SaMBa alapok

Lajber Zoltán

lajber.zoltan@ih.szie.hu

Szent István Egyetem, Informatikai Hivatal

Számítógépes Hálózatok Osztálya

http://zeus.gau.hu/~lajbi

Bevezetés

A SaMBa: SMB protokolt megvalósító programegyüttes

Előadás tematikája:

- SaMBa rövid bemutatása
- Névfeloldás, böngészés
- Kiszolgálók típusai, biztonsági módok
- Account management, Access control, nyomtatás
- finomságok: profile, charset, policies, VFS, backup
- upgrade és migráció: samba 2.2 $\Rightarrow$3.0, nt4 pdc $\Rightarrow$samba

`SaMBa` bemutatása

Samba, Opening Windows to a Wider World!

– kb 30 fejlesztő

– gyakorlatilag bármilyen TCP/IP-re képes hoston tud file- és nyomtató szolgáltatást nyújtani Microsoft Windows klienseknek

– ezen túl adminisztrációs és migrációs segédeszközöket is tartalmaz

Protokollok

NetBT: NetBIOS over TCP/IP: Name, Datagram és Session szolgáltatás.

SMB: NetBT fölötti foleg fájl- és nyomtató megosztás, de named pipes, mailslots, egyebek is.

CIFS: ugyanaz mint az SMB, de közvetlenül TCP/IP fölött.

SMB kapcsolat létrehozásának lépései :

- cél gépet megfelő néven kell szólítani,
- felek a dialektusban megegyeznek,
- erőforrás - például fájl megosztás - kérése (tree connect),
- ha újabb erőforrás kell, akkor a meglévő kapocsolaton belül új tree connect,
- message, echo, server info autentikáció nélkül elérhető.

SMB autentikáció

megosztás (share) szintű autentikáció :

- az SMB kapcsolatfelvételnél nincs autentikáció (bár sokszor küld a kliens session setup-ot, ekkor usernévvel, de jelszó nélkül),
- egy erőforrás eléréshez (tree connect) **csak jelszó** kell, nincs UID,
- feltételezi, hogy egy felhasználó ugyanazt a jelszót használja több helyen,

felhasználó (user) szintű autentikáció :

- az SMB kapcsolat elején dialektus tisztázása után azonnal,
- felhasználói **név és jelszó** kell,
- dialektustól függően a jelszó lehet cleartext vagy challenge-response,
- fallback guest gyakori.

Telepítés egyszerű beállításokkal

apt source: `deb http://www.backports.org/debian stable samba`

Beállítások:

```
; /etc/smb.conf for simple server
[global]
   interfaces = 192.168.242.61/255.255.255.192
   hosts allow = 192.168.242.0/255.255.255.192 192.168.242.189/255.255
   printing = cups
   printcap name = cups
   load printers = yes
   guest account = nobody
   invalid users = root
   security = user
```

```
# browsing
   netbios name = fileserver
   workgroup = demo
   server string = demo celokbol
   wins support = yes
   os level = 254
   domain master = yes
   local master = yes
   preferred master = yes
   name resolve order = host bcast
   dns proxy = yes
```

```
preserve case = yes
short preserve case = yes
unix password sync = false
max log size = 1000
syslog only = no
syslog = 0;
encrypt passwords = true
passdb backend = tdbsam guest
```

```
[homes]
   comment = Home Directories
   browseable = no
   read only = no
   create mask = 0754
   directory mask = 0754
```

```
[kozos]
  comment = kozos terulet
  path=/home/kozos/
  browseable = yes
  public = no
  writable = yes
  printable = no
  force user = kozos
  force group = demo
  create mode = 770
  directory mask = 0770
```

```
[www]
  comment = www.demo.hu fejlesztoi valtozat
  path=/var/www
  browseable = yes
  public = no
  writable = yes
  printable = no
  force user = webmaster
  force group = webmaster
  valid users = @webmaster
  create mode = 775
  directory create mode = 775
```

```
[printers]
   comment = All Printers
   browseable = no
   path = /var/tmp
   printable = yes
   public = no
   writable = no
   create mode = 0700
```

```
[mp3]
  comment = no comment
  path = /home/mp3
  browseable = yes
  public = no
  writable = yes
  printable = no
  force user = mp3
  force group = mp3
  create mode = 770
  directory mask = 0770
```

NetBT Name Service és WINS

- NetBIOS nevek és IP címek nyilvántartása,
- 16 karakter hosszú nevek, de az utolsó karakter mindig funkciókód,
- DNS packeteket használ, de mangled nevek a karakterkészlet miatt,
- NetBT NS és WINS variánsai ugyanannak a szolgáltatásnak, azonos célok, de eltérő módszerek:
  - NetBT NS broadcast alapú, WINS unicast, ezért a NetBT NS nem, de a WINS működik alhálózatok között is,
  - A két szolgáltatás független, nem cserélnek adatot még akkor sem, ha azonos gépen futnak,
  - Ezért pl. ha a WINS szerver nincs beállítva WINS kliensnek, nem szerepelteti saját magát a listájában, és független NetBT NS-t is futtat.

SMB Névfeloldás

Node type:

`HKLM\System\CurrentControlSet\Services\NetBt\Parameters\NodeType:dword`

érték	elnevezés	működési mód
1	**b**roadcast	broadcast és direkt UDP-n és TCP-n
2	**p**oint to point	csak direkt UDP és TCP, ha a megszólított nem elérhető, nem tud belépni a rendszerbe
4	**m**ixed	broadcast, majd ha ez sikertelen, akkor direkt kapcsolat
8	**h**ibrid	direkt megszólítás, ha ez sikertelen, akkor broadcast.

SaMBa: `name resolve order`,

lehetséges értékei: `lmhosts, hosts,wins, bcast`

Computer Browser

- csak humán interface szerepe van,
- számítógép lista, megosztások már a cél gépről,
- nem része a WINS-nek,
- tipikus, hogy egy gép látszik a listán, de nem elérhető, ez nem browser hiba,
- gyakori, hogy egy gép nem látszik a listán, de elérhető, ez browser hiba,
- NetBT NS-hez hasonlóan broadcast alapú, de routerek miatt ...
- idővel több alhálózatos, nagy hálózatokban is stabilizálódik,
- általában egy nagy hálózat a stabilizálódás előtt átkonfigurálódik,

- workgroup (munkacsoport) nyitott: az lehet a tagja, aki ezt állítja magáról,
- domain (tartomány) zárt: belépéshez **gép** autentikációja a tartományvezérlőnél,
- master browser-t munkacsoportonként és alhálózatonként (UDP broadcast domain) választanak a gépek,
- minden alhálózatban külön munkacsoport, hiába azonos a neve
- megoldás összevonásra:
  - közös WINS kijelölés,
  - tartománnyá alakítás,
  - SaMBa `remote announce` opció másik alhálózat broadcast címére.

Master browser

- a master browsert választják a gépek,
- ha nem látszik a master browser, a gépek új választást kezdeményeznek,
- gyakran előfordul, hogy több master browser van, de nem mindegyik rendelkezik teljes géplistával,
- szavazáson az nyer, akinek magasabb a verziószáma (win9x, NT ws + service pack verzió, NT srv + service pack verzió, win2k), uptime...,
- SaMBa opciók:
  - `os level = 33`,
  - `preferred master`,
  - `domain master`,
  - `local master`

Computer Browser frissítések : UDP 138-as port, broadcast.

- host announcement: bootoláskor 3 broadcast,
- local master announcement: 12 percenként,
- workgroup announcement: 15 percenként,
- host announcement: 12 percenként,
- master browser announcement: 15 percenként.

Computer Browser Listacserék : TCP 139-es port, unicast.

- tartomány master browser a WINS-nek: géplista 12 percenként,
- local master browser a tartomány master browsernek: 12 percenként,
- backup browser a tartomány master browsernek: 12 percenként,

WINS - WINS kommunákáció: TCP 42-es port, unicast

Master browser problémák csökkentése

- **WINS, azonos NetBT és DNS host nevek, csak IP protokoll**,
- többlábú gépen samba master browser, de többlábú NT **nem** lehet,
- megosztás nélküli gépek elrejtése a browser listából:

  NT-ken: `HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\Hidden=dword:1`

  win9x-eken: ez elérhető a nyomtató- és fájlmegosztás szolgáltatás eltávolításával.
- hatás: browser lista, választások, a host announcement.
- választások szabályozása `HKLM\System\CurrentControlSet\Services\Browser\Parameters\IsDomainMaster:dword` paraméterrel. Lehetséges értékei: 0 - soha, 1 - mindig, 2 - automatikus, ez az alapértelmezett a munkaállomásokon.

Fejlemények - w2k, samba3

- Működhetnek NetBIOS over TCP/IP nélkül
- ekkor más névfeloldásnak (DNS, LDAP, ADS) működnie kell

Kiszolgáló típusok és biztonsági módok

Ha nem megfelelően használjuk a `SaMBa` -t, akkor nagyon nyűgös, ellenkező esetben pedig barátsagos.

- `SaMBa` 3 ki tud váltani egy NT4-es tartományvezérlőt.
- `SaMBa` 3 nagyon jól együtműködik NT4 stilusú tartományokkal és Active Directory-val
- teljes NT4-es interdomain trust szolgáltatások
- olyan biztonsági módok, amelyek rugalmasabbak az NT4-nél
- többféle user account adatbazist hátteret (account database bakcend) haszálhatunk, az account (jelszó) adatbázis lehet elosztott is.

Tömören: teljes NT4 kompatibilitas, AD-nel fejlettebb (de nem törvényszerűen kompatibilis) szolgáltasokkal

Szerver típusok

- Domain Controller
  - Primary Domain Controller
  - Backup Domain Controller
  - ADS Domain Controller
- Domain Member server
  - Active Directory Domain Server - Ezt nem tudja a `SaMBa` !
  - NT4 Style Domain Domain Server - lásd később
  - machine account -ok kellenek!
- Stand-alone server

Windows XP Home Edition *nem tud* belépni tartományba, sem másféle hálózatba!

Biztonsági módok

Ezek alapja a share vagy user szintű, de ezeken túl bonyolítható.

NT4 style Domain security mód

```
security = domain
workgroup = DEMO
```

majd `net rpc join -U administrator%password` A szerver rendelkezik egy domain trust account-al (machine account) a tartományban. Így a gép egy Doman Member Server. A regi `security=server` használata nem javasolt.

ADS security mód

```
security = ADS
realm = kerberos.REALM
password server = kerberos.server.neve
```

NT4 Style Domain Controller mód

```
[global]
netbios name = fileserver
workgroup = demo
passdb backend = tdbsam
os level = 33
preferred master = yes
domain master = yes  # domain master = no BDC-n!
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
```

Kliensek tartományba tétele

Machine Trust Account: a kliens **gép** autentikálására való. Windows terminológia szerint "Computer Account". Felépítés: `gépnév$`

MTA jelszó: "shared secret" a gép és a DC között, hogy illetéktelen, de azonos NetBIOS nevű gép ne férhessen a tartomány erőforrásaihoz.

kliens korlátozások: win9x, Me, XP home **nem** használja, ezért igazából nem is tagjai a tartománynak.

MTA tárolása: NT4 a registry-ben, w2k az AD-ben, `SaMBa` :

- Domain Security Account a jelszavak között tárolódik. Régi formátumoknal LanMan és NT kódolt jelszó, az újabb adatbázisokban (ldapsam, tdbsam) több információval együtt.
- hozzátartozó UNIX account az `/etc/passwd` -ben.

MTA létrehozása

- Windows NT4 Server Manager, vagy Nexus segitségével, ha adminisztrátorként lépünk be
- Autómatikusan `SaMBa` -t használva - javasolt módszer
- kézzel létrehozva a megfelelő bejegyzéseket

MTA készítés kézzel

- UNIX acc:

```
root# /usr/bin/useradd -g gepek -d /dev/null -c "gep leiras"  -s /l
root# passwd -l gepnetbiosnev$
```

- `SaMBa` acc:

```
root# smbpasswd -a -m gepnetbiosnev
```

Backup Domain Controller

Akinek kérdése van: John H. Terpstra <mailto:jht@samba.org>

PDC	BDC	megjegyzés
Master LDAP	Slave LDAP	optimális megoldás
központi LDAP	központi LDAP	működő megoldás
tdbsam	tdbsam + vampire	látszólag jó
tdbsam	tdbsam + rsync	látszólag jó
smbpasswd	smbpasswd + rsync	szinkronizációs gondok

Jelszavak környéke

- Ha domain userek vannak, akkor is kell egyértelműen megfeleltethető UNIX-os UID. Célszerű nemlétező shell-t beállítani ezeknek. WINBIND!!!
- a win-es jelszó lehet cleartext
- a win-es jelszó lehet MD4 hash
- jelszó nagybetüsre konvertál, feltölt vagy csonkol 14 bájtra. Hozzáfűz 5 byte NULL karaktert, kettéosztja két 56 bites DES kulcsra. Ezzel kódol egy ”bűvös” 8 bájtos értéket. Az eredényként kapott 16 bájt a LanMan hash.
- win95 SP1 elött, NT3.x, NT4 sp3 elötti verziók használhatják mindhármat, de!

- a windows kliensek 10 perc tétlenkedés után hajlamosak eldobni a hálózati meghajtókat
- újrakapcsolásnál password cache-t használ
- hiába állítható a registry-ben, a plain-text jelszavak nem cache-elődnek!
- a samba alapértelmezetten csupa kisbetűre konvertálja a user neveket (mert sok win kliens meg nagyra :)
- néháyn win kliens a plaintext jelszót is konvertálja...

Tanulság: ne használjunk plaintext jelszót.

Jelszó tárolási módok

Régebbi megoldások

plain text: UNIX `/etc/passwd`, illetve PAM, de csak akkor, ha plain text jelszót használnak a kliensek

sbmpasswd: `smbpasswd` fájl, tartalmazza LanMan és NT kódolt jelszavakkal, néhány exta. Nem tartalmaz SAM információkat, nem alkalmas együtműködésre NT/w2k-val. *Csak a kompatibilitás miatt maradt, később megszüntethetik!*

ldapsam_compat: samba 2.2 LDAP használata. Föleg migrációs eszközként biztosítják, bár most a migráció nem eredményez közvetlen előnyöket. Később majd megszüntetik.

Jelszó tárolási módok

Új módszerek

tdbsam: csak helyi használatra, nem alkalmas PDC és BDC esetén. Lényegében a régi `smbpasswd` kiegészítve SAM -al, TDB (trivial database) formátumban. Ha csak egyetlen szerverünk van, akkor az LDAP komplexitása nélkül is teljes képességeket elvezhetünk. Nagyjából 250 felhasználóig javasolt.

ldapsam: Teljes funkciós LDAP háttér, több DC-vel rendelkező tartományoknak, szükség esetén redundanciával. Új LDAP sémát használ, több állítási lehetőséggel (per user profile beállítások, home könyvtárak, account access control, stb). Fő tervezési szempont a skálázhatóság volt.

mysql: mysql-ben tárolt SAM.

xmlsam: XML formátumú adatfileban tárolt SAM. Csak a pdbedit használata javasolt, a használt DTD változhat a jövöben. Föleg migrációra és backupra javasolják.

Csoportok

Windows -os felhasználók, csoportok:

- `Administrator` felhasználó tagja az `Administrators` csoportnak
- ha `jozsi` tagja az `Administrators` csoportnak, admin jogai vannak
- ha a gép tartomány tagja, akkor a PDC `"Domain Admins"` csoport tagjai a helyi gép `Administrators` csoport tagjai lesznek

UNIX és windows csoportok megfeleltetése

- `SaMBa` 2.2: `smb.conf : domain admin group`
- `SaMBa` 3: `net groupmap` parancs
- `SaMBa` 3 nem támogatja az egymásba ágyazott csoportokat.

```
domadm:x:502:joe,john,mary
root# net groupmap add ntgroup=Domain Admins unixgroup=domadm
```

Administrator jogok szükségessek:

- `SaMBa` 3 DC és Domain Member Server/Clienseknek
- Domain Member Windows munkaállomások kezeléséhez.
- felhasználók és csoportkok kezeléséhez - ehhez szükségese UNIX jogok is, uid=0, de legalabb gid=0.
- Ha `ldapsam`-ot használunk, akkor kézzel létre kell hozni a windows-ba beépített felhasználókat és csoportokat.

Well-Known Entity	RID	Type	Essential
Domain Administrator	500	User	No
Domain Guest	501	User	No
Domain KRBTGT	502	User	No

Well-Known Entity	RID	Type	Essential
Domain Admins	512	Group	Yes
Domain Users	513	Group	Yes
Domain Guests	514	Group	Yes
Domain Computers	515	Group	No
Domain Controllers	516	Group	No
Domain Certificate Admins	517	Group	No
Domain Schema Admins	518	Group	No
Domain Enterprise Admins	519	Group	No
Domain Policy Admins	520	Group	No

Well-Known Entity	RID	Type	Essential
Builtin Admins	544	Alias	No
Builtin users	545	Alias	No
Builtin Guests	546	Alias	No
Builtin Power Users	547	Alias	No
Builtin Account Operators	548	Alias	No
Builtin System Operators	549	Alias	No
Builtin Print Operators	550	Alias	No
Builtin Backup Operators	551	Alias	No
Builtin Replicator	552	Alias	No
Builtin RAS Servers	553	Alias	No

Access control

Lehetőségek

- UNIX fájl és könyvtár jogok
- `SaMBa` megosztás definiciók
- `SaMBa` megosztás ACL
- MS Windows ACL ⇒POSIX ACL

UNIX fájl és könyvtár jogok

Nevek: Windows 254 (224) karakter hosszú, UNIX 1023, kiterjesztések jelentősége. Pontal kezdődő fájlnevek.

Kis- és nagybetű: A 8.3-as nevek általában nagybetűsek, hosszabak case preserving, de case insensitive. Addig nincs baj, mig csak `SaMBa` -val érjük el, de file.txt, File.txt ls FILE.TXT létezése esetén...

Könyvtár elválasztójel: `SaMBa` jól konvertál

meghajtó betüjelek: UNIX-ban nincs értelmezve

Short-Cut: UNIX hardlinkek mások, symlinkek hasonlítanak.

egyéb: könyvtár és fájl jogok más értelmezése: fájl törléshez UNIX-ban törleshez könyvtár irási jog kell és elég.

A `SaMBa` olyan jogokkal rendelkezik a UNIX fájlrendszerben, mint a bejelentkezett felhasználó.

`SaMBa` megosztás definiciók

force group: UNIX csoportnév, `SaMBa` ilyen jogokkal rendelkezik a UNIX fájlrendszerben.

force user: UNIX felhasználói név, `SaMBa` ilyen jogokkal rendelkezik a UNIX fájlrendszerben.

read only: yes/no

admin users: adminisztrativ jogok a megosztáson a felsorolt felhasználóknak.

write list: egyéb beállításoktól függetlenül írásjoggal rendelkező felhasználók listája.

read list: egyéb beállításoktól függetlenül csak olvasási joggal rendelkezo felhasználók listája.

guest ok: jelszó nélkül elérhető megosztás

valid users: bejelentkezésre jogosult felhasználók listája

invalid users: bejelentkezésre nem jogosult felhasználók listája

only user: yes/no. megosztás szintü biztonságnél van jelentősége, `SaMBa` nem probálja kitalálni a jelszót...

username: csak akkor kell, ha a kliens nem küld felhasználói nevet

UNIX fáljrendszer jogok: `create mask, directory mask` ... jók, de nehezzen kideríthető hibákhoz is vezethet, megfontoltan használjuk.

`SaMBa` megosztás ACL

- alapértelmezetten `SaMBa` nem használja ezt - `Everyone - Full Control`
- a beállításokat a `share_info.tdb` fájlban tárolja, megtekintése `tdbdump share_info.tdb`
- NT4-en kezelése NT Server Managerből lehetséges
- win2k/XP-n File manager, shared folder, jobbkattint, Sharing, permissions
- win2k és később: Control Panel ⇒Administrative Tools ⇒Computer management. Elindítva Action ⇒Connect to another computer. Gép kiválasztása, majd System Tools ⇒Shared Folders ⇒Share Permissions

Vigyázat!!

Ha minden jogot elveszünk `Everyone` **tól, akkor senkinek semmi joga sem lesz!** Ilyenkor inkább töröljük ezt a felhasználót.

MS Windows ACL ⇒POSIX ACL

- Windows NT kliensek natív biztonsági beállító dialogusokat használhatnak
- `SaMBa` nem terjeszti ki a POSIX ACL-eket, A windows ilyen jellegű beállításait csöndesen figyelmen kívül hagyja.
- A teljes fájlrendszer hozzáférést a UNIX vezérli. Bármilyen hibakeresés esetén fontos, hogy pontosan tudjuk windows felhasználó ⇒UNIX felhasználó megfeleltetést.
- jobbkattintás ⇒Properties ⇒Security ⇒Audit művelethez Administrator jogokk kellenek.

`SaMBa` paraméterek és ACL-ek együtműködése

`security mask` miután a `SaMBa` előállította az rwx hármast, maszkolja ezzel. Ahol 0 bit van, az a jog nem valtozik.

`force security mode`**:** az itt beállított bitek mindig be lesznek állítva a végleges jogoknál is.

`directory security mask`**:** értelem szerűen

`force directory mode`**:** értelem szerűen

Teljes jog adása:

```
security mask = 0777
force security mode = 0
directory security mask = 0777
directory force security mode = 0
```

File and record locking

- `SaMBa` biztosítja az összes zárolással kapcsolatos funkciót
- a zárolás többféle dolgot jelent, és mást értenek alatta UNIX-ban mint windows-ban
- legtöbb `SaMBa` teljesítmény-probléma oka a nem megfelelő zárolás

record locking: fájl egy darabjának zárolása

deny mode: fájl megnyitási módok korlátozása

`SaMBa` **2.2 elött:** a UNIX-os `fcntl()` -t használta, ezért nem mindig tudta korrektül intézni a kliensek kéréseit

`SaMBa` **2.2 után:** `SaMBa` saját, alatta lévő operációs rendszertől független zárolást használ

Zárolás 2

- elvileg minden SMB szervernek minden irási és olvasási művelet elött ellenörzi a zárolást
- ez (többnyire feleslegesen) megterhelheti pl az `rpc.lockd` -t
- a `SaMBa` csak akkor hívja meg a zárolási függvényeket, ha a kliens kifejezetten kéri, vagy ha a `strict locking=yes`
- zárolás letiltható, és érdemes is, pl CDROM-ok esetén (`locking=no`)

Deny modes

- Kliens kérhet: `DENY_NONE, DENY_READ, DENY_WRITE, DENY_ALL`
- különleges esetek: `DENY_FCB, DENY_DOS`

Oplocks

- oplock-ot nem API-n keresztül az alkalmazás kéri, hanem a windows file system
- működését registry-n keresztül szabályozhatjuk
- célja a teljesítmény növelése

  read ahead: a kliens a helyi másolatot olvassa

  write caching: kliens helyi másolatot ír

  lock caching: helyben zárol

Level1 Oplock: a fájlt `DENY_NONE` -al nyitották meg, más process nem használja, oplock-ok engedélyezettek. Ekkor kizárólagos, teljes jogot kap. Ha második process megprobál hozzáférni a fáljhoz, a nyitási kérelem várakozik, amig ”fel nem törik” az eredeti oplock-ot. Ekkor a kliens visszaírja a cache-t a kiszolgálóra, eldobja az előre olvasott adatokat. Ha az eredti nyitás nem `DENY_NONE` volt, akkor a következő nyitás ennek megfelelő lehet csak, oplcok-tól függetlenül.

Level2 oplcok: hasonlo level1-hez, de cache csak olvasásra van, az összes többi művelet a szerveren történik

Filter oplock: nem engedi a fájl irását vagy törlését

Batch oplock: fájl nyitás és zársi műveletek, továbbá fájl attribútumok cache-elését teszi lehetővé.

oplock megfontolások

- akkor érdemes használni, ha kliens oldali cache-elés jó nekünk.
- kizárólagosan használt share-ek esetén (például `home`) tipikusan jó
- többszörös hozzáférésű share-eken teljesítmény csökkenést okozhat
- más módon megosztott (pl. NFS) esetén szinet biztos adatkeveredés
- lassú hálózatok esetén oplock jelentős sebességnövekedést hozhat, de!
- megbizhatatlan, túlterhelt hálózatok esetén oplock break üzenet elveszhet!
- `force user` eseten user valtaskor oplock break megy. Ha ez elveszik, kliens folyamatosan ujrakonnektal ⇒teljesitmeny problémák

Oplock tiltás

level1: share-enként `oplocks = False`

level2: share-enként `level2 oplocks = False`

fájlonként: global vagy share szinten:

```
veto oplock files = /*.mdb/*.MDB/*dbf/*.DBF/
```

kernel oplocks: `kernel oplocks = yes`.

oplock-ok Windows-on

Ismert problémák:

- XP bug: KB 812937, SP1-en javítva, de: KB 811492
- NT és kiszolgálókon le kell tiltani az oplock-ot! KB 300216
- ha workstation OS-t használunk szervernek, le kell tiltani
- `HKLM\System\CurrentControlSet\Services\MRXSmb\Parameters\OplocksDisabled REG_DWORD` legyen 1
- `HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\EnableOplocks REG_DWORD` legyen 0
  `EnableOpLockForceClose REG_DWORD` legyen 0 - default
- `LanmanServer` helyett `LanmanWorkstation`

oplock példa lépések

- gep1 megnyitja a fájlt, kér oplock-ot
- mivel más gép nem használja a fájlt, megkapja az oplock-ot
- gep2 megnyitja a fájlt, kér oplock-ot
- mivel gep1 még nem írt a fájlba, a szerver kéri, hogy gep1 törjön level2 oplock-ra
- gep1 leirja a cache-t a szerverre
- gep1 értesíti a szervert, hogy sikerült a művelet
- szerver engedélyezi a fájlnyitást gep2-nek, level2 oplock-al
- valamelyik gép ír a fáljba
- szerver szól az összes gépnek, hogy törjék fel a level2 oplock-ot, azaz űrítsék az read cache-t is. Gépeknek nem kell visszaszólni!

Nyomtatás

Tervezés

- `SaMBa` sokféle képpen tud nyomtatni, itt csak egy-két esetet mutatok
- CUPS-ot érdemes használni
- *raw* vagy *smart* nyomtatás ⇒CPU
- peer-to-peer nyomtatás helyett központi spool
- driverek telepítése kliensenként, vagy point-and-print
- Windows Terminal Server mint CUPS kliens

Egyszerű nyomtatás - CUPS

```
[global]
load printers = yes
printing = cups
printcap name = cups
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
public = yes
guest ok = yes
writable = no
printable = yes
printer admin = root, @ntadmins
```

CUPS beállítások

- *raw* nyomtatást engedélyezni kell
- windows driver install
  - kézzel, minden kliensen
  - point-and-print ⇒drivereket fel kell tölteni
- driver feltöltési módszerek:
  - GUI kliens gépről: Add Printer Wizard
  - parancssorból: `smbclient/rpcclient`
  - CUPS `cupsaddsmb` eszköz

Az ismeretlen segédeszköz - `cupsaddsmb`

- *csak* meghatározott driverekkel működik
  - Adobe Postscript Driver for Windows - win9x/Me
  - CUPS Postscript Driver for Windows - NT, w2k, XP
- pontos lapszámlálás
- nagyobb CPU igény a nyomtatószerverben
- Adobe driver esetén: ”Optimize for Portability”!
- Windows Terminal Server esetén erősen javítja a stabilitást

Driver feltöltés

- elhelyezkedés:
  - `print$` share
  - `W40/0` win9x/ME driverek
  - `W32X86/2` NT kernel mód driverek
  - `W32X86/3` NT új user space driverek
- feltöltés: `smbclient` -el a kliensnek megfelelő alkönyvtárba
- *nem* szabad a 0,2,3 könyvtárba tölteni!
- `rpcclient -c 'addriver...` parancsal regisztrálni
- ellenőrzés: `rpcclient -c 'enumdrivers...` parancs

Egyéb

backup

– szerver backupra **tob**
`<ftp://ftp.icce.rug.nl/pub/unix/tob-X.YY.tar.gz>`

– több szerver esetén nekem bevált a **backuppc**
`<http://backuppc.sourceforge.net>`

– munkaállomás backup kell?

VFS

- `SaMBa` minden beérkező kérést átenged egy virtual file system-en
- VFS modulok stackelhetők `vfs object = audit recycle`,
- **sorrend számít!**

`SaMBa` VFS modulok

audit: connect, dir open/create/remove, file open/close/rename/unlink/chmod syslog -ba

extd_audit: syslog és smbd log, 0-2 log level

fake_perms: hasznos read only roaming profile-okhoz

recycle: nem windows, sajat `.recycle` dir, sok opció:
`keeptree, maxsize, versions, exclude, ...`

netatalk almásoknak

shadow_copy: MS shadow copy client, shadow share, LVM vagy EVMS, snapshot

külső VFS modulok

DatabaseFS: read-only, adatbázis lekérdezésen alapuló könyvtárszerkezet, eredetileg MP3 kezelésére (Artist, Song, Keyword)
`<http://www.css.tayloru.edu/\~elorimer/databasefs/index.php>`

vscan: VFS demo viruskeresők használatához.
`<http://www.openantivirus.org/>`

VFS trükkök

```
[test]
comment = VFS TEST
path = /data
writeable = yes
browseable = yes
vfs objects = example:example1 example example:test
example1: parameter = 1
example: parameter = 5
test: parameter = 7
```

Winbind

- domain user ⇒UNIX user uid lekérdezés
- nss -t használ, gyakorlatilag mint NIS
- akkor kell, ha UNIX felhaszálokat akarunk tartományvezérlőből
  - meglévő win-es tartány, néhány UNIX gép
  - UNIX kiszolgálók tartományban, pl nyomtató szerver

MSDFS

<http://www.microsoft.com/NTServer/nts/downloads/winfeatures/NTSDistrF

- szegény ember HA `SaMBa` -ja
- biztonsági okoból lényeges a dfsroot könyvtár tulajdonosa és jogok
- windows klienseket újra kell indítani, ha egy megosztás DFS képessége változik
- msdfs symlinkek **teljes** elérési útja legyen **csupa kisbetűs**

```
cd /export/dfsroot
chown root /export/dfsroot
chmod 755 /export/dfsroot
ln -s msdfs:storagea
sharea linka
ln -s msdfs:serverb
share,serverc
share linkb
[global]
netbios name = gandalf
host msdfs = yes
[dfs]
path = /export/dfsroot
msdfs root = yes
```

Biztonság

gép szintű biztonság: `bind interfaces,bind interfaces onyl ,`
`hosts allow, hosts deny`

felhasználó szintű biztonság: `valid users = @group, user`

tűzfal:

proto	port	program
UDP	137	nmbd
UDP	138	nmbd
TCP	139	smbd
TCP	445	smbd

IPC$: mindig elérhető guest-ként $\Rightarrow$`[IPC$], host allow`

Biztonság 2

protokoll: ha kell, akkor csak NTLMv2 engedélyezése:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"lmcompatibilitylevel"=dword:00000003

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0]
"NtlmMinClientSec"=dword:00080000
```

Biztonság 3

Tipikus reklamáció: felhasználó látja más felhasznűló home-ját

UNIX megoldás: ha a UNIX-ban a `cd /home/masikuser;ls` engedélyezett, ez teljesen normális ⇒file, dir jogok UNIX-ban

`SaMBa` **megoldás:** home share hozzáférés szűkítés:

```
[homes]
 ...
 valid users = %S
 ...
```

upgrade és migráció

samba 2.2 ⇒3.0

- `SaMBa` 3 **megközelítőleg** úgy viselkedik, mint `SaMBa` 2.2
- új dolgok, paraméterek
- néhány régi paraméterek eltávolítva (domain group map...)
- néhány paraméter alapértelmezett értéke megváltozott
- új LDAP séma, de `passdb backend = ldap_compat` és ldif konvertáló eszköz.
- új `net` parancs
- NT4 pdc ⇒`SaMBa` 3: doksiban leírva

Összefoglalás

The Official Samba-3 HOWTO and Reference Guide

http://hu.samba.org/samba/docs/Samba-HOWTO-Collection.pdf

http://zeus.gau.hu/~lajbi