Samba Server: Korak za korakom

Ying Zhang, prevedel: Damir Horvat, *damir.horvat@ibe.si* 19. september 1999

Prevod skripte "Samba Server, Step-by-Step Guide" by Ying Zhang

Kazalo

1 Zahvala

Hvala vsem, ki so me kakorkoli spodbujali k uporabi Linuxa in Sambe, in mi pomagali s svojimi nasveti in odgovori na moja, ne vedno pametna vprašanja.

Hvala Ying Zhang-u za njegovo Samba Server, Step-by-Step Guide skripto.

Hvala tudi celotnemu timu razvijalcev Sambe za dobro opravljeno delo!

2 Predstavitev

Ta dokument vas bo popeljal skozi nastavitev Sambe na vaši Linux mašini. Na koncu tega dokumenta boste imeli:

- nastavljeno Sambo server na vaši Linux mašini s skupno rabo
- nastavljene Windows 95/98 kliente za dostop do Linux mašine

Ta dokument (HOW-TO) ni zamenjava za odlično dokumentacijo, ki pride skupaj z distribucijo Sambe. Namenjen je hitro in delujočo nastavitev Sambe. Preberite tudi originalno dokumentacijo Sambe!

2.1 Pravno stališče

Ne jamčim točnost in pravilnost informacij, ki jih predstavljam v tem dokumentu. V nikakršnem smislu nisem povezan z Samba team-om in vse kar opisujem tukaj je v osnovi tisto, kar sem naredil za delovanje Samba serverja na moji Linux mašini. Ne krivite mene, če se karkoli izjalovi. Vse delate na lastno odgovornost!

Po drugi strani pa, če imate kakršnokoli vprašanje, komentar ali predlog, mi lahko pošljete email na *damir.horvat@ibe.si*. Po svojih najboljših močeh se bom potrudil in vam odgovoril, ali vas vsaj usmeril k boljšim izvirom pomoči.

Dokument je preveden z dovoljenjem avtorja.

2.2 Ozadje

Moje domače lokalno omrežje sestavljajo trije računalniki, ena Linux in dve Windows 98 mašini. Linux mašina opravlja malo morje procesov, eden od njih je tudi serviranje datotek mojima Win98 računalnikoma preko Samba serverja.

Za lažje razumevanje, sem dal vsem trem mašinam imena. Moja Linux mašina je Homer, dve Win98 mašini pa sta Lisa in Bart. Vsi trije pa pripadajo delovni skupini Simpsons. Homerjev IP naslov je 192.168.0.1, Bartov 192.168.0.2 in Lisin 192.168.0.3.

Delovne dokumente, domače naloge in ostale osebne dokumente bom shranjeval v imeniku skupne rabe (shared directory) z imenom data. Ta imenik bo dostopen z obeh Win 98 mašin (mapiran kot M: disk).

Rad bi imel tudi imenik skupne rabe, do katerega bi imel dostop vsakdo; to bo imenik public. Ta bo dostopen iz obeh Win98 mašin in tudi vsakemu, ki bo imel račun (account) na Homerju.

Na koncu, Homer bo tudi primarni WINS server za moje lokalno omrežje, tako da ni potrebno imeti datoteke `imhosts` na Lisi in Bartu.

3 Zahteve

V nastajanju tega dokumenta predpostavljam, da imate:

- osnovno znanje kaj Samba je in za kaj jo želite
- delujoče TCP/IP omrežje
- delujočo Linux mašino na katero boste namestili Sambo
- potrebne pakete za kompajliranje Linux programov
- delujoče Windows 95/98 mašine pripravljene za povezovanje
- da nimate že nameščene Sambe; če jo imate, jo zaustavite in odstranite

3.1 Nastavitveni načrt

Sedaj morate narditi načrt, kako boste nastavili Sambo. Napisal vam bom svojega; nekatere stvari bodo mogoče prišle v poštev tudi za vas.

Homer ima nameščen RedHat Linux 5.1 z 2.2.3 kernelom, zato bom opisal namestitev Sambe za RedHat (z RPM-ji). Če uporabljate drugo distribucijo Linuxa, verjetno ne boste mogli dobesedno slediti kaj delam jaz, zato imejte to v mislih!

Bart in Lisa imata oba nameščene Windows 98. Ne bo velikih razlik, če imate Windowse 95. Če imate nameščene Windows NT, bodo koraki malce drugačni, vendar koncept je enak.

Ker imam v mreži samo tri računalnike, nisem zaskrbljen glede varnosti. Uporabljal bom šhare levelštopnjo varnosti v Sambi. V resnici sam uporabljam en račun na obeh, Lisi in Bartu, in TweakUI za samodejno prijavo.

3.2 Kako do Sambe

V času pisanja tega dokumenta je 2.0.3 zadnja stabilna verzija Sambe. Potrebovali boste izvorno kodo, datoteka je samba-2.0.3.tar.gz, ki jo dobite na domači strani Sambe `<http://www.samba.org/>`.

4 Namestitev Sambe

Najprej razširite izvorno kodo Sambe. Predpostavljam, da ste jo prenesli v imenik `/tmp` in naredite naslednje (ni še potrebno da ste root):

```
$ tar -zxvf samba-2.0.3.tar.gz
```

Če je šlo vse v redu in niste dobili nobenih sporočil o napakah, bi morali imeti razširjene datoteke v imeniku `samba-2.0.3`. Skupaj s Sambo pride kup paketnih skript. Najzanimivejše so tiste, ki naredijo RPM pakete za nas. Pa naredimo tako (sedaj morate biti root):

```
$ su
# cd samba-2.0.3/packaging/RedHat
# sh makerpms.sh
```

To bo vzelo nekaj časa, dokler se naredijo RPM paketi. Če je šlo kaj po zlu, bo potrebno, uh, pač prebrati dokumentacijo Sambe. Če je šlo dobro, sta bili narejeni naslednji datoteki:

- /usr/src/redhat/RPMS/i386/samba-2.0.3-19990228.i386.rpm
- /usr/src/redhat/RPMS/i386/samba-2.0.3-19990228.src.rpm

Super ne? Dobro, pa namestimo to Sambo:

```
# rpm -Uvh /usr/src/redhat/RPMS/i386/samba-2.0.3-19990228.i386.rpm
```

A je lahko sploh enostavneje? Sedaj bomo naredili novega uporabnika in novo skupino, nato pa nov imenik. Priredili bomo nekaj datotek za uporabo Šamba Web Administration Tool - SWAT".

5 Kreiranje

Hmm, tudi kakšno boljše ime bi si lahko spomnil, vendar bomo tukaj kreirali (naredili) uporabiške račune, imenike, skupine in datoteke.

5.1 Nov uporabnik in skupina

Ker bomo uporabljali šhare levelštopnjo varnosti, moramo narediti gost račun (guest account). Ta uporabnik bo smbuser in bo pripadal skupini smb.

Vse datoteke, ki jih Bart in Lisa pišeta v imenika skupne rabe, data in public, bodo v lasti smbuser-ja in pripadale v skupino smb.

Če imate Linuxconf, uporabite to za umazano delo. Drugače pa uporabite ukaza useradd in groupadd za kreiranje novih računov.

1. Naredite skupino smb
2. Naredite uporabnika smbuser, domači imenik naj bo v /home/public

Preprečite prijavo za račun smbuser, ker se dejansko nihče ne bo prijavljal pod tem imenom.

5.2 Imenik `pub`

Sedaj naj bi že imeli imenik `/home/public`. Bil naj bi v lasti smbuser-ja in pripadal skupini smb. Ker bodo vse datoteke v tem imeniku vedno pripadale skupini smb, bomo tako nastavili SGID. Vsak bo imel možnost branja in pisanja v ta imenik, zato bodo dovoljenja nastavljena tako:

```
# chown smbuser:smb /home/public
# chmod 2777 /home/public
```

Vsaka datoteka, ki je narejena v imeniku /home/public pripada skupini smb, ne glede na to, kdo jo naredi.

5.3 Imenik `data`

Moj data imenik je v `/home/samba/data`. Ta imenik bo dostopen samo določenim ljudem, tistim, ki pripadajo smb skupini. to naredimo takole:

```
# mkdir /home/samba
# chown smbuser:smb /home/samba
# chmod 2770 /home/samba

# mkdir /home/samba/data
# chown smbuser:smb /home/samba/data
# chmod 2770 /home/samba/data
```

Tudi na te imenike sem nastavil SGID tako, da vse, kar se naredi v teh imenikih pripada smb skupini.

Ker hočem tudi jaz imeti dostop do teh imenikov, se dodam v smb skupino. To lahko naredim z Linixconf ukazom, ali pa ročno spremenim datoteko `/etc/group`.

5.4 Pregled datoteke `hosts`

Imeli naj bi datoteko `/etc/hosts`, ki mapira imena gostiteljev (host names) v IP naslove. Moja izgleda takole:

```
# /etc/hosts

127.0.0.1       localhost       localhost.localdomain
192.168.0.1     homer
192.168.0.2     bart
192.168.0.3     lisa
```

5.5 Kreiranje datoteke Imhosts

Imhosts datoteka mapira imena gostiteljev (host names) ali IP naslove LanManager-ju imena računalnikov. Normalno bi verjetno radi imeli enaka imena za LanManager-ja in imena gostiteljev:

```
# /etc/Imhosts

localhost        homer
bart             bart
lisa             lisa
```

Izgleda malo smešno, ampak stvar na levi strani je ime gostitelja, stvar na desni pa ime LanManager-ja.

6 Uporaba SWAT

Za uporabo SWAT moramo preveriti `/etc/services` in `/etc/inetd.conf` datoteke. Po originalnih nastavitvah SWAT dela na portu 901. To sicer lahko spremenimo, vendar pustimo zaenkrat tako.

Poglejmo datoteko `/etc/services`, če vsebuje naslednjo vrstico:

```
swat      901/tcp     #Add swat service used via inetd
```

Če jo imate, potem dobro. Če je nimate, jo dodajte na konec datoteke.

Potem preverimo datoteko /etc/inetd.conf, če vsebuje vrstico:

```
swat stream tcp nowait.400 root  /usr/sbin/swat swat
```

6.1 Varovanje SWAT

Če vas varovenje SWAT ne zanima, lahko preskočite to poglavje. Jaz sam se počutim mnogo bolje, če mi "TCP wrappers"ščitijo SWAT. Spremenim prejšnjo vrstico takole:

```
swat stream tcp nowait.400 root /usr/sbin/tcpd /usr/sbin/swat
```

Če ne veste kaj so "TCP wrappers", potem preberite man strani:

```
# man hosts.allow
```

Vaš `/etc/hosts.deny` naj ima vrstico, ki pravi `ALL:ALL`. Dodajmo še to v vašo datoteko `/etc/hosts.allow`:

```
# swat:      127.0.0.1  192.168.0.
```

To dovoljuje Homerju, Lisi in Bartu dostop do SWAT.

6.2 Poganjanje SWAT

Najprej še enkrat zaženimo datoteko inetd:

```
# killall -HUP inetd
```

Sedaj pojdite z najljubšim internet brskalnikom na naslov: `http://192.168.0.1:901`. Če je vse u redu, bi morali vnesti uporabniško ime in geslo. Za uporabniško ime vnesite root, za geslo pa vaše root geslo.

6.3 Nastavitev Sambe

SWAT sedaj dela. Probajte vse gumbe in se spoznajte s njim. SWAT kreira `/etc/smb.conf` za vas. Sedaj bomo malo pogoljfali. Namesto, da bi šli skupaj čez vsako vrstico datoteke `/etc/smb.conf`, vam bom napisal svojo (imeni računalnika in delovne skupine sta spremenjeni, da zaščitim svojo sistemsko indetifikacijo).

Preglejte to in preprosto skopirajte v svojo `/etc/smb.conf` datoteko. Ne pozabite je prirediti za svoj sistem:

```
# Samba config file created usin SWAT
# from bart (192.168.0.2)
# Date: 1999/02/02 18:27:26

#Global parametes
        workgroup = SIMPSONS
        server string = Samba SMB Server
        interfaces = 192.168.0.1/24 127.0.0.1/24
        bind interfaces only = Yes
        security = SHARE
        log file = /var/log/samba/log. %m
        max log size = 50
```

```
        read bmpx = No
        time server = Yes
        socket options = TCP_NODELAY
        os level = 65
        preferred master = Yes
        dns proxy = No
        wins support = Yes
        guest account = smbuser
        hide dot files = No

[public]
        comment = Public
        path = /home/public
        read only = No
        create mask = 0664
        directory mask = 0775
        guest ok = Yes

[data]
        comment = Data
        path = /home/samba/data
        read only = No
        create mask = 0660
        directory mask = 0770
        guest ok = Yes
```

7 Zagon Sambe

Sambo lahko zaženete na dva načina: uporabite SWAT ali z ukazom v konzoli. Če bi radi uporabili SWAT, pojdite na stran STATUS in kliknite start SMBD in NMBD. Če je bila Samba že zagnana, pritisnite stop in še enkrat start, da boste videli nastavitveno datoteko.

Za zagon Sambe z ukazom v konzoli:

```
# /etc/rc.d/init.d/smb stop
# /etc/rc.d/init.d/smb start
```

Če niste opazili nobenih napak, potem vse deluje. No pa jo testirajmo.

7.1 Testiranje Sambe

Poglejmo, kaj sploh dela:

```
# smbclient -L localhost
```

Mogoče vpraša za geslo. Če, pritisnite Enter, in videti bi morali nekaj podobnega:

```
Domain=[SIMPSONS]    OS=[Unix]    Server=[Samba 2.0.3]
     Sharename           Type         Comment
     ---------           ----         -------
     public              Disk         Public
     data                Disk         Data
     IPC$                IPC          IPC Service (Samba SMB Server)
```

```
Server                        Comment
-----                         -------
HOMER                         Samba SMB server

Workgroup                     Master
---------                     ------
SIMPSONS                      HOMER
```

Vse u redu? Super! Sedaj nam preostaneta le še stroja z Windows.

8 Nastavitev Windows sistema

Ker Samba server dela na Homerju, je sedaj čas, da se posvetimo tudi Bartu in Lisi. Ta del je veliko lažji. Najprej se prepričajmo, da so mrežne komponente pravilno nameščene in da v *Nastavitve/Nadzorna plošča/Sistem/Upravitelj naprav* ni nobenih konfliktov.

Pazite da so v *Mrežnih nastavitvah/zavihek Osebna izkaznica* navedena pravilna imena računalnika in delovne skupine. Za naš primer: Bart naj bi imel ime računalnika Bart in delovno skupino Simpsons. Enako za Liso.

Nadzor dostopa naj bo na ravni skupne rabe. V lastnostih, pa obkljukajmo Wins server za Homerja.

Da bi spremembe začele veljati, je potrebno znova zagnati računalnik. Ko se Windowsi naložijo, bi morali v *Omrežni soseščini* videti tudi Samba Server.

V naslednjem poglavju si bomo ogledali, kako zaščititi Sambo pred zunanjimi napadi.

9 Varovanje Sambe

Vsakič ko dodate servis, je vaša mašina bolj ispostavljena crackerjem. Tukaj bomo obravnavali zaščito Samba serverja.

9.1 S Sambo

V Sambini nastavitveni datoteki `/etc/smb.conf` lahko povemo, katerim portom naj prisluškuje:

```
interfaces = 192.168.0.1/24 127.0.0.1/24
bind interfaces only = Yes
```

Tukaj seveda navedite vaše naslove IP. Ker sem nezaupljiv, bom dodal še eno plast varovanja, filtriranje portov.

9.2 Filtriranje portov

SMB uporablja port 137-139. Da bi bil varen, blokiram oba TCP in UDP porta 137-139. Če uporabljate 2.0 verzijo kernela, boste verjetno uporabljali program `ipfwadm`. Z jedrom 2.1 in 2.2, uporabljajte `ipchains`.

9.2.1 Uporaba ipfwadm

Dodajte naslednje vrstice v vašo datoteko /etc/rc.local:

```
ipfwadm -I -P tcp -a deny -S any/0 137:139 -W eth0
ipfwadm -I -P udp -a deny -S any/0 137:139 -W eth0
ipfwadm -O -P tcp -a deny -S any/0 137:139 -W eth0
ipfwadm -O -P udp -a deny -S any/0 137:139 -W eth0
```

9.2.2 Uporaba ipchains

Dodajte naslednje vrstice v vašo datoteko `/etc/rc.local`:

```
ipchains -A input -p tcp -j DENY --destination port 137:139 -i eth0
ipchains -A input -p ucp -j DENY --destination port 137:139 -i eth0
ipchains -A output -p tcp -j DENY --destination port 137:139 -i eth0
ipchains -A output -p ucp -j DENY --destination port 137:139 -i eth0
```

10 Zaključek

S tem zaključujem ta mini Korak za Korakom vodič skozi namestitev Samba Serverja. Ta dokument nikakor ne nadomešča originalne dokumentacije! Če potrebujete več informacij, pojdite na naslov `<http://www.samba.org/>` in preberite njihovo dokumentacijo.

Upam, da vam bo ta dokument uporaben.