

Sostituire un Server Windows NT/2000 con Linux e SAMBA



by Sebastian Sasías
<sasias(at)linuxmail(dot)org>

About the author:

Ha utilizzato Linux per svariati anni come strumento di supporto per lo sviluppo di soluzioni tecnologiche.

Attualmente lavora su sistemi di controllo che utilizzano Linux, su sistemi di trattamento di segnale, su sistemi di comunicazione e sulla sicurezza di rete.

Elettronico professionista – Informatico specializzato nelle automazioni.

Ha attivamente contribuito allo sviluppo di Software Libero con licenza GNU/GPL.

Translated to English by:
Sebastian Sasías

<sasias(at)linuxmail(dot)org>



Abstract:

Questo articolo vuole essere un complemento di alcuni aspetti presentati su altri articoli di LinuxFocus che parlano di SAMBA e del suo uso per condividere risorse in reti eterogenee composte da macchine Unix e Windows. Particolarmente questo articolo si concentrerà nel fornire alcuni servizi tipicamente forniti dal sistema operativo Windows.

Questa non vuole essere solo una dimostrazione della potenza e della flessibilità di Linux dato che ciò ha delle forti ripercussioni nell'ambito economico:

- Un grosso risparmio nel non pagare licenze per i Server Windows.
- Risultati simili possono essere facilmente raggiunti, ricorrendo a sistemi più modesti dal punto di vista hardware (in termini di processore e di RAM).

Un server Linux equipaggiato con SAMBA e propriamente configurato può sostituire una macchina WindowsNT/2000, che di norma condivide delle cartelle, fornisce il servizio di Active Directory (ADS), ma può anche fare da PDC (Primary Domain Controller), permettendo l'autenticazione dei client Windows2000/NT/98/95, gestire le condivisioni e personalizzare le sessioni utenti.

Questo articolo si concentrerà principalmente su questi aspetti.

Come risultato finale, in molte situazioni dove la macchina Windows ricopre queste funzioni, una macchina Linux con SAMBA sostituisce il server Microsoft senza che sia necessaria alcuna modifica di configurazione ai client.

Per questo articolo assumiamo che: SAMBA sia già installato e correttamente funzionante sulla macchina che andremo ad utilizzare come server e che il lettore abbia conoscenza dei concetti basilari sui server Windows e Linux.

Analisi del problema

Prendiamo in considerazione un server Linux/Samba che funziona come PDC, dove ogni utente autenticato ha accesso a due directory condivise sul server, una appartenente ad una condivisione pubblica e l'altra personale. In questo articolo considereremo spesso il caso in cui si debba accedere a dei dati personali, o l'accesso ad una cartella personale per ogni utente.

I dettagli da prendere in considerazione:

Il Nome NetBIOS del Server Linux/Samba: **SMBServer**

Il nome del dominio (o gruppo di lavoro) in Windows: **THEDOMAIN**

Porzione personale di ogni utente: Disco di rete H: in ambiente Windows => **/home/** (sul Server Linux)

Porzione ad accesso pubblico: Disco di rete P: in ambiente Windows => **/home/public**

La figura 1 ci mostra una semplice schematizzazione di rete con dei client Windows che accedono alle risorse di un server WindowsNT/2000. Ebbene questo server può essere sostituito con il nostro server Linux/SAMBA.

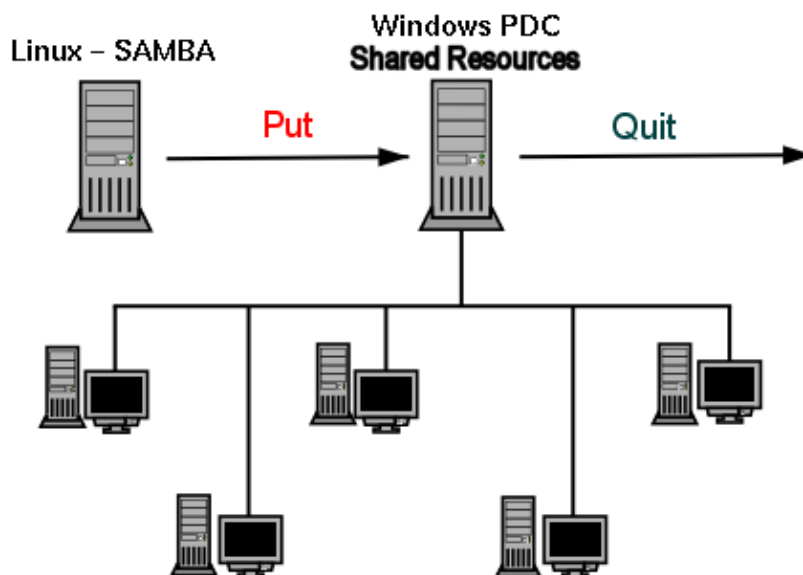


Fig. 1 – PDC e File Server in ambiente Windows

La configurazione

Seguite queste operazioni:

1) Create gli utenti che dovranno poi essere autenticati dal server PDC (che in questo caso sarà Linux/SAMBA).

Per questa operazione potete ricorrere ai comandi: **adduser**, **useradd**, **userconf**, oppure potete ricorrere a

strumenti di amministrazione che abbiano un'interfaccia grafica (WebMin, Linuxconf, YAST, ecc.).

Controllate che gli utenti abbiano accesso solo ai servizi Linux/SAMBA, se lo preferite. In tal caso gli utenti è bene che non abbiano alcun accesso alla shell. Una soluzione per ottenere questo risultato consiste nell'assegnare loro come shell **/bin/false** e come home directory **/dev/null**.

2) Convertire gli utenti UNIX in utenti Linux/SAMBA/Windows, per mezzo della creazione del file **smbpasswd**.

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

Un altro modo per ottenere questo risultato è quello di dare i seguenti comandi di Samba per la creazione degli utenti e per l'assegnazione della password:

smbadduser smbpasswd

Questi comandi funzionano similmente ai comandi adduser e passwd.

3) Modificare il file di configurazione di Samba(smb.conf), accertandosi di includere o di rimuovere i caratteri di commento, per ottenere un file simile a questo:

```
netbios name = SMBServer
workgroup = THEDOMAIN
server string = Linux Samba NT Server
log file = /var/log/samba/%m.log
max log file = 0
security = user
encrypt password = yes
smb password file = /etc/samba/smbpasswd
ssl CA certificate = /usr/share/ssl/.... (rimuovete il commento)
socket options = (rimuovete il commento)
local master = yes
preferred master = yes
domain master = yes
domain logons = yes
logon script = logon.bat
wins support = yes
```

Nota:

*Se preferite uno script di login dipendente dall'utente allora dovrete sostituire il valore di logon script con %U.bat, ma ciò implica che ogni utente debba avere uno script di accesso al sistema che ha come nome il nome stesso dell'utente. Se volete potete utilizzare anche %u al posto di %U. Se volete ricorrete all'utilizzo dei gruppi di appartenenza all'utente, potrete utilizzare %g o %G. I significati precisi di questi parametri possono essere reperiti nelle pagine del manuale (**man smb.conf**).*

4) Creazione delle risorse da condividere

Modificate il file **smb.conf** e inserite i commenti su tutti gli esempi di "condivisione", apportando i dovuti cambiamenti alle seguenti informazioni:

```
[netlogon]
comment = Script di accesso
path = /home/netlogon
read only = yes
guest ok = yes
browseable = no
```

```
[home]
comment = Cartella Utente
path = /home/%U
browseable = yes
writable = yes
```

```
[public]
comment = Cartella Pubblica
path = /home/public
browseable = yes
writable = yes
guest ok = yes
create mask = 0777
force create mask = 0777
```

Salvate il file **smb.conf**.

5) Potete verificare la corretta sintassi del file smb.conf con il seguente comando:

testparm

Questo comando analizza il file smb.conf e ne riporta gli eventuali errori.

6) Create le cartelle **/home/netlogon** e **/home/public** con i permessi settati a 0754(netlogon) e 0777 (public).

7) Modificate lo script di accesso: **logon.bat**.

Importante: Utilizzate un editor di testo per ambiente DOS/Windows (per esempio Notepad o EDIT) per creare il file logon.bat (dimodochè esso sia salvato in un formato compatibile con MS). Oppure potete utilizzare un editor di testo in Linux e poi convertire il file nel corretto formato. Ad esempio con vim potete utilizzare il comando ":set textmode" per ottenere il formato di a capo compatibile MS, oppure potete ricorrere all'uso di una utility come unix2dos.

net time \\SMBServer /y (potete anche utilizzare /yes invece di /y)

net use H: \\SMBServer\home -y (potete anche utilizzare /yes o /y al posto di -y)

net use P: \\SMBServer\public -y

8) Aggiungete le informazioni inerenti il SMBServer nel file lmhosts

Modificate il file **/etc/samba/lmhosts** (or /etc/lmhosts) ed aggiungete la seguente riga:

SMBServer, i.e: **192.168.0.10 SMBServer**

9) Avvio/Riavvio del demone Samba (smbd)

service smb restart

Se il succitato comando non avesse successo nella vostra distribuzione Linux, potete ricorrere a:

```
ps -auxgx | grep smb  
kill -9 <ID del processo di smb>  
smbd
```

10) Utilizzo di smbclient per verificare se la configurazione precedentemente specificata funziona correttamente.

smbclient -L //SMBServer

Se comparisse una richiesta di password ("Password:") semplicemente premete il tasto invio e vi verranno mostrare le risorse condivise.

11) Effettuate un accesso con un computer Windows95/98/NT al dominio THEDOMAIN, utilizzando degli utenti Linux/SAMBA precedentemente creati (passi 1 e 2).

In Windows98/95/ME, si deve procedere così:

Start => Impostazioni => Pannello di controllo=> Rete =>Client per reti Microsoft => Proprietà.

Per quel che concerne Windows NT e 2000 il concetto è simile anche se la sequenza è diversa.

Un esempio di file di configurazione

Vi mostro qui di seguito un file di configurazione per SAMBA completo. Questo file è stato testato con svariate distribuzioni di Linux. Il lettore potrà modificarlo a piacere per ottenere i risultati ottenuti in questo articolo. Ogni istruzione presente è sufficientemente commentata.

Come ultima opzione, per coloro che vogliono una configurazione rapida di samba, possono installare i moduli di Webmin o ricorrere all'utilizzo di SWAT. Entrambi quest'ultimi sono strumenti per la configurazione basati su di una interfaccia grafica, permettendo una configurazione più semplice.

```
#=====#  
# /etc/smb.conf  
#-----#  
# Si tratta del principale file di configurazione di SAMBA  
# File schematico per la configurazione  
# modificate i parametri secondo le vostre necessità.  
#-----#  
# Verificato con: Solaris e le seguenti distro di Linux:  
# RedHat 6.0, 7.0 e 7.1  
# Solaris 7  
# Slackware 7.x  
# Mandrake 6.1, 7.0 e 8.1  
# SuSe 7.2  
#-----#  
# Last changes: 08/12/2001  
# Sebastian Sasia - sasia(at)linuxmail(dot)org
```

```

#=====#
#
# Questo file è stato creato seguendo le specificazioni presenti
# nella documentazione di SAMBA e nelle pagine di manuale di smb.conf(5)
#
# Nota: dopo aver modificato questo file controllatene la
# sintassi con il comando "testparm"
#
#===== Opzioni Globali =====#
#
# Configurazione Generale
#
[global]
#.....#
# workgroup = Nome-del-dominio-NT o Nome-del-gruppo-di-lavoro, per esempio: THEDOMAIN
# Dominio del PDC
workgroup = THEDOMAIN
#.....#
# Il nome con qui questa macchina sarà nota alle altre macchine
netbios name = SMBServer
#.....#
# Questo commento apparirà nelle proprietà della macchina nelle risorse di rete.
server string = Samba Server de este lugar
#.....#
# Questa riga ha importanza per un fattore di sicurezza: solo i
# computer nella rete locale avranno accesso alle risorse.
# In questo specifico esempio solo i computer appartenenti all rete 192.168.8.0
# (una comune classe C) e dall'interfaccia di "loopback" possono accedere.
# Per ulteriori dettagli consultate il manuale di smb.conf
# Mi spiego: solo i computer il cui indirizzo di rete inizi per
# 192.168.8 o per 127 potranno accedere alle risorse (In questo caso la riga è però commentata)
; hosts allow = 192.168.8. 127.
#.....#
# Se volete avere a disposizione l'intera lista delle stampanti, invece di creare
# una risorsa specifica per ognuna, utilizzate questa opzione
; load printers = yes
#.....#
# Se vogliamo possiamo scavalcare il file printcap di sistema
; printcap name = /etc/printcap
#.....#
# In ambiente SystemV printcap deve avere delle corrispondenze
# nella cartella contenente le code di stampa, altrimenti automaticamente verranno
# aggiunte delle voci (oh.. adorabile ridondanza dei sistemi SystemV :-))
; printcap name = lpstat
#.....#
# Di norma non è necessario specificare il sistema di stampa, almeno che esso non sia standard.
# Attualmente i sistemi supportati sono:
# bsd, sysv, plp, lprng, aix, hpux, qnx
; printing = bsd
#.....#
# Rimuovete il commento se desiderate poter avere un account con le caratteristiche di guest
# dovrete anche aggiungere questo user al file di password di sistema,
# o samba utilizzerà l'account nobody

```

```

; guest account = pcguest
#.....#
# Se preferite avere log separati per ogni client che accede
# al nostro SAMBA server
log file = /var/log/samba/log.%m
#.....#
# È bene porre un limite di dimensione al file di log (la sua dimensione è espressa in Kb).
max log size = 50
#.....#
# Leggete accuratamente il file security_level.txt.
# Questo file vi spiega le differenze di modalità di accesso alle risorse condivise
# livello security = user: ogni utente accederà per mezzo della propria password
security = user
#.....#
# Se il livello è impostato su server, l'autentica degli utenti avviene per mezzo di un
# ulteriore server
# Utilizzate l'opzione "password server" solo quando avete impostato come livello di
# sicurezza server security = server
# password server = [indirizzo IP del server che autentifica gli utenti].
; password server = <Nome-del-server-NT>
#.....#
# Se volete utilizzare le password criptate in rete, per cortesia leggete ENCRYPTION.TXT,
#
# Non attivate questa opzione se non sapete che state facendo.
# Per vostra informazione: Windows95b (o superiore), Windows98 e
# WindowsNT sp3 (o superiore) utilizzano le password criptate.
encrypt passwords = yes
#.....#
# La seguente riga vi spiega come utilizzare una configurazione
# differenziata per ogni macchina presente in rete.
# %m rappresenta il nome della macchina client.
; include = /usr/local/samba/lib/smb.conf.%m
#.....#
# La documentazione e voci di corridoio suggeriscono che
# che questa opzione permetta delle performance migliori
# Leggete il file speed.txt e le pagine del manuale per maggiori dettagli.
socket options = TCP_NODELAY
#.....#
# Configurazione di SAMBA se la macchina ha più interfacce di rete.
# Se il vostro server ha più schede di rete, le dovrete elencare come nel seguente esempio.
# (consultate le pagine del manuale per una spiegazione dettagliata).
; interfaces = 192.168.8.2/24 192.168.12.2/24
#.....#
# Opzioni inerenti la funzione di browser:
# Assegnate il valore no se NON volete che il server divenga un master browser.
local master = yes
#.....#
# Il parametro OS Level aumenta le possibilità che il nostro server divenga il master browser nel
# caso di una elezione. Ovvero, se abbiamo più server PDC quello con il valore
# più elevato avrà più possibilità di essere il master browser
# Nella maggior parte dei casi il valore predefino è sufficiente.
; os level = 33
#.....#

```

Domain Master dice a SAMBA di comportarsi come un Domain Master Browser.
Questa opzione permette a SAMBA di funzionare come supervisore di dominio,
permettendo di vedere, ed essere visto, su più sottoreti.
Non abilitate questa opzione se avete già un server WindowsNT/2000 con questa funzione.

domain master = yes

#.....#

L'opzione permette a SAMBA di cercare di assumere la supervisione del dominio.
Dà anche qualche ulteriore possibilità al server di divenire il supervisore
Se nella nostra rete abbiamo più server, questa opzione fa sì che
esso sia visto come il server principale allorché un client cerca un server in rete

preferred master = yes

#.....#

Utilizzate questa opzione SOLO se avete un server WindowsNT/2000 nella vostra rete che
stia facendo la funzione di PDC (primary domain controller).

; domain controller = <NT-Domain-Controller-SMBName>

#.....#

Utilizzate questo parametro solo se volete che il server SAMBA divenga il
"domain logon server" per le workstation Windows9x/ME.

domain logons = yes

#.....#

Se abilitate la funzione di server di accesso al dominio, allora
dovrete avere uno script per l'accesso.

Se preferite uno script specifico per ogni macchina

; logon script = %m.bat

Se preferite uno script specifico per ogni utente

; logon script = %U.bat

#.....#

Dove salvare i roaming profile (valido per Win95 e WinNT)

Il parametro %L è il valore del nome macchina in ambiente NetBIOS, %U quello dell'utente

Dovrete anche rimuovere il commento dalla condivisione [Profiles] presente più sotto.

; logon path = \\%L\Profiles\%U

#.....#

Supporto per il servizio Windows Internet Name Service:

WINS Support istruisce NMBD di abilitare il proprio server.

Il protocollo WINS, converte i nomi macchina in indirizzi IP.

Lavora in ambiente TCP/IP similmente al DNS.

; wins support = yes

#.....#

WINS Server – istruisce i componenti di NMBD di comportarsi come un client WINS

il server SAMBA può essere o Client o Server, ma mai entrambi allo stesso tempo

#

In tal caso qui si deve specificare l'indirizzo IP del server WINS

; wins server = 192.168.8.1

#.....#

WINS Proxy – istruisce SAMBA a risolvere i nomi macchina a beneficio di macchine che

non siano in grado di utilizzare il protocollo WINS.

È però necessaria la presenza di un server WINS nella rete.

Il valore predefinito è NO.

; wins proxy = yes

#.....#

DNS Proxy – istruisce SAMBA se debba risolvere o meno i nomi per mezzo di un nslookup.
Fino alla versione 1.9.17 il valore predefinito era yes, dalle seguenti è no.

Qui possiamo appunto istruire SAMBA se debba o meno svolgere questo incarico.

dns proxy = yes

dns proxy = no (la risoluzione dei nomi avverà per mezzo del file lmhosts)

#.....#

Se il disco di rete non viene specificato, esso verrà connesso

automaticamente assegnandogli la lettera Z

logon drive = P:

#.....#

All'accesso verrà eseguito il seguente script: /etc/samba/netlogon/SAMBA.BAT

e verrà connesso un disco di rete per mezzo del comando "net use"

logon script = SAMBA.BAT

#===== Definizioni delle condivisioni =====#

Cartella personale del singolo utente

Disco di rete P:

[homes]

comment = Cartella Home

browseable = no

writable = yes

readonly = no

force create mode = 0700

create mode = 0700

force directory mode = 0700

directory mode = 700

#-----#

Cartella per file temporanei

Disco di rete T:

[tmp]

comment = File temporanei

path = /tmp

readonly = no

public = yes

writable = yes

force create mode = 0777

create mode = 0777

force directory mode = 0777

directory mode = 0777

#-----#

CD-ROM del server

Disco di rete L:

[cdrom]

comment = CD-ROM

path = /mnt/cdrom

public = yes

writable = no

#-----
Cartella di gruppo, che corrisponde a /home/grp.name_group
/home/user/group è un link a /home/grp.name_group
grp.name_group ha come permessi 770
Disco di rete G:

[group]
comment = Cartella del gruppo
path = /home/%u/group
writable = yes
readonly = no
force create mode = 0770
create mode = 0770
force directory mode = 0770
directory mode = 0770

#-----
Questa unità è dedicata all'archiviazione di applicativi, d' installazione software,
di software aziendale, etc.
I permessi di /net e /net/install sono 755. Nel nostro
esempio: root è il possessore di questa cartella
Disco di rete N:

[net]
comment = Cartella Net
path = /net
writable = yes
readonly = no
force create mode = 0750
create mode = 0750
force directory mode = 0750
directory mode = 0750

#-----
[netlogon]
comment = Fornisce il servizio di Logon alla rete
path = /etc/samba/netlogon
guest ok = yes
writable = no
locking = no
public = no
browseable = yes
share modes = no

#-----
#=====

Considerazioni finali

Il pacchetto SAMBA, come altri strumenti per Linux, è in costante evoluzione. È quindi possibile che alcune informazioni qui presentate non siano più valide. Difatti nel percorso evolutivo di SAMBA, alcuni nomi di parametri nel file di configurazione sono leggermente cambiati, con lo scopo di ottenere una struttura migliore.

Se durante la configurazione di SAMBA otterrete alcuni errori riguardo ad alcuni parametri a voi non noti, avete essenzialmente due semplici soluzioni:

- Scorrere il file `smb.conf` installato dal sistema, in quanto esso, di norma, contiene alcune righe commentate che potrebbero risolvere i vostri problemi specifici.
- Leggere accuratamente la configurazione di SAMBA, magari iniziando con il file relativo ai cambiamenti specifici dalle versioni precedenti.

Referenze: Bibliografia e strumenti

- SAMBA, il sito ufficiale: <http://www.samba.org>
- Webmin, il sito ufficiale: <http://www.webmin.com> uno strumento che vi permette di amministrare da remoto la vostra macchina Unix.
- Il progetto GNU Project e la Free Software Foundation: <http://www.gnu.org>
- Un sito utile per trovare i pacchetti RPM: <http://www.rpmfind.net>
- La home page di LinNeighborhood: <http://www.bnro.de/~schmidjo>, un interessante strumento per utilizzare le risorse condivise nelle reti "SMB".

Note sui diritti d'autore

SAMBA è un prodotto distribuito secondo la licenza GPL

Linux è un marchio registrato di Linus Torvalds.

Solaris è un sistema operativo ed il suo marchio è registrato da Sun Microsystems.

MS Windows è un marchio registrato di Microsoft.

L'utilizzo di SAMBA può far risparmiare soldi non dovendo comperare licenze di Microsoft.

Webpages maintained by the LinuxFocus Editor team

© Sebastian Sasías

"some rights reserved" see linuxfocus.org/license/

<http://www.LinuxFocus.org>

Translation information:

es --> -- : Sebastian Sasías <sasias(at)linuxmail(dot)org>

es --> en: Sebastian Sasías <sasias(at)linuxmail(dot)org>

en --> it: Toni Tiveron <toni(at)amicidelprosecco(dot)com>