Samba Windowsban is otthon (4. rész)

A cikksorozat előző részeiben az Olvasó megismerkedhetett a Samba alapvető használatával, azokkal a funkciókkal, amelyekkel egy Windows-os hálózatot ellátó kiszolgálót fel lehet építeni. Így az alapfunkciók tárgyalásának befejeztével rátérnék azokra a funkciókra, amelyekkel az eddigieknél magasabb szinten tudjuk a rendszert a felmerülő igényekhez alakítani.

A hálózat tallózása

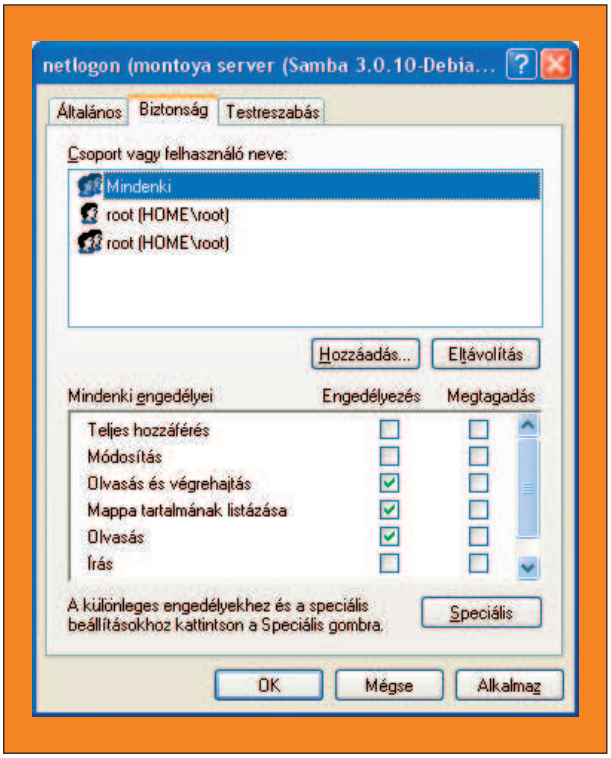
A hálózat tartalmának tallózása egy pofon egyszerű dolognak tűnik. Megnyitjuk a ***Network neighborhood*** – a magyar ***Windows*** alatt ***Hálózatok*** – ablakot és ott megtalálható a hálózatban jelenlévő gépek listája. A listából egy tetszőleges gépet kiválasztunk, ráklikkelünk és máris tallózhatjuk az adott gép tartalmát. A működés bár tényleg egyszerűnek tűnik, rengeteg szolgáltatás egyidejű együttműködését követeli meg.

Először is a ***Windows*** kliensnek regisztrálnia kell magát a hálózatban és tudatni a rendszerrel, hogy mostantól ő is aktív résztvevője annak. Majd ezek után a gépnek minden másik gép tudomására kell hozni a jelenlétét, hogy elérhetővé váljon. Egy, vagy több gépnek a hálózatban listába kell gyűjtenie a hálózatban elérhető gépeket, és a belépő munkaállomásnak ennél a gépnél regisztrálnia kell magát. A kliens gépeknek képeseknek kell lenniük arra, hogy a gépnév alapján meghatározzák egymás IP címét, hiszen egy ***TCP/IP*** alapú hálózatban a gépek címzése csak ezen a módon történhet. Végül pedig a kliens gépünk ezeken a szolgáltatásokon keresztül csatlakozni tud a kiszemelt célgéphez és elérheti annak erőforrásait.

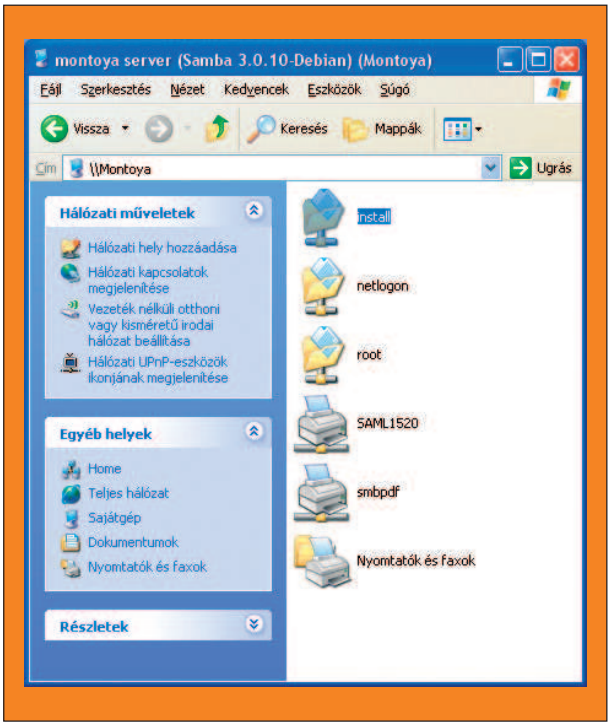
A ***Samba*** rendszer ***nmbd*** komponense biztosítja, hogy a hálózat tallózása, a gépek listába gyűjtése megtörténjen. A ***Samba*** kiszolgálón, a konfigurációs állományban pedig állítható akár kézzel is, hogy melyik gép végezze a listába gyűjtést. Mivel alapesetben ezt a szerepet (úgynevezett ***master browser***) bármelyik hálózati gép megkaphatja annak terhelésétől függően, ezért az adott gép kiválásával elképzelhető, hogy pillanatnyi fennakadás állhat elő- Különösen igaz ez akkor, ha például munkaidő végén a munkaállomások tömegesen hagyják el a hálózatot. Éppen ezért célszerű – természetesen a terhelések figyelembevételével – ezt a szerepet a kiszolgálóink valamelyikére kiosztani.

A NetBIOS protokoll

A ***Samba*** a ***Windows*** hálózatokban használt ***NetBIOS*** protokollon keresztüli kommunikációra is fel van készítve, hasonlóan a ***Windows*** kliensekhez a ***Samba*** is képes a ***TCP/IP*** fölött folytatni a ***NetBIOS*** protokollon keresztüli kommunikációt. A Windows kliensek hálózati kommunikációjának egy része – így többek között a gépek felderítése – üzenetszórással történik a hálózatban. Mivel azonban az útválasztók ezeket az úgynevezett ***broadcast üzeneteket*** nem engedik át, így amennyiben nagyméretű, de legalábbis útválasztók által szabdalt hálózat esetén a ***Sambát*** úgy kell beállítani, hogy ***unicast*** üzeneteket használjon. Ezen beállítások az ***smb.conf*** állományban végezhetőek el. ***Unicast*** üzenetek használata esetén a ***Sambát*** úgy kell beállítani, hogy támogassa a ***WINS*** alapú névfeloldást. Amennyiben több kiszolgálónk van a hálózatban, úgy lehetőségünk van a ***WINS*** kiszolgáló replikálására a hálózatban terheléselosz-



1. ábra Egy megosztás jogosultságai Windows alól nézve



2. ábra Egy Debian kiszolgáló tartalma Windows alól

tás és tartalékképzés céljából. Sajnos azonban jelenleg ***Windows*** és ***Samba*** kiszolgálók között ez a megoldás még nem támogatott, így amennyiben ***Samba*** kiszolgáló is van a hálózatban és az „master browser" szerepet tölt be, úgy csak az az egy ***nmbd*** entitás futhat.
Végezetül jegyezzük meg, hogy a névlisták összeállítása 15 perces intervallumonként automatikusan létrejövő hálózati üzenetek alapján történik, így egy-egy pontos, jól működő lista előállítása nagyobb hálózat esetén akár 45 percet is igénybe vehet.
Nézzük meg gyorsan, hogy milyen úton is halad végig egy név feloldása egy ***Windows*** munkaállomásnál. Először a kliens megnézi a lokális ***hosts*** állományt, amely teljesen hasonló a ***Linux*** rendszereken az ***/etc/hosts*** állományhoz, csak ez a ***%SystemRoot%\System32\Drivers\etc*** könyvtárban található. Amennyiben a ***hosts*** állomány alapján nem végezhető el a névfeloldás, akkor a kliens a beállított ***DNS*** kiszolgálóhoz fordul a keresett gép ***IP*** címéért. Amennyiben a ***DNS*** sem tartalmaz bejegyzést a keresett géphévhez, akkor harmadik lépésben a ***NetBIOS cache*** kerül vizsgálatra, majd pedig a beállított ***WINS*** kiszolgáló. Amennyiben egyik kiszolgáló sem tudott információval szolgálni, akkor egy ***broadcast*** üzeneteken alapúló keresés indul és minden gép megszólításra kerül, hátha válaszol a címzett. Amennyiben ez sem vezet eredményre, úgy utolsó lépésben a teljes ***LMHOSTS*** lekérdezésre kerül, amely alapértelmezésben a ***%SystemRoot%\System32\Drivers\etc*** könyvtárban helyezkedik el.

Kommunikáció TCP/IP felett NetBIOS használata nélkül

Az újabb ***Windows*** kliensek, mint a ***Windows 2000*** és ***Windows XP*** már támogatják a lokális hálózat használatát a ***NetBIOS*** protokoll nélkül, teljes egészében a szabványos ***DNS*** struktúrára épülve. Ebben az esetben a kliensek a hozzájuk tartozó tartományban automatikusan elvégzik a szükséges bejegyzések módosítását. ***Active Directory*** használata esetén ez olyannyira működik, hogy ***Active Directory*** létrehozásához szükség van egy megfelelően beállított és működő ***DNS*** kiszolgálóra.
A dinamikus ***DNS*** használata több szempontból is jó dolog, egyfelől egy szabványos, minden hálózati alkalmazás által támogatott protokollt használ, másfelől nekünk a munkaállomásnak csak egy nevet kell adni, valamint egy ***DHCP*** által kiosztott ***IP*** címet és a cím-név összerendelés automatikusan megtörténik. Ez a módszer egy tökéletesen működő megoldás ***Active Directory*** esetén, azonban mivel jelenleg a ***Samba*** nem működik ***Active Directory Serverként***, ezért ***Samba*** tartománykiszolgáló használata esetén kénytelenek vagyunk ***NetBIOS***-t használni. Amennyiben a ***Samba*** kiszolgálónk egy ***Active Directory*** tagja, akkor természetesen a dinamikus ***DNS*** használata megoldható. (A linuxos dinamikus ***DNS*** használatához először tájékozódjunk a ***BIND9*** leírásában!)

Munkacsoport tallózás beállítása

Amennyiben a hálózatunkon munkacsoportokba gyűjtjük a munkaállomásokat és szeretnénk lehetővé tenni a hálózaton keresztüli tallózást, úgy a ***Samba*** kiszolgálónkat a hálózat úgynevezett ***Domain Master Browserévé*** kell tennünk. Ez nem azonos a tartományvezérlővel, bár az elsődleges tartományvezérlő a hálózatban szintén ellátja ezt a feladatot. A ***Domain Master Browser*** feladata, hogy összegyűjtse a ***Local Master Browserektől*** az adott alhálózatban szereplő gépek listáját. A ***Domain Master Browser*** szolgáltatás hiányában a hálózatunk nem lesz több, mint lokális alhálózatok csoportja, amelyek egymással való kommunikációra ***Windows*** hálózat használatával egyszerűen képtelenek.
Egy munkacsoportos környezetben a ***Domain Master Browsernek*** a ***Samba*** kiszolgálót kell kijelölni és egy adott munkacsoporthoz csak egy ***Domain Master Browser*** tartozhat. Ennek a szerepnek a kiosztását a ***Samba*** konfigurációs állományában tehetjük meg a `domain master = yes` paraméter megadásával. A ***Samba*** kiszolgálót érdemes úgy beállítani, hogy a saját alhálózatának ő legyen a ***Domain*** és ***Local Master Browsere*** egy személyben. Ehhez a globális beállításokat egészítsük ki a következő bejegyzésekkel:

```
[global]
domain master = yes
local master = yes
preferred master = yes
os level = 65
```

Ha ezzel megvagyunk, akkor győződjünk meg arról, hogy minden alhálózatunknak is megvan a saját ***Local Master Browser*** gépe. ***Local Browser*** szerepére nem feltétlenül kell kijelölnünk egy ***Samba*** kiszolgálót, ezt a szerepet bármely Windows munkaállomás betöltheti. Amennyiben azonban úgy döntünk, hogy a ***Samba*** végezze ezt a feladatot is, akkor a ***Local Master Browser*** gép beállításai közé vegyük fel az alábbi paramétereket:

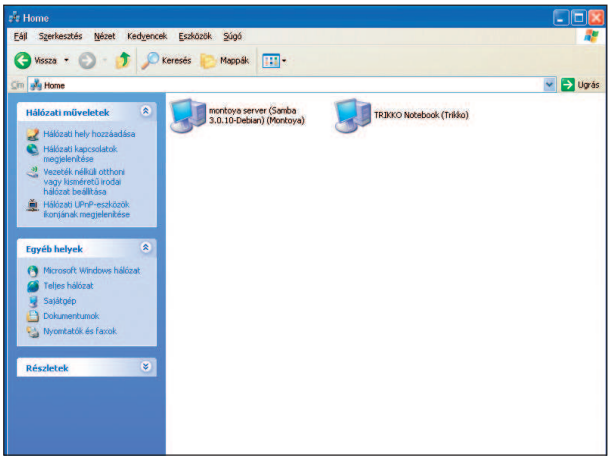
```
[global]
domain master = no
local master = yes
preferred master = yes
os level = 65
```

Fontos azonban, ahogy ***Domain Master Browserből*** is csak egy lehet a hálózatban, ***Local Master Browserből*** is csak egy lehet az adott alhálózaton. Ha tehát beállítunk még egy ***Samba*** kiszolgálót erre a feladatra, akkor a két szerver csúnyán össze fog veszni, aminek az lesz a következménye, hogy szép ki hálózati forgalmat generálnak, mellesleg nem is fognak rendesen működni.
Ha végeztünk a hálózati struktúra kialakításával, akkor most nézzük meg, hogy miként is tudjuk a megosztásokon a hozzáférési jogokat beállítani, akár megosztásonként különböző módon. Erre nagy szükségünk lehet egy bonyolultabb felhasználói struktúra esetén és az adatok biztonság érdekében nagy odafigyelést igényel.

Tartományi felhasználók és munkaállomások

Amennyiben ***Samba*** kiszolgálót használunk ***Windows*** tartomány kezelésére, úgy a rendszerben természetes módon létre kell hozunk azokat a felhasználókat, akiknek a későbbiekben tartományi elérést szeretnénk biztosítani. Ekkor a felhasználó egyfelől bekerül a ***Linux passwd*** állományába, másfelől a ***Samba*** háttér adatbázisába. A felhasználók kezelése mellett szükség van továbbá azokra a munkaállomásokra is, amelyeknek lehetőséget szeretnénk biztosítani a tartományi eléréshez, így ezeket a munkaállomásokat is nyilván kell tartani. A munkaállomások nyilvántartása egy helyen történik a felhasználók tárolásával, annyi különbséggel, hogy ezek az objektumok speciális felhasználói fiókként jönnek létre. A specialitás abban jelentkezik, hogy a felhasználói név $ karakterrel kezdődik, valamint az alapértelmezett munkakörnyezet a ***/bin/false***, tehát ilyen felhasználó a ***UNIX*** rendszerbe nem tud belépni, valamint a saját könyvtára a ***/dev/null***, tehát semmilyen személyes adat nem kerül tárolásra.
A munkaállomás felhasználói fiókjának létrehozása akkor történik, amik a ***Windows***-zal csatlakoztatjuk a munkaállomást a tartományhoz. Ezt a műveletet minden esetben csak tartományi rendszergazda jogokkal bíró felhasználó teheti meg – mint alapesetben a root felhasználó.
Windows rendszerekben megszokott dolog, hogy bizonyos felhasználói körökhöz speciális jogokat lehet rendelni, így például a tartományhoz való munkaállomás csatolást. Ilyen egyedi jogkörök kialakítása jelenleg még nem támogatott, de a ***Samba 3.0.11***-es verziótól kezdve folyamatosan fognak ezek a funkciók is bekerülni a rendszerbe.
A felhasználók jogosultsági szintekhez való hozzárendelése úgy fog kinézni, hogy egyfelől engedélyezni kell majd a ***Samba*** beállításai között ezt a funkciót a `enable privileges = yes` paraméter beállításával, valamint az egyes jogosultsági szintekhez hozzá kell adni a felhasználókat.
Jelenleg (3.0.11-es változat) a következő öt szint létezik:

- `SeMachineAccountPrivilege` – Ezek a felhasználók gépeket csatolhatnak a tartományhoz.



3. ábra Egy tartomány, ahol egy Debian a kiszolgáló

- `SePrintOperatorPrivilege` – Ezek a felhasználók menedzselhetik a nyomtatókat.
- `SeAddUsersPrivilege` – Ezzel a jogosultsági szinttel rendelkező felhasználók új felhasználókat és csoportokat adhatnak a tartományhoz.
- `SeRemoteShutdownPrivilege` – Ezzel a joggal rendelkező felhasználók használhatják a tartományban a távoli leállítás funkciót.
- `SeDiskOperatorPrivilege` – Ezek a felhasználók pedig szabályozhatják a lemezeke kiosztását.

Jogosultságok megadása a megosztásokra

Az előbb áttekintettük, hogy miként lehet az egyes felhasználóinkhoz jogosultsági csoportokat rendelni, most pedig nézzük meg, hogy miként lehet az egyes megosztásokhoz a felhasználóink hozzáférését szabályozni.
Azt szeretnénk elérni, hogy a különböző megosztásokat a rendszerben az egyes felhasználók láthassák, vagy éppen ne láthassák, az ott lévő állományokat megnyithassák olvasásra, vagy éppen írásra, továbbá hasznos lenne az is, ha adott megosztásra a megosztást elérő felhasználók egy adott felhasználói jogosultsággal végeznének munkát.
Mivel a windowsos és a ***UNIX***-os felhasználói jogosultság filozófiája jelentősen különbözik egymástól, ezért a jogosultságok megfeleltetés és kialakítása nem egyszerű feladat. Látnunk kell, hogy a két rendszer alapfelfogása különböző. Míg a ***UNIX*** rendszerekben a történelmi gyökerek, az akadémiai felhasználás miatt egy-egy dokumentum tulajdonosa és ezáltal a jogosultságok kiosztására hivatott felhasználó az adott dokumentumot létrehozó egyén, addig a ***Windows*** rendszerekben a kereskedelmi struktúra miatt egy-egy dokumentum nem a létrehozójának, hanem a rendszer felügyelője által beállított személy, vagy csoport tulajdonába kerül. Ez a szemléletbeli különbség kis problémát jelent, ám ügyes szervezéssel könnyen áthidalható, méghozzá oly módon, hogy egyes vélemények szerint a végén egy könnyebben átlátható és karbantartható rendszert kapunk.

1. táblázat

Paraméter	Leírás	Használat
`admin users`	Ebbe a listába felsorolt felhasználók az adott megosztásra rendszergazdai jogokkal rendelkeznek, így minden olyan utasítást végre tudnak hajtani, amit a `super-user` végrehajthat.	`admin users = user1, user2`
`force group`	Ennek a paraméternek adott érték azt a UNIX csoportot jelenti a rendszerben, amelynek tulajdonába fog kerülni minden az adott megosztáson elhelyezett állomány.	`force group = users`
`force user`	Hasonlóan működik a `force group`-hoz, csak itt felhasználót kell megadni.	`force user = root`
`guest ok`	Amennyiben ez a paraméter aktív, akkor az adott megosztás elérésére jelszó és hitelesítés nélkül is lehetőség van. Érdemes a nyilvános mappák használatánál alkalmazni.	`guest ok = yes/no`
`invalid users`	Ez egy nagyon hasznos beállítási lehetőség, felsorolhatjuk azokat a felhasználókat akiket explicit nem akarunk hozzáférési joggal felruházni. Nagyon hasznos, ha sok felhasználó esetén egy-két felhasználót kell letiltani.	`invalid users = user1, user2`
`only user`	Ez szintén egy bináris kapcsoló, bekapcsolva beállíthatjuk, hogy csak csak olyan felhasználókkal kezdeményezett kapcsolatok épüljenek ki, ahol a felhasználó neve szerepel a felhasználói listában.	`only user = yes/no`
`read list`	A `read list` listában felsorolt felhasználók jogosultak az adott megosztáson olvasási joggal hozzáférni a tárolt adatokhoz. A `read only` paraméter beállításától teljesen függetlenül ezek a felhasználók csak olvasási joggal fognak a megosztáson rendelkezni.	`read list = user1, user2`
`valid user`	Amennyiben implicit módon szeretnénk egy megosztásra definiálni azon felhasználók körét, akik hozzáféréssel rendelkeznek a megosztáshoz, akkor a `valid user` listába kell őket felvenni. Azok a felhasználók akik nem szerepelnek a listában hozzáférés megtagadása hibaüzenetet fognak kapni.	`valid user = user1, user2`
`write list`	A `read list`-hez hasonlóan ebben a listában azokat a felhasználókat kell felsorolni, akik írási joggal is rendelkeznek a szóban forgó megosztáson.	`write list = user1, user2`

Talán a legegyszerűbb megoldás, ha a rendszerben meglévő dokumentumokat két részre bontjuk. Az egyik a minden felhasználó által elérhető publikus anyagok, a másik az egyes felhasználók által használt privát, vagy bizalmas anyagok. Érdemes ezek után a struktúrát oly módon kialakítani, hogy a publikus, közös anyagokat egy külön kiosztás keretében oly módon tesszük közzé, hogy ahhoz minden felhasználó korlátlan módon hozzáférjen.
A bizalmas jellegű, vagy csak néhány felhasználó által használt anyagokat pedig olyan könyvtárstruktúrában helyezzük el, amit aztán a ***Linux*** kiszolgálón az adott felhasználó személyes mappájába – a ***HOME*** kiosztásba – linkelés útján helyezünk el.
Ez a megoldás már egy egész jó jogosultságkezelést biztosít, ám előfordulhat, hogy szeretnénk olyan megosztásokat készíteni, amit egyes felhasználók csak olvashatnak, mások írhatnak, míg megint mások nem is láthatnak. Erre szolgálnak az alábbi paraméterek, amelyeket a ***Samba*** konfigurációs állományában az adott megosztásnál kell elhelyezni.

Ezzel sikerült is áttekintenünk a ***Samba*** és a ***Windows*** rendszerek közötti jogosultságkezelési megoldásokat, amelyek segítségével a legbonyolultabb felépítésű hálózat kialakítása sem jelenthet problémát. Mielőtt azonban erőből nekiesünk egy-egy hozzáférés kialakításának, fordítsunk időt a tervezésre, mert egy felhasználók által elfogadott és programokba beállított struktúra átalakítása sok problémával és fejfájással járhat. Jobb az ilyet messze elkerülni.
A sorozat következő részében folytatjuk a ***Samba*** haladó funkcióinak áttekintését, addig is mindenkit arra ösztönzök, hogy próbálgassa a fent leírtakat.

Illés Viktor (viktor@ei.hu)
23 éves, a BME műszaki informatikus szakának hallgatója, mellette weblapokkal, linuxos és windowsos rendszerekkel foglalkozik. Szabadidejét legszívesebben a szabadban tölti, teniszezik és kerékpározik.