majd az alábbi paranccsal indítsuk el az új szolgát:

```
# service ypserv start
```

A katasztrófa utáni helyreállítás tervét ne felejtsük el frissíteni, és jelezzük benne, hogy a szolga *NIS*-kiszolgáló függ a mester *NIS*-kiszolgálótól.

## Az ügyfelek beállítása

Az összes ügyfélre telepítsük a legújabb ypbind, yp-tools és portmap *RPM*-eket. A */etc/yp.conf* fájlt írjuk át; adjuk meg benne a *NIS*-kiszolgálót:

```
ypserver nismester.pelda.com
```

A szolga kiszolgálókat külön-külön sorokban kell megadnunk. Az ügyfeleken próbáljuk véletlenszerűen felsorolni a kiszolgálókat, így a terhelést viszonylag egyenletesen tudjuk elosztani közöttük.

A */etc/sysconfig/network* fájlhoz az alábbi sort írva adjuk meg az ügyfél *NIS*-tartományát:

```
NISDOMAIN=nis.pelda.com
```

Állítsuk be a *NIS*-tartománynevet:

```
# domainname nis.pelda.com
```

Indítsuk el a portmappert:

```
# service portmap start
```

illetve a *NIS*-ügyfelet:

```
# service ypbind start
```

az összes ügyfélen.

Az `ypwhich` parancsnak most azt a *NIS*-kiszolgálót kell kiírnia, amelyhez az ügyfél kötődik.

A *NIS*-térképek tartalmát az `ypcat` paranccsal tudjuk megvizsgálni. Például:

```
% ypcat passwd
```

Következő teendők az, hogy az ügyfeleket úgy állítsuk be, hogy minden keresést *NIS* segítségével végezzenek. Ezt a névszolgáltatás-kapcsoló `/etc/nsswitch.conf` beállító fájljának módosításával érhetjük el. A `passwd`, a `group` és a `netgroup` bejegyzéseket a következőképpen kell módosítanunk:

```
passwd:      compat
group:       files nis
netgroup:    nis
```

A fentiek értelmében a *csoport (group)* kereséseket a helyi `/etc/group` fájljal kell kezdeni, majd egy *NIS*-kereséssel kell folytatni. A hálózati *csoportokat (netgroup)* kizárólag *NIS* alatt kell keresni. A `passwd` mögött álló `compat` kulcsszóról később ejtünk szót.

Megjegyezném, hogy az *nscd névszolgáltatás-gyorsítótárazó (name service caching)* démonnak időnként gondjai vannak belső gyorsítótárának frissítésével. Ennek hatásaként előfordulhat, hogy a valamelyik *NIS*-térképben végrehajtott módosítások egy-egy ügyfélen nem látszanak. Ilyenkor az egyetlen megoldás az adott gép `nscd`-jének újraindítása.

### Jellemző felhasználások

Ha *NIS* alól információkat akarunk lekérdezni, akkor két paranccsal mindenképpen érdemes megismerkednünk; az egyik az `ypcat`, a másik az `ypmatch`. Az `ypcat` végigmegegy az adott *NIS*-térkép összes kulcsán, és kiírja a benne szereplő értéket. Például az `ypcat passwd` paranccsal a `passwd` *NIS*-térkép bejegyzéseit listázhatjuk ki. Az `ypmatch` a megadott *NIS*-térképből egy vagy több kulcs értékét írja ki; az `ypmatch julia passwd` parancs például a `julia` nevű fiók `passwd` bejegyzését adja meg.

### *NIS* csoporttérkép

A *NIS* csoporttérkép jellegzetes használata a több felhasználó közötti fájlmegosztás lehetővé tétele. A megoldás helyi és *NFS*-en található fájlokkal egyaránt működik. Lássuk a beállításokat. Tegyük fel, van két felhasználónk (az eljárás

tetszőleges számú felhasználóval is működik), ők a következő bejegyzésekkel rendelkeznek a `passwd` térképben:

```
julia:*:1234:42:julia:/home/julia:/bin/bash
janos:*:5678:57:Janos:/home/janos:/bin/bash
```

A fentiek értelmében az *elsődleges* csoportazonosító `julia` esetében 42, `janos`-nál pedig 57.

A *NIS* csoporttérképpel egy további, *másodlagos* csoporttagságot is megadhatunk a fiókokhoz. A

```
tervezetX:*:127:julia,janos
```

csoportbejegyzés egy új, `tervezetX` nevű csoportot ad meg, jelszó nélkül (\*), 127-es csoportazonosítóval és két taggal.

A csoportfájlban nem lehetnek megjegyzések.

Ha most egy könyvtárra olvasási/írási/futtatási jogot adunk a `tervezetX` csoportnak:

```
# mkdir /tervezetek/X/
# chgrp tervezetX /tervezetek/X/
# chmod g+wx /tervezetek/X/
```

akkor a `tervezetX` csoport minden tagja olvasási/írási/futtatási jogot kap a könyvtár fájljaira. Lehetséges, hogy a felhasználónak először ki kell adnia a `newgrp tervezetX` parancsot. Ha hozzá kell adnunk egy fiókot egy csoporttérképhez, illetve, ha el kell távolítanunk belőle ilyet, akkor azt a mester *NIS*-kiszolgálón, a `/etc/NIS/group` fájl módosításával és a következő parancsok kiadásával tegyük meg:

```
% cd /var/yp
% sudo make group
```

Ekkor létrejön az új csoporttérkép, amelynek révén az összes ügyfél azonnal láthatja a változásokat. A módosítás elvégzéséhez az ügyfelek közelébe sem kell menni – hiszen minden központosítva van egy helyre, a *NIS*-kiszolgálóra.

### *NIS* hálózati csoportok

A *hálózati csoportok (netgroup)* teljesen eltérők a csoportoktól. A hálózati csoportok két típusra oszthatók, felhasználói és állomás hálózati csoportokra. Mindkét típusú hálózati csoport további hálózati csoportokat is tartalmazhat tagként, vagyis a hálózati csoportok hierarchiába rendezhetők. Mindkét típus megadása ugyanabban a *netgroup* fájlban történik. Ebben a fájlban megjegyzések is lehetnek. A `/etc/NIS/netgroup` fájl állomás hálózati csoport megadásai így néznek ki:

```
# Tervezetcsoporthoz csoportja:
tervezetek \
    tervezetA \
    tervezetB \
    tervezetX
# Az X tervezet állomáscsoportja
tervezetX \
    (allomas1.pelda.com,-) \
    (allomas2.pelda.com,-) \
    (allomas3.pelda.com,-)
```

A fenti állomás hálózati csoportok révén lehetővé válik, hogy például egy *NFS* tárterületet csak a munkaállomások egy részéről lehessen elérni. *NFS* kiszolgálónk */etc/exports* fájljában például a következő elérhetőségeket írhatjuk elő:

```
# a /tervezetek könyvtár elérhetővé tétele az
# összes olyan gép számára,
# amely a "tervezetek" hálózati csoportban
# található
/tervezetek @tervezetek(rw,root_squash)
# a 'tervezet x' csak azokról a gépekről
# érhető el, amelyek a "tervezetX"
# hálózati csoport
# tagjai
/tervezetek/x @tervezetX(rw,root_squash)
```

Az állomások hozzáadása a hálózati csoportokhoz, illetve kivétele belőlük az előbbihez hasonló módon a mester *NIS*-kiszolgálón található */etc/NIS/netgroup* fájl átírásával végezhető el. A *NIS*-térképet a `cd /var/yp; sudo make netgroup` parancsokkal frissíthetjük. A változások mindenhol azonnal megjelennek.

### Felhasználói hálózati csoportok

A felhasználói hálózati csoportoknak felhasználók a tagjai, szerepük elsősorban az egyes számítógépekre való bejelentkezések korlátozására terjed ki. A felhasználói hálózati csoportok megadása kicsit eltér az állomás hálózati csoportokétól:

```
# Tervezet felhasználói csoportok csoportja
u-tervezetek \
    u-tervezetA \
    u-tervezetB \
    u-tervezetX
```

```
# Az X tervezet felhasználócsoportja
u-tervezetX \
    (-,julia,) \
    (-,janos,) \
    (-,norbert,)
```

A *felhasználói (user)* hálózati csoportokat hagyományosan az *u-* előtaggal különböztetik meg az állomás hálózati csoportoktól.

A fenti definíciók birtokában a gépek helyi */etc/passwd* fájljában lévő, hasonló típusú bejegyzésekkel tudjuk engedélyezni vagy éppen tiltani a bejelentkezést az egyes gépekre. A *passwd* fájlok legvégéről vegyük ki a + jelet, ha van ilyen:

- A hozzáférés az *u-tervezetek* hálózati csoportban lévő fiókokra történő korlátozása:

```
+@u-tervezetek
```

- A hozzáférés korlátozása az *u-tervezetX* hálózati csoport tagjaira:

```
+@u-tervezetX
```

- Hozzáférés biztosítása azoknak, akik az *u-tervezetek* csoportnak tagjai, de az *u-tervezetX* csoportnak nem:

```
-@u-tervezetX
+@u-tervezetek
```

Ez esetben fontos a sorrend. Mindig az első egyezés szabja meg, hogy mi történik.

- Engedély megadása az *u-tervezetA* csoport tagjainak és a *norbert* fióknak:

```
+@u-tervezetA
+norbert
```

A *norbert* fiókkal kapcsolatos adatok (kezdőkönyvtár, bejelentkezési héj stb.) a *NIS passwd* térképből származnak. Kifejezett fiókneveket ide inkább ne helyezünk, mert ezeknek a bejegyzéseknek a kezelése nincs központosítva.

A +/- jelekre alapuló írásmód működéséhez az ügyfelek */etc/nsswitch.conf* fájljába a következő sort kell beilleszteni:

```
passwd: compat
```

### Összefoglalás

Ha a *NIS*-kiszolgáló telepítésének és a jogosultság-kezelési adatok egységesítésének gondján-baján túlestünk, a központosítással könnyebbé válik az életünk. A hálózati csoportok révén összetett, kifinomult, központi hozzáférés-vezérlést valósíthatunk meg.

*Linux Journal* 2005. március, 131. szám



**Dr. Alf Wachsmann**

1999 óta a Stanford Linear Accelerator Center (SLAC) munkatársa. Ő felelős az önműködő Linux-telepítések minden mozzanatáért, egyaránt ide értve a farmok csomópontjainak, a kiszolgálóknak és az asztali gépeknek a kezelését. Munkája során elsősorban az aktív fájlkészletek (AFS) támogatásával, a Kerberos 5-re való áttéréssel, egy felhasználónyilvántartó tervezettel és felhasználói tanácsadással foglalkozik.

### KAPCSOLÓDÓ CÍMEK

➔ [www.tldp.org/HOWTO/NIS-HOWTO/index.html](http://www.tldp.org/HOWTO/NIS-HOWTO/index.html)

➔ [www.padl.com/OSS/MigrationTools.html](http://www.padl.com/OSS/MigrationTools.html)