Samba – Windowsban is otthon (2. rész)
Tartományvezérlők beállítása

A cikksorozat előző részében megpróbáltam ízelítőt adni abból, minként lehet egy nyílt forráskódú, ingyenes rendszert egy drága üzleti szoftver kiváltására használni. A sorozat első részét tekinthetjük egy ízelítőnek, kedvcsinálónak ahhoz, hogy komolyabban foglalkozzunk a Sambával.

Aki végigolvasta az előző cikket, az a végére érve olyan tudás birtokában volt, amellyel az első lépéseket megtehette, készíthetett egy nagyon egyszerű állománykiszolgálót, valamint kellő alapot – és remélem motivációt – kapott, amelyre a továbbiakban már bátran építkezhetünk.
Ahhoz, hogy egy olyan rendszert építsünk, amelyik megállja a helyét üzleti környezetben is, nem elég pusztán egy olyan konfigurációt felállítani, ahol vannak kiosztások, és ahhoz bizonyos felhasználók hozzáférhetnek. Vállalati környezetben ennél többre van szükség. Szeretnénk a hálózat minden kiszolgálójához azonos felhasználói paraméterekkel hozzáférni és szeretnénk ezen paraméterek beállításait és tárolását központosítani. Szeretnénk, ha a felhasználók a belépéskor a rendszerben olyan és csak olyan jogokat szerezhetnének, amelyekre szükségük van, illetve szeretnénk azt is biztosítani, hogy a felhasználók a hálózat bármely munkaállomását is vegyék igénybe, azonos munkakörnyezetet kapjanak. Erre a *Windows* világában a ***tartománykezelés (domain control)*** a megoldás. Mivel jelenleg az a célunk, hogy a *Windows* munkaállomásainkat összeházasítsuk a linuxos kiszolgálóinkkal, ezért nekünk is el kell merülni ebben a világban. Nézzük tehát a ***Samba Domain Controller*** szerepét.

Elméleti alapok

Mielőtt mélyebbre ásnánk magunkat, néhány alapvető fogalommal mindenképpen meg kell ismerkednünk. Szeretném továbbá, ha az olvasók az alábbi szemléletben járnának el a rendszer telepítése és használata során:
„...Az teljesen helyénvaló, hogy hibákat kövessünk el, abban az esetben, ha azokat a hibákat ott és akkor követjük el, ahol ennek a helye van. Semmiképpen nincs helye hibák elkövetésének ott, ahol ezzel mások munkáját akadályozhatjuk, vagy ezzel másoknak kárt okozhatunk.
Amennyiben kísérletezni szeretnénk egy rendszeren, tanulni szeretnénk annak szolgáltatásait, azt mindenképpen egy olyan tesztkörnyezetben tegyük, ahol ezzel mások munkáját nem hátráltatjuk."
(A ➲ samba.org útmutatása alapján.)

Miért is kell nekünk a tartomány, mi előnyünk származik belőle?

A válasz egy mondatban összefoglalható, ez pedig a ***Single Sign On***, avagy az egyszerű bejelentkezés. *Windows* rendszerekben azokra a munkaállomásokra, amelyek a tartomány tagjai a felhasználó mindenhol ugyanazokkal a felhasználói paraméterekkel léphet be és munkájához ugyanazt a munkakörnyezetet és erőforrásokat használhatja.
Nézzük melyek azok a szolgáltatások, amelyeket a ***Samba 3***-as verziója ezen a téren kínál nekünk. Először is úgynevezett ***trust relationship***-et, vagyis bizalmi kapcsolatot tudunk létesíteni az egyes *Windows NT4*-es tartományokkal, valamint ezek tagjaival. Ez azért hasznos nekünk, mert két olyan tartomány, amelyek bizalmi kapcsolatban állnak, különösebb problémák nélkül tudnak erőforrásokat megosztani egymással. Csak zárójelben jegyezném meg, hogy a *Windows Server* család *Small Business* kiadásai nem tudnak más rendszerekkel ***bizalmi viszonyt*** kialakítani. Ez egy beépített korlátozás, mivel ezeket a szoftvereket kisvállalati környezetre tervezték és a *Microsoft* filozófiája szerint egy kisvállalati környezetben maximum egy kiszolgálót használnak. Ez van sajnos. Nézzük meg, mit veszünk, mielőtt a bomba vételből bomba meglepetés lesz.
Egy másik kényelmi szolgáltatása a ***Samba 3***-as rendszernek, hogy a tartományban lévő munkaállomásokról a beépített *Windows NT* segédprogramokkal tudjuk kezelni többek között a felhasználókat. Fontos, hogy csak a *Windows NT 4*-es verziójához járó segédprogramok felelnek meg a feladatra, a *Windows 2000*, *XP* és *2003 Server* nem. A programok megtalálhatóak az *SVRTOOLS* csomagban, amely letölthető a Microsoft weblapjáról, vagy lemásolható bármely *Windows NT 4 Server CD*-ről. Szintén új szolgáltatása a ***Samba 3***-asnak, hogy a felhasználói adatbázist tartalmazó háttérszolgáltatás cserélhető, tehát bármelyik olyan úgynevezett ***backendet*** használhatjuk, amelyik a céljainknak megfelel és a *Samba* is támogatja. Így lehetséges például *LDAP*, vagy *MySQL backend* használata. Az utolsó nagy újítás, amit kiemelnék az a ***Unicode*** támogatás, amelyre a legújabb *Windows* kliensek esetén már szükségünk lehet.

Mire nem használható a Samba

A *Samba* nem képes jelenleg *Windows* kiszolgáló ***kisegítő tartományvezérlőjeként (Backup Domain Controller)*** működni és *Windowst* futtató kiszolgálóhoz sem tudunk *Samba BDC*-t illeszteni. Ez van, tervezzünk ügyesen és éljünk ezzel együtt, amíg megoldás nem születik rá.
A *Samba* annak ellenére, hogy rendelkezik némi támogatással a *Windows 2000* tartományvezérléshez, a *Samba* nem tudja helyettesíteni a *Windows 2000* tartományvezérlők minden funkcióját. A dokumentáció szerint azonban az illetékesek dolgoznak a problémán és várhatóan a *Samba 3* egy későbbi kiadása során, vagy az azt követő verzióban már szerepelni fog ez a szolgáltatás is.

A „titokzatos" tartományvezérlők

A tartományvezérlőknek három típusát különböztetjük meg, a *PDC-t*, vagyis ***elsődleges tartományvezérlőt*** (***Primary Domain Contoroller***), a ***kisegítő tartományvezérlőt (Backup Domain Controller; BDC)***, valamint a *Windows 2000 Server* és *Windows Server 2003* rendszerek esetén az *ADS Domain Controller*, amely egy *Active Directory* támogatással rendelkező tartományvezérlő.
A *PDC* szerepe kiemelt egy tartomány életében, hiszen a rendszerben az azonosítási feladatok ellátása ennek a gépnek a feladata. Él ugyanakkor egy tévhit a köztudatban, miszerint az elsődleges tartományvezérlőt érdemes a hálózatban a legizmosabb gépre telepíteni. Ez nem feltétlenül igaz sőt, nagy hálózatokban érdemes a szolgáltatásokat több különálló tartománybeli kiszolgálóra szétosztani. Ez erőforrás elosztás és skálázhatóság tekintetében is egy jó ötletnek tűnik.
A *BDC* szerepe egy tartomány életében annyi, hogy állandóan másolja a *PDC* tartomány adatbázisát és amennyiben az elsődleges tartományvezérlő elérhetetlenné válna, úgy átveszi annak szerepét. Látszik, hogy tartalék tartományvezérlő megléte nem szükséges, de nagy hálózatok és kritikus környezetek esetén hasznos lehet.
A *Windows 2000 Server* és utódai esetén a tartományvezérlés egy kicsit megváltozott. Megszűnt az elsődleges és tartalék szerep, helyette a tartományvezérlők egy fa struktúrába vannak rendezve. Egy tartományvezérlő felelős az ő részfájában található gépek kiszolgálásáért, valamint tudni kell azt is, hogy ezen szolgáltatásokat a fában feljebb álló kiszolgálók felüldefiniálhatják. *Samba 3* esetén ez a működés *LDAP backend* használatával hasonló módon megvalósítható.
Windows NT 4-es környezetben egy kiszolgáló négy szerepet tölthet be. Ezek közül kettő a már említett elsődleges és tartalék tartományvezérlő, míg a további két szerep a ***stand-alone***, tehát egyedülálló szerver, valamint ***domain member***, tehát tartománytag kiszolgáló. Ennek a szerepnek az eldöntéséről a kiszolgáló telepítésekor kell dönteni. Amennyiben valamelyik tartományvezérlőt választjuk típusnak, úgy lehetőség van arra, hogy menet közben áttérjük a másik típusú tartományvezérlő szerepre, amennyiben erre a hálózat felépítése lehetőséget ad. Egyéb változtatások elvégzésére egyetlen út van, a kiszolgáló újratelepítése.
Amennyiben ***domain member*** kiszolgálót telepítünk, úgy a ***felhasználó-hitelesítő adatbázisunkat (Security Account Manager; SAM)*** az elsődleges tartományvezérlő fogja biztosítani. Amennyiben ***stand-alone*** kiszolgálót telepítünk, akkor a kiszolgáló ezeket az adatokat lokálisan fogja tárolni, így amennyiben változtatni szeretnénk, úgy a változásokat ezen a kiszolgálón kell átvezetni.
Már említettem, hogy a *Samba* egyelőre csak kísérleti stádiumban van ami a *Windows 2000 Active Directory* tartományvezérlést illeti, ugyanakkor a *Samba 3*-as kiszolgálók teljes értékű tartományi tagkiszolgálóként (***domain member)*** képesek egy ilyen környezetben is működni.
A sok-sok elmélet után nézzük miként is lehet megszerzett tudásunkat a gyakorlatban is alkalmazni.

A tartományvezérlés előkészítése

A *Windows* kliensek kétféle módon tudnak egymással hálózati kapcsolatba kerülni. Az első, hogy egy munkacsoport, úgynevezett ***munkacsoport (workgroup)*** tagjaivá tesszük őket, a másik, hogy a tartomány tagjaivá válnak. Előbbi a gyakorlatban nem jelent többet annál, minthogy van egy munkaállomásunk, amelyik más munkaállomásokhoz hozzáférhet, ha azon a megszólított munkaállomáson ez engedélyezve van. Amennyiben a kliensünket a tartomány tagjává tesszük, úgy az biztonságosan és szabadon tud kommunikálni a tartomány többi gépével.
Tartomány használata esetén a tartományi adatbázisba nem csak a felhasználók kerülnek bejegyzésre, hanem minden olyan kliens is, amelyiket hozzáadtuk a tartományhoz, így a biztonságosan használható klienseket is tároljuk.
Nézzük milyen feltételeknek kell egy *Samba 3*-as kiszolgálónak megfelelni, hogy az egy *Windows NT 4*-es tartományvezérlő szolgáltatásait biztosítsa a kliensek felé:

- Össze kell állítanunk egy működő *TCP/IP*-s *Windows* hálózatot. Ez úgy gondolom elég triviális dolog.
- A *Samba* beállításainál a megfelelő biztonsági szabályt kell választani, amely a `security = user` változó-paraméter párral lehetséges.
- A hálózatnak kell rendelkeznie egy jó beállított névfeloldással.
- A klienseket tartományi belépésre kell beállítani
- Ajánlatos a felhasználói profilokat úgynevezett ***barangoló profilként (roaming profile)*** létrehozni, így a felhasználó a használt munkaállomástól függetlenül minden gépen azonos környezetben dolgozhat.
- A kliensek felé biztosítani kell a *Netlogon* szolgáltatást, amelyet a konfigurációs állományban lehet beállítani.
- Javasolt, hogy a kiszolgáló vegye át a rendszerben az úgynevezett *Master Browser* szerepet, ugyanis ezzel hatékonyabbá lehet tenni a működést.

Nézzünk egy példát a beállításokra:

```
[global]
netbios name = MYSERVER
workgroup = MYDOMAIN
passdb backend = tdbsam
os level = 33
preferred master = yes
domain master = yes
local master = yes
security = user
domain logons = yes
```

```
logon path = \\%N\profiles\%U
logon drive = H:
logon home = \\homeserver\%U\winprofile
logon script = logon.cmd

[netlogon]
path = /var/lib/samba/netlogon
read only = yes
write list = ntadmin

[profiles]
path = /var/lib/samba/profiles
read only = no
create mask = 0600
directory mask = 0700
```

A passdb backend tartalmazza az összes felhasználóifiók és csoport információt. A lehetséges értékek: `smbpasswd`, `tdbsam`, és `ldapsam`. Amennyiben *BDC*-t is használni szeretnénk a rendszerben, úgy az egyetlen értelmes választási lehetőség az `ldapsam`, mivel az `smbpasswd` és `tdb` adatbázisok lokálisak, így nem lehet őket a hálózatban elterjeszteni.

A tartományvezérlő paraméterei

A tartományvezérlő lehetséges paraméterei: `os level`, `preferred master`, `domain master`, `security`, `encrypt passwords`, és `domain logons`.
Ezek természetesen központi szerepet játszanak a tartományvezérlő tulajdonságainak kialakításakor. Az `os level` változó értékét mindenképpen állítsuk 32-nél nagyobbra, hogy a megfelelő prioritást megadjuk a kiszolgálónak.
A `preferred master` változót szintén állítsuk igaz értékre, mivel ezzel tudjuk aktiválni azt, hogy a tartományban ez a gép legyen a `master browser`. A `domain master` változónak adjuk a `yes` értéket, amennyiben a kiszolgáló egy elsődleges tartományvezérlő, amennyiben azonban egy tartalék tartományvezérlőt állítunk be, úgy logikusan a `no` értéket adjuk a változónak.
Tartományvezérlő beállítása esetén a `security` változó a `user` értéket kapja, ami azt jelenti, hogy a megosztásokhoz való hozzáférés alkalmával a kapcsolatot kezdeményező kliens egy felhasználói azonosításon is átesik, a megadott felhasználónak léteznie kell a kiszolgáló adatbázisában.
A tartományvezérlő helyes működéséhez a klienseknek és a kiszolgálónak is támogatnia kell a *Microsoft* titkosított jelszókezelését. Ehhez a kiszolgálón az `encrypt passwords` változót állítsuk `yes` értékre.
Végül, de nem utolsó sorban ahhoz, hogy a kliensek igénybe vehessék a *Network Logon* szolgáltatást, a `domain logons` paraméternek is adjunk `yes` értéket. A *Network Logon* szolgáltatáshoz kapcsolódni kell továbbá egy `netlogon` kiosztás meglétének is, ahol a rendszerbe belépő kliensek megtalálják a *login szkriptet*, tehát azt a futtatható állományt, amit minden tartományba való belépéskor le kell futtatniuk.

Környezeti változók

A lehetséges környezeti változók a következők: `logon path`, `logon home`, `logon drive`, és `logon script`.

Ezek segítségével olyan működési környezetet tudunk kialakítani az ügyfelek és a felhasználók számára, amely a legjobban illeszkedik az elvárt igényekhez.
A `logon path` változó értékének a felhasználói profil helyét kell megadni. Az elérési út megadásánál használhatunk reguláris kifejezéseket is. A `logon drive` annak a meghajtónak a betűjelét mutatja, amely hálózati meghajtón keresztül a klienseken a `logon home` változó értékének megadott könyvtárat érhetik el. Ez a könyvtár lesz a felhasználó privát hálózati meghajtója. Amennyiben a rendszerben vannak olyan felhasználók is, akik notebookokról érik el a hálózatot, akkor náluk az újabb *Windows* rendszerekben érdemes a kapcsolat nélküli elérhetőséget erre a hálózati meghajtóra beállítani.
A `logon script` az az állományt mutatja, amelyik a felhasználók belépésekor lefut minden gépen.

A NETLOGON megosztás

A `NETLOGON` megosztás egy alapértelmezett megosztás minden Microsoft tartományvezérlőn. Ez a mappa tárolja a *logon scriptet*, a házirend állományokat (*NTConfig.POL* állomány, amelyben az ügyfél és a felhasználó hozzáférését tudjuk korlátozni az egyes rendszerbeállításokhoz), valamint minden olyan állományt,amelynek a belépési procedúra során feldolgozásra kell kerülnie.

A PROFILE megosztás

Ebben a megosztásban tárolja a *Windows* a felhasználók profiljait. Amikor egy felhasználó belép a rendszerbe, akkor a kliens gép lekéri a felhasználói profilját, betölti a szükséges környezetet és átadja munkára a felhasználónak. Kilépéskor ugyanez megtörténik ellenkező irányban, tehát a felhasználó minden megváltozott beállítása elmentésre kerül. Érdemes a *UNIX* jogosultságokat úgy beállítani, hogy az adott felhasználói profilhoz csak a tulajdonosa férhessen hozzá. Ez növelheti a rendszer biztonságát.
Ezzel cikkem végére is értem. Mostanra sikerült egy tartományvezérlőt beállítani és elsajátíthattuk a kapcsolódó ismeretek alapjait. Annyit azért érdemes megjegyezni, hogy egy *Samba* kiszolgáló jelenleg még nem képes minden *Windows* szolgáltatás teljes kiváltására és valószínűleg mindig egy lépéssel a *Microsoft* mögött fog járni, de már ez az egy lépés hátrány olyan mértékűvé csökkent, amikor érdemes elgondolkozni azon, hogy a két rendszer tudásbeli és szemléletbeli különbsége közötti arány van-e olyan mértékű, amikor még érdemes lehet egy *Windows* kiszolgálót üzembe állítani.
Aki komolyan szeretne a témával foglalkozni, az kövesse továbbra is figyelemmel a *Linuxvilág magazint*, mert ez a téma ezen a cikksorozaton kívül is egész biztosan felmerül majd. Érdemes továbbá a nyílt forráskódú rendszerekkel foglalkozó portálokat is sűrűn látogatni, mert minden nap újabb és újabb megoldások kerülnek fel a hálózatra.
Végezetül mindenkit arra buzdítok, hogy nyugodtan játsszon a rendszerrel, próbálgassa a beállításokat – persze ha lehet, akkor a *Samba* fejlesztőinek ajánlásait betartva.

Illés Viktor