SAMBA, la guida definitiva

di Henry 'WebWolf'

Le operazioni di condivisione all'interno di una rete Windows funzionano attraverso un protocollo di alto livello che ha il compito di proiettare sulla rete locale alcune entità come file, cartelle e stampanti. Il nome di questo protocollo è SMB (Short Message Block).

Qualunque sistema operativo che implementi questo protocollo è in grado di accedere a risorse in una rete Windows o a fornire le proprie risorse a una rete di computer.

Luinux dispone di una ottima implementazione di SMB, contenuta in un pacchetto denominato SAMBA (www.samba.org).

Il progetto nacque per piattaforme Unix e col tempo è diventato una dei pacchetti open source più importanti. Grazie a Samba è possibile far colloquiare sistemi Unix/Linux con i largamente usati sistemi Microsoft.

Attualmente la versione più diffusa di Samba è la 2, ma è disponibile per il download la versione 3, le cui implementazioni sono descritte sul sito ufficiale.

Samba si compone di due demoni: nmbd e smbd. Il primo si occupa della risoluzione dei nomi (servizio Wins e Master Browser List), il secondo è responsabile delle connessioni e delle operazioni di condivisione.

NMBD

il Master Browser List è un servizio molto importante in una rete di computers. Quando visualizziamo le 'Risorse di Rete' e vediamo le icone dei pc connessi, in realtà si sta leggendo un elenco mantenuto da un pc incaricato di questa operazione.

Quando un nuovo pc accede alla rete cerca il 'gestore' dell'elenco e gli comunica la propria esistenza. Questa operazione non è immediata: questo è il motivo per cui i pc ci mettono un po' di tempo ad apparire nelle Risorse di rete. Analogamente quando si spegne un pc esso rimane per molto tempo all'interno dell'elenco.

Il pc che gestisce l'elenco è detto appunto Master Browser List. L'MBR viene scelto tra il 'migliore' di tutti i pc collegati in rete. Nelle reti miste Linux/Windows generalmente il compito è assegnato al pc Linux con samba poiché generalmente ha le caratteristiche di 'server'.

WINS è un meccanismo che permette la risoluzione di un nome esteso (es. Utente_1) in un indirizzo ip (192.168.100.5).
L'accesso ad una rete avviene tramite gli indirizzi ip. I nomi testuali devono essere tradotti prima di poter essere utilizzati.

Se non c'è un servizio WINS la risoluzione avviene tramite il broadcast: il pc interroga tutti i computer connessi alla rete fino ad individuare la macchina che dispone del nome di rete che si vuole contattare. L'operazione, a seconda del numero di pc in rete, genera un traffico inutile e ritardi.

E' molto meglio far riferimento ad un archivio dove sono mantenuti i nomi associati ai relativi indirizzi ip.

WINS è simile al DNS, seppur con notevoli differenze. WINS non opera a livello di reti geografiche, è un elenco senza struttura gerarchica, che deve operare a livello di reti locali. (Non pretendo di essere stato esaustivo sulla differenza tra WINS e DNS, ma credo che una trattazione completa porterebbe troppo lontano dallo scopo di questa guida).

SMBD

I due demoni di samba devono essere lanciati nell'ordine esatto: prima nmbd e poi smbd.

/etc/init.d/nmbd start
/etc/init.d/smbd start

In alcune distribuzioni potrebbe esistere la forma abbreviata:

/etc/init.d/smb start

Verificate gli script di avvio oppure utilizzate *ntsysv* per fare in modo che essi partano automaticamente all'avvio di Linux. (NOTA: su SuSE occorre andare in Centro di controllo YaST -> Editor dei runlevel e attivare nmb e smb).

Altri comandi opzionali potrebbero essere:

Start Samba

/etc/rc.d/init.d/samba start
o
/usr/sbin/smbd -D and /usr/sbin/nmbd –D

Stop Samba

/etc/rc.d/init.d/samba stop
o
killall -TERM smbd and killall -TERM nmbd

Restart Samba

/etc/rc.d/init.d/samba restart
o
killall -HUP smbd and killall -HUP nmbd

Potrebbe capitare che la vostra versione abbia una sintassi ancora diversa da quelle che ho elencato precedentemente. Il concetto fondamentale è quello di attivare i due demoni nmbd e smbd.

Controllate con:

ps aux

tutti i processi in esecuzione e trovate i due demoni. Se non sono presenti e i comandi che vi ho dato non funzionano dovete verificare come avviarli nella vostra distribuzione.

All'avvio samba legge il file di configurazione smb.conf presente nella cartella /etc/samba. Il file già presente nel sistema è un file di esempio, si sconsiglia di 'adattare' questo file alla nostra rete, è preferibile creare una copia di backup e crearne uno nuovo ritagliato su misura per la nostra rete.

Se samba è attivo occorre fermarlo:

/etc/init.d/smbd stop

o usate uno dei comandi sopra riportati.

Andare nella cartella /etc/samba e creare la copia di backup:

mv smb.conf smb.conf.default

Ora si puo' creare il nuovo file:

vi smb.conf

NOTA: vi a prima vista potrà sembrare ostico e difficoltoso. Molti potrebbero essere portati ad utilizzare un editor grafico o pico. Per esperienza mi sento di consigliarvi di imparare almeno i comandi fondamentali di vi. Esso è presente in tutte le distribuzioni e se vi troverete di fronte ad uno schermo nero col cursore che lampeggia e l'unico modo per ripristinare il sistema è intervenire manualmente sui file di configurazione, beh, vi sarà la vostra bacchetta magica !

Tutti i file smb.conf hanno una struttura precisa fatta a 'sezioni'.

La sezione principale (la prima che si deve definire) è [global]. Un file smb.conf può contenere anche solo questa sezione, ma se si vogliono condividere in rete file, cartelle e stampanti non è sufficiente.

Faremo un esempio di una rete (1 Linux e gli altri Windows) che devono condividere in lettura scrittura una cartella chiamata [public_folder] e in sola lettura una cartella chiamata è [read_folder].

Iniziamo con la sezione principale:

[global]
workgroup = MYNET
netbios name = server_linux
server string = SuSE93
security = SHARE

mynet è il nome del gruppo di lavoro. Su Windows il nome di default è WORKGROUP. Assicuriamoci che il nome della rete sia lo stesso sui sistemi windows (specialmente XP).

netbios name è il nome del computer che sarà visualizzato in Risorse di rete (di solito visualizzato tra parentesi).
server string è il nome che apparirà fuori parentesi.

security contiene le direttive di sicurezza per l'accesso al server da parte degli utenti. Le opzioni sono due: SHARE e USER

La modalità SHARE permette la condivisione delle risorse senza autenticazione, solo attraverso una password, se configurata.

La modalità USER, invece, richiede sia un user id che una password per accedere alle cartelle condivise.

Intanto lasciamo security = SHARE e creiamo le due cartelle da condividere, sotto la sezione [global] aggiungiamo:

[public_folder]
comment = cartella comune
path = /home/public_folder
public = YES
writable = YES

il nome tra parentesi sarà il nome visualizzato nelle risorse condivise. Nel nostro caso la cartella verrà vista col nome public_folder

path è ovviamente la collocazione sul server della cartella. Essendo in /home, assicuriamoci che tutti possano utilizzarla, quindi occorre cambiare i permessi della cartella:

chmod 777 /home/comune

Ora creiamo l'altra cartella:

[read_folder]
comment = scrivete il commento
path = /home/read_folder
public = YES
writable = NO

Ora il file smb.conf è terminato. Salviamo e prima di far ripartire smbd possiamo testare se non abbiamo commesso errori con il comando:

testparm

Questo comando fa parte della suite samba. E' utile poiché i demoni non controllano il file smb.conf, quindi potremmo essere indotti a credere che le nostre cartelle siano condivise senza esserlo. Se avete usato commenti di oltre 12 caratteri potreste ricevere un messaggio di avvertimento di poca compatibilità con i vecchi sistemi.

Un altro comando utile è smbclient. Potete vederne gli usi con *man smbclient*.

Ora è giunto il momento di riavviare il servizio:

/etc/init.d/smbd restart

Gestione avanzata utenti

Supponiamo che all'interno della nostra rete si voglia creare una cartella accessibile solo a determinati utenti (ad esempio una cartella contenente tutti i video di Sylvia Saint … mai sentita nominare, è un nome a caso … ;)). Sarebbe imbarazzante se qualcuno, cercando della modulistica, capitasse per caso in questa cartella.

La sicurezza a livello di condivisione (share) non risponde più alle nostre esigenze. Occorre passare alla sicurezza utente (user).
Modifichiamo (ricordiamoci di fermare smbd) la sezione [global]:

[global]
workgroup = MYNET
netbios name = server_linux
server string = SuSE93
security = USER
smb passwd file = /etc/samba/smbpasswd
encrypt password = YES

La riga 5 indica il percorso del file che contiene le password e la 6 dice di utilizzare password criptate.

ATTENZIONE: nei sistemi old, tipo windows 95, NT 3 e NT 4 senza il service pack 3 ci possono essere problemi poiché le password sono trasmesse in chiaro da questi sistemi.

Creiamo ora la cartella ad accesso riservato. Alla fine del smb.conf aggiungiamo:

[restricted_area]
comment = documenti inutili
path = /home/restricted_area
valid users = webwolf
writable = YES

Volendo si possono indicare gli utenti che NON devono accedere a questa cartella:

[restricted_area]
comment = documenti inutili
path = /home/restricted_area
valid users = webwolf
invalid users = pippo pluto topolino
writable = YES

Indicare gli utenti validi non basta. Innanzitutto occorre che gli utenti che accedono alle risorse di rete siano utenti accreditati ad accedere alla macchina Linux. Quindi occorre creare gli utenti in Linux o utilizzando gli strumenti grafici o tramite i comandi:

useradd webwolf
passwd webwolf

Ora che gli utenti son creati bisogna creare le password per samba. L'utility per impostare le password in samba è smbpasswd. Questo comando aggiunge righe di autebticazione nel file smbpasswd contenuto in /etc/samba.

smbpasswd –a webwolf

Seguite le indicazioni (chiede di digitare due volte la password .. le solite cose) e l'utente ora è aggiunto.

La password per samba può essere diversa dalla password per Linux, ma si consiglia di settarle uguali per omogeneità.
Se le credenziali di accesso alla rete Windows sono le stesse di Linux i valid users accederanno alla cartella senza notifica, altrimenti si aprirà la finestra di richiesta user id e password.

Riavviate il servizio e tutto dovrebbe andare.

Cartelle personali

Se volete che ogni utente delle rete possa avere ed accedere ad una sua cartella personale sul server Linux, si possono aggiungere a smb.conf le seguenti righe:

[homes]
comment = cartella personale
writable = YES
browsable = NO
valid users = %S
 # path = /usr/sambausers/%S

Son tutte cose più o meno già vsite. L'opzione browsable e necessaria per evitare che si vedano le cartelle di tutti gli altri utenti.

la novità è nella variabile %S che contiene il nome della condivisione corrente. Samba dispone di diverse variabili. Esempio %v restituisce la versione di samba, %h il nome DNS del server e %L il nome netbios.
Con %S facciamo in modo che la cartella condivisa sia quella con lo stesso nome di login. Quindi l'utente webwolf potrà accedere solo alla cartella webwolf.

Ovviamente bisogna controllare che le singole cartelle appartengano ai rispettivi utenti. Se così non fosse occorre usare il comando *chown*.
Inoltre alle singole cartelle andrebbero assegnati i diritti 770.

Ho lasciato per ultima la spiegazione della riga commentata (#). Lasciando la sezione [homes] così, oppure togliendo proprio la riga #, le cartelle utenti saranno le cartelle tipiche del sistema Linux: /home/webwolf (ad esempio).

In questo modo, accedendo da un sistema Windows si vedranno i file dot personali di Linux. Se tutti fossero utenti Linux, saprebbero di non toccare o di come toccare quei file, ma molto spesso chi ha necessità di creare server Linux ha a che fare con utenti windows (e va già di lusso).

E' consigliabile allora creare le cartelle di condivisione samba in un punto differente. Decommentate le riga e assicuratevi di creare il percorso e le singole cartelle utente con tutti i giusti privilegi nella nuova posizione.

Condividere una unità ottica

Se volessimo fare in modo di condividere un cdrom possiamo aggiungere queste righe:

```
[cdrom]
comment = mio_cdrom
browsable = YES
writable = NO
path = /mnt/cdrom
```

Questa sezione crea una condivisione fissa con il cdrom. E' utile se gli utenti della rete devono utilizzare dei documenti/fotografie o risorse presenti solo nel cdrom che per qualche motivo non possiamo copiare in una cartella condivisa (ad esempio un dvd con 4 giga di dati).

Se volessimo invece essere liberi di togliere e mettere diversi cd rom dobbiamo modificare la sezione in :

```
[cdrom]
comment = mio_cdrom
browsable = YES
writable = NO
path = /mnt/cdrom
root preexec =mount /dev/cdrom
root postexec = umount /mnt/cdrom
```

Le due aggiunte non fanno altro che montare e smontare il cdrom durante l'accesso alla condivisione.

Sicurezza

Come dico sempre: "L'unico pc sicuro è un pc spento".
Ogni volta che condividiamo qualcosa stiamo certi che ci sarà sempre qualcuno pronto ad approfittare di questo fatto.
Ovviamente queste considerazioni assumono un valore crescente al crescere dell'estensione della rete e delle connessioni esterne.

Una prima cosa che si può fare è il controllo degli indirizzi ip che possono accedere alla condivisione.
Nella sezione [global] aggiungiamo:

host allow = 127.0.0.1 192.168.100.0/24
host deny = 192.168.100.13

Sintassi abbastanza chiara, ritengo, che può essere inserita anche in una sezione diversa da [global]. Commentate host deny se non volete fermare nessun host.
Samba inoltre condivide le sue risorse indipendentemente dalle interfacce di richiesta. Ossia se il pc è collegato ad internet utenti esterni possono accedere a samba e sfogliare le cartelle.
Per impedire questo si possono indicare a samba quali sono le interfacce abilitate alla condivisione:

interfaces = eth0 lo
bind interfaces = YES

In questo caso sono prese in considerazione solo le richieste provenienti dal pc stesso (lo = loopback) e dalla prima scheda di rete (eth0). La seconda riga dice che il traffico è consentito solo nelle interfacce specificate nel comando interfaces.

Utile è anche fermare i link simbolici eventualmente presenti nelle cartelle:

follow symlinks = NO

Se infine vogliamo tenere traccia di quello che accade in samba possiamo configurare un file di log:

log file = /var/log/samba/%m.log
max log size = 100
log level = 3

%m fa in modo di creare un file di log per ogni sistema differente che accede a samba. Per sistema si intende il netbios name della macchina.
Max log size indica la dimensione massima del file. Dimensione 0 significa file infinito. Se si

raggiungono le dimensioni specificate il file è salvato come .old e se ne crea uno nuovo.
log level specifica il grado di dettaglio dei log. Il valore 3 è il più dettagliato, ma anche quello che crea un file di log di maggiori dimensioni.
Potete provare. I valori possibili sono 3, 2 o 1.

Ricapitolando la sezione [global] diventa:

```
[global]
workgroup = MYNET
netbios name = server_linux
server string = SuSE93
security = USER
smb passwd file = /etc/samba/smbpasswd
encrypt password = YES
host allow = 127.0.0.1 192.168.100.0/24
# host deny = 192.168.100.13
interfaces = eth0 lo
bind interfaces = YES
follow symlinks = NO
log file = /var/log/samba/%m.log
max log size = 100
log level = 3
```

Mi pare che possa essere più che sufficiente per poter utilizzare il protocollo Samba senza impazzire. Ci potrebbero essere molte altre cosette da spiegare, ma sono più adatte ad server aziendale che ad una piccola rete casalinga (esempio creazione di un Dominio o di un DNS).

Non esitate a comunicarmi errori di stumpa (;)) o di concetto.

WebWolf
web_wolf@libero.it

Bibliografia:

- Un po' (…) di esperienza personale;
- Il sito www.samba.org;
- Il testo: "Linux Server" di Silvio Umberto Zanzi