Samba

9. dubna 2001

Obsah

1 Co je to samba **2**
1.1 Co umí 2
1.1.1 Protokol 2
1.1.2 Bližší popis uvedených možností 2
1.2 Aktuální verze + co nás čeká 3

2 Rozdělení samby **3**
2.1 smbd 3
2.1.1 Fungování smbd 3
2.1.2 Start smbd 4
2.1.3 (důležité) Volby smbd 4
2.2 nmbd 4
2.3 smbpasswd 5
2.4 smbclient 5
2.4.1 Volání smbclient 5
2.4.2 Základní příkazy 5
2.5 Testování konfigurace 6
2.5.1 testparm 6
2.5.2 testprns(1) 6
2.6 Ostatní 6

3 Konfigurace samby **6**
3.1 swat 6
3.2 lmhosts 7
3.3 smbpasswd(5) (soubor) 7
3.4 Samotná konfigurace (smb.conf) 7
3.4.1 Sekce 7
3.4.2 substituce 10
3.4.3 Vyhledávání jmen (DNS, NetBIOS) a komunikace 10
3.4.4 Přihlašování a hesla 12
3.4.5 Soubory 16
3.4.6 Různé konfiguráky pro různé klienty atp.. 18
3.4.7 Problémy s Visual Basic a podobně 18

4 Co tady není **19**
4.1 Logovací a debugovací volby 19
4.2 Jak se tvářit (a fungovat) jako stroj pro 95/98 doménu, případně NT doménu 19
4.3 Příkazy ovládající tiskárnu 19
4.4 Timeouty 19
4.5 Magic script 19

4.6 Mapování home z NIS 19
4.7 Drobnosti mapování DOS<=>UNIX práv 19
4.8 Některé síťové volby 19
4.9 ssl stuff 20
4.10 veto soubory 20

5 Dokumentace 20

1 Co je to samba

Samba je skupina programů pro **UNIX** (v současné době i pro některé další systémy), která umožňuje několik druhů akcí prováděných skrze SMB/CIFS protokol (dříve SMB, nyní CIFS). Tento protokol je někdy také nazýván NetBIOS (a ještě jinak) a pro nás nejpodstatnější je to, že ho využívají veškeré **MS** produkty, které se chtějí bavit po síti (ne vždy lokálně).

Samba umožňuje následující:

1. Sdílení diskových služeb
2. Sdílení tiskáren
3. Podpora browzdání přes NetBIOS protokol (+ WINS server)
4. Přihlašování uživatelů do Windowz domény (95/98, čím vyšší verze, tím lépe chodí i NT doména)
5. Plést pod to **UNIX**-fashion věci, či spíše využívat je. Třeba NFS, NIS apod.

Při tom všem se naše Samba může tvářit jako NT server (klidně jako osm NT serverů), takže nám poskytuje krásný nástroj pro poskytování výše uvedených služeb na Windowz síti - nemluvě o **UNIX**ové spolehlivosti pod tím.

1.1 Co umí

1.1.1 Protokol

Jak už bylo řečeno, používá protokol SMB (Server Message Block) a jeho rozšíření CIFS (Common Internet File Services), někdy také nazývaný NetBIOS. (pozn. v budoucnu chtějí **MS** oddělit NetBIOS a CIFS). Zkratek máme ještě málo, takže WINS = **Windows** Internet Naming Service.

1.1.2 Bližší popis uvedených možností

(1) Sdílení diskových služeb

Umí nabízet jednotlivé adresáře, a to jak pro autentifikované uživatele, tak pro guest přístup. Umí v nich omezovat čtení/zápis, implementovat zámky na souborech, mapovat **DOS**ová práva, schovávat některé soubory... Klidně i provádět mountování svazků při připojení na službu. S poskytovanými "*disky*" se může na klientech normálně pracovat.

(2) Sdílení tiskáren

Funguje jako síťová tiskárna na NT serveru. Kecám. Tam nefunguje. Zato v sambě ano. **MS** by si z ní měli vzít příklad. Na ovládání tiskárny se pak dají definovat **UNIX**ové příkazy pro její ovládání. Je používán /etc/printcap. Máme klasickou tiskovou frontu atd. Určité tiskárny se dají před uživateli skrýt.

(3) Browzdání přes NetBIOS + WINS server

Windowz znají (kromě klasických) dva nové způsoby, jak zjistit kdo je v okolí. První z nich je kontaktovat WINS server, který poskytuje NetBIOS jména počítačů (nejen) v jiných segmentech sítě. Tyto servery si pak mezi sebou mohou "*listy*" vyměňovat. Druhý způsob je poptat se na sousedy svého lokálního master browseru, který zase tlachá s domain master browserem atd. Jedna z hlavních částí samby se jmenuje nmbd a umí jak tvořit si vlastní list, tak jej někomu cpát, tak stát se local master browserem a dokonce i domain master browserem (pokud chcete, můžete k tomu dokonce nmbd donutit, viz později). nmbd se také umí chovat jako WINS server.

(4) Přihlašování uživatelů do Windowz domény

Kromě toho, že umí na požádání autentifikovat uživatele u nějakého NT serveru umí samba také provozovat doménu (být domain masterem). Momentálně je tady jeden fallback, viz níže, ale ve skutečnosti bychom měli být dostat docela schopně fungující **Windows** doménu - navíc nám bude v tomto případě (pokud vhodně nastavíme) velice dobře fungovat browzdání ve Windowz - budeme např. vidět všechny pracovní skupiny, připojení nebude trvat moc dlouho apod.

(5) **UNIX**-runs-behind

Není co komentovat. Snad jen, z trochu jiného soudku, že samba umí používat ssleay, kdežto drtivá většina **MS** klientů ne. Samba *zatím* neumí kerbera ani hierarchické NT domény. To ovšem zatím neumí ani NT server (chystá se to už dlouho).

1.2 Aktuální verze + co nás čeká

Aktuální verze samby je **2.2.** Celý referát byl psán podle dokumentaci k této verzi.

Do budoucna se chystají (hlavně) dvě věci. Za prvé má samba podporovat Unicode, čímž se stane dostatečně kompatibilní s NT domain serverem (výše uvedený fallback) a za druhé bude dále implementovat některé další věci týkající se právě NT domény.

V dokumentaci je několik voleb označených jako **EXPERIMENTAL** nebo jako samba **3.0** only. Ty všechny jsou zde vynechány.

2 Rozdělení samby

Samba se, podle staré **UNIX**ové filozofie, dělí na několik programů a každý z nich se snaží dělat jednu věc.

2.1 smbd

smbd je "*největší*" část samby. Je to server poskytující CIFS služby klientům. Tím se myslí diskové, tiskové a IPC(?) služby.

2.1.1 Fungování smbd

Při každém požadavku na otevření session se vytvoří kopie smbd, která bude klienta obsluhovat. Tato kopie obsluhuje všechny klientovy požadavky a ukončí se až poté, co se klient odpojí.

Konfigurační soubor je reloadován každou minutu, nebo na **HUP** signál. Reload neovlivní jednou započaté sessiony.

smbd akceptuje další dva signály, a to **USR1** a **USR2**. První z nich zvedá log level o jedničku a druhý zase snižuje.

smbd může běžet buďto jako démon, nebo z inetd. Pokud běží jako démon, spojení budou rychlejší, pokud jako inetd, ušetříme nějakou paměť a můžeme použít nějaký tcp-wrapper.

Není doporučeno ukončovat sambu pomocí **KILL** signálu - mohla by být poškozena manipulovaná data. Pokud chcete smabu rychle ukončit, použijte raději normální **TERM** signál (kill pid).

2.1.2 Start smbd

Pokud chcete zprovoznit smbd z inetd, je třeba několik věcí:

(1) Přidat do souboru /etc/services řádku:
`netbios-ssn 139/tcp`
nebo jaký port chceme. Pozor, při změně portu si se smbd budeme moci hrát s **UNIX**u, ale většinu Windowz klientů k přihlašování na jiný port nedonutíme.

(2) Nyní musíme inetd říci, aby při kontaktu na výše uvedený port pustil sambu. Do /etc/inetd.conf, nebo kde konfigurák inetd(8) máme, přidáme řádku (jednu):
`netbios-ssn stream tcp nowait root /usr/local/samba/bin/smbd`

Jestli chceme, aby samba běžela jako démon, pustíme ji s parametrem -D, například z nějakých startovacích skriptů. Typicky se nás instalační package-manager zeptá již při instalaci balíku, jak si přejeme provozovat sambu a vše nainstaluje. Nicméně je dobré vědět, jak daná věc funguje - v případě samby naprosto standardním způsobem.

2.1.3 (důležité) Volby smbd

-D ... samba se odpojí od terminálu a poběží jako démon

-d <debuglevel> ... od 0 do 10, pro normální běh je doporučeno 1, při problémech zvyšovat až na 3.

-l <logfile> ... použij daný file pro logování

-p <číslo portu> ... defaultně ja 139. Pokud si chce se sambou hrát běžný uživatel, pravděpodobně bude potřebovat >1024

-s <configuration file> ... použij specifikovaný konfigurák

2.2 nmbd

nmbd je NetBIOS name server, který poskytuje NetBIOS jména klientům. Dá se nakonfigurovat, aby sloužil jako local master browser i domain master browser (viz níže). Může fungovat i jako WINS nobo WINS proxy.

Stroj, kde běží samba, má taktéž své NetBIOS jméno. Defaultně je to hostname.

Co se týče signálů, pracuje nmbd podobně jako smbd, s rozdílem **SIGHUP**, který způsobí výpis aktuálního namelistu (namelist.debug) do adresáře var/locks v instalaci samby, dále také vypíše databázi serverů do log.nmb.

Volby jsou velice podobné jako u smbd, spíše řečeno stejné. Pokud chcete změnit NetBIOS jméno, dělá se to v konfiguračním souboru smb.conf (viz níže)

Poku pouštíme nmbd skrze inetd, napíšeme do inetd.conf něco jako
`netbios-ns dgram udp wait root /usr/local/samba/bin/nmbd`
a do /etc/services
`netbios-ns    137/udp`

2.3 smbpasswd

Je program sloužící ke změně hesel na kterémkoliv serveru, který provozuje tato hesla - třeba na lokální sambě. Hesla jsou obyčejně ukládána v souboru smbpasswd(5) o kterém bude řeč později.

Pokud je program spuštěn jako root, umožňuje měnit heslo kteréhokoliv lokálního uživatele a manipulaci s účty.

pouští se:

```
smbpasswd [volby] [username]
```

Důležité volby jsou:

-a ... přidej uživatele

-x ... smaž uživatele

-d ... zavře účet

-e ... otevře účet

-n ... nastavit prázdné heslo uživateli (v smb.conf je nutno povolit null passwords = yes, aby se tito uživatelé mohli nalogovat)

-r <NB hostname> ... NetBIOS jmeno stroje, kde se má heslo změnit

-j <doména> ... přidej sambu do NT domény. Viz volba security v smb.conf (později). Po provedení této akce budou uživatelé aktualizováni v NT doméně (samba si stáhne hashovaná hesla).

-U <login> ... při změně hesla na vzdáleném stroji se mění heslo tohoto uživatele

2.4 smbclient

Je **UNIX**ový klient pro přístup k SMB/CIFS serveru. Většinou jej používají **UNIX**oví uživatelé pro stahování věcí z Windowz/Samby, nebo se používá k testování konfigurace samby.

smbclient nabízí (po připojení ke službě) textové ftp-like rozhraní.

2.4.1 Volání smbclient

```
smbclient {jméno sdílené služby} [-d debuglevel] [-S server] [-U username]
[-W workgroup [-p port] [-s samba_config_file] [-L] [password]
```

Má ještě další volby, ty ale viz smbclient(1).

{jméno sdílené služby} je ve formě //server/služba, kde server je NetBIOS jméno serveru.

pokud nespecifikujeme heslo, objeví se prompt.

Username může být ve tvaru username%password.

Volba -L způsobí výpis všech služeb na serveru.

Nastavením workgroup se změní implicitní skupina ze smb.conf.

2.4.2 Základní příkazy

? příkaz ... vypíše help k danému příkaz

exit ... skončí session

cd, ls, del, dir, rm ... jako obvykle

mask maska ... nastaví masku, která se bude používat při rekurzivním mget/mput

mkdir, md, rmdir, rd ... tvoří a maže adresáře

mget maska, mput maska ... stejně jako u ftp

print soubor, vezme lokální soubor a pošle jej tiskové službě na serveru

printmode graphics/text ... self-explanatory

get remote_file [local_file], ... jasné (stejně tak **put**)

prompt, recurse ... jako u ftp

smbclient umí používat tar, viz smbclient(1)

2.5 Testování konfigurace

Kromě výše uvedeného smbclient, který je pro testování hodně silný nástroj, máme ještě některé další.

2.5.1 testparm

testparm(1) slouží k testování souboru smb.conf. Pokud testparm na nějakém souboru uspěje, znamená to pouze, že jej při startu samba v pořádku načte, ne že by všechno co jste chtěli muselo fungovat.

Při nalezení chyby vrací tesparm returnlevel 1, a navíc na stdout vypíše seznam chyb, které našel.

Spustí se

`testparm [-L servername] [konfig_file] [hostname hostIP]`

-L servername ... mastaví makro %L na hodnotu servername (viz později)

hostname hostIP ... vypíše, ke kterým službám bude mít daný host přístup

2.5.2 testprns(1)

`testprns jmeno_tiskarny [printcap_soubor]`

Prohledává specifikovaný printcap, a řekne, jestli je daná tiskárna dostupná (ne jestli tiskne).

2.6 Ostatní

K balíku programů kolem samby patří například i program nmblookup(1), který provádí převod NetBIOS jmen na IP, nebo třeba program smbtar(1), což je shellscript, provádějící zálohy sdílených "*disků*" rovnou na **UNIX**ové pásky.

3 Konfigurace samby

Zde popíši konfigurační soubory samby a způsoby její konfigurace. Hlavní část je v bodě 3.4.

3.1 swat

swat je program poskytující možnost spravovat nastavení samby přes www rozhraní, a to jak lokálně, tak i vzdáleně - podporuje totiž SSL. HTML stránky odpovídají standardu, lze je tedy pohodlně browsovat lynxem nebo linksem. Pro uživatele nabízí možnost změny hesla, pro roota pak změny hesel uživatelů a taktéž změny konfigurace - jak globálních nastavení, tak jednotlivých sdílených služeb

3.2 lmhosts

Něco jako hosts file, akorát že obsahuje k NetBIOS jménům IP adresy.

Příklad: (aisa)

```
nereus 147.251.52.111
```

3.3 smbpasswd(5) (soubor)

Soubor se sambími hesly. Jsou v zakódované podobě - a to jak Lanmanager, tak NT. Obě funkce jsou hashovací - nepoužívají ovšem sůl, čili dva uživatelé se stejným heslem budou mít stejný hash záznam (:-). Ke každému heslu obsahuje soubor username, **UNIX** uid, flagy a datum poslední změny hesla.

Více viz smbpasswd(5), ENCRYPTION.txt

3.4 Samotná konfigurace (smb.conf)

Všechno důležité týkající se poskytovaných služeb včetně způsobů poskytování a přístupu k nim je uvedeno v souboru smb.conf.

Tento soubor najdeme povětšinou na /etc/samba/smb.conf

Na každém řádku může být buďto specifikace sekce (později), komentář (znaky # nebo ;), nastavení hodnoty v sekci

jmeno = hodnota

(mezery kolem = se mohou vynechat)

nebo může být řádek prázdný (přeskakuje se). Dva řádky můžeme spojit pomocí \. Hodnota je buď řetězec, číslo, nebo pravdivostní hodnota (1,0,yes,no,true,false).

Každý z parametrů může být uveden buďto pouze globálně (značený (G)), nebo v kterékoliv sekci (tedy i v globální) - značeno (S)

3.4.1 Sekce

Specifikace sekce

Každá sekce má jméno v []. Může specifikovat souborovou/tiskovou službu. Vždy je uveden adresář, ke kterému se služba vztahuje. Máme tři speciální sekce, a to [global], [homes] a [printers]. Jediná sekce [global] v celém souboru nepopisuje sdílenou službu a proto nemá specifikovaný adresář. Sekce končí uvedením další sekce nebo koncem souboru.

Někteří **DOS**oví klienti umějí sekce s max. 8 znaky dlouhým názvem. Jméno sekce poté ořežou a tudíž se na službu nemohou napojit. Další problém může vzniknout s mezerami. Obecně je lepší používat podtržítka.

Příklad sekce:

```
[moje_killdos_sekce]
        path = /mnt/dos
        writeable = yes
```

Sekce [homes]

Tato sekce slouží pro připojování k uživatelským home (jméno sekce je vyhrazeno). Pokud se při přihlášení nenajde v poskytovaných službách žádaná služba, samba se pokusí autentizovat jako uživatel (se jménem požadované služby). Pokud se jí to povede, je použita sekce [homes]. Jméno poskytované služby se ještě on-the-fly změní na uživatelovo jméno. Pokud není nalezena cesta podle vzoru v [homes], aktuální adresář se změní podle záznamu v /etc/passwd. Cesta v [homes] se nastaví pomocí substituce %S (viz dále), např:

```
[homes]
        path = /mnt/home/%S
        writeable = yes
```

Existuje ještě druhá možnost připojení na home - pokud klient uvede jako požadovanou službu "home". V tomto případě se název služby nemění (v některých případech vhodné).

Pozor na "guest" !

Sekce [printers]

Uživatelé se mohou připojit na kteroukoliv tiskárnu uvedenou v printcap (obvykle /etc/printcap). Pokud chcete omezit dostupné tiskárny, je třeba udělat pseudo-printcap a udělat na něj odkaz v sekci [global] - viz dokumentace, hledejte "*pseudo*".

Připojování k sekci probíhá podobně jako připojování k [homes], resp. pokud není požadovaná služba autentifikována jako uživatel, projde se printcap.

Sekce [printers] musí být "printable".

Sekce [global]

Parametry v této sekci se aplikují na všechny služby. Navíc se zde specifikují obecná nastavení samby.

Související parametry

path (S) ... cesta ke sdílené službě (adresář). Defaultní neexistuje. Je třeba zadat u každé služby.

available (S) ... (default yes) - pokud no, tak všechny požadavky a danou službu selžou.

copy (S) ... kopíruje volby z jiné služby. Nově specifikované parametry přebijí zkopírované parametry. Například

```
[nar]
        path = /mnt/nar
        writeable = yes
        comment = "Nar, the ultimate killer"
[nar_guest]
        copy = nar
        writeable = no
        quest ok = yes
```

volume (S) ... změní název služby. Užitečné pro instalační CD-ROMs.

default service (G) ... specifikuje, která služba se má defaultně otevřít, pokud nemůže být nalezena služba požadovaná. Např.

```
default service = nar_guest
```

force user (S) ... specifikuje uživatele, který se použije pro přístup k souborům. Tato změna identity se použije až poté, co se klient úspěšně autentifikuje. Např.

```
force user = kobzol
```

force group (G) ... specifikuje skupinu, která má být použita jako primární skupina všech uživatelů, připojujících se k dané službě. Přeflákne i primární skupinu uživatele vynuceného pomocí force user.

guest account (S) ... určuje **UNIX**ového uživatele, který se použije pro anonymní přístupy (guest přístupy).

guest ok (S) ... boolean, default no. Na danou službu je možno přihlásit se jako guest (viz níže)

hide local users (G) ... boolean, default no. Schovat lokální **UNIX**ové uživatele (root, floppy,...) ?

invalid users (S) ... vynikající volba pro optimisty (pro mě). Dá se jí například s naprostou jistotou zamezit nahlášení roota (mimo to, že ten by stejně neprošel ani omylem, ale my optimisté...). Naprosto redundantní, zbytečné, ale krásné je například:

```
[global]
        invalid users = root
```

username (S) ... seznam uživatelů, oproti kterým se *také* bude testovat heslo (viz 3.4.4.1). Synonymem je user. Příklad:

```
username = hisaak, bralin, kobul
```

read list (S) ... list uživatelů, kteří dostanou přístup pouze pro čtení, i kdyby byl writeable nastaven na yes. Je možno specifikovat skupinu uživatelů přes @.

write list (S) ... list uživ., kteří dostanou read-write, i kdyby bylo writeable nastaveno na no. Silnější než read list.

only user (S) ... boolean, default no. Pokud yes, tak se může přihlásit pouze uživatel uvedený v username listu.

max connections (S) ... počet maximálních napojení na službu, defaultně 10

preexec (S) ... příkaz, který se provede při připojení na službu. Defaultně nic. Například

```
[xxx_site]
          preexec = /bin/bash -c 'echo BAAAAAAAAAAA GOTCHA!, user %U
from %m at service %S! Telling everybuddy around...' | /usr/bin/smbclient
-M %m -I %I' &
```

Pošle hezkou WinPopup zprávu každému, kdo se připojí na xxx_site. Pokud se připojuje z něčeho co umí WinPopup (třeba samba (a ta to třeba pošle mail adminovi (ať se pobaví :-))).

root preexec (S) ... příkaz se provede pod rootem. Defaultně nic. Např pro přimountování cdrom. V takovém případě je ale lepší v /etc/fstab povolit o=user a mountovat jako uživatel, to je ale na delší diskuzi.

preexec close (S) ... má se služba zavřít pokud se nepovede preexec? Default no.

root preexec close (S) ... má se služba zavřít pokud se nepovede preexec? Default no.

postexec (S) ... příkaz, který se má vykonat při odkonektění od služby. Defaultně nic. (např odmountování cdrom)

root postexec (S) ... postexec jako root

message command (G) ... co dělat, když server dostane WinPopup zprávu. Je možno ji poslat pomocí mail atp. Příkaz se musí ihned vrátit (např. pustit na pozadí). Defaultně nejsou message command. Příklad:

```
message command = rm %s
```

(%s je soubor obsahující zprávu, %t komu byla poslána a %f od koho je)

3.4.2 substituce

Při psaní parametrů máme k dispozici několik užitečných maker, např.:

%S ... service ... jméno služby, ve které se nacházíme (použití v např. [homes])

%u ... user ... jméno uživatele

%U ... session user name ... požadované jméno uživatele (mohl dostat jiné)

%h ... hostname ... jméno stroje, kde běží samba

%m ... client machine ... NetBIOS jméno klientova stroje

%L ... NetBIOS server name

%N ... NIS home directory server

%p ... path ... cesta k home adresáři služby na NIS

%R ... protocol

%I ... klientova IP addresa

%$(envar) ... value of environment variable "envar"

Další viz dokumentace.

3.4.3 Vyhledávání jmen (DNS, NetBIOS) a komunikace

Nalezení hosta

name resolve order (G) ... v jakém pořadí se bude hledat IP adresa ke jménu. Čtyři možné hodnoty, resp. zadává se jejich kombinace ve zvoleném pořadí: lmhosts, hosts, wins, bcast.

lmhosts ... hledá se v souboru lmhosts (viz výše)

hosts ... standardní /etc/hosts, NIS, DNS (v pořadí podle /etc/nsswitch). Tento typ je použit tehdy a jen tehdy pokud se vyhledává NetBIOS server.

wins ... zeptej se na jméno wins serveru (viz níže). Pokud není wins server specifikován, tento typ hledání se ignoruje

bcast ... broadcast na všech lokálních interfaces. Pokud není klient na lokále, nenajde ho.
Defaultně: name resolve order = lmhosts host wins bcast

wins server (G) ... IP adresa wins serveru
wins server slouží k tomu, aby různé podsítě byly schopny dostat NetBIOS jména počítačů z ostatních podsítí a také k resolvování těchto jmen zpět na IP.
jako wins server může sloužit i nmbd, o tom ale v BROWSING.txt, wins support a wins hook v smb.conf(5) a nmbd(8).

remote announce (G) ... nmbd bude periodicky posílat "*já jsem tady a kde jsi ty; neváhej a připoj se*" zprávy na uvedené IP (list). Může to být buďto IP browse master (nepravděpodobné), nebo broadcast adresa cílové sítě. Dále je možno uvést skupinu, pod kterou bude samba viditelná. Jediný účel je protlačit se tam, kam nás normálně vody NetBIOSu nezanesou. Příklad:

```
192.194.38.255/BEAUTY, 149.250.18.255/AND, 147.251.48.255/BEAST
```

remote browse sync (G) ... periodická synchronizace browse listu, pouze s další sambou! Opět se zvolí broadcast adresa cílové sítě.

Pohled zvenku

server string (G) ... Co se objeví u jména stroje, u tiskárny a IPC. Defaultně:
`server string = Samba %v`
(%v je verze)

netbios name (G) ... NetBIOS jméno samby. Defaultně jako hostname.

netbios aliases (G) ... další jména, pod kterými je znám Samba server. Velice užitečné pokud chceme mít různé konfigurace - viz 3.4.6

workgroup (G) ... jméno pod kterým je samba vidět. Pokud je použito security=domain (viz níže), znamená i jméno domény.

auto services (G) ... list služeb automaticky viditelných zvenku (při browse)

browseable (S) ... boolean, určuje, zda je služba zvenku viditelná. Také browsable.

comment (S) ... obsahuje komentář k příslušné službě. Například comment="*this is not warez*"

local master (G) ... boolean, default yes. Má se samba pokusit stát se lokálním master browserem?

preffered master (G) ... boolean, samba (nmbd) se za každou cenu pokusí stát local master browser. Pokud jsou na stejném subnetu TNT nebo Windowz 0.98/0.95 a pokládají se za preffered master, budou vyvolávat local master browser election každou chvíli (jednou jsem tu zeď hlavou neprorazil, tak co za chvilku?). Default no.

os level (G) ... hodnota pro local master browser election. Defaultně 20 (přebije 95/98, pustí NT, 60 přebije cokoliv (kromě jiné samby :-))

domain master (G) ... boolean, default no, nmbd se pokusí stát "domain master browser" - bude sbírat browse listy lokálních master browserů a zasílat jim je zpátky, skloubené dohromady. Problém když je nějaký NT PDC - pokusí se tento status získat také.

fstype (S) ... filesystem typ, který vidí klient. Defaultně NTFS.

lm announce (G) ... užitečné pouze pro OS2. Hodnoty jsou false, true, auto. Default auto. (broadcastování "*haló, tady jsem*")

lm interval (G) ... interval v sekundách, jak často se vysílá. Default 60.

allow a deny
Povolování a zakazování některých hostů. Chová se přesně jak bychom očekávali (vypíšeme koho allow - ostatní jsou deny atp.).

hosts allow (S) ... list hostů, pokud specifikovaný globálně, aplikuje se na všechny služby nezávisle na jejich vlastních allow, deny. List je oddělen mezerami, tabulátory nebo čárkami. Můžeme uvést i IP adresy, dokonce i oblast (např. vynecháme poslední část adresy). Můžeme použít klíčové slovo EXCEPT. Přesněji viz hosts_access(5). Localhost pojede vždy, dokud jej explicitně nezakážeme v deny. Příklad:
`hosts allow = 147.251. happypuppy.here.and.there @hackit`

hosts deny (S) ... specifikace jako u hosts allow, například
`hosts deny = 147.251.48.`

Další volbou je hosts equiv (G), určující jméno souboru, obsahujícího jména hostů, kteří se mají hlásit bez hesla. Užitečné v případě klientů neposílajících heslo, nicméně nebezpečné.

Související volby

allow trusted domains (G) ... boolean, pokud provádí autentifikaci někdo jiný než lokální samba:
yes ... (default) povolí připojení z kterékoliv NT domény, které věří server provádějící autentifikaci
no ... povolí připojení pouze z NT domény, ve které je samba.

bind interfaces only (G) ... slouží ke svázání samby jen k určitým síťovým zařízením. Vhodné pro běh několika serverů, viz smb.conf(5).

interfaces (G) ... další způsob omezení interface, viz smb.conf(5)

max xmit (G) ... maximální velikost packetu, s jakou bude samba operovat. Defaultně 65535. Zmenšením je (někdy) možno dosáhnout lepšího výkonu.

3.4.4 Přihlašování a hesla

Postup při přihlášení
Přihlašování probíhá následovně: (pokud se neuplatní žádný z bodů, je spojení odmítnuto)
Pokud je service "guest only = yes" skáče se rovnou na 6. krok.

(1) username/passwd se ověřuje proti **UNIX** uživateli

(2) pokud klient poslal již dříve username, ověřuje se heslo (**UNIX**)

(3) klientovo NetBIOS jméno a dříve použití uživatelé jsou ověřeni (s poslaným heslem) (**UNIX**)

(4) pokud se klient již dříve autentizoval username/passwd a prokáže se platným tokenem, je vpuštěn

(5) každá dvojice user+poslané heslo, kde user se bere z “username =” uvedeného u služby, je ověřena proti **UNIX** uživateli (viz popis volby user).

(6) pokud je služba “guest ok”, spojení se vytvoří pod uživatelem uvedeným v “guest account =”

Konzistence UNIX/NT databáze uživatelů

Aby se mohl uživatel na systém přihlásit i v případě že na něm nemá účet, ale je právoplatným uživatelem na NT a my mu chceme přihlášení (po ověření totožnosti proti NT) povolit, uděláme následující:

(1) Zvolíme si NT server, který bude provádět autentizaci za nás. Bude ji provádět vždy, takže nad ním musíme mít absolutní kontrolu (a nikdo jiný). Nastavíme hodnotu password server (G):

```
[global]
password server = NT_PSWDS, NT_PSWDSW2
```

Jméno se uvádí v NetBIOS formě. Je možno použít %m, čímž necháme klienta ověřit na sobě samém - to má ovšem dva háčky: jednak to jeho OS musí umět (podporovat příslušný protokol, jet na něm NT) a druhak tím automaticky věříme všem klientům. Je na místě omezit klienty (volba “hosts allow”).

(2) Nastavení security (G)

Parametr security musíme nastavit na hodnoty server nebo domain. Pokud použijeme domain, v password server musíme uvést Primary Domain Controller nebo Backup Domain Controllers počítače. Autentifikace pak bude probíhat přesně jako v NT doméně.

V současné době není security = domain úplně použitelné, protože komunikace s Domain Controller se vede v unicode a samba zatím do unicode moc nepřevádí. Použijeme security = server.

(3) Přidání uživatele

Po úspěšné autentizaci se samba pokusí projít skrze /etc/passwd ale to se jí zřejmě nepovede a tak musíme specifikovat volbu “add user script =”. Tato volba ukazuje na skript, který je schopen přidat uživatele do **UNIX**ového systému. Skript musí být schopen akceptovat jméno uživatele. Skript je pouštěn pod rootem.

```
add user script = /usr/local/samba/bin/add_user %u
```

můžete vyzkoušet třeba

```
add user script = /usr/sbin/useradd %u
```

(4) Zapneme encrypt passwords (G)

```
encrypt passwords = yes
```

Kryptovaná hesla lokálně

Pokud chceme používat kryptovaná hesla lokálně - tzn. nemáme NT doménu a nechceme aby hesla chodila nekryptovaná, musíme se smířit s tím, že je nebudeme schopni ověřovat proti **UNIX**ovému uživateli (kryptování se na straně klienta provádí hashovací funkcí). Hesla tedy budou schována v lokálním smbpasswd(5) souboru.

Máme dvě možnosti. Buďto uděláme soubor sami (jiní uživatelé než v **UNIX**u) a specifikujeme parametr add user script (viz výše). Nebo vytvoříme smbpasswd(5) výcucem z /etc/passwd (samozřejmě hesla nevytáhneme). Uživatelé si budou schopni měnit heslo pomocí smbpasswd(8) (programu), ověřování bude probíhat proti tomuto souboru a **UNIX**oví uživatelé budou existovat.

Soubor se vytvoří takto:

```
cat /etc/passwd | mksmbpasswd.sh >/usr/local/samba/private/smbpasswd
```

nebo pro NIS:

`ypcat passwd | mksmbpasswd.sh >/usr/local/samba/private/smbpasswd`

Více o formátu souboru viz manové stránky smbpasswd(5) a dokumentace - soubor ENCRYPTION.txt v distribuci dokumentace.

Snad jen, že v souboru lze nastavit různé vlastnosti účtu uživatele (pozastavit jej, povolit přístup bez hesla,...)

Popis security (G)

možnosti: share, user, server, domain

Ve starší verzi samby byla defaultní hodnota share, nyní to je user.

security=share Používá se hlavně pro volnější přístup. Klient zasílá username/heslo až při požadavku na službu, ve skutečnosti není nucen zasílat username. Username se zjišťuje několika způsoby (viz manuálová stránka smb.conf, hledejte security (g)).

V tomto módu se nedají použít zakódovaná hesla. Uživatel se opět ověřuje proti **UNIX**ovému účtu. Je velice jednoduché udělat guest účty:

```
[global]
        guest account = guest
[warez]
        path = /mnt/warez
        guest ok = yes
```

Parametr "guest ok" znamená logování pro uživatelem uvedeném v "guest account", BEZ hesla.

Je možno použít parametr "guest only = yes", čímž způsobíme možno zalogovati se toliko jako uživatel v "guest account". Musíme ale zároveň specifikovat "guest ok".

Dále je k dispozici volba "username map (G)", která ukazuje na soubor obsahující mapování uživatelů na klientech na **UNIX**ové uživatele. Díky němu je možno automaticky namapovat Windowz jména uživatelů (i s mezerami) na **UNIX**ové uživatele, mapovat několik uživatelů na jednoho (velice užitečné), a klidně i jako poslední paranoidní záchranu (pravidla guest = root a guest = *) jednak kvůli bezpečnosti a jednak kvůli tomu, aby se nám kterýkoliv uživatel nějak namapoval. Soubor obsahuje na každém řádku jedno mapování, více viz smb.conf(5). Ještě je třeba mít na paměti, že uživatel neví, na koho se vlastně namapoval. Poslední poznámka je k výše uvedenému řádku guest = *. Pokud nám přibude uživatel, při hlášení z NT se automaticky namapuje na guest. Je tedy třeba soubor udržovat. Při mnoha uživatelích přestávají mít pravidla neco = * a různá rozdělení do skupin smysl.

!!! Poznámka: uživateli odpovídajícímu "guest account" přidělíme v /etc/passwd neplatný shel - nedovolíme mu nalogovat se (např. /bin/false)

security=user Toto nastavení je daleko výhodnější, neboť umožňuje použít volbu "encrypt passwords = yes".

Problém ovšem nastává pro guest přístup, neboť název požadované služby se předává až po úspěšné autentizaci. Tuto situaci částečně řeší parametr "map to guest (G)", který smbd říká, co má dělat, pokud nenajde specifikovaného uživatele v /etc/passwd (resp. v smbpasswd(5) při "encrypt passwords = yes"). Parametr může nabývat následujících hodnot:

Never ... loginy pod špatným heslem (i neexist. uživ.) jsou ignorovány (default)

Bad User ... když špatné heslo, tak pokud daný uživatel neexistuje, požadavek se mapuje na “guest account”. Pokud pak nebude mít požadovaná služba “guest ok=yes”, připojení samozřejmě selže.

Bad Password ... neúspěšný login i na existujícího uživatele bude považován za guest login. Uživatel se nedozví jako co se přilogoval (nepřijde mu "*špatné heslo*").

security=server Samba se pokusí autentifikovat uživatele u daného NT serveru (viz 3.4.4.2). Pokud se jí to nepovede, spadne na security=user. V tomto okamžiku má buďto smbpasswd(5) soubor a heslo checkne, nebo selže (nemůže heslo odhashovat a porovnat s /etc/passwd).

Je možno použít “encrypt passwords = yes”.

Co se guest loginu týká, platí totéž jako u security=user (viz výše)

security=domain Předpokládá se “encrypt passwords = yes”. Samba ověřuje heslo u Domain Controlleru (viz 3.4.4.2). Na lokále se stále musí použít nějaký **UNIX**ový uživatel.

Při přihlašování do domény může samba obdržet hlášku user no longer exist (noba tak nějak) a může tedy uživatele smazat (z **UNIX**ového účtu!). Pokud vytváříte uživatele dynamicky a nemáte stejná jména, můžete tuto featuru využít. Stačí zadefinovat skript, který provede smazání uživatele:

`delete user script = /usr/local/samba/bin/del_user %u`

možná by mohlo fungovat

`delete user script = /usr/sbin/userdel %u`

Co se guest loginu týká, platí totéž jako u security=user (viz výše)

Změna hesla pro UNIX

Tyto volby jsou všechny špatné (kromě unix password sync = no), protože špatné je používat styl autentizace přes **UNIX**ový /etc/passwd (nemožno encrypt passwords). A pokud se používá encrypt passwords, ověřuje se proti smbpassdw(5), takže je možno maximálně udržovat stejné heslo na NT a **UNIX**, jenže to stejně pravděpodobně máme jiné uživatele tam a tam a navíc se /etc/passwd mění hrubou silou (není známo staré heslo), nu, škoda mluvit (nebo psát).

min password length (G) ... minimální akceptovatelná délka hesla při měnění hesla.

unix password sync (G) ... boolean, default no. Pokusit se udržet (jednostrannou! nekontrolovatelnou! přemáznete si **UNIX**ové uživatele!) synchronizaci s unixovými hesly? (NE!)

passwd program (G) ... specifikace programu pro změnu hesla. Defaultně /bin/passwd.

password level (G) ... tolerance u/l case v hesle. Někteří klienti mají potíže s mixováním case, tedy pokud je heslo AHOJ a password level je 1, zkusí se AHOJ, aHOJ, AhOJ, AHoJ a AHOj. atp. Defaultně 0. Lepší než tohle měnit je říci lidem používajícím problémové klienty ať používají hesla o stejném case (třeba ať si zapnou caps lock), většinou to povede k vyšší bezpečnosti než zvyšování password level.

user level (G) ... podobně jako passwdord level, defaultně 0. Je zřejmé, že není tak nebezpečné jako password level (jména uživatelů se u rozumného admina liší více než jen case).

passwd chat (G) ... určuje, jak bude probíhat komunikace s programem měnícím heslo. Default: passwd chat = *old*password* %o\n *new* password* %n\n *new*password* %n\n *changed*

Související volby

smbd passwd file (G) ... lokace souboru smbpasswd(5)

admin users (S) ... list uživatelů, kteří mají u dané služby rootovský přístup

null passwords (G) ... povolit prázdná hesla? Default no. Viz smbpasswd výše a smbpasswd(5)(8)

3.4.5 Soubory

Case

Bližší rozpis v manuálové stránce smb.conf(5) (hledejte NAME MANGL), zde stručně:

Jedná se hlavně o problém upper/lower/mix case. Různí Windowz klienti se chovají různě. Defaultně se samba chová jako NT server - tedy case zachovává, ale při požadavcích na soubory je case intensive.

Volby: (mohou se nastavit globálně)

mangle case = yes/no <no> ... mají se case-nevyhovující znaky přenastavit?

case senzitive = yes/no <no>

default case = upper/lower <lower>

preserve case = yes/no <yes> ... zachovávat case?

short preserve case = yes/no <yes> ... zachovat i case 8.3 souborů (upper) ?

Native znakové sady

Převod jmen souborů mezi codepage **UNIX**<=>Windowz.

character set (G) ... codepage na serveru. U nás ISO8859-2.

client code page (G) ... v případě serveru ISO8859-2 musí být nastaveno na 852. (client code page=852)

Tvorba souborů a adresářů

Při tvorbě souborů a adresářů se jejich iniciální práva mapují podle **DOS**ových práv, a dále se uplatňují následující parametry (v uvedeném pořadí):

Soubory:

create mask (S) ... ořezání práv. Provádí se AND těchto práv s **DOS**ovými, default je 0744. Také create mode.

force create mode (S) ... minimální práva. Provádí se OR. default je 0000

Adresáře:

directory mask (S) ... jako create mask, pro adresáře, default 0755, také directory mode.

force directory mode (S) ... jako u souborů, default 0000.

Další možností je použít inherit permissions, kde podadresáře dědí práva od adresářů a soubory taktéž (částečně). viz smb.conf(5).

Dalšími z parametrů jsou force directory security mode, security mask, force security mode, všechny (S), určují, jak se má samba chovat při měnění přes "*NT security dialog box*". Viz smb.conf(5).

Manipulace se soubory a adresáři, procházení stromem

delete readonly (S) ... povolí mazání read-only souborů (normální **DOS**ové chování)

dont descend (S) ... obsahuje list adresářů, ve kterých samba nepůjde níž, například
`dont descend = /proc`

follow symlinks (S) ... boolean, default yes.

getwd cache (G) ... cache algoritmus pro redukce času spotřebovaného getwd() voláními. Defaultně no.

hide dot files (S) ... boolean, default yes. Schovat tečkové soubory?

hide files (S) ... masky pro schování souborů, jsou mezi sebou odděleny pomocí '/', např:
`hide files /*.swp/*kobzol*/`

oplocks (G) ... default yes. (opportunistic locks)

kernel oplocks (G) ... default yes, umí je zatím jen **IRIX** a **Linux 2.4**

level2 oplocks (G) ... umožňuje on-the-fly downgrade oplocku z read-write na read-only. Zatím v testovací fázi. Není garantováno. pokud se používají kernel oplocks, default no.

locking (S) ... boolean, default yes. Má se opravdu provádět lockování? Pokud no, zámky se budou pro klienty tvářit že uspěly, ale ve skutečnosti se neuskuteční. Vypínat pouze na read-only fs!

root directory (G) ... samba se chrootne do výše uvedeného adresáře. Nepoužívá se příliš často. Ač tato volba zaručuje určitou míru optimistického přístupu, vznikají problémy s /etc/passwd - i když takto můžeme mít krásně unix passwd sync a nekonfliktíme s **UNIX**ovými uživateli, nebudou nám v reále sedět uid a gid a pro **UNIX**ové uživatele vznikne chaos - za předpokladu, že nemáme homey **UNIX** x samba odděleně. Pokud ano, můžeme toto použít (samba bude dělat uid a gid podle nesmyslného passwd, ale bude k těmto souborům přistupovat pouze podle něj, takže se nic špatného dít nebude.) a okopčit některé důležité věci do sambího stromu. Samba tak bude moct dělat bordel jen na svém písečku a všichni ostatní budou happypuppy.

wide links (S) ... povolit linky vedoucí ven z adresářového podstromu dané služby? Default yes.

3.4.6 Různé konfiguráky pro různé klienty atp..

Máme k dispozici dvě hinty jak upravit konfigurační soubor on-the-fly.

První je drsnější:

config file (G) ... obsahuje jméno souboru, kde je uložen konfigurák. Dosavadní parametry se zahodí a začne se číst znovu, pokud soubor existuje. Pokud ne, pokračuje se v tomto konfiguračním souboru.

Užitečné to je samozřejmě díky substitucím, např.:
config file = /etc/samba/smb_%m_.conf

Můžeme mít několik konfiguračních souborů pro speciální klienty (nabídnout jim více). %m je NetBIOS jméno klienta.

Ještě lepší je:
config file = /etc/samba/smb_%L_.conf

Kde %L je NetBIOS jméno, pod kterým jsme byli zavoláni. Můžeme například poskytovat tytéž služby pod dvěma jmény serveru, kde jednou budou hesla krytá (pro NT) a jinde ne, a spoustu jiných věcí. (například po této volbě uplatnit ještě následující include %m substituci v dalších konfiguracích atp.)

Druhá, měkčí varianta:

include (G) ... zahrň konfigurační soubor

include = /etc/samba/smb_%m_include.conf

Nám dovolí na místo zahrnout konfigurační soubor. Je to naprosto vynikající volba pro poskytování extra služeb pro některé klienty. Tuto volbu ovšem musíme dát na konec [global] - pokud ve vnořených konfig. specifikujeme nějaké služby.

3.4.7 Problémy s Visual Basic a podobně

Problém s časem

Granularita času poslední modifikace souboru ve FAT je 2 sekundy. Pokud si VB myslí, že se soubor mění, ale přitom se nemění, je to řešitelné nastavením samba granularity také na 2s, takto:

```
dos filetime resolution = yes
```

dos filetime resolution (S) ... default no.

Další problém s časem

Když pod **DOS**em někdo zapíše do souboru, automaticky se změní čas poslední modifikace. Pod **UNIX**em může timestamp měnit pouze root. Pokud tedy uživatel (jeho programy) modikuje soubor a přitom není jeho vlastníkem, mohou si programy stěžovat, že se timestamp nemění (či spíše něco neudělat). Řešení je "dos filetimes = yes" (S), default no.

Pro změnu zase problém s časem

FAT má datum vytvoření pro každý adresář. **UNIX** ne. VC++ makefiles budou velice často překompilovávat spoustu souborů, protože budou "*staré*" (starší než adresář). Pokud zapnete "fake directory create times = yes" (S), def. no, budou se všechny adresáře tvářit jako 1-1-1980, 00:00.

Problém s volným místem

Pokud není klientský systém správně schopen interpretovat volné místo na sdíleném disku, můžeme ho nastavit pomocí max disk size (G), defaultně 0 = bez limitu. Například:

```
max disk size = 350
```

nastavíme velikost disku jako 350. Pokud se klient podívá na cokoliv (včetně volného místa), dostane maximálně 350 MB. A když pak zapíše 250 MB, může třeba dostat volných opět 350 MB (:-) (neverending pytel?)

Problém s ukládáním souborů

Tento problém je na straně serveru v případě mnoha klientů a mnoha otevřených souborů. V logu se objeví:

```
ERROR smb_shm_alloc : alloc of XX bytes failed
```

Řeší se nastavením parametru shared mem size (G) na vyšší hodnotu. Default 1048576 (1 MB). Je to množství sdílené paměti mezi smbd procesy.

4 Co tady není

4.1 Logovací a debugovací volby

Viz popis v smb.conf(5)

4.2 Jak se tvářit (a fungovat) jako stroj pro 95/98 doménu, případně NT doménu

Tyto featury ještě všechny nejsou úplně naimplementovány, ač většina běžných věcí se dělat dá.

Viz direktivy v smb.conf(5), začínající na logon.

4.3 Příkazy ovládající tiskárnu

Opět v smb.conf(5), např. lppause, lpq ..., lpresume, lprm, printer ..., printcap

4.4 Timeouty

Většinou fungují defaultní, viz smb.conf(5)

4.5 Magic script

Soubor do kterého může klient nahrát příkazy a samba je pak pustí. Toto je věc v experimentálním stadiu vývoje.

4.6 Mapování home z NIS

Většinou se týká logování do domény, viz smb.conf(5)

4.7 Drobnosti mapování DOS<=>UNIX práv

Například mapování atributů skrytý, souborový z **DOS** na group a other execute bit na **UNIX**u, Viz map hidden, map system.

4.8 Některé síťové volby

Např. flagy socketů, ttl, mux atp.

4.9 ssl stuff

4.10 veto soubory

Už se mi nechtělo (:-0). Jsou to soubory, které nejsou ani viditelné, ani přístupné. Souvisí s nimi několik dalších voleb - jestli se adresáře obsahující pouze veto soubory mohou mazat a zda se mohou mazat veto adresáře obsahující neveto soubory atp. Viz veto files v smb.conf(5).

5 Dokumentace

Velice dobrá dokumentace k sambě je již v samotných manuálových stránkách.

Veškerá potřebná dokumentace je v release samby, případně v balíčkovaném stavu pro **Linux**ové distribuce (samba-doc pro debian, samba pro redhat (dohromady se sambou)). Zahrnuje spoustu rad od kompilace přes instalaci až k provozu + FAQ + hints (doporučuji, zde zahrnuty nebyly) + gotchas + using samba html příručka.

Dokumentace ve své nejnovější podobě je k dispozici na www.samba.org (resp. na jejích mirrorech - na www.samba.org najdete jen odkazy)

Tádydádidá, TO JE VŠE.