6

Felhasználók, biztonság és tartományok

Ebben a fejezetben arról olvashatunk, hogy miként konfigurálhatjuk a Samba kiszolgálóhoz csatlakozó felhasználókat. A feladat első hallásra egyszerűnek tűnhet, de hamarosan látni fogjuk, hogy a művelet során számos problémával kell szembenéznünk. A Samba rendszergazdáknak például komoly nehézséget okoz a felhasználók hitelesítése – a Samba levelezőlistáira a jelszavakkal és a biztonsággal kapcsolatban érkezik a legtöbb kérdés. Ha megtudjuk, hogy a különböző hitelesítő mechanizmusok hogyan működnek bizonyos architektúrákban (és másokban miért nem), akkor rengeteg időt takaríthatunk meg a Samba felhasználóinak tesztelése és a hibakeresés során.

Felhasználók és csoportok

Mielőtt még belefognánk a részletekbe, fel kell hívnunk a Samba rendszergazdák figyelmét arra, hogy ha Windows 98 vagy NT 4.0 Workstation SP3 rendszert használó ügyfelek is kapcsolódnak a kiszolgálóhoz, akkor a kiszolgálót úgy kell konfigurálniuk, hogy képes legyen titkosított jelszavak kezelésére. Ezek az operációs rendszerek ugyanis titkosított jelszavakat küldenek, és a Sambának vissza kell tudni fejtenie ezeket. Erről a konfigurálásról a fejezet későbbi részében lesz szó.

Kezdjük a feladatot egyetlen felhasználóval. Felhasználó telepítésének legegyszerűbb módja az, hogy a kiszolgálón elkészítünk a számára egy Unix fiókot (és a home könyvtárát), majd tájékoztatjuk a Sambát a felhasználó létezéséről. Az utóbbit olyan lemezmegosztás készítésével is megtehetjük, amely leképzi a felhasználó home könyvtárát a Samba konfigurációs fájlban, és az érvényes felhasználókra korlátozza az ehhez való hozzáférést. Például:

```
[dave]
        path = /home/dave
        comment = Dave home könyvtára
        writeable = yes
        valid users = dave
```

A `valid users` beállítás azokat a felhasználókat sorolja fel, akik számára engedélyezve van a megosztáshoz való hozzáférés. A példánkban ez csak a *dave* nevű felhasználó. Az előző fejezetekben a `guest ok` beállítást használva bármely felhasználónak engedélyeztük a hozzáférést. Mivel most nem ez a célunk, nem használjuk ezt a beállítást. Ha akar-

nánk, természetesen engedélyezhetnénk, hogy mind a hitelesített felhasználók, mind a vendég felhasználók hozzáférhessenek egy adott megosztáshoz. A kétféle hozzáférés közötti különbség az egyes fájlokra megadott hozzáférési jogokkal függ össze.

Emlékezzünk arra, hogy a felhasználó home könyvtárát a `%H` változóval rövidíthetjük. Emellett a Unixos felhasználónév helyett a `%u`, és/vagy az ügyfél felhasználóneve helyett a `%U` változót használhatjuk a beállításokban. Például:

```
[dave]
    comment = %U home könyvtár
    writeable = yes
    valid users = dave
    path = %H
```

A fenti példák mindaddig megfelelően működnek, amíg a Samba számára ügyfélként megjelenő Unix felhasználónak olvasási és írási hozzáférése van az elérési útban (`path`) megadott könyvtárhoz. Másként fogalmazva az ügyfélnek először át kell haladnia a Samba biztonsági mechanizmusán (titkosított jelszavak, `valid users` beállítás stb.), és meg kell felelnie a Unix oldali normál fájl- és könyvtárengedélyeknek is, mielőtt megkapná a megosztáshoz való hozzáférés olvasási/írási jogát.

Abban az esetben, ha csak egyetlen felhasználónak kell hozzáférnie egy home könyvtárhoz, a hozzáférési jogosultságok megadása akkor történik meg, amikor az operációs rendszer létrehozza a felhasználó fiókját. Ha viszont csoportelérésű megosztott könyvtárat készítünk, ennél valamivel több lépésre van szükség. Próbáljunk meg egy csoportmegosztást létrehozni az *accounting* részleg számára az *smb.conf* fájlban:

```
[accounting]
    comment = Accounting részleg könyvtára
    writeable = yes
    valid users = @account
    path = /home/samba/accounting
    create mode = 0660
    directory mode = 0770
```

Elsőként az tűnhet fel, hogy a példában a valid users (érvényes felhasználók) beállításhoz nem egy vagy több felhasználónevet, hanem az `@account` értéket rendeltük. Ez a rövidítés azt jelenti, hogy az érvényes felhasználókat a Unix `account` csoportfiókja tartalmazza. Ezeket a felhasználókat fel kell vennünk a rendszer csoportfájljában (*/etc/group*) lévő account csoportbejegyzésbe, hogy a Samba a csoport tagjainak tekinthesse őket. Miután ez megtörtént, a Samba ezeket a felhasználókat olyan érvényes felhasználóknak tekinti, akik hozzáférhetnek az adott megosztáshoz.

Ezt követően el kell készítenünk azt a megosztott könyvtárat, amelyhez a csoport tagjai hozzáférhetnek. Ezt a `path` konfigurációs beállítással tehetjük meg. Az alábbi Unix parancsokkal hozhatjuk létre az accounting részleg megosztott könyvtárát (feltételezve, hogy létezik a */home/samba* könyvtár):

```
# mkdir /home/samba/accounting
# chgrp account /home/samba/accounting
# chmod 770 /home/samba/accounting
```

Két másik beállítás is szerepel ebben az *smb.conf* példában, amellyel már találkoztunk az előző fejezetben. Ez a `create mode` és a `directory mode` beállítás, amelyek azokat a maximális fájl- és könyvtárengedélyeket határozzák meg, amelyekkel egy újonnan létrehozandó fájl vagy könyvtár rendelkezhet. Az esetünkben a megosztástól minden világi hozzáférést megtagadtunk. (Ezt a *chmod* parancs is megerősíti.)

A [homes] megosztás

Térjünk vissza egy pillanatra a felhasználói megosztásokhoz. Ha több felhasználóhoz kell létrehoznunk megosztott home könyvtárakat, akkor ehhez a 4. fejezetben megismert speciális `[homes]` megosztást használhatjuk. Ebben a megosztásban mindössze a következőket kell megadnunk:

```
[homes]
    browsable = no
    writable = yes
```

A [homes] megosztás a Samba konfigurációs fájljának egyik különleges szakasza. Ha egy ügyfél olyan normál megosztáshoz próbál hozzáférni, amely nem szerepel az *smb.conf* fájlban (például a Windows Intézőjében egy UNC-címmel megadva), a Samba egy `[homes]` megosztást fog keresni. Ha talál ilyet, akkor feltételezi, hogy a kért megosztásnév egy felhasználó neve, és lekérdezi a jelszóadatbázisát (ami az */etc/passwd* vagy egy ehhez hasonló fájlban van). Ha megtalálja a felhasználó nevét, akkor feltételezi, hogy az ügyfél unixos felhasználó, aki a saját home könyvtárához próbál meg kapcsolódni.

Példaként tegyük fel, hogy egy `sofia` nevű felhasználó megpróbál kapcsolódni a Samba kiszolgálón lévő `[sofia]` nevű megosztáshoz. A konfigurációs fájlban nincs ilyen nevű megosztás, de van benne `[homes]` megosztás, és a jelszóadatbázis is tartalmaz egy `sofia` nevű felhasználót. A Samba ekkor a következő lépéseket hajtja végre:

1. Létrehoz egy `[sofia]` nevű új lemezmegosztást a `[homes]` szakasz `path` beállításában megadott elérési úttal. Ha a `[homes]` szakaszban nincs megadva `path` beállítás, akkor létrehoz egy elérési utat a home könyvtárhoz.
2. Inicializálja az új megosztás beállításait a `[global]` szakaszban található alapértelmezett értékekkel és a `[homes]` szakasz felülbíráló értékeivel, a `browseable` beállítás kivételével.
3. A `sofia` nevű ügyfelet összekapcsolja ezzel a megosztással.

A `[homes]` megosztás gyors és kényelmes megoldást kínál a felhasználók megosztásainak létrehozásához anélkül, hogy meg kellene kettőznünk az *smb.conf* fájlban a jelszóadatbázis adatait. Van azonban néhány olyan különlegessége, amire itt ki kell térnünk:

- A `[homes]` szakasz olyan fiókokat is készíthet a gépen, amelyek nem mindig kívánatosak. Így például olyan nevekhez is létrehozhat megosztást, mint *root*, *bin*, *sys*, *uucp* és ehhez hasonlók (ez ellen a globális hatókörű `invalid users` beállítással védekezhetünk.)

- A `browseable` konfigurációs beállítás jelentése ebben a szakaszban eltér a más megosztásokban betöltött szerepétől. Itt azt jelzi, hogy csak a `[homes]` szakasz nem jelenik meg a helyi tallózólistában, és nem vonatkozik az `[alice]` megosztásra. Amikor a Samba (a kapcsolódást követően) létrehozza az `[alice]` szakaszt, a browseable beállítás értékét az adott megosztás `[global]` szakaszából és nem a `[homes]` szakaszából veszi ki.

Amint említettük, nincs szükség a path beállításra a `[homes]` szakaszban, ha a felhasználóknak Unix home könyvtáruk van a kiszolgáló */etc/passwd* fájljában. Gondoskodnunk kell azonban arról, hogy létezzen érvényes home könyvtár, mert a Samba ezt nem hozza automatikusan létre egy felhasználó számára, és megtagadja a kapcsolatot, ha nem létezne ilyen könyvtár vagy nem lenne elérhető.

Megosztások elérésének szabályozása

Biztonsági okokból gyakran korlátozni kell a felhasználókat adott megosztások elérésében. Ezt a Sambában könnyen megtehetjük, mert számos olyan beállítást bocsát a rendelkezésünkre, amelyek segítségével gyakorlatilag bármilyen biztonsági óvintézkedést megtehetünk. Lássunk néhány olyan konfigurációs beállítást, amelyet a Samba telepítésekor használhatunk.

Itt is elmondjuk, hogy azok az ügyfelek, akik Windows 98 vagy a 3-as szervizcsomaggal kiegészített NT 4.0 operációs rendszert vagy ezek újabb verzióit használva kapcsolódnak a Samba kiszolgálóhoz, titkosított jelszavakat küldenek a kiszolgálóra. Ha a Sambát nem készítjük fel az ilyen jelszavak fogadására, akkor a kiszolgáló nem hozza létre ezeket a kapcsolatokat. Ennek a fejezetnek a „Jelszavak" részében olvashatunk arról, miként konfigurálhatjuk a Sambát a titkosított jelszavak fogadásához.

Az előbb láttuk, hogy mi történik, amikor érvényes felhasználókat adunk meg. Megadhatjuk azonban az érvénytelen felhasználók listáját is – azon felhasználókat, akiknek sohasem engedélyezzük, hogy hozzáférjenek a Sambához vagy valamely megosztásához. Ezt az `invalid users` beállítás segítségével tehetjük meg. Ennek a beállításnak a gyakori használatára már korábban utaltunk a `[homes]` szakasz kapcsán: egy globális hatókörű beállítással gondoskodhatunk arról, hogy különböző rendszerhasználók és kiemelt felhasználók ne kerülhessék meg a tiltást. Például:

```
[global]
    invalid users = root bin daemon adm sync shutdown \
                    halt mail news uucp operator gopher
    auto services = dave peter bob
[homes]
    browsable = no
    writeable = yes
```

A `valid users` beállításhoz hasonlóan az `invalid users` beállításhoz is rendelhetők csoportnevek. Abban az esetben, ha egy felhasználói vagy csoportnév mindkét listában előfordul, az `invalid users` beállításnak van elsőbbsége, és az ide tartozó felhasználók vagy csoportok nem férhetnek hozzá a megosztáshoz.

Ennek ellentéteként az `admin users` beállítás segítségével kifejezetten azokat a felhasználókat is megadhatjuk, akik szuperfelhasználóként (root) férhetnek hozzá egy megosztáshoz. Tekintsük az alábbi példát:

```
[sales]
        path = /home/sales
        comment = Fiction Corp Sales Data
        writeable = yes
        valid users = tom dick harry
        admin users = mike
```

Ehhez a beállításhoz felhasználói és csoportnevek is rendelhetők. Ezen túlmenően az @ karakter előreírásával NIS hálózatcsoportokat is specifikálhatunk; ha a Samba nem talál hálózatcsoportokat, akkor azt feltételezi, hogy egy normál Unixos csoportra hivatkozunk.

Legyünk óvatosak, amikor teljes csoportnak adunk rendszergazdai privilégiumokat egy megosztás eléréséhez. A Samba fejlesztői semmiképpen sem javasolják ezt, mert ezzel az adott megosztáshoz root szintű hozzáférést engedélyezünk a specifikált felhasználók vagy csoportok részére.

Ha egy adott megosztáshoz hozzáférő felhasználók számára csak olvasási vagy olvasási és írási jogokat akarunk megadni, akkor ezt a `read list` és a `write list` beállítások segítségével tehetjük meg. Például:

```
[sales]
        path = /home/sales
        comment = Fiction Corp Sales Data
        read only = yes
        write list = tom dick
```

A `write list` beállítással nem bírálhatók felül a Unix engedélyek. Ha anélkül hoztunk volna létre egy megosztást, hogy a Unix rendszerben engedélyeztük volna a felhasználó számára az írási hozzáférést, a felhasználó nem férhet hozzá a megosztáshoz, bármi legyen is a `write list` beállítás értéke.

Vendéghozzáférés

Amint korábban szó volt róla, megadhatunk olyan felhasználókat, akik vendégként férhetnek hozzá egy megosztáshoz. A vendéghozzáférések beállításai egyszerűen használhatók. Az első beállítás, a `guest account` azt a Unix fiókot adja meg, amelyhez a vendégfelhasználók tartozni fognak, amikor kapcsolódnak a Samba kiszolgálóhoz. A beállítás az alapértelmezés szerinti értékét a Samba lefordításakor kapja meg, ami tipikusan a `nobody` (=senki). Ezt az értéket azonban módosíthatjuk például az `ftp` értékre, ha problémát okoz a különböző rendszerszolgáltatások elérése.

Ha egy megosztáshoz való hozzáférést csak a vendégekre akarjuk korlátozni – vagyis azt szeretnénk, hogy a felhasználók csak vendégként férhessenek hozzá a megosztáshoz –, akkor a `guest only` beállítást a `guest ok` beállítással együtt használhatjuk az alábbiak szerint:

```
[sales]
        path = /home/sales
        comment = Fiction Corp Sales Data
        writeable = yes
        guest ok = yes
        guest account = ftp
        guest only = yes
```

Győződjünk meg arról, hogy ebben a szereposztásban mind a `guest only`, mind a `guest ok` beállításhoz a `yes` értéket rendeltük, mert ellenkező esetben a Samba nem használná a megadott guest account fiókot.

Hozzáférést szabályozó beállítások

A megosztások elérését szabályozó beállítási lehetőségeket a 6.1. táblázat foglalja össze.

6.1. táblázat. Megosztás szintű hozzáférési beállítások

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`admin users`	Karakterlánc (felhasználónevek listája)	Azon felhasználók listáját adja meg, akik rootként végezhetnek műveleteket.	Nincs	Megosztás
`valid users`	Karakterlánc (felhasználónevek listája)	Azon felhasználók listáját adja meg, akik hozzáférhetnek egy megosztáshoz.	Nincs	Megosztás
`invalid users`	Karakterlánc (felhasználónevek listája)	Azon felhasználók listáját adja meg, akik nem férhetnek hozzá egy megosztáshoz.	Nincs	Megosztás
`read list`	Karakterlánc (felhasználónevek listája)	Azon felhasználók listáját adja meg, akik csak olvasásra férhetnek hozzá egy írható megosztáshoz.	Nincs	Megosztás
`write list`	Karakterlánc (felhasználónevek listája)	Azon felhasználók listáját adja meg, akik olvasásra és írásra férhetnek hozzá egy csak olvasható megosztáshoz.	Nincs	Megosztás
`max connections`	Numerikus	Megadja a megosztáshoz egyidejűleg létrehozható hozzáférések maximális számát.	0	Megosztás

6.1. táblázat folytatása

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`guest only` (`only guest`)	Boolean érték	Azt jelzi, hogy a megosztáshoz csak vendég férhet hozzá.	`no`	Megosztás
`guest account`	Karakterlánc (fiók neve)	Megadja a vendéghozzáféréshez használt Unix fiók nevét.	nobody	Megosztás

admin users

Ehhez a beállításhoz azon felhasználók nevét rendelhetjük, akik rootként hajthatnak végre fájlműveleteket. Ez azt jelenti, hogy az ilyen felhasználók más felhasználók munkáit módosíthatják vagy akár tönkre is tehetik, bármilyen engedélyek is tartozzanak a fájlokhoz. Az ilyen felhasználók által létrehozott fájloknak a `root` lesz a tulajdonosa, és a rendszergazdai jogú felhasználók alapértelmezés szerinti csoportja használhatja ezeket. Az `admin users` beállítás arra használható, hogy a PC-s felhasználók rendszergazdaként dolgozhassanak adott megosztásokon. Lehetőség szerint kerüljük ennek a beállításnak a használatát.

valid users és invalid users

A fenti két beállítás segítségével azokat a felhasználókat és csoportokat sorolhatjuk fel, akik, illetve amelyek számára meg akarjuk adni, illetve meg akarjuk tiltani egy adott megosztás elérését. A listában a neveket szóköz választja el, és a csoport neve elé írt @ karakterrel NIS vagy Unix csoportnevet is megadhatunk.

E két beállítás használatával kapcsolatban fontos tudnunk, hogy az `invalid users` beállításhoz rendelt lista egyetlen felhasználója vagy csoportja számára sincs engedélyezve a hozzáférés, még akkor sem, ha szerepel a nevük (bármilyen formában) a `valid users` beállítás listájában. Alapértelmezés szerint egyik beállításhoz sem tartozik lista. Ha egyik beállításhoz sincs rendelve lista, akkor bármelyik felhasználó hozzáférhet a megosztáshoz.

read list és write list

A `valid users` és az `invalid users` beállításokhoz hasonlóan ez a beállításkettős azokat a felhasználókat adja meg, akik csak olvasásra férhetnek hozzá egy írható megosztáshoz, illetve írásra és olvasásra férhetnek hozzá egy csak olvasható megosztáshoz. Mindkét beállításhoz felhasználók listája rendelhető. A `read list` beállítás a Samba által megadott összes engedélyt felülbírálja, akárcsak a kiszolgáló rendszerén a Unix fájlengedélyeket, vagyis megtagadja a felhasználóktól az írási jogot. A `write list` beállítás felülbírálja a Samba által írásra megadott engedélyeket, de nem adhat írási engedélyt, ha a felhasználónak a Unix rendszeren nincs joga írni a fájlba. A listában a csoport neve elé írt @ karakterrel NIS vagy Unix csoportneveket is megadhatunk (mint például `@users`). Alapértelmezés szerint egyik beállításhoz sem tartozik lista.

max connections

Ezzel a beállítással azon felhasználók maximális számát adhatjuk meg, akik egyidejűleg kapcsolódhatnak egy megosztáshoz. Ha a kapcsolódások száma eléri az itt megadott számot, a Samba az újabb kérelmeket elutasítja. A beállításhoz alapértelmezés szerint a 0 érték tartozik, ami azt jelenti, hogy a kapcsolatok száma nincs korlátozva. Ezt az értéket az alábbiak szerint módosíthatjuk:

```
[accounting]
    max connections = 30
```

Ennek a beállításnak akkor vehetjük a hasznát, ha korlátozni akarjuk egy licencprogramot vagy egy adathalmazt egyidejűleg használó felhasználók számát.

guest only

Ez a megosztás szintű beállítás (amit esetenként az `only guest` alakban is használnak) a `guest account` beállításban megadott felhasználói fiókhoz létrehozandó kapcsolatot kényszeríti ki. A megosztásba kifejezetten be kell venni a `guest ok = yes` beállítást, hogy a Samba észlelje a fiókot. A `guest only` beállításhoz alapértelmezés szerint a `no` érték tartozik.

guest account

Ez a beállítás annak a fióknak a nevét adja meg, amelyet a Sambában a vendégek használnak a megosztások eléréséhez. A beállításhoz tartozó alapértelmezett érték rendszerről rendszerre változó, de gyakran a `nobody` (=senki) az értéke. Egyes alapértelmezés szerinti felhasználói fiókoknak problémáik vannak a vendégfelhasználóként való hozzáférésekkel. Ha ilyen problémák lépnének fel a rendszerünkben, akkor a Samba fejlesztői azt javasolják, hogy az ftp fióknevet használjuk a vendégfelhasználók fióknéveként.

Felhasználói nevek beállításai

A 6.2. táblázat két olyan beállítást mutat be, amelyek segítségével a Samba kijavíthatja a Windows és a Unix rendszerekben használt felhasználónevek közötti eltéréseket.

6.2. táblázat. Felhasználói nevek beállítási lehetőségei

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`username map`	Karakterlánc (teljes elérési út)	Megadja a felhasználónevet leképező fájl nevét.	Nincs	Globális
`username level`	Numerikus	Megadja a felhasználónév illesztése során használható nagybetűk számát.	0	Globális

username map

Amíg egy SMB hálózaton a felhasználói nevek viszonylag hosszúak lehetnek (max. 255 karakter), addig a unixos hálózatok általában nyolc karakternél hosszabb neveket nem tesznek lehetővé. Ez azt jelenti, hogy egy felhasználónak az ügyfélgépen hosszabb, a Samba kiszolgálón pedig rövidebb (másik) neve lehet. Ezen a problémán úgy segíthetünk, hogy a nagyobb szabadsággal megválasztható ügyfélnevet egy nyolc vagy ennél kevesebb karakterből álló unixos névnek feleltetjük meg, és a megfeleltetéseket normál, szöveges fájlban tároljuk. A megfeleltetések formátumára rövidesen kitérünk. Ezt követően a globális hatókörű `username map` beállításban megadjuk a fájl elérési útját. Korlátozzuk ennek a fájlnak az elérhetőségét: tegyük a rootfelhasználót a fájl tulajdonosává, és mindenki más számára tiltsuk meg a fájl elérését. Ha nem tennénk így, akkor egy meghatalmazás nélküli felhasználó, aki hozzáférne a fájlhoz, könnyen leképezhetné a felhasználónevét a Samba rootfelhasználói nevére.

A beállítást az alábbi módon használhatjuk:

```
[global]
    username map = /etc/samba/usermap.txt
```

A felhasználónevek megfeleltetését tartalmazó fájlban az egyes bejegyzéseknek a következő formátumúaknak kell lenniük: Unix felhasználói név, utána egy egyenlőségjel (=), amit egy vagy több szóközzel elválasztva követnek az SMB ügyfél felhasználói nevek. Jegyezzük meg, hogy ha nem intézkedünk másként (vagyis ha nem vendégkapcsolatról van szó), akkor a Samba mind az ügyfél, mind a kiszolgálói felhasználónévhez ugyanazt a jelszót várja. Az @ karakter segítségével NT csoportokat is megfeleltethetünk egy vagy több Unix csoportnak. Néhány példa a fentiekre:

```
jarwin = JosephArwin
manderso = MarkAnderson
users = @account
```

Egy bejegyzésben csillag (*) karakterrel jelölhetünk olyan megfeleltetést, amely bármilyen ügyfél felhasználói nevet jelenthet:

```
nobody = *
```

A fájlban létra (#) vagy pontosvessző (;) karakterekkel kezdődő sorokban helyezhetünk el megjegyzéseket.

Jegyezzük meg, hogy ezt a fájlt arra is használhatjuk, hogy egy Unix felhasználót másik Unix felhasználóra irányítsunk át. Legyünk azonban óvatosak ezzel, mert előfordulhat, hogy a Samba és az ügyfelünk nem értesíti arról a felhasználót, hogy át lett irányítva, és a Samba más jelszót várhat tőle.

username level

Az SMB ügyfelek (például a Windows ügyfelek) az SMB kapcsolatkéréseik során a felhasználói nevüket gyakran csupa nagybetűs alakban küldik el, vagyis nem különböztetik meg feltétlenül a kis- és a nagybetűket. Egy Unix kiszolgáló viszont különbséget tesz közöttük:

az ANDY felhasználói nevet nem tekinti azonosnak az andy névvel. Alapbeállítás szerint a Samba a következőképpen hidalja át ezt a problémát:

1. Az ügyfél által küldött névvel pontosan egyező név alapján megkeresi a felhasználó fiókját.
2. Megvizsgálja a felhasználónevet csupa kisbetűs alakban.
3. Megvizsgálja a felhasználónevet úgy, hogy csak az első betűjét alakítja át nagybetűsre.

A globális hatókörű `username level` beállítás segítségével további nagy- és kisbetűs kombinációk vizsgálatát is előírhatjuk a Samba számára. A beállításhoz egész értékeket rendelhetünk, amelyek azt mondják meg, hogy a felhasználói névben hány betűt kell nagybetűs alakra átalakítani, amikor egy felhasználó hozzá akar férni egy megosztáshoz. A beállítást a következő módon használhatjuk:

```
[global]
    username level = 3
```

A fenti példában a Samba a felhasználóneveken minden olyan permutációt elvégez, ami három nagybetűvel végrehajtható. Minél nagyobb ez a szám, annál több számítást kell végeznie a Sambának, és annál tovább tart a hitelesítés.

Hitelesítési biztonság

Ezen a ponton elérkeztünk oda, hogy megvizsgáljuk, miként hitelesíti a Samba a felhasználókat. A felhasználónak minden olyan megosztásra irányuló kapcsolatkérés esetén, amely nem engedélyezi a vendéghozzáférést, el kell küldenie egy jelszót, hogy létrejöhessen a kapcsolat. A `security` beállítás megfelelő használatával írhatjuk elő, hogy mit kezdjen a Samba a jelszóval, és milyen hitelesítési stratégiát alkalmazzon a megfelelő biztonság eléréséhez. Jelenleg a Samba négy különböző szinten támogatja a hálózati biztonságot: megosztási, felhasználói, kiszolgálói és tartományi szinten.

Megosztás szintű biztonság
: A munkacsoportban minden egyes megosztáshoz egy vagy több jelszó tartozik. Bárki, aki ismer egy érvényes jelszót, hozzáférhet az adott megosztáshoz.

Felhasználói szintű biztonság
: A munkacsoport megosztásai úgy vannak konfigurálva, hogy bizonyos felhasználóknak engedélyezzék a megosztások elérését. A Samba kiszolgáló ellenőrzi a felhasználókat és a jelszavukat arra vonatkozóan, hogy hozzáférhetnek-e az adott megosztáshoz.

Kiszolgálói szintű biztonság
: Ez azonos a felhasználói szintű biztonsággal azzal a kivétellel, hogy a Samba külön SMB kiszolgálót használ a felhasználók és a jelszavak érvényesítésére, mielőtt engedélyezné adott megosztások elérését.

Tartomány szintű biztonság

A Samba egy Windows tartomány tagjává válik, és a tartomány elsődleges tartományvezérlőjét (PDC) használja a hitelesítés elvégzéséhez. Miután megtörtént a hitelesítés, a felhasználó egy speciális „tokent" kap, ami lehetővé teszi számára, hogy hozzáférjen azokhoz a megosztásokhoz, amelyekre ez a token feljogosítja. Miután a felhasználó a token birtokába jutott, az elsődleges tartományvezérlő nem vizsgálja újra a felhasználó jelszavát minden olyan alkalommal, amikor a tartományon belül más megosztásokhoz akar hozzáférni.

Ezek a biztonsággal kapcsolatos „házirendek" a globális `security` beállítás segítségével valósíthatók meg (lásd a 6.3. táblázatot).

6.3. táblázat. Biztonsági beállítások

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`security`	`domain`, `server`, `share` vagy `user`	A Samba kiszolgáló által használt biztonsági szintet jelzi.	`user` (Samba 2.0) vagy `share` (Samba 1.9)	Globális

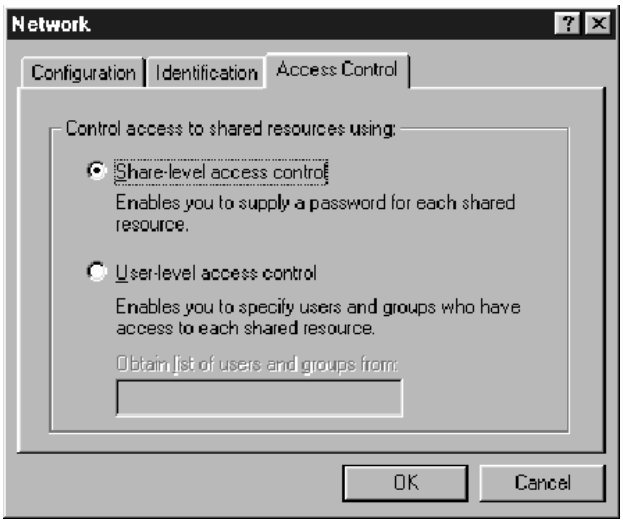
Megosztás szintű biztonság

Megosztás szintű biztonság alkalmazásakor minden egyes megosztáshoz egy vagy több jelszó tartozik. A biztonságnak ez a típusa annyiban különbözik a biztonság többi típusától, hogy a megosztáshoz való hozzáférés nem valamely felhasználóhoz vagy felhasználókhoz kapcsolódik. Bárki, aki ismeri a jelszót, hozzáférhet a megosztáshoz. A megosztásokhoz gyakran több jelszó is tartozik. Így például az egyik jelszó csak olvasható hozzáférést engedélyez, míg egy másik az írási engedélyt is megadja, és így tovább. A biztonság mindaddig garantált, amíg jogosulatlan felhasználók nem jutnak a számukra tiltott megosztások jelszavának birtokába.

Mind az OS/2, mind a Windows 95/98 támogatja az erőforrásaira vonatkozó, megosztás szintű biztonságot. Windows 95/98-as rendszerben a Hálózat párbeszédablak Hozzáférési jogok lapján a Megosztásszintű hozzáférés választógomb bekapcsolásával állíthatjuk be a megosztás szintű biztonságot (lásd a 6.1. ábrát). Miután bekapcsoltuk ezt a választógombot, kattintsunk az OK gombra.

Ezt követően kattintsunk az egér jobb oldali gombjával valamelyik erőforrásra, például a merevlemezre vagy a CD-ROM meghajtóra. Ekkor megnyílik az Erőforrás tulajdonságok párbeszédablak. Válasszuk a Megosztás lapot, és kapcsoljuk be a Megosztva az alábbi néven feliratú választógombot. Ekkor megadhatjuk, hogy az erőforrás milyen néven jelenjen meg az egyes felhasználók számára, milyen hozzáférési jogok tartozzanak a megosztáshoz (csak olvasásra, teljes, jelszótól függő), és mi legyen a jelszó.

Ha valaki azt gondolná, hogy ez a biztonsági modell nem kellőképpen jó a Samba kiszolgálón, annak igaza van. Csakugyan, ha a Samba konfigurációs fájljában a `security = share` beállítást alkalmaznánk, a Samba a rendszer jelszófájljaiban újra használná a fel-



6.1. ábra. Megosztás szintű biztonság választása Windows rendszerben

használónév/jelszó kombinációt egy hozzáférés hitelesítéséhez. Közelebbről nézve a Samba az alábbi lépéseket végzi el, amikor egy ügyfél kapcsolatot akar létrehozni egy megosztás szintű biztonsággal védett megosztáshoz:

1. A kapcsolatfelvétel kérésekor a Samba fogadja a felhasználó jelszavát és (amennyiben elküldésre került) a nevét.
2. Ha a megosztás `guest only` (vagyis csak vendégek férhetnek hozzá), a Samba azonnal elérhetővé teszi a felhasználó számára a megosztást a `guest account` beállításban megadott jogokkal, és nem vizsgálja a jelszavát.
3. A többi megosztást illetően a Samba a felhasználó nevét felveszi azon felhasználók listájába, akik hozzáférhetnek a megosztáshoz. Csak ezt követően vizsgálja a felhasználónévvel együtt megadott jelszót. Ha érvényesnek találja, engedélyezi a megosztás elérését a felhasználóhoz rendelt jogokkal. A felhasználót nem kell újra hitelesíteni, hacsak nem szerepel a megosztáson belül a `revalidate = yes` beállítás.
4. Ha nem sikerült a hitelesítés, a Samba megpróbálja azon felhasználók szerint érvényesíteni a jelszót, akiket a korábbi kapcsolatok létrehozásakor már lefordított magának, vagy akik a konfigurációs fájlban az illető megosztásban megadásra kerültek. Ha a jelszó egyik felhasználónévhez sem tartozik (a neveket a rendszer jelszófájlja, tipikusan az */etc/passwd* tartalmazza), a felhasználó ezen a felhasználói néven nem kap engedélyt a megosztás elérésére.
5. Ha viszont a megosztáshoz engedélyezett a `guest ok` vagy a `public` beállítás, a felhasználó hozzáférhet a megosztáshoz a `guest account` (vendégfiók) beállításhoz megadott jogokkal.

A `username` beállítás segítségével megadhatjuk, hogy induláskor mely felhasználók kerüljenek be azon felhasználók listájába, akikre a megosztás szintű biztonság vonatkozik:

```
[global]
    security = share
[accounting1]
    path = /home/samba/accounting1
    guest ok = no
    writable = yes
    username = davecb, pkelly, andyo
```

Ha a fenti beállításnak megfelelően egy felhasználó megpróbál kapcsolódni egy megosztáshoz, akkor a Samba a küldött jelszót megvizsgálja az egyes felhasználók szerint a saját listájában, majd a `davecb`, `pkelly`, és az `andyo` felhasználók jelszava szerint. Ha bármelyik helyen egyezőséget talál, elfogadja a kapcsolatkérést, és engedélyezi a felhasználónak a hozzáférést. Ellenkező esetben sikertelen az adott megosztás elérése.

A megosztás szintű biztonság beállításai

A 6.4. táblázat a megosztás szintű biztonság tipikus beállításait sorolja fel.

6.4. táblázat. A megosztás szintű biztonság beállításai

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`only user`	Boolean érték	Azt jelzi, hogy csak a `username` beállításban megadott felhasználónevek fogadhatók el.	`no`	Megosztás
`username` (felhasználó vagy felhasználók)	Karakterlánc (felhasználónevek listája)	Megadja azon felhasználók listáját, akik szerint egy ügyfél jelszavát meg kell vizsgálni.	Nincs	Megosztás

only user

Ez a kétféle értéket felvehető beállítás azt határozza meg, hogy a Samba a megosztás szintű biztonságot használva csak azon felhasználóknak engedélyezze-e egy megosztás elérését, akik a `username` beállításban vannak felsorolva, vagy azoknak, akiket a belső listájába lefordított. A beállításhoz alapértelmezés szerint a `no` érték tartozik, amit azonban egy megosztásban felülbírálhatunk:

```
[global]
    security = share
[data]
    username = andy, peter, valerie
    only user = yes
```

username

Ehhez a beállításhoz azon felhasználók listája tartozik, akiknek a Samba megvizsgálja a jelszavát, amikor kapcsolódni akarnak egy megosztáshoz. Ezt tipikusan azon ügyfelekhez használják, akikre megosztás szintű biztonság vonatkozik annak érdekében, hogy egy minősítő jelszó alapján férhessenek hozzá egy adott megosztáshoz – ebben az esetben a jelszó egy adott felhasználóhoz tartozó jelszóval egyezik meg:

```
[global]
    security = share
[data]
    username = andy, peter, terry
```

Ez a beállítás nem javasolható, hacsak nem megosztás szintű biztonsággal akarjuk felépíteni a Samba kiszolgálónkat.

Felhasználói szintű biztonság

A Samba rendszer konfigurálásakor ez az előnyben részesítendő biztonsági szint. Ezt a mechanizmust használva az egyes megosztások adott felhasználókhoz vannak rendelve, akik hozzáférhetnek ezekhez a megosztásokhoz. Amikor egy felhasználó kapcsolódni próbál egy megosztáshoz, a Samba úgy végzi el a hitelesítését, hogy a megadott felhasználónevet és jelszót összeveti a konfigurációs fájlban megadott meghatalmazott felhasználókkal és a Samba kiszolgálón lévő jelszóadatbázisban tárolt jelszavakkal. Amint a fejezet elején említettük, az egyes megosztásokhoz alkalmazott `valid users` beállítás segítségével különíthetjük el azokat a felhasználókat, akik számára engedélyezett egy adott megosztás elérése:

```
[global]
    security = user
[accounting1]
    writable = yes
    valid users = bob, joe, sandy
```

A listában megadott mindegyik felhasználó kapcsolódhat a megosztáshoz, ha a jelszava megegyezik a kiszolgálón a jelszóadatbázisban tárolt jelszóval. Ha az induláskor sikeres volt a hitelesítés, akkor a felhasználónak nem kell újra megadnia a jeszavát, ha újra hozzá akar férni a megosztáshoz, hacsak nem tartalmazza a megosztás a `revalidate = yes` beállítást.

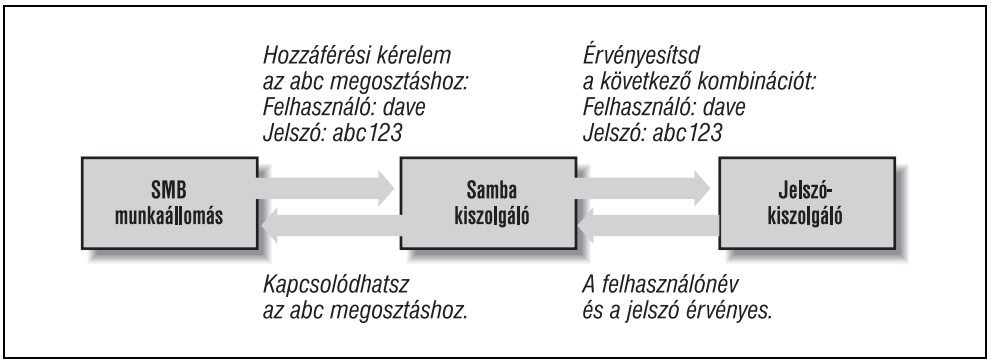
A jelszavak titkosítva és titkosítás nélkül is elküldhetők a Samba kiszolgálóra. Ha a hálózatunkban mindkét típusú rendszer egyidejűleg létezik, akkor biztosítanunk kell, hogy az egyes felhasználókhoz tartozó jelszavak a hagyományos adatbázisban és a Samba titkosított jelszóadatbázisában is meglegyenek. Ilyen módon a meghatalmazott felhasználók bármilyen típusú ügyfélként hozzáférhetnek a megosztásaikhoz.* Ha viszont fontos

* Az, hogy a hálózatunkban titkosított és nem titkosított jelszavakat is használó ügyfelek lehetnek, ugyancsak oka annak, hogy a Samba miért teszi lehetővé olyan beállítások felvételét a konfigurációs fájljába, amelyek változókat használnak az ügyfél operációs rendszerek azonosításához.

szempont a biztonság, akkor az javasolható, hogy titkosított jelszavakhoz konfiguráljuk a rendszerünket, és ne engedélyezzük a titkosítás nélkülieket. A fejezet „Jelszavak" részében olvashatunk arról, miként használhatunk mind titkosított, mind titkosítás nélküli jelszavakat.

Kiszolgálói szintű biztonság

A kiszolgálói szintű biztonság hasonló a felhasználói szintű biztonsághoz. A különbség az, hogy kiszolgálói szintű biztonság alkalmazásakor a Samba a jelszavak hitelesítését egy másik SMB jelszó-kiszolgálóra, tipikusan egy, a hálózatban elsődleges tartományvezérlőként működő Samba vagy Windows NT Server gépre bízza. Jegyezzük azonban meg, hogy a Samba az *smb.conf* fájljában továbbra is vezet listát a megosztásairól és azok beállításairól. Amikor egy ügyfél kapcsolatot próbál létrehozni egy megosztáshoz, a Samba megvizsgálja, hogy az ügyfél valóban jogosult-e a megosztás elérésére. Ezt követően a Samba egy ismert protokollon keresztül kapcsolatba lép az SMB jelszó-kiszolgálóval, és megkísérli annál is hitelesíteni a jelszót. Ha ez utóbbi kiszolgáló elfogadja a jelszót, akkor létrejön az ügyféllel a kapcsolat. A kapcsolat felépülését a 6.2. ábra szemlélteti.



6.2. ábra. Egy kapcsolat tipikus felépülése kiszolgálói szintű biztonság mellett

Kiszolgálói szintű biztonság esetén a globális hatókörű `password server` beállítással konfigurálhatjuk a Samba kiszolgálót külön jelszó-kiszolgáló használatához az alábbiak szerint:

```
[global]
    security = server
    password server = PHOENIX120 HYDRA134
```

Figyeljük meg, hogy egynél több gépet is megadhatunk jelszó-kiszolgálóként; ha a Samba nem tudja elérni az elsőként megadott kiszolgálót, akkor a listában utána következőhöz fordul. A jelszó-kiszolgálókat a NetBIOS nevük, és nem a DNS nevük vagy az ezeknek megfelelő IP címek azonosítják. Ha a felsorolt kiszolgálók mindegyike visszautasítja a jelszót, a kapcsolatkérés automatikusan elutasításra kerül – a Samba más kiszolgálókat nem keres meg.

Egy hiányosság: hiába használjuk ezt a beállítást, a Samba kiszolgálón továbbra is kell léteznie egy, a felhasználóhoz tartozó fióknak. Ennek az az oka, hogy a Unix operációs rendszernek szüksége van a felhasználónévre a különböző Be/Ki műveletek végrehajtásához. A probléma úgy kerülhető meg, hogy a Samba kiszolgálón ugyan létrehozunk a felhasználóhoz egy fiókot, de a fiókhoz tartozó jelszót letiltjuk azzal, hogy a rendszer jelszófájljában (*/etc/passwd*) a jelszót egy csillag (*) karakterrel helyettesítjük.

Tartomány szintű biztonság

A tartomány szintű biztonság hasonló a kiszolgálói szintű biztonsághoz. A fő különbség az, hogy tartomány szintű biztonság alkalmazásakor a Samba kiszolgáló egy Windows tartomány tagjaként szerepel. Emlékezzünk vissza az 1. fejezetre, ahol arról olvashattunk, hogy minden tartományban kell lennie legalább egy *tartományvezérlőnek* (ez általában egy Windows NT kiszolgáló), amely elvégzi a jelszavak hitelesítését. E tartományvezérlők mellett a munkacsoportban kell lennie még egy kinevezett jelszó-kiszolgálónak is. A tartományvezérlők a saját hitelesítő moduljukban (SAM, security authentication module) kísérik figyelemmel a felhasználókat és a jelszavaikat, és hitelesítik az egyes felhasználókat, amikor első alkalommal jelentkeznek be, és kísérlik meg a kapcsolódást egy másik gép megosztásaihoz.

Amint a fejezet korábbi részében már említettük, a Samba hasonló módon képes felhasználói szintű biztonságot nyújtani, csakhogy ez a Unixra épül, és abból indul ki, hogy a hitelesítést a Unix jelszófájljai végzik el. Ha a Unix gép egy NIS vagy egy NIS+ tartomány tagja, akkor a Samba a felhasználók hitelesítését megosztott jelszófájlok számára is átláthatóvá teszi. Ekkor a Samba engedélyezi, hogy Windowsból is elérhető legyen a NIS vagy a NIS+ tartomány. Természetesen semmiféle összefüggés sincs a között, hogy miként kezeli a NIS és miként a Windows a tartományait.

Tartomány szintű biztonság alkalmazása esetén lehetőségünk van az NT saját, belső védelmi mechanizmusának használatára. Ez többféle előnnyel jár:

- Lényegesen szorosabb integrációt tesz lehetővé az NT rendszerrel: a Windows legtöbb szolgáltatásához képest kevesebb trükköt kell használni az *smb.conf* fájlban a tartományok kezeléséhez. Ennek köszönhetően nagyobb mértékben használhatók az NT olyan kezelőeszközei, mint a tartományok felhasználói kezelője (User manager for Domains), ami lehetővé teszi, hogy a felhasználók a Samba kiszolgálókat nagy NT gépekként kezelhessék.
- A magasabb fokú integráltság olyan protokollokat is magával hoz, amelyek lehetővé teszik a Samba fejlesztőinek az NT megvalósítások követését. Az NT 4-es szervizcsomagja kijavítja a protokoll különböző hibáit, és az integráltságból adódóan a Samba is könnyebben alkalmazkodhat az ilyen módosításokhoz.
- Kevesebb adminisztráció terheli az elsődleges tartományvezérlőt, mert eggyel kevesebb állandó kapcsolatot kell fenntartania a Samba kiszolgálóval. A Samba a `security = server` beállításban megadott protokolltól eltérően csak akkor hajthat végre távoli hívást (Remote Procedure Call, RPC), ha hitelesítési információra van szüksége. Csak ebből a célból nem tarthat fenn állandó kapcsolatot.
- Az NT tartományi hitelesítő mechanizmusa a felhasználó összes jellemzőit visszaküldi, nem csak azt, hogy sikeres vagy sikertelen volt-e a hozzáférési kísérlet. A visszaküldött jellemzők a Unix azonosító és az NT csoportok bővebb változatait, valamint más adatokat is tartalmaznak a következők szerint:

  - felhasználónév;
  - teljes név;
  - leírás;
  - biztonsági azonosító (a Unix uid tartomány méretű kiterjesztése);
  - NT csoporttagság;
  - bejelentkezési órák és tájékoztatás arról, hogy azonnal ki kell-e kényszeríteni a felhasználó kijelentkezését;
  - a felhasználó számára engedélyezett munkaállomások;
  - a fiók lejáratának dátuma;
  - home könyvtár;
  - bejelentkezési szkript;
  - profil;
  - fiók típusa.
- A Samba fejlesztői tartomány szintű biztonságot használtak a Samba 2.0.4-es verziójában tartományi felhasználók félautomatikus felvételéhez és törléséhez. Emellett ez a biztonság helyet biztosít más, olyan NT-szerű kiegészítésekhez is, mint a hozzáférésvezérlő listák és a fájlengedélyek ügyfelek általi módosításának támogatása.

Ez a megközelítés azzal az előnnyel jár, hogy kevesebb az adminisztráció: mindössze egyetlen hitelesítő adatbázist kell szinkronizálni. A Samba kiszolgálónak helyileg csak annyi adminisztrációs feladatot kell elvégeznie, hogy létrehozza a felhasználók számára azokat a könyvtárakat, amelyekben majd dolgozni fognak, és elkészítse az */etc/passwd* fájlban a felhasználói azonosítójukat és csoportjaikat.

Samba kiszolgáló felvétele Windows NT tartományba

Ha már létrehoztunk egy NT tartományt, könnyen felvehetünk bele Samba kiszolgálót. Először is le kell állítanunk a Samba démonjait. Ezt követően a „Windows NT Server Manager for Domains" (Windows NT kiszolgáló tartománykezelője) eszköz segítségével fel kell vennünk a Samba kiszolgálót az elsődleges tartományvezérlőn (PDC) lévő NT tartományba. Amikor kérdést kapunk a számítógép típusára vonatkozóan, válasszuk a „Windows NT Workstation or Server" (Windows NT munkaállomás vagy kiszolgáló) lehetőséget, és adjuk meg a Samba kiszolgáló NetBIOS nevét. Ezzel létrehozzuk a Samba gép fiókját az NT kiszolgálón.

Következő lépésként az *smbpasswd* parancs segítségével generáljunk a géphez egy Microsoft formátumú jelszót (az eszköz használatára rövidesen kitérünk). Ha például a tartományunknak SIMPLE a neve, és az elsődleges tartományvezérlő szerepét betöltő Windows NT gépnek `beowulf` a neve, a Samba kiszolgálón az alábbi parancs kiadásával végezhetjük el a név generálását:

```
smbpasswd -j SIMPLE -r beowulf
```

Végül vegyük fel az *smb.conf* fájl `[global]` szakaszába akövetkező beállításokat, és indítsuk újra a Samba démonjait.

```
[global]
    security = domain
    domain logins = yes
    workgroup = SIMPLE
    password server = beowulf
```

Ezzel a Sambát tartomány szintű biztonsággal konfiguráltuk. A tartományi bejelentkezési beállításokról a fejezet későbbi részében lesz bővebben szó.

Jelszavak

A jelszavak meglehetősen komoly problémát okoznak a Sambában. A Samba telepítésekor általában ez jelenti az első jelentősebb nehézséget, és a Sambát támogató levelezőcsoportok is ezekkel kapcsolatban kapják a legtöbb kérdést. A korábbi fejezetekben azzal kerültük meg ezt a problémát, hogy a konfigurációs fájlokban a `guest ok` beállítást használtuk, ami lehetővé teszi a hitelesítés nélküli kapcsolódást. Most azonban elérkeztünk ahhoz a ponthoz, ahol már részletesebben foglalkoznunk kell a jelszavakkal, és meg kell vizsgálnunk, hogyan használhatók ezek a hálózatban.

Az ügyfelek által küldött jelszavak titkosítottak vagy titkosítás nélküliek lehetnek. A titkosított jelszavak természetesen jóval biztonságosabbak. A nem titkosított jelszó könnyen elolvasható egy hálózatfigyelő programmal, mint amilyen például a módosított *tcpdump*, amit a 3. fejezetben már használtunk. A Samba kiszolgálóhoz csatlakozó gépen futó operációs rendszer határozza meg azt, hogy titkosított-e a jelszó. A 6.5. táblázat felsorolja azokat a Windows operációs rendszereket, amelyek titkosítják a jelszavakat, mielőtt még hitelesítés céljából elküldenék őket az elsődleges tartományvezérlőre. Ha az ügyfelünk gépén nem Windows operációs rendszer fut, akkor a rendszer dokumentációjából tudhatjuk meg, hogy titkosítja-e az SMB jelszavakat.

6.5. táblázat. Jelszótitkosító Windows operációs rendszerek

Operációs rendszer	Titkosított vagy nem titkosított
Windows 95	Nem titkosított
Windows 95 SMB frissítéssel	Titkosított
Windows 98	Titkosított
Windows NT 3.x	Nem titkosított
Windows NT 4.0 a 3-as szervizcsomag előtt	Nem titkosított
Windows NT 4.0 a 3-as szervizcsomag után	Titkosított

Az operációs rendszerek kétféle titkosítási eljárást használnak: a Windows 95 és 98 rendszerek a LAN Manager hálózati szoftverből örökölt eljárással titkosítják a jelszavakat, míg a Windows NT rendszerek ennél újabb titkosító rendszerrel dolgoznak.

Ha az operációs rendszer támogatja a jelszótitkosítást, akkor a Samba a titkosított jelszavakat egy *smbpasswd* nevű fájlban tárolja. Alapbeállítás szerint ez a fájl a Samba disztribúció *private* nevű könyvtárában van (*/usr/local/samba/private*). Ezzel egyidejűleg az ügy-

fél gép is tárolja a jelszó titkosított változatát. A jelszót a maga normál, titkosítatlan formájában sohasem tárolja egyik rendszer sem. Mindkét rendszer automatikusan titkosítja a jelszót egy ismert algoritmus szerint a jelszó létrehozásakor vagy módosításakor.

Amikor egy ügyfél olyan SMB kiszolgálóval akarja felvenni a kapcsolatot, amelyik támogatja a titkosított jelszavakat (mint például a Samba vagy a Windows NT), a két számítógép az alábbi egyeztetést végzi:

1. Az ügyfél kéri a kiszolgálótól a protokoll egyeztetését.
2. A kiszolgáló jelzi a használandó protokollt, és közli, hogy támogatja a titkosított jelszavakat. Ezzel egyidejűleg elküld egy véletlenszerűen generált 8 bájtos karakterláncot.
3. Az ügyfél ezt a karakterláncot használja az általa korábban már titkosított jelszó titkosításához – ehhez a második titkosításhoz az egyeztetett protokollban előírt algoritmust használja. Az eredményt visszaküldi a kiszolgálónak.
4. A kiszolgáló ugyanezt a műveletet elvégzi az adatbázisában tárolt, titkosított jelszón is. Ha a két művelet azonos eredménnyel zárul, akkor a két jelszó azonos, és megtörtént az ügyfél hitelesítése.

Jegyezzük meg, hogy ugyan az eredeti jelszót nem használja a hitelesítő művelet, nagyon kell vigyáznunk arra, hogy az *smbpasswd* fájlban tárolt titkosított jelszóhoz se férhessenek hozzá illetéktelenek. Ha nem lennénk eléggé óvatosak, egy jogosulatlan felhasználó az előző algoritmust végrehajtva betörhet a rendszerünkbe. A titkosított jelszavak pontosan olyan érzékeny adatoknak számítnak, mint a titkosítatlanok. Természetesen arról is gondoskodni kell, hogy az ügyfelek is megvédjék a titkosítatlan jelszavaikat illetéktelenekkel szemben.

A Sambát azzal készíthetjük fel titkosított jelszavak fogadására, hogy az *smb.conf* fájlba felvesszük az alábbi, globális hatókörű kiegészítéseket. Figyeljük meg, hogy kifejezetten megadtuk a Samba jelszófájljának a helyét:

```
[global]
    security = user
    encrypt passwords = yes
    smb passwd file = /usr/local/samba/private/smbpasswd
```

Ahhoz azonban, hogy a Samba fogadni tudja a titkosított jelszavakat, még inicializálni kell az *smbpasswd* fájlt.

Titkosított jelszavak tiltása az ügyfélnél

Bár a Unix már hosszú ideje használja a hitelesítést, beleértve a *telnet* és az *rlogin* internetes hozzáféréseket is, a művelet jól ismert biztonsági kockázatokat rejt magában. A jelszavakat az eredeti alakjukban küldi el az interneten keresztül, és rosszindulatú emberek az elfogott TCP csomagokból kideríthetik ezeket. Ha viszont úgy gondoljuk, hogy biztonságos a hálózatunk, és az összes ügyfelünknél a Unix standard */etc/passwd* hitelesítését akarjuk használni, akkor azon Windows ügyfeleinknél, akik alapértelmezés szerint titkosított jelszavak használnának, meg kell tiltanunk az ilyenek használatát.

Ennek érdekében egy fájl telepítésével módosítanunk kell a Windows regisztrációs adatbázisát. Az illető operációs rendszertől függően ez a fájl vagy az *NT4_PlainPassword.reg*, vagy a *Win95_PlainPassword.reg* fájl. A telepítést úgy végezhetjük el, hogy a

Samba disztribúció */docs* könyvtárából a megfelelő *.reg* fájlt átmásoljuk egy hajlékonylemezre, majd az ügyfél gépén a Start menüben a Futtatás parancsot választjuk. Érdekesség, hogy a Windows 95 *.reg* fájlja Windows 98-as rendszerben is működik.

A számítógép újraindítását követően az ügyfél jelszava nem lesz titkosítva mielőtt elküldésre kerülne a kiszolgálóra. Ez azt jelenti, hogy a hálózatba szétküldött TCP csomagok a jelszót az eredeti alakjában fogják tartalmazni. Éppen ezért ez az eljárás nem javasolható, hacsak nem vagyunk abszolút meggyőződve a rendszerünk biztonságáról.

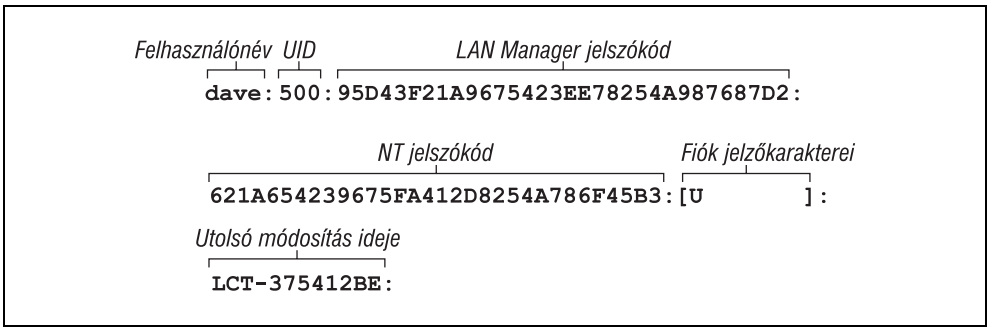
A Samba konfigurációs fájljában az alábbi módon jelezhetjük, hogy nem titkosított jelszavakkal dolgozunk:

```
[global]
    security = user
    encrypt passwords = no
```

Az smbpasswd fájl

A Samba a titkosított jelszavakat az *smbpasswd* nevű fájlban tárolja, amely alapbeállítás szerint a */usr/local/samba/private* könyvtárban található. Ezt a fájlt legalább annyira védenünk kell, mint a *passwd* fájlt; olyan könyvtárban kell tartanunk, amelyhez csak rootfelhasználónak van olvasási/írási hozzáférési joga. Minden más felhasználótól még az olvasási jogot is meg kell vonni.

Mielőtt használhatnánk a titkosított jelszavakat, az *smbpasswd* fájlban minden egyes Unix felhasználóhoz el kell készítenünk egy bejegyzést. A fájl nagyjából hasonló felépítésű, mint a Unix *passwd* fájlja, de attól eltérőek a mezői. A 6.3. ábra szemlélteti az *smbpasswd* fájl szerkezetét, a benne látható bejegyzés a fájl egyik sora.



6.3. ábra. Az smbpasswd fájl szerkezete (a fájl egyik sora)

Az egyes mezők jelentése:

Felhasználónév
: A fiókhoz tartozó felhasználó neve. Közvetlenül a rendszer jelszófájljából másolódik ide.

UID

A fiókhoz tartozó felhasználó azonosítója. A felhasználónévhez hasonlóan ez is közvetlenül a rendszer jelszófájljából származik, és meg kell egyeznie az ott tárolt azonosítóval.

LAN Manager jelszókód

Ez a 32 bites hexadecimális jelsorozat képviseli a Windows 95/98 ügyfél jelszavát. A jelsorozat a `KGS!@#$%` karakterlánc 56 bites DES algoritmussal való titkosításával jött létre, kulcsként kétszer a felhasználó jelszavát használva (az első 14 bájt alapján, nagybetűkre alakítva). Ha a felhasználóhoz nem tartozik jelszó, akkor a kód első 11 karakterhelyén a `NO PASSWORD` szöveg, a többin pedig X karakterek állnak. A megosztáshoz jelszó nélkül, bárki hozzáférhet. Ha viszont nem engedélyezzük jelszó használatát, akkor az összes karakterhelyen az X karakter áll. A Samba nem engedélyezi a jelszó nélküli hozzáférést a felhasználóknak, hacsak nem tartalmazza a konfigurációs fájlja a `null passwords` beállítást.

NT jelszókód

Ez a 32 bites hexadecimális jelsorozat képviseli a Windows NT ügyfél jelszavát. A jelsorozat a jelszó MD4 eljárással történő kódolásával jön létre (a jelszót 16 bites little-endian Unicode sorozat alkotja). A jelszó betűi előzőleg nem alakulnak át nagybetűsre.

Fiók jelzőkarakterei

Ez a mező 11 karakterből áll (beleértve a kezdő és a lezáró szögletes zárójelet). A zárójelek között az alábbi karakterek bármelyike állhat tetszőleges sorrendben. A nem használt karakterek helyén szóközök állnak.

U Normál felhasználói fiók.

D Ezt a fiókot tiltja a Samba, és semmilyen bejelentkezést nem fogad el hozzá.

N Ehhez a fiókhoz nem tartozik jelszó.

W Egy munkaállomás meghatalmazott fiókja, amelyről a Samba elsődleges tartományvezérlőként konfigurálható, ha Windows NT gépek kapcsolódhatnak a tartományához.

Utolsó módosítás ideje

A mező a `LCT` (Last Change Time) karaktereket, és az 1970. január 1-je óta a bejegyzés utolsó módosításig eltelt, másodpercekben mért időtartamot tartalmazza hexadecimális alakban.

Bejegyzések felvétele a smbpasswd fájlba

Többféle módon is felvehetünk bejegyzéseket az *smbpasswd* fájlba:

- Az *smbpasswd* programot az `-a` kapcsolóval futtatva automatikusan felvehetünk olyan felhasználót, akinek standard Unix rendszerfiókja van a kiszolgálón. A program a */usr/local/samba/bin* könyvtárban található.
- A */usr/local/samba/bin* könyvtárban lévő *addtosmbpass* programot is futtathatjuk. Ez egyébként egy egyszerű *awk* szkript, amely elemzi a rendszer jelszófájlját, majd kiveszi a felhasználónevet és az azonosítót azokból a bejegyzésekből, amelyeket fel akarunk

venni az SMB jelszófájlba. Ezt követően a felhasználói bejegyzések többi mezőjébe elhelyezi az alapbeállításokat, melyeket a későbbiekben az *smbpasswd* program segítségével megváltoztathatunk. Ahhoz, hogy használni tudjuk ezt a programot, esetleg szerkesztenünk kell a fájl első sorát, hogy létrejöjjön a rendszerünkben az *awk* szkriptre mutató hivatkozás.

- Abban az esetben, ha a fenti eljárások egyike sem lenne használható, kézzel is elkészíthetünk egy alapértelmezés szerinti bejegyzést az *smbpasswd* fájlban. A bejegyzés például az alábbihoz hasonló lehet (a mezőket kettősponttal kell egymástól elválasztani):

  ```
  dave:500:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:XXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXX:[U]:LCT-00000000:
  ```

  A bejegyzés a felhasználónevet és az azonosítót tartalmazza a rendszer jelszófájljának megfelelően, ami után két, egyenként pontosan 32 X karakterből álló mező következik. Az utána következő két mező a fiók jelzőkaraktereit, illetve az utolsó módosítás idejét tartalmazza. Miután elkészítettük ezt a bejegyzést, az *smbpasswd* program futtatásával meg kell változtatnunk ennek a felhasználónak a jelszavát.

Titkosított jelszó módosítása

Ugyancsak az *smbpasswd* programot kell futtatnunk akkor is, ha módosítanunk kell egy titkosított jelszót. Figyeljünk arra, hogy ennek a programnak ugyanaz a neve, mint a titkosított jelszófájlé, ezért legyünk óvatosak, és ne keverjük össze a jelszófájlt a jelszómódosító programmal.

Az *smbpasswd* program majdnem azonos azzal a *passwd* nevű programmal, amelyet Unix jelszavak módosításához használhatunk. A program egyszerűen bekéri a régi jelszót (hacsak nem rootfelhasználók vagyunk), és létrehozza az eredeti bejegyzés másolatát az új jelszóval. A képernyőn egyik jelszó sem jelenik meg.

```
# smbpasswd dave
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user dave
```

Miután lefutott a program, ellenőrizhetjük az *smbpasswd* fájlban, hogy a jelszó LAN Manager és NT kódja a megfelelő helyre került. Azt követően, hogy a felhasználók titkosított jelszava ilyen módon bekerült az adatbázisba, a felhasználók a titkosított jelszavukat használhatják a megosztások eléréséhez.

A jelszó szinkronizálása

A jelszavak módosításakor problémát jelenthet, ha ugyanannak a jelszónak a normál és a titkosított alakja is létezik. Szerencsére a Samba ad némileg korlátozott segítséget a jelszavak szinkronizálásához. Két olyan beállítási lehetőséget nyújt, amelyek segítségével automatikusan frissíthetjük a normál unixos jelszót, ha módosul a rendszerben a titkosított jelszó. Ezt a képességét a globális hatókörű `unix password sync` beállítással vehetjük igénybe:

```
[global]
    encrypt passwords = yes
    smb passwd file = /usr/local/samba/private/smbpasswd

    unix password sync = yes
```

Ha a `yes` értéket rendeljük ehhez a beállításhoz, akkor a Samba (rootként) megváltoztatja a felhasználó normál jelszavát, amikor az *smbpasswd* programmal módosítjuk a titkosított jelszavát. Ahhoz azonban, hogy ez sikerüljön, még két másik feladatot is el kell végeznünk.

A könnyebbet a `passwd` program segítségével oldhatjuk meg. Ez a program azt a Unix parancsot adja meg, amelyet a felhasználó normál rendszerjelszavának módosításához használunk. Alapbeállítás szerint ez a `/bin/passwd %u` parancs. Egyes Unix rendszerekben ez megfelelő, és semmit sem kell változtatni rajta. Más esetben, például a Red Hat Linux rendszerben ehelyett a */usr/bin/passwd* parancsot kell használni. Az is lehetséges, hogy a jövőben másik programot vagy szkriptet kell futtatni a feladat elvégzéséhez. Példaként tegyük fel, hogy egy `changepass` nevű szkriptet akarunk futtatni egy felhasználó jelszavának módosításához. Emlékezzünk arra, hogy az aktuális Unix felhasználó neve helyett a `%u` változót használhatjuk. Ekkor így alakul a példánk:

```
[global]
    encrypt passwords = yes
    smb passwd file = /usr/local/samba/private/smbpasswd

    unix password sync = yes
    passwd program = changepass %u
```

Figyeljük meg, hogy a programot rootfelhasználóként kell meghívni, ha a `unix password sync` beállításhoz a `yes` érték tartozik. Erre azért van szükség, mert a Samba nem feltétlenül ismeri a felhasználó régi, titkosítatlan jelszavát.

A nehezebb feladat a `passwd chat` beállítás konfigurálása. A `passwd chat` beállítás hasonlóan működik, mint egy Unix *chat* (beszélgetős) szkript. Kiküld egy sor karakterláncot, valamint kiküldi azokat a válaszokat is, amelyeket a `passwd program` beállításban megadott programtól vár. Az alábbi részlet a `passwd chat` beállítás alapértelmezés szerinti alakjára mutat példát. Az egyes karaktercsoportokat szóközök választják el egymástól:

```
passwd chat = *old*password* %o\n *new*password* %n\n *new*password*
%n\n *changed*
```

Az első karaktercsoport a jelszómódosító programtól várt választ jelenti. Figyeljük meg, hogy helyettesítő karaktereket (*) tartalmaz, hogy segítse a programot a hasonló kifejezések megtalálásában is. Itt a `*old*password*` sorozat azt jelzi, hogy a Samba minden olyan sort elfogad a jelszóprogramtól, amelyben előfordul az `old` és a `password` szó, bármi álljon is a két szó előtt, között és után. Ha nem érkezik válasz, sikertelen lesz a jelszómódosító művelet.

A második karaktercsoport azt jelzi, amit a Samba kiküld abban az esetben, ha az első csoportnak sikerült egyezőséget találnia. A példánkban a második csoport a `%o\n` karak-

tersorozat. Ez tulajdonképpen két választ jelent: a `%o` a régi jelszót képviseli, míg a `\n` az újsor karakter. Lényegében az történik, hogy a karaktercsoport „begépeli" a régi jelszót a jelszómódosító program bemenetére, majd „lenyomja" az Enter billentyűt.

A második karaktercsoportot ismét egy válaszcsoport követi, ami után a jelszómódosító programnak visszaküldendő adatok következnek. (Az ilyen válasz/küldés mintát követő sorozatok végtelen sorban követhetik egymást bármelyik normál Unix beszélgetős szkriptben.) A szkript futása mindaddig tart, amíg megtörténik az utolsó minta egyeztetése.*

A jelszóprogram által küldött válasz karakterláncok egyeztetését a 6.6. táblázatban felsorolt karakterek használatával segíthetjük. A 6.7. táblázatban felsorolt karaktereket a válasz kialakításához használhatjuk.

6.6. táblázat. Az egyeztetést segítő karakterek

Karakter	Jelentés
*	Bármely karakter egyszeri vagy többszöri előfordulása.
" "	Lehetővé teszi olyan karakterláncok egyeztetését is, amelyekben szóközök vannak. A csillagok akkor is helyettesítő karaktert jelentenek, ha idézőjelek között vannak, és két, egymást követő idézőjellel üres választ jelezhetünk.

6.7. táblázat. A válaszban használható karakterek

Karakter	Jelentés
`%o`	A felhasználó régi jelszava
`%n`	A felhasználó új jelszava
`\n`	Soremelés karakter
`\r`	Kocsivissza karakter
`\t`	Tabulátor karakter
`\s`	Szóköz

A `passwd chat` beállítást például az alábbiak szerint módosíthatjuk. Ez olyan esetekben használható, amikor nem kell beírnunk a régi jelszót. Emellett a Red Hat Linux által kiküldött `all tokens updated successfully` üzenetet is kezeli.

```
passwd chat = *new password* %n\n *new password* %n\n *success*
```

Megismételjük, hogy az alapértelmezés szerinti chat szkript a legtöbb Unix rendszerben jól működik. Ha nem így lenne, akkor a `passwd chat debug` beállítás segítségével új chat szkriptet készíthetünk a jelszómódosító programhoz. A `passwd chat debug` beállítás a jelszómódosítás során bekövetkező minden eseményt naplóz. A beállítás a Boolean értékek valamelyikét veheti fel:

* Ez nem igaz a Red Hat Linux rendszerre, mert abban a jelszóprogram a „Password changed" helyett az „All authentication tokens updated successfully" üzenetet küldi. A fejezet későbbi részében kitérünk ennek a hibának a kijavítására.

```
[global]
    encrypted passwords = yes
    smb passwd file = /usr/local/samba/private/smbpasswd

    unix password sync = yes
    passwd chat debug = yes
    log level = 100
```

Miután engedélyeztük a `passwd chat debug` beállítást, a Samba által a beszélgetős szkripten keresztül vett Be/Ki műveletek 100-as hibakeresési szinttel bekerülnek a Samba naplófájljaiba. Mivel ez a szint gyakran nagyon sok naplófájlt készít, hatékonyabb lehet, ha saját szkriptet használunk, és a `passwd program` beállításban a */bin/passwd* helyett ezt adjuk meg a módosítások során bekövetkezett események rögzítéséhez. A naplófájlokat is szigorú engedélyekkel védjük meg, és mihelyt megkaptuk a szükséges információkat, azonnal töröljük őket – ugyanis ezek a normál alakjukban tartalmazhatják a jelszavakat.

A Sambát futtató operációs rendszerek szigorú követelményeket támaszthatnak az érvényes jelszavakkal szemben, hogy érzéketlenebbek legyenek a szótári és ehhez hasonló támadásokkal szemben. A felhasználóknak is tisztában kell lenniük az ilyen korlátozásokkal, amikor módosítják a jelszavukat.

A korábbiakban említettük, hogy a Samba korlátozott mértékben segíti a jelszavak szinkronizálását. Ennek az az oka, hogy nem létezik a titkosított *smbpasswd* fájl fordított szinkronizálása arra az esetre, amikor egy felhasználó frissíti a normál unixos jelszavát. Bár ismertek különböző stratégiák ennek megkerülésére, így például a NIS és más ingyen hozzáférhető, beépíthető hitelesítő modulok (PAM), de a problémát igazából egyikük sem oldja meg. A Windows 2000 megjelenésével várhatóan nagyobb lesz az összhang a LDAP (Lightweight Directory Access Protocol) protokollal, ami remélhetőleg fölöslegessé teszi a jelszavak szinkronizálását.

A jelszó beállítási lehetőségei

A 6.8. táblázatban felsorolt beállítási lehetőségek abban segíthetnek, hogy miként dolgozzunk a jelszavakkal a Sambában.

6.8. táblázat. A jelszó beállítási lehetőségei

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`encrypt passwords`	Boolean érték	Bekapcsolja a titkosított jelszavakat.	`no`	Globális
`unix password sync`	Boolean érték	Ha `yes` az értéke, a Samba frissíti a standard Unix jelszóadatbázist, amikor egy felhasználó módosítja a titkosított jelszavát.	`no`	Globális
`passwd chat`	Karakterlánc (chat parancsok)	Megadja azon parancsok sorozatát, amelyeket ki kell küldeni a jelszóprogramnak.	Lásd a beállítással kapcsolatos korábbi részeket.	Globális

6.8. táblázat folytatása

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`passwd chat debug`	Boolean érték	Jelszómódosítással kapcsolatos bejegyzéseket készít a naplófájlokba 100-as hibakeresési szinttel.	`no`	Globális
`passwd program`	Karakterlánc (Unix program)	Megadja a jelszómódosításhoz használandó programot.	`/bin/passwd %u`	Globális
`password level`	Numerikus	Megadja azon nagybetűk számát, amelyeken permutációt kell végezni egy ügyfél jelszavának egyeztetéséhez.	Nincs	Globális
`update encrypted`	Boolean érték	Ha `yes` az értéke, a Samba frissíti a titkosított jelszófájlját, amikor egy felhasználó a normál jelszavát használva akar hozzáférni egy megosztáshoz.	`no`	Globális
`null passwords`	Boolean érték	Ha `yes` az értéke, a Samba engedélyezi a null jelszavú felhasználóknak a hozzáférést.	`no`	Globális
`smb passwd file`	Karakterlánc (teljes elérési út)	Megadja a titkosított jelszófájl nevét.	`/usr/local/samba/private/smbpasswd`	Globális
`hosts equiv`	Karakterlánc (teljes elérési út)	Megadja annak a fájlnak a nevét, amely a jelszó használata nélkül kapcsolódható gazdákat és felhasználókat tartalmazza.	Nincs	Globális
`use rhosts`	Karakterlánc (teljes elérési út)	Megadja annak az .rhosts fájlnak a nevét, amely lehetővé teszi a felhasználóknak a jelszó nélküli kapcsolódást.	Nincs	Globális

unix password sync

A globális hatókörű `unix password sync` beállítás lehetővé teszi, hogy a Samba frissítse a standard Unix jelszófájlját, amikor egy felhasználó módosítja a titkosított jelszavát. A Samba kiszolgáló a titkosított jelszót az *smbpasswd* fájlban tárolja, amely alapbeállítás szerint a */usr/local/samba/private* könyvtárban van. A Sambának ezt a képességét a beállítás bekapcsolásával aktivizálhatjuk:

```
[global]
    unix password sync = yes
```

Ha engedélyezzük ezt a beállítást, akkor a Samba amellett, hogy módosítja a titkosított jelszót, a standard unixos jelszó módosítását is megkísérli. Ezt úgy teszi meg, hogy a `passwd program` beállításban (lásd korábban) megadott programnak átadja a felhasználónevet és az új jelszót. Ne feledjük, hogy a Samba nem fér hozzá feltétlenül a felhasználó normál (titkosítás nélküli) jelszavához, ezért rootként kell meghívnia a jelszómódosító programot.* Ha bármilyen oknál fogva meghiúsul a unixos jelszó módosítása, az SMB jelszó sem módosul.

encrypt passwords

A globális hatókörű `encrypt passwords` beállítás segítségével a Sambát a normál jelszó alapján történő hitelesítésről a titkosított jelszó alapján történő hitelesítésre kapcsolhatjuk át. Ha a beállításhoz a `yes` értéket rendeljük, akkor a Samba titkosított jelszót vár az ügyfeleitől.

```
encrypt passwords = yes
```

Alapbeállítás szerint a Windows NT 4.0 a 3-as szervizcsomaggal és e fölött, valamint a Windows 98 titkosított jelszavakat küld ki a hálózatra. Ha engedélyezzük a titkosított jelszavakat, léteznie kell egy érvényes *smbpasswd* fájlnak, amelynek tartalmaznia kell a titkosított jelszavak hitelesítéséhez használt felhasználóneveket (lásd a fejezet *„Az smbpasswd fájl”* című részét). Emellett a Sambának ismernie kell az *smbpasswd* fájl helyét is, ha az nem az alapértelmezés szerinti helyén van (ez tipikusan a */usr/local/samba/private/smbpasswd*). A fájl helyét az `smb passwd file` beállítással adhatjuk meg.

Ha akarjuk, az `update encrypted` beállítás segítségével ki is kényszeríthetjük, hogy a Samba mindannyiszor frissítse a titkosított jelszavakkal az *smbpasswd* fájlt, amikor egy ügyfél nem titkosított jelszóval akar kapcsolódni.

Ha biztosítani akarjuk, hogy azok a gazdák, akiknek titkosított jelszóhitelesítésre van szükségük, valóban így is legyenek hitelesítve, akkor vegyünk fel egy `include` beállítást. Ezzel a beállítással egyedi konfigurációs fájlokat készíthetünk, amelyek aszerint kerülnek beolvasásra, hogy a kapcsolódó fél számítógépe milyen operációs rendszert használ (`%a`), vagy mi a gép neve (`%m`). Az ilyen rendszer- vagy gazdaspecifikus konfigurációs fájlokba bevehetjük az `encrypted passwords = yes` beállítást, ami csak akkor lép érvénybe, ha ilyen ügyfelek kapcsolódnak a kiszolgálóhoz.

passwd program

A `passwd program` beállítás segítségével a Unix alatt futó Samba kiszolgálón azt a programot adhatjuk meg, amelyet a Samba a rendszer standard jelszófájljának frissítéséhez használhat, amikor frissítődik a titkosított jelszófájl. A beállításhoz alapértelmezés szerint a standard *passwd* program tartozik, ami általában a */bin* könyvtárban található. A beállításban tipikusan a `%u` képviseli a felhasználót a parancs végrehajtásakor. A program bemenetét és kimenetét a program végrehajtása során a `passwd chat` beállításban megadott szkript kezeli. Ezzel a beállítással bővebben a fejezet *„A jelszó szinkronizálása”* részében foglalkoztunk.

* Ennek az az oka, hogy a Unix *passwd* programja, amely általában ennek a műveletnek a célpontja, megszorítások nélkül engedélyezi a `root` hozzáférést a felhasználó jelszavának módosításához.

passwd chat

Ehhez a beállításhoz a Unix *chat* (beszélgetős) szkriptjeihez hasonlóan küldött és visszaküldött karakterláncok sorozatát adhatjuk meg, amelyet a Samba kiszolgálón futó jelszómódosító program használhat. Ezzel a beállítással is a fejezet *„A jelszó szinkronizálása"* részében foglalkoztunk bővebben.

passwd chat debug

Ha ehhez a beállításhoz a `yes` értéket rendeljük, akkor a globális hatókörű `passwd chat debug` beállítás naplózza azokat az üzeneteket, amelyeket a Samba a jelszóról folytatott párbeszéd során küldött vagy kapott. A beérkező és kimenő üzenetek 100-as hibakeresési szinttel a Samba naplófájljaiba kerülnek. Meg kell adnunk a `log level = 100` beállítást, ha azt akarjuk, hogy rögzítésre kerüljenek az információk. A fejezet korábbi, *„A jelszó szinkronizálása"* részében bővebben foglalkoztunk ezzel a beállítással. Ha használjuk ezt a beállítást, akkor legyünk tisztában azzal, hogy a hibakereső naplófájlokban megjelenhetnek a jelszavak a normál, titkosítatlan alakjukban, és ez potenciális veszélyt jelent, ha nem védjük meg a naplófájlokat.

password level

Az SMB rendszerek a nem titkosított (vagyis az eredeti alakjuk szerinti) jelszavakat – akárcsak a felhasználóneveket – nagybetűsre alakítva küldik el. Számos unixos felhasználó viszont vegyesen használja a kis- és nagybetűket a jelszavában. A Samba alapbeállítás szerint teljes egészükben kisbetűk szerint végzi el a jelszavak egyeztetését, és nem változtatja nagybetűsre a jelszó első karakterét.

A `username level` beállításhoz hasonlóan van egy `password level` beállítás is, amit arra használhatunk, hogy nagybetűkkel különböző permutációkat végezzünk a jelszavakon. A beállításhoz egész érték rendelhető, amely előírja, hogy a jelszóban hány betűt kell nagybetűsre alakítani, amikor a jelszó tulajdonosa kapcsolódni próbál egy megosztáshoz. A beállítást a következő módon használhatjuk:

```
[global]
    password level = 3
```

Ebben az esetben a Samba három nagybetűs karakterrel végzi el az összes lehetséges permutációt. Minél nagyobb ez a szám, annál több számítást kell végeznie a Sambának a jelszó egyezőségére vonatkozóan, és annál tovább tart egy adott megosztáshoz való kapcsolódás engedélyezése.

update encrypted

A Samba ezzel a beállítással segíti az átmenetet azokon a helyeken, ahol az ügyfelek át akarnak térni a titkosított jelszó használatára. Az `update encrypted` beállítás megkönnyíti a normál jelszó titkosított jelszóvá történő átalakítását. A beállítást az alábbi módon kapcsolhatjuk be:

```
[global]
    update encrypted = yes
```

Ez a beállítás arra utasítja a Sambát, hogy az *smbpassw* fájlban hozza létre mindegyik felhasználó unixos jelszavának titkosított alakját, amikor az illető kapcsolódik egy megosztáshoz. Ha engedélyezzük a beállítást, akkor az `encrypt passwords` beállításhoz a `no` értéket kell rendelnünk, hogy a felhasználók a normál alakú jelszavukat küldjék a Sambára a fájlok frissítése érdekében. Miután már mindegyik felhasználó legalább egyszer kapcsolódott a kiszolgálóhoz, ismét a `yes` értéket rendelhetjük az `encrypt passwords` beállításhoz, hogy a későbbiekben már csak a titkosított jelszavakat engedélyezzük. Ekkorra már létrejöttek a felhasználók érvényes bejegyzései az *smbpasswd* fájlban.

null passwords

Ez a globális hatókörű beállítás arról tájékoztatja a Sambát, hogy engedélyezett-e a hozzáférés azon felhasználók számára, akiknek null jelszavú (titkos vagy titkosítatlan) a fiókjuk. A beállításhoz alapértelmezés szerint a `no` érték tartozik, amit azonban a következő szerint felülírhatunk:

```
null passwords = yes
```

Ennek a beállításnak a használata csak azok számára ajánlott, akik tisztában vannak a vele együtt járó biztonsági kockázatokkal; beleértve a rendszer jelszófájljában lévő azon rendszerhasználók véletlen elérését is, akiknek null a jelszavuk.

smb passwd file

Ezzel a globális hatókörű beállítással a titkosított jelszavakat tartalmazó adatbázis helye adható meg. Alapbeállítás szerint ez a */usr/local/samba/private/smbpasswd*, de meg is változtatható:

```
[global]
    smb passwd file = /etc/smbpasswd
```

Különböző változatok, például a Red Hat számos disztribúciója is ezt a helyet használja.

hosts equiv

Ez az ugyancsak globális hatókörű beállítás annak a standard Unix *hosts.equiv* fájlnak a nevét adja meg, amely azon gazdák és felhasználók nevét tartalmazza, akik jelszó megadása nélkül férhetnek hozzá a megosztásokhoz. A fájl helyét a következő módon adhatjuk meg:

```
[global]
    hosts equiv = /etc/hosts.equiv
```

Alapértelmezés szerint a beállításhoz semmilyen fájlnév sem tartozik. Mivel egy ilyen fájl használata óriási kockázatot jelent, semmiképpen sem javasolható a beállítás felvétele, hacsak nem tartjuk teljesen biztonságosnak a hálózatunkat.

use rhosts

Ez a globális hatókörű beállítás annak a standard unixos felhasználói *.rhost* fájlnak a nevét adja meg, amely a megosztásokhoz jelszó megadása nélkül hozzáférhető idegen gazdákat tartalmazza. A fájl helyét a következő módon adhatjuk meg:

```
[global]
    use rhosts = /home/dave/.rhosts
```

Alapértelmezés szerint a beállításhoz semmilyen fájlnév sem tartozik. Akárcsak az előbb említett *hosts equiv*, az *.rhost* fájl is biztonsági kockázatot jelent, ezért ezt a beállítást is csak akkor használjuk, ha tökéletesen megbízunk a hálózatunkban.

Windows tartományok

Most, hogy már megismerkedtünk a Samba kiszolgálóhoz kapcsolódó felhasználókkal és a kiszolgálón használható jelszavakkal, tekintsük át, miként konfigurálhatjuk úgy a kiszolgálót, hogy elsődleges tartományvezérlő (PDC) lehessen Windows 95/98 és Windows NT gépek számára. Miért van szükség egyáltalán tartományokra? Ahhoz, hogy erre egyértelmű választ adhassunk – főként a Windows 95/98 esetében –, be kell pillantanunk a kuliszszák mögé.

Emlékezzünk arra, hogy egy hagyományos munkacsoportban a Windows 95/98 egyszerűen elfogadja a rendszerbe bejelentkezők nevét és jelszavát. A Windows 95/98 rendszerben egyszerűen nem léteznek jogosulatlan felhasználók: ha bejelentkezik egy új felhasználó, az operációs rendszer megkérdezi a jelszavát, és ettől kezdve ezzel a jelszóval tartja nyilván. A Windows 95/98 csak akkor igényli a jelszó használatát, ha a felhasználó másik megosztáshoz akar kapcsolódni.

Ezzel szemben a tartományi bejelentkezések a Unix rendszerekben szokásos bejelentkezésekhez hasonlóak. Ahhoz, hogy valaki bejelentkezhessen egy tartományba, eleve rendelkeznie kell érvényes felhasználónévvel és jelszóval, amit a rendszer az elsődleges tartományvezérlőn tárolt jelszóadatbázis alapján hitelesít. Ha a jelszó érvénytelen, a rendszer tájékoztatja erről a felhasználót, és nem engedi belépni a tartományba.

Ha viszont érvényes a jelszó, a felhasználó beléphet a tartományba, és azon belül bármely olyan megosztáshoz hozzáférhet, amihez joga van anélkül, hogy újra hitelesíttetnie kellene magát. Pontosabban fogalmazva az elsődleges tartományvezérlő visszaküld a sikeres bejelentkezőnek egy tokent, amellyel bármely megosztást elérheti anélkül, hogy engedélyt kellene kérnie az elsődleges tartományvezérlőtől. Lehet ugyan, hogy ez első hallásra nem tűnik fontosnak, mégis komoly jelentősége van a hálózati forgalom csökkentésében. (A `revalidate` beállítás segítségével kikapcsolható ez a képesség.)

A Samba konfigurálása Windows rendszerű tartományi bejelentkezéshez

Ha engedélyezni szeretnénk, hogy a Samba tartományvezérlő legyen, akkor a fejezet most következő részeiben leírtak szerint konfiguráljuk a Sambát és az ügyfeleit.

Tartományok létrehozásával kapcsolatos további tudnivalók a Samba disztribúció részét képező *DOMAINS.TXT* fájlban találhatók.

Windows 95/98 ügyfelek

Meglehetősen egyszerűen konfigurálhatjuk a Sambát elsődleges tartományvezérlőként Windows 95/98 ügyfelek számára. A kiszolgálón csak a következőket kell biztosítani:

- Az aktuális munkacsoportban csak a Samba legyen az elsődleges tartományvezérlő.
- Legyen a hálózatban egy WINS kiszolgáló, ami akár egy Samba, akár egy Windows NT kiszolgáló is lehet (a WINS kiszolgálóval kapcsolatban a *„Nyomtatás és névfeloldás”* című 7. fejezetben olvasható további információ).
- A Samba felhasználói szintű biztonságot használjon (vagyis ne bízza senki másra a jelszóhitelesítést). Nincs szükség tartomány szintű biztonságra, ha maga a Samba az elsődleges tartományvezérlő.

Ezt követően vegyük fel az alábbi beállításokat a Samba konfigurációs fájljába:

```
[global]
    workgroup = SIMPLE
    domain logons = yes

# Legyen felhasználói szintű a biztonság!

    security = user

# A Samba legyen az elsődleges tartományvezérlő!

    os level = 34
    local master = yes
    preferred master = yes
    domain master = yes
```

A `domain logons` beállítás engedélyezi, hogy a Samba tartományi hitelesítést végezzen el a bejelentkező ügyfeleken. A tartománynak ugyanaz lesz a neve, mint amit a Samba konfigurációs fájljában a munkacsoport nevének választottunk, vagyis az esetünkben a SIMPLE.

Ezt követően létre kell hoznunk egy nem írható, nem közzétehető és nem tallózható megosztást, aminek a `[netlogon]` nevet adjuk (mindaddig, amíg minden Windows ügyfél hozzáférhet ehhez a megosztáshoz, nincs jelentősége, hogy hová mutat a megosztás):

```
[netlogon]
    comment = The domain logon service
    path = /export/samba/logon
    public = no
    writeable = no
    browsable = no
```

Windows NT ügyfelek

Ha Windows NT ügyfelek is kapcsolódnak a hálózathoz, akkor valamivel több lépést kell megtennünk ahhoz, hogy a Samba elsődleges tartományvezérlőként jelenhessen meg számukra.

Csak a Samba 2.1-es és későbbi verziói teszik lehetővé, hogy a Samba teljes mértékben elsődleges tartományvezérlőként működhessen Windows NT ügyfelekkel szemben. A korábbi verziókban csak korlátozott módon lehetett hitelesíteni a Windows NT ügyfeleket. A könyv nyomdába adásának idején a Samba 2.0.5 volt a legfrissebb verzió, de már a 2.1-est is le lehetett tölteni a CVS segítségével. A Samba alfa verzióinak letöltéséről az E függelékben olvashatók további tudnivalók.

Mint korábban, most is biztosítanunk kell, hogy az aktuális munkacsoportban a Samba legyen az elsődleges tartományvezérlő, és hogy felhasználói szintű legyen a biztonság. Most azonban arról is gondoskodnunk kell. hogy a Samba titkosított jelszavakat kezeljen. Ezért a korábbi példa `[global]` beállításai közé vegyük fel az `encrypted passwords = yes` beállítást az alábbiak szerint:

```
[global]
    workgroup = SIMPLE
    encrypted passwords = yes
    domain logons = yes

    security = user
```

Megbízható fiókok létrehozása NT ügyfelek számára

Ezt a lépést kizárólag Windows NT ügyfelek esetében kell elvégezni. A megbízható fiókokat (*trust accounts*) az elsődleges tartományvezérlőhöz kapcsolódó NT ügyfelek használják. Az ilyen fiók lehetővé teszi, hogy egy gép magára az elsődleges tartományvezérlőre, és ne valamelyik megosztására jelentkezzen be. Ebben az esetben a tartományvezérlő megbízhatónak tekinti az illető ügyfél felhasználóival létesítendő kapcsolatokat. Mindent egybevéve azonban a megbízható fiók lényegében azonos egy felhasználói fiókkal. A példáinkban mi is standard unixos felhasználói fiókokkal utánozzuk a Samba kiszolgáló megbízható fiókjait.

A megbízható fiókhoz tartozó számítógép bejelentkezési neve magának a számítógépnek a neve, a végén egy $ jellel kiegészítve. Ha például a Windows NT gépünknek `chimaera` a neve, akkor a bejelentkezési fióknév `chimaera$`. A fiókhoz kezdetben tartozó jelszó a számítógép neve kisbetűs alakban. A megbízható fiók elkészítéséhez a Samba kiszolgálón létre kell hoznunk egy unixos fiókot a számítógép nevével, valamint az *smbpasswd* fájlba fel kell venni a titkosított jelszó bejegyzését.

Lássuk a feladat első részét. Itt csak a */etc/passwd* fájlt kell úgy módosítanunk, hogy támogassa a megbízható fiókot; nincs szükség home könyvtárra, és héjprogramot sem kell rendelnünk a „felhasználóhoz”, mert csak az érdekes, hogy engedélyezett-e a bejelentkezés. Ezért egy „ál” fiókot hozunk létre az alábbi bejegyzéssel:

```
chimaera$:*:1000:900:Trust Account:/dev/null:/dev/null
```

Figyeljük meg, hogy a csillag (*) karakter beírásával letiltottuk a jelszó használatát. Azt akarjuk ugyanis, hogy a Samba az *smbpasswd* fájlban tárolt jelszót használja, és nem szeret-

nénk, hogy valaki telnet eléréssel használja a fiókot. A fiók neve mellett ezért csak a fiók UID azonosítóját adjuk meg (1000) a titkosított jelszóadatbázis számára. Ehhez a számhoz az NT kiszolgálón egy egyedi erőforrás-azonosítót kell megfeleltetni, ami semmilyen más erőforrás-azonosítóval nem kerülhet összeütközésbe. Ezért egyetlen más NT felhasználó vagy csoport sem feleltethető meg ennek a számnak – ellenkező esetben hibaüzenetet küld a hálózat.

Következő lépésként az *smbpasswd* parancs kiadásával vegyük fel a titkosított jelszót:

```
# smbpasswd -a -m chimaera
Added user chimaera$
Password changed for user chimaera$
```

Az `-m` kapcsoló azt a gépet adja meg, amelyikhez a megbízható fiókot létrehozzuk. Az *smbpasswd* program automatikus létrehozza az induló titkosított jelszót a gép NetBIOS nevének kisbetűs alakja alapján – nekünk nem kell beírnunk a nevet. A parancssorba beírt név után ne írjuk be a $ jelet – ezt a program elvégzi helyettünk. Miután ilyen módon felvettük a titkosított jelszót, a Samba kész fogadni az illető NT gép tartományi bejelentkezéseit.

Windows ügyfelek konfigurálása tartomány bejelentkezéshez

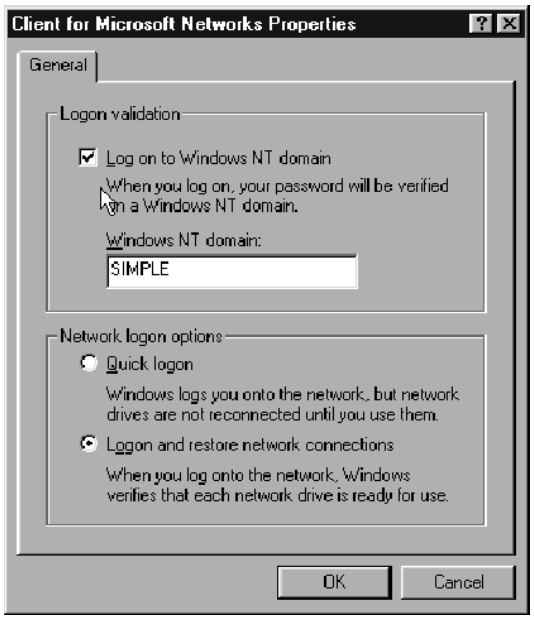
Miután a Sambán elvégeztük a tartományi bejelentkezésekhez szükséges konfigurációs lépéseket, a Windows ügyfeleket is úgy kell konfigurálnunk, hogy induláskor bejelentkezhessenek a tartományba.

Windows 95/98

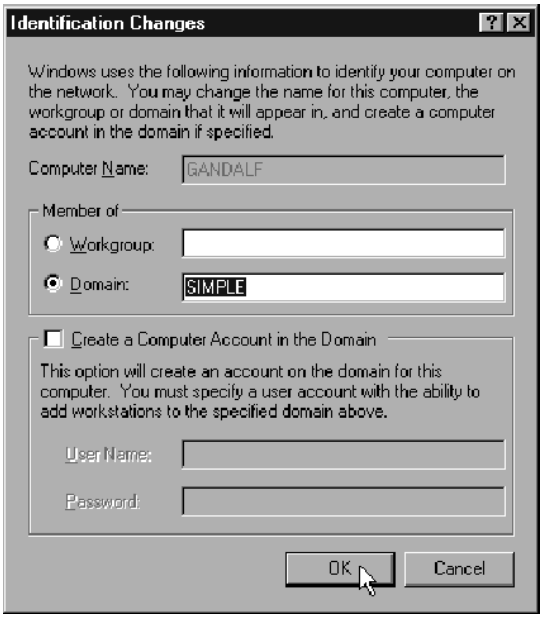
Windows 95/98-ban ezt úgy tehetjük meg, hogy a Vezérlőpulton megnyitjuk a Hálózat párbeszédablakot, kijelöljük benne a „Microsoft Network ügyfél" tételt, és a Tulajdonságok gombra kattintunk. Ekkor a 6.4. ábrán láthatóhoz hasonló párbeszédablaknak kell megnyílnia. Jelöljük be az ablak felső részén lévő „Belépés a Windows NT tartományba" feliratú négyzetet, és a Windows NT tartomány neveként írjuk be a Samba konfigurációs fájljában megadott csoportnevet. Kattintsunk az OK gombra, és indítsuk újra a számítógépet, ha felszólítást kapunk erre.

Ha a Windows azt közölné, hogy már bejelentkeztünk egy tartományba, akkor valószínűleg van egy élő kapcsolatunk a munkacsoport valamelyik megosztásával (például a leképzett hálózati meghajtóval). Ebben az esetben egyszerűen szakítsuk meg átmenetileg a kapcsolatot úgy, hogy az egér jobb oldali gombjával az ikonjára kattintunk, és a megnyíló helyi menüben a Szétkapcsolás parancsot választjuk.

Miután betöltődött a Windows, a szokásos bejelentkezési párbeszédablak jelenik meg, kiegészülve a tartományra vonatkozó mezővel. A mezőnek már tartalmaznia kell a tartomány nevét, ezért csak annyi a teendőnk, hogy beírjuk a jelszavunkat, és az OK gombra



6.4. ábra. Windows 95/98 ügyfél konfigurálása tartományi bejelentkezéshez



6.5. ábra. Windows NT ügyfél konfigurálása tartományi bejelentkezéshez

kattintunk. Ekkor a Windows felveszi a kapcsolatot az elsődleges tartományvezérlővel (ami a Samba), és megtörténik a jelszó vizsgálata. (A naplófájlokban utánanézhetünk ennek a műveletnek.) Ha túljutottunk az ellenőrzésen, gratulálhatunk magunknak. Úgy konfiguráltuk a Sambát, hogy elsődleges tartományvezérlőként szerepeljen a hálózatban Windows 95/98 gépekkel szemben, és az ügyfél is sikeresen kapcsolódott hozzá.

Windows NT 4.0

Windows NT gép tartományi bejelentkezésének konfigurálásához nyissuk meg a Vezérlőpulton a Hálózat párbeszédablakát. Az elsőként megjelenő párbeszédlap a számítógép azonosítóit tartalmazza.

A Change (Módosítás) gombra kattintva nyissuk meg a 6.5. ábrán látható párbeszédablakot. Az ablak „Member of" (Tagság) csoportjában jelöljük be a Domain (Tartomány) választógombot, majd írjuk be annak a tartománynak a nevét, amelybe ügyfélként be akarunk jelentkezni. Ez ugyanaz a név legyen, mint amit a Samba konfigurációs fájljában a munkacsoport neveként használtunk. Ne jelöljük be a „Create a Computer Account in the Domain" négyzetet – a Samba jelenleg nem támogatja ezt a képességet.

A Windows 95/98-hoz hasonlóan az NT is közölheti, hogy már bejelentkeztünk egy tartományba. Ekkor valószínűleg van egy élő kapcsolatunk a munkacsoport valamelyik megosztásával (például a leképzett hálózati meghajtóval). Ebben az esetben egyszerűen szakítsuk meg átmenetileg a kapcsolatot úgy, hogy az egér jobb oldali gombjával az ikonjára kattintunk, és a megnyíló helyi menüben a Szétkapcsolás parancsot választjuk.

Miután az OK gombra kattintottunk, a Windows egy párbeszédablakot jelenít meg, amelyben a tartomány üdvözletét olvashatjuk. Ekkor újra kell indítanunk a Windows NT számítógépet. Miután betöltődött az operációs rendszer, a Windows 95/98 ügyfeléhez hasonló bejelentkezési párbeszédablak nyílik meg. Bármely olyan fiókra bejelentkezhetünk, amelyet úgy konfiguráltunk a Samba kiszolgálón, hogy fogadja a bejelentkezéseket.

Győződjünk meg arról, hogy a Windows NT bejelentkezési párbeszédablakában a megfelelő tartományt választottuk. Miután kiválasztottuk a tartományt, eltarthat egy ideig, amíg a Windows NT elkészíti a rendelkezésre álló tartományok listáját.

Miután beírtuk a jelszavunkat, a Windows NT felveszi a kapcsolatot az elsődleges tartományvezérlővel (ami a Samba), és megtörténik a jelszó vizsgálata. (A naplófájlokban most is utánanézhetünk ennek a műveletnek.) Ha túljutottunk az ellenőrzésen, gratulálhatunk magunknak. Úgy konfiguráltuk a Sambát, hogy elsődleges tartományvezérlőként szerepeljen a hálózatban Windows NT gépekkel szemben, és az ügyfél is sikeresen kapcsolódott hozzá.

Tartományi beállítások

A 6.9. táblázat a tartományi bejelentkezésekkel kapcsolatos leggyakrabban használt beállításokat sorolja fel.

6.9. táblázat. Windows 95/98 tartományi bejelentkezési beállítások

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`domain logons`	Boolean érték	Azt jelzi, hogy Windows tartományi bejelentkezéseket kell-e használni.	`no`	Globális
`domain group map`	Karakterlánc (teljes elérési út)	A Unixot Windows NT tartománycsoportokra leképző fájl neve.	Nincs	Globális
`domain user map`	Karakterlánc (teljes elérési út)	A Unixot Windows NT tartományi felhasználókra leképző fájl neve.	Nincs	Globális
`local group map`	Karakterlánc (teljes elérési út)	A Unixot Windows NT helyi csoportokra leképző fájl neve.	Nincs	Globális
`revalidate`	Boolean érték	Ha `yes` az értéke, a Samba megköveteli, hogy a felhasználók minden megosztáshoz való kapcsolódáskor hitelesítessék magukat.	`no`	Megosztás

domain logons

Ez a beállítás úgy konfigurálja a Sambát, hogy elsődleges tartományvezérlőként fogadhasson tartományi bejelentkezéseket. Miután az ügyfél sikeresen bejelentkezett egy tartományba, a Samba egy különleges „zsetont" küld vissza, amelynek birtokában az ügyfél hozzáférhet a tartományi megosztásokhoz anélkül, hogy újból hitelesíttetnie kellene magát a tartományvezérlőnél. Jegyezzük meg, hogy ehhez a Sambának felhasználói szintű biztonságot kell használnia (`security = user`), és elsődleges tartományvezérlőnek kell lennie. Emellett a Windows gépek még azt is elvárják, hogy legyen a Samba kiszolgálón egy `[netlogon]` megosztás (lásd *„A Samba konfigurálása Windows rendszerű tartományi bejelentkezéshez"* szakaszt a fejezet előző részében).

domain group map

Ezzel a beállítással annak a fájlnak a helyét és nevét adhatjuk meg, amely a Windows NT tartománycsoportok nevét Unix csoportok nevére képezi le. A fájlnak a Samba kiszolgálón kell lennie. Például:

```
/usr/local/samba/private/groups.mapping
```

A fájlnak egyszerű a formátuma:

```
UnixGroup = NTGroup
```

Egy példa a leképzésre:

```
admin = Administrative
```

A megadott Unix csoportnak érvényes csoportnak kell lennie az */etc/group* fájlban. Az NT csoportnak azt a nevet kell adnunk, amilyen névre a Unix csoportot az NT ügyfélnél le akarjuk képezni. Ez a beállítás csak Windows NT ügyfeleknél használható.

domain user map

Ezzel a beállítással annak a fájlnak a helyét és nevét adhatjuk meg, amely a unixos felhasználóneveket Windows NT tartományi felhasználónevekre alakítja át. A fájlnak a Samba kiszolgálón kell lennie. Például:

```
/usr/local/samba/private/domainuser.mapping
```

A fájlnak egyszerű a formátuma:

```
UnixUsername = [\\Domain\\]NTUserName
```

Így nézhet ki egy bejegyzés:

```
joe = Joseph Miller
```

A megadott unixos névnek érvényes felhasználónévnek kell lennie az */etc/passwd* fájlban. Az NT névnek annak a felhasználónévnek kell lennie, amelyet az NT ügyfél részére unixos felhasználónévként meg akarunk jeleníteni. Ez a beállítás csak Windows NT ügyfeleknél használható.

Aki többet szeretne tudni arról, hogy miként kezeli a Windows NT a tartományi felhasználóneveket és a helyi csoportokat, olvassa el Eric Pearce *Windows NT in a Nutshell* című könyvét (kiadó: O'Reilly).

---

local group map

Ezzel a beállítással annak a fájlnak a helyét és nevét adhatjuk meg, amely a Windows NT helyi csoportok nevét Unix csoportnevekre képezi le. Helyi csoportnevek az olyan nevek is, mint az Administrator vagy a Users. A fájlnak a Samba kiszolgálón kell lennie. Például:

```
/usr/local/samba/private/localgroup.mapping
```

A fájlnak egyszerű a formátuma:

```
UnixGroup = [BUILTIN\]NTGroup
```

Így nézhet ki egy bejegyzés:

```
root = BUILTIN\Administrators
```

A beállítás csak Windows NT ügyfeleknél használható.

revalidate
Ez a megosztás szintű beállítás azt közli a Sambával, hogy kényszerítse ki a felhasználóktól a jelszavas hitelesítésüket minden olyan esetben, amikor egy gépen másik megosztáshoz akarnak kapcsolódni, függetlenül attól, hogy milyen szintű biztonság van beállítva a Samba kiszolgálón. A beállításhoz alapértelmezés szerint a `no` érték tartozik – ilyen esetben az egyszer már sikeresen hitelesített felhasználónak nem kell újból hitelesíttetnie magát. A beállítást az alábbi módon bírálhatjuk felül:

```
revalidate = yes
```

Ezzel ugyan növelhetjük a rendszerünk biztonságát, ugyanakkor kényelmetlenséget okozunk a felhasználóknak azzal, hogy bármely más megosztáshoz való kapcsolódáskor újból hitelesíttetni kell magukat.

Bejelentkezési szkriptek

A Samba támogatja a Windows olyan bejelentkezési szkriptjeit (ezeknek .BAT vagy .CMD a kiterjesztésük), amelyek akkor futnak le az ügyfélgépen, amikor egy felhasználó bejelentkezik egy Windows tartományba. Jegyezzük meg, hogy ezeket a szkripteket a Unix oldal tárolja, és a hálózaton keresztül akkor kerülnek át a felhasználó gépére, és futnak le ott, amikor a felhasználó bejelentkezik a hálózatra. Az ilyen szkripteknek óriási szerepük van a hálózat dinamikus konfigurálásában. A hátrányuk az, hogy mivel Windows rendszer alatt futnak, a Windows hálózati konfigurációs parancsait kell használniuk.

Ha valaki többet szeretne tudni a NET parancsokról, olvassa el az O'Reilly kiadónál megjelent *Windows NT in a Nutshell* és a *Windows 98 in a Nutshell* című kézikönyveket.

A Sambát a `logon script` beállítás segítségével utasíthatjuk egy bejelentkezési szkript lefuttatására:

```
[global]
    domain logons = yes
```

```
    security = user
    workgroup = SIMPLE

    os level = 34
    local master = yes
    preferred master = yes
    domain master = yes
    logon script = %U.bat

[netlogon]
    comment = The domain logon service
    path = /export/samba/logon
    public = no
    writeable = no
    browsable = no
```

Figyeljük meg, hogy a fenti példában a `%U` változót használva a bejelentkező felhasználó testére szabhatjuk a szkriptet. Általában szokás, hogy a tartományba bejelentkező felhasználótól vagy számítógéptől függjön, hogy melyik szkript fusson le. Ezekben a szkriptekben figyelembe vehetjük az egyes felhasználók vagy ügyfelek egyéni konfigurációs igényeit.

A bejelentkezési szkripteket a `[netlogon]` megosztás helyén kell tárolni. Ha ez az */export/samba/logon* könyvtár, és a bejelentkezési szkriptnek *jeff.bat* a neve, akkor a szkriptet a következő módon kell elhelyezni: */export/samba/logon/jeff.bat*. Amikor a felhasználó egy induló szkriptet tartalmazó tartományba jelentkezik be, egy kis párbeszédablakot lát, amely tájékoztatja a szkript futásáról, és a szkript kimeneteit kiírja egy MS-DOS ablakba.

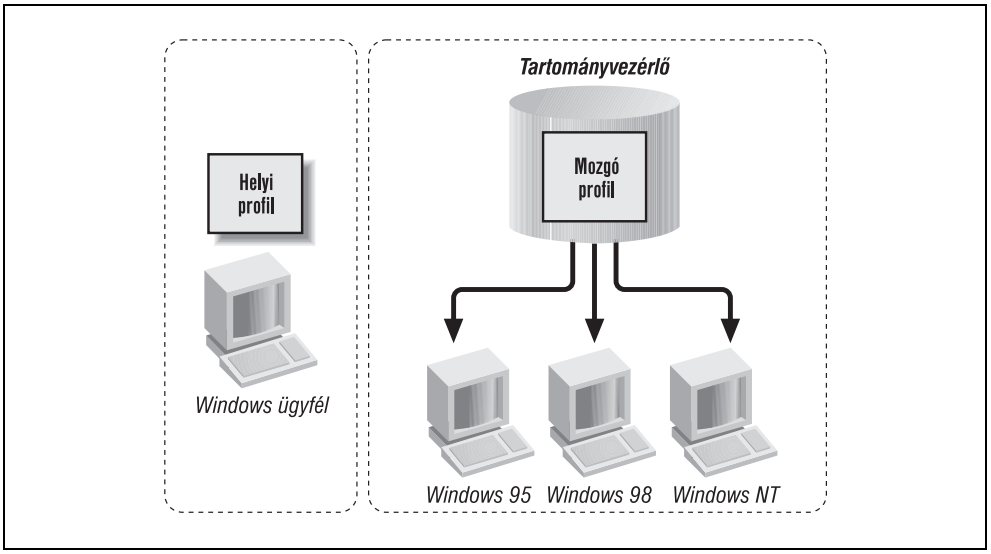
Figyelem: mivel ezeket a szkripteket a Windows tölti be, és a Windows oldalon futnak le, a Unix kocsivissza karakterei helyett a DOS kocsivissza/sorelemelés karaktereit kell tartalmazniuk. Ezért ajánlatos, hogy az ilyen szkripteket DOS vagy Windows alapú szövegszerkesztőben készítsük el.

Az alábbiakban olyan bejelentkezési szkriptre mutatunk példát, ami az aktuális időt a Samba kiszolgálón lévő időre állítja be, továbbá a `h` és az `i` hálózati meghajtókat két megosztásra képezi le a kiszolgálón:

```
#  Az aktuális idő beállítása a kiszolgálón lévő időre.
#  Ehhez az smb.conf fájlba fel kell venni a
#  "time server = yes" beállítást.

echo Az aktuális idő beállítása ...
net time \\hydra /set /yes

#  Két hálózati meghajtót leképezünk a Samba
#  kiszolgáló megosztásaira

echo Hálózati meghajtók leképezése a Hydra Samba kiszolgálóra...
net use h: \\hydra\data
net use i: \\hydra\network
```

Mozgó profilok

Windows 95/98 és NT rendszerekben minden felhasználónak saját *profilja* lehet. A profilok olyan információkat tartalmaznak, mint a rendszer Asztalának a megjelenítése, a Start menüben elhelyezett alkalmazások, a háttér színe és más, ezekhez hasonló jellemzők. Ha a profilt helyi lemez tárolja, akkor ezt *helyi profilnak* nevezzük, mert a helyi felhasználóval kapcsolatos információkat tartalmazza. Ha viszont a profilt a kiszolgáló tárolja, akkor a felhasználó ugyanazt a profilt töltheti le, bármelyik ügyfélgépről is kapcsolódik a kiszolgálóhoz. Ez utóbbit *mozgó profilnak* nevezik, mert a felhasználó gépről gépre vándorolhat, és miközben „mozog", mindig ugyanazt a profilt használhatja. Ennek különösen akkor vehetjük hasznát, ha valaki egyik nap az irodai gépéről, másik nap pedig a hordozható számítógépéről jelentkezik be. A mozgó profilokat a 6.6. ábra szemlélteti.



6.6. ábra. Helyi és mozgó profilok

A Sambában létrehozhatunk mozgó profilokat, ha a kiszolgálót tartományi bejelentkezésekhez konfiguráltuk, és ha a `logon path` beállítással megadtunk egy könyvtárfát. A beállításban általában változókkal helyettesítik a felhasználókat az alábbi példa szerint:

```
[global]
    domain logons = yes
    security = user
    workgroup = SIMPLE
    os level = 34
    local master = yes
    preferred master = yes
    domain master = yes

    logon path = \\hydra\profile\%U
```

A profilok támogatásához új megosztást kell létrehozni – ez olyan alap lemezmegosztás, amelyhez csak a Samba processzeinek használója (`root`) férhet hozzá. A megosztásnak írhatónak kell lennie, de nem lehet tallózható. Ezen túlmenően minden olyan felhasználóhoz, aki be akar jelentkezni, létre kell hoznunk egy könyvtárat (attól függően, hogy miként adtuk meg `logon path` beállításban a könyvtárat), amelyhez csak az illető felhasználó férhet hozzá. A biztonság növelése érdekében a megosztásba a `directory mode` és a `create mode` beállításokat is felvettük, hogy a megosztáshoz kapcsolódó személyek előtt ne jelenjenek meg az ezekben a könyvtárakban létrehozásra kerülő fájlok, és ne is módosíthassák ezeket.

```
[profile]
    comment = Felhasználói profilok
    path = /export/samba/profile
    create mode = 0600
    directory mode = 0700
    writable = yes
    browsable = no
```

Miután először bejelentkezett egy felhasználó, a Windows ügyfél – attól függően, hogy milyen operációs rendszer fut a gépén – elkészít egy *user.dat* vagy egy *ntuser.dat* nevű fájlt. Ezt követően az ügyfél feltölti az Asztalának, a Start menüjének, a Hálózatának (Network Neighborhood) és a programmappáinak tartalmát az adott könyvtár különböző mappáiba. Amikor az ügyfél ismét bejelentkezik, ezek a tartalmak letöltődnek a kiszolgálóról, és aktivizálódnak azon az ügyfélgépen, amelyről a felhasználó bejelentkezett. Amikor a felhasználó kijelentkezik, a tartalmak ismét feltöltődnek a kiszolgálóra. Ha megnézzük egy profilmappa könyvtárlistáját, akkor például az alábbiakat látnánk:

```
# ls -al

total 321
drwxrwxr-x   9 root  simple    Jul 21 20:44 .
drwxrwxr-x   4 root  simple    Jul 22 14:32 ..
drwxrwx---   3 fred  develope  Jul 12 07:15 Application Data
drwxrwx---   3 fred  develope  Jul 12 07:15 Start Menu
drwxrwx---   2 fred  develope  Jul 12 07:15 cookies
drwxrwx---   2 fred  develope  Jul 12 07:15 desktop
drwxrwx---   7 fred  develope  Jul 12 07:15 history
drwxrwx---   2 fred  develope  Jul 12 07:15 nethood
drwxrwx---   2 fred  develope  Jul 19 21:05 recent
-rw-------   1 fred  develope  Jul 21 21:59 user.dat
```

A *user.dat* fájlok bináris konfigurációs fájlok, amelyeket automatikusan hoz létre a Windows. A Windows ügyfélnél a Profile Editor programmal szerkeszthetők, de ez nem túl egyszerű feladat. A Samba egészen az NT 5.0 béta verzióig támogatja ebben az ügyfeleket.

A bejelentkezési szkriptek kezelésével kapcsolatban a Samba dokumentációs könyvtáraiban található fájlokban olvashatunk további részleteket (*docs/textdocs/DOMAIN.txt* és *docs/textdocs/PROFILES.txt*).

Kötelező profilok

A felhasználókhoz *kötelező profilok* is tartozhatnak – ezek olyan mozgó profilok, amelyek nem módosíthatók. Ha például egy kötelező profillal rendelkező felhasználó kedden felvesz a Start menüjébe egy parancsot, majd szerdán ismét bejelentkezik, nem fogja látni az előző napon felvett parancsot. A kötelező profil nem más, mint egy *user.dat* fájl *user.man* névre átnevezett változata, ami csak olvashatóvá lett átminősítve a Unix kiszolgálón. Általában azokat a beállításokat tartalmazza, amelyeket a felhasználónak a rendszergazda kívánsága szerint mindig végre kell hajtania. Ha például egy rendszergazda állandó felhasználói konfigurációt akar létrehozni, akkor a következőket teheti:

1. Létrehozza a Samba kiszolgálón az írható és olvasható könyvtárt.
2. Az *smb.conf* fájlban a `logon path` beállításhoz ezt a könyvtárt rendeli.
3. Felhasználóként bejelentkezik a Windows 95/98 rendszerből, hogy az ügyfél bekerüljön a könyvtárba.
4. A létrejövő *user.dat* fájlt *user.man* névre nevezi át.
5. A könyvtárat és a tartalmát csak olvashatóvá minősíti át.

Az ilyen kötelező profilokat általában nem használják. Ezzel szemben a mozgó profilok a Windows és a Samba legnépszerűbb szolgáltatásai közé tartoznak.

A bejelentkezési szkript beállításai

A 6.10. táblázat a Windows tartományi bejelentkezési szkriptjeivel kapcsolatos leggyakoribb beállításokat sorolja fel.

6.10. táblázat. Bejelentkezési szkriptek beállításai

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`logon script`	Karakterlánc (DOS elérési út)	A DOS/NT parancsfájl neve.	Nincs	Globális
`logon path`	Karakterlánc (a kiszolgáló és a megosztás UNC neve)	A felhasználó mozgó profiljának helye.	`\\%N\%U\profile`	Globális
`logon drive`	Karakterlánc (meghajtó azonosítója)	A bejelentkezési meghajtót adja meg a home könyvtárhoz (csak NT).	`Z:`	Globális
`logon home`	Karakterlánc (a kiszolgáló és a megosztás UNC neve)	A tartományba bejelentkezett ügyfelek home könyvtárainak helyét adja meg.	`\\%N\%U`	Globális

logon script

Ez a beállítás egy Windows rendszerben futtatható .BAT vagy .CMD kiterjesztésű parancsfájlt ad meg, amelyben az egyes parancssorokat a kocsivissza/soremelés karakterpár zárja le. A fájl végrehajtására azt követően kerül sor, hogy a felhasználó bejelentkezett a tartományba. A bejelentkezési szkripteket egy `[netlogin]` nevű megosztásban kell tárolni (a részletekről *„A Samba konfigurálása Windows rendszerű tartományi bejelentkezéshez”* című előző fejezetrészben volt szó). A beállításban gyakran használják a `%U` vagy a `%m` változót (a felhasználó vagy a számítógép NetBIOS neve). Példa:

```
logon script = %U.bat
```

A fenti beállítás hatására végrehajtásra kerül a felhasználó nevével meghatározott, a `[netlogin]` nevű megosztásban található szkript. Ha bejelentkező felhasználónak `fred` a neve, és a `[netlogin]` megosztásban elérési útként az */export/samba/netlogin* könyvtár van megadva, akkor a szkript az */export/samba/netlogin/fred.bat* lesz. Mivel ezeket a szkripteket a Windows tölti be, és a Windows oldalon futnak le, a Unix kocsivissza karakterei helyett a DOS kocsivissza/sorelemelés karaktereit kell tartalmazniuk.

logon path

Ezzel a beállítással a mozgó profilok helyét adhatjuk meg. Amikor bejelentkezik egy felhasználó, a kiszolgálóról letöltődik a mozgó profilja arra a gépre, amelyről bejelentkezett, és így a megszokott környezetében dolgozhat. Amikor kijelentkezik a felhasználó, a profilja visszatöltődik a kiszolgálóra, és ott tárolódik, amíg legközelebb ismét bejelentkezik.

Gyakran biztonságosabb külön megosztást készíteni kizárólag a felhasználói profilok tárolására:

```
logon path = \\hydra\profile\%U
```

A beállításról részletesebben a fejezet korábbi, *„Bejelentkezési szkriptek”* című részében volt szó.

logon drive

Ezzel a beállítással annak a lemezmeghajtónak az azonosító betűjét adhatjuk meg, amelyre a `logon home` beállításban meghatározott home könyvtárt képezzük le egy NT ügyfélnél. Ez a beállítás csak Windows NT ügyfeleknél használható. Példa:

```
logon drive = I:
```

Olyan betűt kell használnunk, amelyik nem ütközik az ügyfél gépében lévő merevlemezes meghajtók azonosítójával. A beállításhoz alapértelmezés szerint a Z betű tartozik, amit meg is hagyhatunk, mert a lehető legtávolabb van az A, a C és a D betűktől.

logon home

Ez a beállítás egy felhasználó home könyvtárának a helyét adja meg a DOS NET parancsai számára. A Samba kiszolgálón lévő valamely megosztást például az alábbi módon adhatjuk meg home könyvtárként:

```
logon home = \\hydra\%U
```

Megjegyezzük, hogy a home könyvtár a `[homes]` szakaszon keresztül is megtalálható, de bármely más könyvtár is megadható. A bejelentkezési szkripteket tartalmazó home könyvtárak az alábbi paranccsal képezhetők le:

```
NET USE I: /HOME
```

A Windows NT felhasználó-kezelőjében (User Manager) a felhasználó tulajdonságai alatt, a környezeti profil segítségével ellenőrizhetjük is, hogy valóban létrejött-e a home könyvtár.

Egyéb kapcsolódási szkriptek

Miután egy felhasználó bejelentette azt a szándékát, hogy hozzá szeretne férni a Samba valamelyik megosztásához, a Samba a maga oldalán egy program végrehajtásával előkészítheti a megosztás használatát. A Samba lehetővé teszi, hogy akár a megosztáshoz való kapcsolódás előtt, akár utána lefusson egy szkript. Ehhez Windows tartományok használatára sincs szükség. A 6.11. táblázat néhány ilyen előkészítő beállítást sorol fel.

6.11. táblázat. Kapcsolódási szkriptek beállításai

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`root preexec`	Karakterlánc (Unix parancs)	Megadja azt a parancsot, amelynek rootként kell lefutnia a megosztáshoz való kapcsolódás előtt.	Nincs	Megosztás
`preexec (exec)`	Karakterlánc (Unix parancs)	Megadja azt a Unix parancsot, amelynek felhasználóként kell lefutnia a megosztáshoz való kapcsolódás előtt.	Nincs	Megosztás
`postexec`	Karakterlánc (Unix parancs)	Megadja azt a Unix parancsot, amelynek felhasználóként kell lefutnia a megosztásról való lekapcsolódás után.	Nincs	Megosztás
`root postexec`	Karakterlánc (Unix parancs)	Megadja azt a Unix parancsot, amelynek rootként kell lefutnia a megosztásról való lekapcsolódás után.	Nincs	Megosztás

root preexec

Ehhez a beállításhoz egy Unix parancs tartozik, ami *rootfelhasználóként* kerül végrehajtásra, mielőtt még megtörténne a megosztáshoz való kapcsolódás. A beállítás segítségével olyan műveleteket végezhetünk el, amelyek rootprivilégiumot igényelnek. A `root pre-`

`exec` beállítást használva például CD-ROM-ot csatlakoztathatunk egy megosztáshoz, hogy elérhetővé tegyük őket az ügyfelek számára, vagy könyvtárakat hozhatunk létre. Az alábbi részlet arra mutat példát, miként használhatunk egy parancsot CD-ROM csatlakoztatására:

```
[homes]
    browseable = no
    writeable = yes
    root preexec = /etc/mount /dev/cdrom2
```

Ne feledjük, hogy ezek a parancsok rootfelhasználóként futnak. Ezért a biztonság érdekében sohase engedélyezzük, hogy a felhasználók módosítsák a `root preexec` beállításhoz tartozó parancsot.

preexec

A `preexec` beállításhoz – amit esetenként `exec` alakban is használnak – tartozó parancs szintén a kapcsolódás előtt fut le. Ez normál, nem privilegizált parancs, amelyet a Samba a `%u` változóval megadott felhasználóként futtat le. A parancsot általában a bejelentkezés elvégzéséhez használják az alábbi módon:

```
[homes]
preexec = echo "%u connected to %S from %m (%I)\" >/tmp/.log
```

Legyünk tisztában azzal, hogy a parancs által a standard kimenetre küldött parancsok nem jelennek meg a felhasználó előtt, hanem megsemmisülnek. Ha `preexec` szkriptet akarunk használni, akkor teszteljük, mielőtt még engednénk, hogy meghívja a Samba.

postexec

Miután egy felhasználó lekapcsolódik egy megosztásról, felhasználóként végrehajtásra kerül a Samba kiszolgálón a `postexec` beállításban megadott parancs. Ez általában az utólagos tisztogatási műveleteket végzi el. Erre a parancsra is vonatkozik, hogy a `%u` változóval megadott felhasználóként fut le, és a standard kimenetre küldött üzenetei nem jelennek meg.

root postexec

A `postexec` beállítással megadott parancsot követően a `root postexec` beállításban megadott parancs végrehajtására kerül sor (amennyiben van ilyen). A beállításhoz megadott parancs *rootfelhasználóként* fut le, miután a felhasználó lekapcsolódott a megosztásról. Ebben a beállításban olyan parancsokat adhatunk meg, amelyek végrehajtásához rootprivilégium tartozik.

Együttműködés NIS és NFS rendszerrel

Végül megemlítjük, hogy a Samba NIS és NIS+ rendszerekkel is képes együttműködni. Ha a hálózatban egynél több fájlkiszolgáló van, és mindegyiken fut a Samba, akkor célszerű, hogy az SMB ügyfél ahhoz a kiszolgálóhoz kapcsolódjon, amelyiknek a merevlemezei a home könyvtárát tartalmazzák. Általában nem jó megoldás, hogy a fájlokat először NFS

rendszerrel elküldjük egy Samba kiszolgálóra, hogy onnan SMB rendszerrel újra az ügyfélhez kerüljenek. (A Samba sebessége mintegy a harmadára esne vissza.) Ezért léteznek olyan beállítások, amelyek segítségével tájékoztathatjuk a Sambát arról, hogy a NIS ismeri a megfelelő kiszolgáló nevét, és jelezhetjük, hogy melyik NIS képezi le az információkat. A 6.12. táblázat két ilyen, a felhasználókat segítő beállítást sorol fel.

6.12. táblázat. NIS beállítások

Beállítás	Paraméterek	Funkció	Alapértelmezett érték	Hatókör
`nis homedir`	Boolean érték	Ha `yes` az értéke, akkor a felhasználó home könyvtárát nem az */etc/passwd* fájlban, hanem a NIS-ben kell keresni.	`no`	Globális
`homedir map`	Karakterlánc (NIS leképzés neve)	A NIS leképzést kell használni a felhasználó home könyvtárának kereséséhez.	Nincs	Globális

nis homedir és homedir map

A `nis homedir` és a `homedir map` beállítást azokon a hálózatokon használják a Samba kiszolgálók, amelyeken a Unix home könyvtárakat az NFS (automounter) és a NIS (Yellow Pages) szolgáltatja.

A `nis homedir` beállítással az jelezhető, hogy a felhasználó home könyvtárát tartalmazó kiszolgálót a NIS-ben kell keresni. A `homedir map` beállítás viszont arról tájékoztatja a Sambát, hogy melyik NIS leképezésben keresse ezt a kiszolgálót. A NIS kiszolgálónak Samba kiszolgálónak kell lennie, hogy az ügyfél SMB kéréssel kapcsolódhasson hozzá, a többi Samba kiszolgálóra pedig rá kell telepíteni a NIS rendszert, hogy elvégezhető legyen a keresés.

Ha például egy `joe` nevű felhasználó egy `[joe]` nevű megosztáshoz akar kapcsolódni, és a `nis homedir` beállításhoz a `yes` érték tartozik, akkor a Samba a `homedir map` beállításban megadott fájlban fogja keresni `joe` home könyvtárát. Ha megtalálja, akkor az ezt tartalmazó gép nevét visszaküldi az ügyfélnek. Az ügyfél ekkor megpróbál ehhez a géphez kapcsolódni, és azon kísérli meg a megosztások elérését. A NIS-ben való kereséseket az alábbi módon engedélyezhetjük:

```
[global]
    nis homedir = yes
    homedir map = amd.map
```