http://keynes.scuole.bo.it/linux/samba/
18 may 05

Samba e le reti Windows

1) Struttura e utilità

Samba si presenta come un insieme di applicazioni che si avvalgono del protocollo SMB (Server Message Block) comune ad altri sistemi operativi di largo utilizzo, come Microsoft Windows e OS/2. Da qui la possibilità di fare fronte a diverse necessità di un network:
--condividere file
--condividere stampanti
--assistere i client nella ricerca delle risorse disponibili (Local Master Browser e Domain Master Browser)
--autenticare i client che si collegano a un donlinio Windows
--assumere la funzione di WINS server.

Samba è reperibile all'indirizzo *http://www.samba.org*

1.1 Analisi e configurazione di base

Come già accennato in precedenza, Samba si presenta come un insieme di programmi con diverse finalità. In realtà sono due i più importanti, meglio definiti con il termine demoni: smbd e nmbd.
Smbd è il demone responsabile della gestione delle risorse condivise tra il server Samba e i client collegati; fornisce ai client SMB l'accesso ai file condivisi, alle risorse di stampae la visualizzazione delle risorse nella navigazione di rete; è responsabile delle notifiche di funzionamento tra server e client e dell'autenticazione degli utenti.
Nmbd è il demone che imita le funzionalità di un server WINS e NetBIOS; rimane in ascolto delle chiamate dei client fornendo le informazioni appropriate per il collegamento ; è responsabile della lista
dei nomi che compare nella navigazione delle risorse di rete e partecipa nella scelta del server browser primario.
Esistono altri programmi di supporto forniti a corredo:
-- *smbclient*: un client Unix con una interfaccia simile a quella ftp che può essere utilizzato per connettersi alle condivisioni Samba;
-- *smbtar*: un piccolo ma efficiente script per eseguire dei backup di dati condivisi SMB/CIFS direttamente su unità nastro;
-- *nmblookup*: utilizzato per interrogare nomi NetBIOS e mapparli ai loro rispettivi indirizzi IP in un network che fa uso del procotollo NBT (NetBIOS su TCP/IP);
-- *smbpasswd*: permette di cambiare le password criptate usate da Samba;
-- *smbstatus*: programma che visualizza le connessioni alle condivisioni in corso
-- *testparm*: semplice utility per verificare la correttezza di un file di

configurazione smbd. Se non restituisce nessun errore si può essere sicuri che la configurazione verrà caricata da smbd, tenendo presente che il controllo non assicura di ottenere i risultati attesi ma solo di non avere commesso errori formali.
A questo punto si è pronti per generare il file di configurazione, chiamato *smb.conf*. Questo file è fondamentale per gestire il comportamento di Samba dal momento che contiene tutti i parametri necessari al funzionamento nel suo complesso. La fase di installazione non lo genera automaticamente (anche se spesso vengono rilasciati dei file di esempio nella documentazione); si procederà alla sua creazione integrandovi pochi comandi esclusivamente allo scopo di verificare il funzionamento del server. Durante il corso abbiamo visto la generazione di tale file utilizzando l'interfaccia grafica SWAT, in questo articolo si entra più nel dettaglio, non prima di avere spiegato nel suo insieme il funzionamento di una rete Microsoft per una migliore comprensione delle procedure.

1.2 I protocolli: SMB e TCP/IP

La grande popolarità di Samba risiede nell'ottima compatibilità del server con le reti Microsoft grazie al comune utilizzo del protocollo SMB (Server Message Block). Per affrontare con la dovuta preparazione l'argomento, è doveroso analizzare i concetti che stanno alla base di una rete SMB: il NetBIOS di IBM e il successivo NBT.
Il primo venne creato da IBM nel 1984 per affrontare in modo rudimentale il problema della connessione e della condivisione di dati tra computer; consisteva in una semplice interfaccia API (application programming interface) il cui acronimo significava per esteso Network Basic Input/Output System. L'anno successivo ne venne rilasciata una versione migliorata definita NetBEUI che permetteva di creare piccole reti locali (LAN) dove ciascuna macchina possedeva un unico nome di riconoscimento di 15 caratteri per un totale massimo di 255 nodi.
La fondamentale differenza che intercorre tra protocollo NetBIOS e TCP/IP consiste nella rappresentazione dei client sulla rete: il primo si avvale esclusivamente di nomi sotto forma di un range di caratteri alfanumerici; il secondo di un gruppo di triplette numeriche come ad esempio 192.168.1.100. Da qui nacque l'esigenza di unire i due protocolli e nel 1987, l'Internet Engineering Task Force (IETF) pubblicò una serie di documenti (RFC 1001-1002) che esponevano come adattare NetBIOS a reti TCP/UDP; il risultato fu l'implementazione di NetBIOS over TCP/IP (NBT). Il protocollo NBT consiste di tre servizi di rete:
-- *un servizio di risoluzione nome-indirizzo*
-- *un servizio Datagram* che si incarica di spedire pacchetti di dati direttamente o in broadcast senza accertarsi dell'arrivo a destinazione (UDP)
-- *un servizio Session* che instaura una comunicazione che permette di rilevare problemi o inoperabilità di connessione (TCP).

Nel sistema di connessione NetBIOS ogni volta che una macchina accede alla rete, cerca di identificarsi con un nome; questa operazione viene anche definita *name registration* (fig. 1-2)..

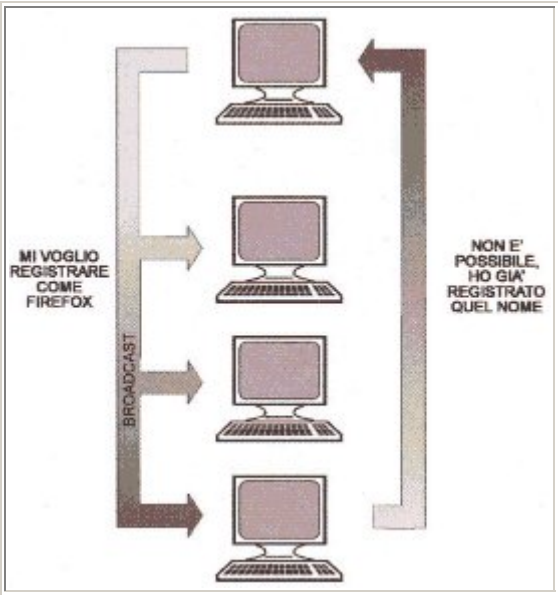

Fig 1: Registrazione del nome senza un NetBIOS Name server.

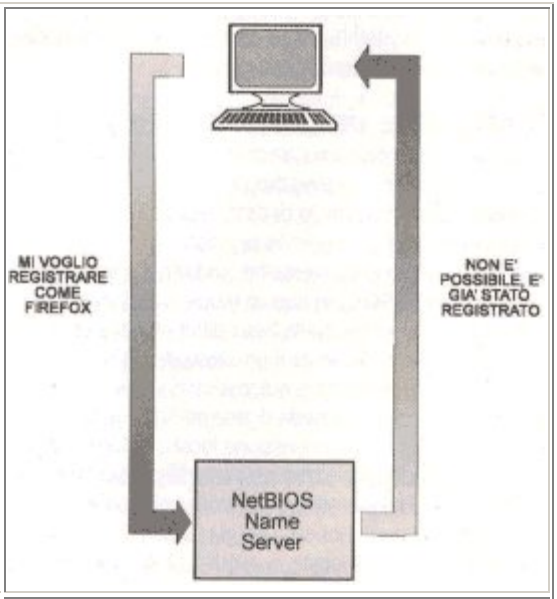

Fig 2: Registrazione del nome con un NetBIOS Name Server.

Ovviamente il maggiore problema che si può riscontrare in questa fase è nella verifica che non esistano due macchine con lo stesso nome in un dato momento. Due sono le soluzioni utilizzabili: avvalersi di un NetBIOS Name Server (NBNS) che tenga traccia delle differenti identità nomemacchina, oppure lasciare che sia compito del client “difendere” il proprio nome. Oltre al problema sopra esposto si deve garantire l'abbinamento tra un nome NetBIOS a uno specifico indirizzo IP; questa fase è anche conosciuta con il termine *name resolution* (fig. 3-4).

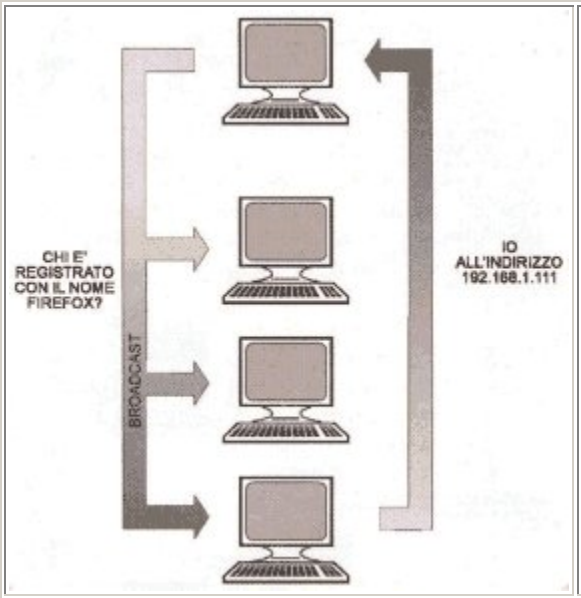

Fig 3: Risoluzione del nome senza un NetBIOS Name Server.

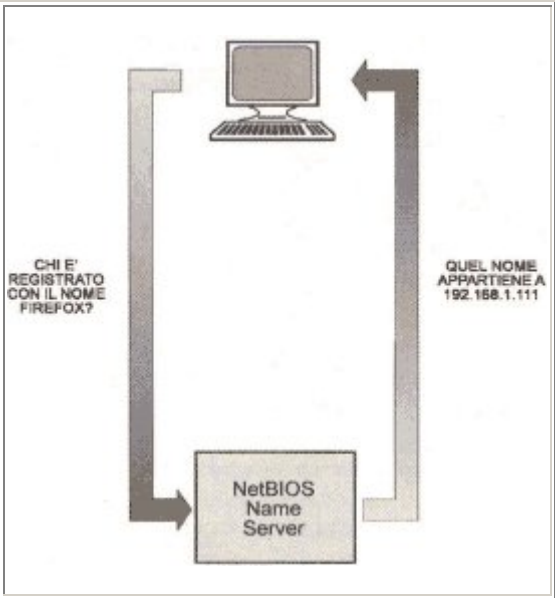

Fig 4 Risoluzione del nome con un NetBIOS Name Server.

NBT affronta il problema permettendo a ciascuna macchina di rispondere a una richiesta in broadcast del nome NetBIOS con il proprio indirizzo IP o, in alternativa, awalendosi di un NBNS nella risoluzione nomi NetBIOS/indirizzi IP. Di seguito si può vedere la tabella dei tipi di nodi NBT:

Tabella 1: tipi di nodi NBT

Tipo	Valore
b-node	registrazione in broadcast e risoluzione diretta
p-node	registrazione point-to-point e risoluzione diretta
m-node	registrazione in broadcast e notifica a **NBNS**; risoluzione in broadcast e notifica a **NBNS** in caso di errore
h-node (hybrid)	registrazione e risoluzione via **NBNS**; broadcast se **NBNS** non è disponibile

Se si desidera verificare il tipo di nodo utilizzato
da una macchina Windows, digitare al prompt dei comandi MSDOS

C:\>ipconfig /all

La finestra restituita dovrebbe mostrare alla voce "tipo di nodo" il termine ibrido (scelta usuale nelle reti Microsoft).

2) Funzionamento delle reti Microsoft

Quanto detto fino ad ora permette di descrivere il funzionamento tipico di una rete Microsoft fornendo le necessarie informazioni per il successivo approfondimento dei parametri di configurazione smb.conf.

2.1 Windows Domains

È possibile definire un gruppo di lavoro (workgroup) come un insieme di computer SMB che risiedono in una sottorete (subnet) e che accedono allo stesso gruppo SMB. Un dominio Windows consiste in un workgroup con un server in qualità
di domain controller.
Questa mansione è di fondamentale importanza dal momento che:
-- *gestisce il processo di autenticazione* (garantire o negare l'accesso a risorse condivise attraverso l'uso di password)
-- *gestisce il sistema di controllo username-password per mezzo di un security account manager* (SAM)
Una volta che un client viene autenticato, non necessita
più di una seconda verifica e viene considerato collegato
al workgroup; (riferirsi alla figura 5 per lo schema di funzionamento).
Il domain controller attivo in un dominio viene anche dèfinito Primary Domain Controller (PDC); esiste anche la possibilità di configurare una seconda macchina in qualità di Backup Domain Controller (BDC) nel caso (non così infrequente) che il PDC diventi inaccessibile.
Questa lunga disgressione ci permette di asserire che Samba può assumere il ruolo di PDC in luogo di soluzioni ben più costose.

2.2 Sistema di Browsing

Ogni volta che una macchina collegata a un workgroup ricerca le risorse condivise, effettua una operazione di browsing.
In un network SMB ne esistono di due tipi:
-- *browsing di una lista di macchine* (con delle risorse condivise)
-- *browsing di risorse condivise di una particolare macchina*.

In un workgroup Windows, la macchina adibita al mantenimento di una lista aggiornata di macchine si chiama
Local Master Browser.

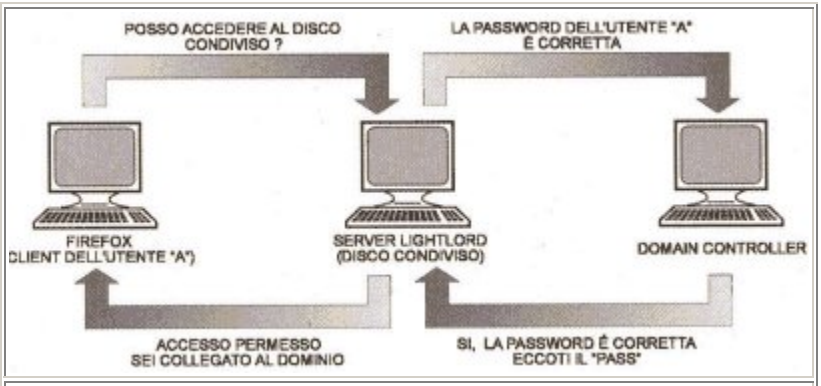

Fig 5: Autenticazione con un domain controller

L'accesso alle risorse di una singola macchina awiene invece attraverso il collegamento diretto alla stessa. Il ruolo del Local Master Browser è di grande importanza poiché ogni volta che un server si autentica in workgroup con un nome NetBIOS, lo comunica al LMB. In una rete Microsoft praticamente tutti i S.O. Windows possono ricoprire tale mansione, quindi per decidere il responsabile di questo compito si deve effettuare un'elezione (election). Una "elezione" consiste nell'invio in broadcast del proprio ruolo ricoperto nella rete attraverso il servizio datagram; questa informazione consiste in un valore numerico (si entrerà nel dettaglio più avanti). Ovviamente anche Samba vi partecipa attivamente. Accanto al ruolo di LMB è possibile trovare quello di Domain Master Browser. Quest'ultimo entra in gioco quando si hanno più subnet collegate tra loro: i vari LMB comunicano e si sincronizzano con il DMB permettendo l'aggiornamento delle liste delle risorse a disposizione di tutto il dominio Windows (spesso impossibile con un semplice broadcast dal momento che molti amministratori di rete bloccano questa operazione sui router).
La figura 6 riassume quanto esposto.

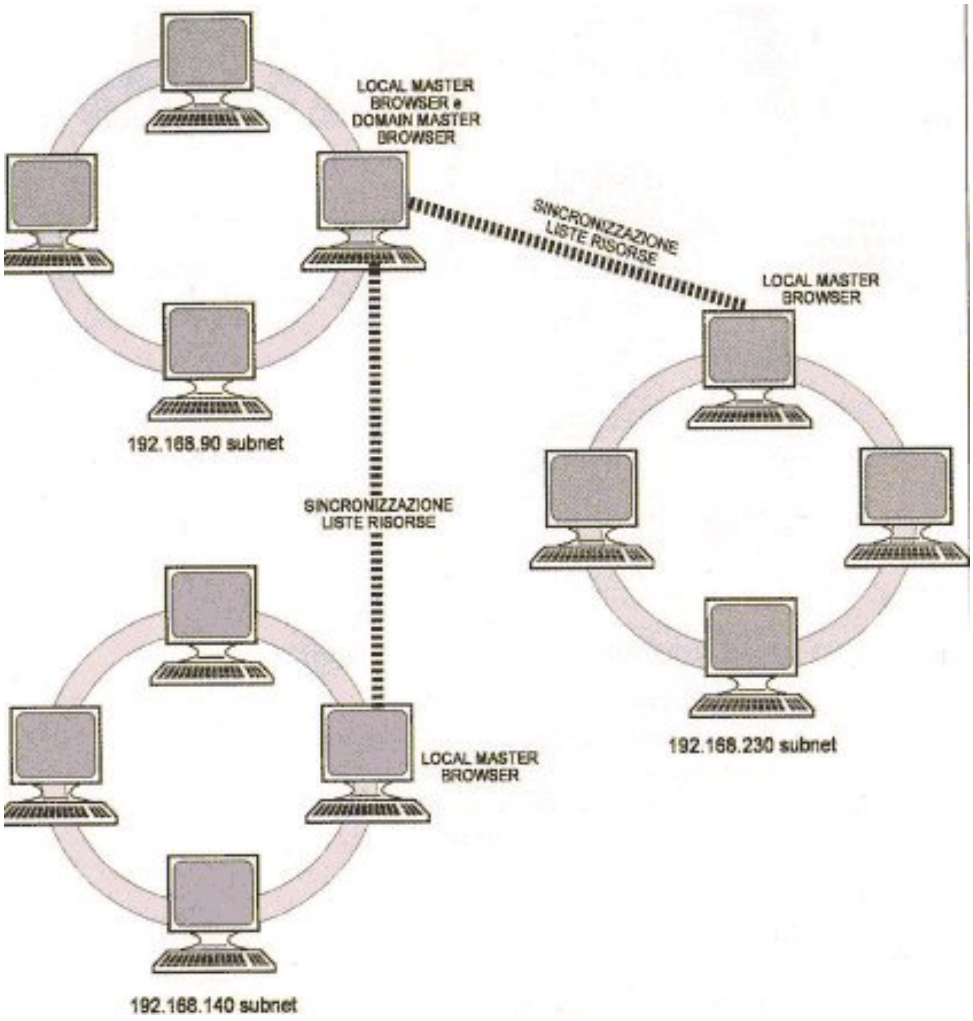

Fig 6: Wins Server

2.3 Il server WINS

Ultimo argomento da trattare a sommario completamento della panoramica sulle reti Microsoft è il Windows Internet Name Service (WINS). Questo servizio è la risposta Microsoft a NBNS, grazie ad esso è possibile gestire i client con i loro nomi, indirizzi e workgroup di appartenenza. Anche in questo caso esiste un WINS server attivo definito col nome di Primary WINS Server; accanto a esso si può collocare un server secondario che entra in azione nel caso che il principale non sia più disponibile. Samba può rivestire il ruolo di primary WINS Server come vedremo più avanti nell'analisi del file di configurazione.

2.4 Configurare un client Windows XP

È ora possibile inoltrarsi nella configurazione di una macchina Windows per un primo tentativo di accesso al server Samba. La scelta di Windows XP è legata principalmente alla sua attuale diffusione e alla presenza di alcuni problemi di connessione (come nel caso di Samba con mansione di PDC); in questo modo si ha l'occasione di approfondire questi aspetti assai dibattuti nella comunità Internet. Windows XP rende il processo di configurazione della rete abbastanza semplice e automatizzato (ora si può “addirittura” modificare i paramwetri di rete senza necessità di riavviare il sistema!!). Il riconoscimento della presenza di una scheda di rete ethernet genera automaticamente una connessione locale; dovrebbe essere solamente necessario impostare i parametri di collegamento (ip, dns, wins). Dal pannello di controllo selezionare "connessioni di rete", nel caso sia già presente una connessione alla rete locale, si procederà direttamente alla configurazione dell'indirizzo IP e subnet mask. Per crearne una nuova utilizzare "Crea nuova connessione" oppure "Installa una rete domestica o una piccola rete aziendale". La prima permette di configurare il singolo client, la seconda dà la possibilità di creare un disco d'installazione con i parametri scelti da applicare a tutte le macchine del workgroup. Una volta fatta la scelta, si passa alla fase vera e propria di configurazione. La finestra che segue richiede la tipologia di collegamento che si desidera installare per gli scopi prefissati, la terza opzione (installazione di una rete domestica o di una piccola rete aziendale) può andare bene. A questo punto Windows XP ci vuole informare riguardo a come il client è collegato alla rete; si scelga l'opzione più appropriata. Infine si arriva alle richieste che coinvolgono più direttamente i concetti fino a qui esposti: il nome NetBIOS della macchina e il workgroup di appartenenza. Gli esempi qui riportati utilizzano rispettivamente FIREFOX ed ESEMPIO: sostituiteli con quelli impostati nella vostra rete. Ultimato il processo di rilevamento, si dovrebbe essere in grado di visualizzare l'icona di connessione in "Connessioni di rete". Nel caso il client non abbia raccolto i dati necessari (in assenza di un DHCP server), si dovrà procedere all'inserimento manuale dei parametri: la richiesta delle "proprietà" sull'icona sopra citata aprirà la finestra di dialogo per cambiare i parametri TCP/IP della macchina.
Per le prove qui eseguite è stata configurata con: indirizzo IP 192.168.1.111,subnet mask 255.255.255.0, WINS server 192.168.1.100 (gestito da Samba). Si presti attenzione nel caso d'utilizzo di valori differenti di mantenere nella stessa subnet l'indirizzo del server samba e quello del client di prova. Comunque, è possibile (anche se meno elegante e flessibile) utilizzare il file */etc/hosts* sotto Linux e *c:\windows\hosts* nelle macchine Windows per la risoluzione dei nomi e dei loro rispettivi indirizzi IP.

2.6 Il file di configurazione smb.conf

Abbiamo visto il comando:

#***~smbclient -L localhost***

per testare il funzionamento del servizio; ègiunto il momento di verificare l'utilità di Samba con una macchina remota Windows. Per prima cosa è necessario cambiare i permessi d'accesso della cartella /prova affinché utenti non registrati sulla macchina Linux possano comunque operare in lettura e scrittura:

#***~chmod 777 /prova***

Chiaramente, l'impostazione di una così scarsa politica di sicurezza di accesso è da sconsigliare; in questo caso tornerà utile per agevolare l'introduzione di parametri più complessi su una condivisione pubblica. Spostiamoci sul client FIREFOX di prova (si consiglia di impostare una connessione ssh per il controllo remoto del server per evitare inutili e faticosi sposta menti di consolle) e cerchiamo all'interno delle "Risorse di Rete" la condivisione "test su Samba Server" impostata. Se non si riuscisse a visualizzarla, selezionare dal menu a sinistra "Tutta la rete": a questo punto, dovrebbe comparire il workgroup di appartenenza e le relative condivisioni, tra le quali il server Samba predisposto. Ora si è operativi con una cartella pubblica; si provi a copiarvi dei dati all'interno, rinominarli e cancellarli per testarne il buon funzionamento. Il file di configurazione *smb.conf* è strutturato in diverse sezioni, delimitate da alcuni parametri tra parentesi quadre:

[global]
...

[homes]
...

[printers]
...

[test]
...

Tutte le sezioni indicano qualche sorta di condivisione risorse, che sia una parte di disco o una stampante, ad eccezione della prima [global] che racchiude i parametri generali di Samba e comuni al resto del file di configurazione. All'interno di ciascuna di esse sono raccolti i parametri sotto forma di

opzione = valore

È anche possibile inserire delle linee aggiuntive di informazione (commenti) preceduti dal segno "#" o"**;**".

Passiamo all'inserimento di nuovi comandi nella sezione global, che dovrebbe mostrare le seguenti linee:

[global]
 # Parametri di configurazione Server

netbios name =LIGHTLORD
server string = Samba %v on (%L)
workgroup = ESEMPIO
security = share

Le due righe di comandi inserite annunciano rispettivamente, la presenza del server Samba sul network NBT con il nome LIGHTLORD e come descrizione aggiuntiva, la versione in uso e di nuovo il nome del server. L'utilizzo delle variabili, indicate con il segno %<n>, sono utili laddove occorra in casi particolari; nel box qui sotto il significato delle varibili

Tabella 2: variabili di smb.conf

Variabile	Stringa ID/Definizione
Client	
%a	Architettura del client (Samba, WfWg, WinNT, Win95, o UNKNOWN)
%I	Indirizzo IP del client (ad es. 192.168.220.100)
%m	Nome NetBIOS del client
%M	Nome DNS del client
Utente	
%g	Gruppo primario di %u
%G	Gruppo primario di %U
%H	Home directory di %u
%u	Nome utente Unix attuale
%U	Nome utente richiesto dal client
Share	
%p	Percorso dell'automounter alla directory radice della share, se diversa da %P
%P	Attuale directory radice della share
%S	Nome attuale della share
Server	
%d	Attuale PID del server
%h	Hostname DNS del server Samba
%L	Nome NetBIOS del server Samba
%N	Server delle home directory, come indicato nella mappa dell'automounter
%v	Versione di Samba
Altre	
%R	Il livello del protocollo SMB che è stato negoziato
%T	La data e l'orario attuali

Procediamo con le altre opzioni.
Inserire nella sezione

[global]
hosts deny = 192.168.1.111

e ritentare la connessione dopo avere riavviato Samba (*/etc/init.d/samba restart - come root*). Si potrà verificare l'impossibilità a connettersi: si è negato l'accesso a Samba dall'IP indicato. Il funzionamento di hosts deny (e il suo contrario, hosts allow) è simile a quello di */etc/hosts.allow* e */etc/hosts.deny*. Se quindi si procede all'inserimento (dopo l'eliminazione del parametro sopra riportato):

hosts allow = 192.168.1. except 192.168.1.111
hosts deny = all

Si otterrà un risultato identico al precedente, con una importante differenza: l'accesso alle condivisioni è garantito all'intero range di indirizzi 192.168.1 tranne che al client FIREFOX che usiamo di prova, oltre che a bloccare tutti gli IP al di fuori della subnet. I comandi appena mostrati possono tornare utili se si vuole permettere l'accesso di certi client a un server (attraverso una policy basata sul file /etc/hosts) con un secondo controllo da parte di Samba per l'utilizzo delle risorse condivise. Rimettiamo in funzione la mini rete di prova, con i concetti di sicurezza sopra esposti:

[global]
 # Parametri di configurazione Server

netbios name = LIGHTLORD server string = Samba %v on (%L) workgroup = ESEMPIO
security = share

#Parametri diconfigurazione permessi di accesso globali
hosts allow = 191.168.1. 127.0.0.1
hosts deny = all

Un ulteriore elemento di controllo sono i parametri interfaces e bind interfaces. Il primo permette di definire le schede di rete da utilizzare per comunicare (di default eth0); il secondo istruisce nmbd a respingere i dati che provengono dal broadcast tranne che dalle subnet definite da interfaces. Nel caso della macchina in prova, la eth0 ha come IP 1.15.141.42 mentre la eth1 192.168.1.100; definiremo nella sezione global:

#Parametri di scelta interfaccia
interfaces = 192.168.1.0/255.255.255.0 127.0.0.1
bind interfaces only = yes

Come è possibile notare, non si introduce l'IP esatto della scheda ma la subnet di appartenenza, con l'inserimento dell'indirizzo localhost altrimenti c'è il rischio che lo script smbpasswd non sia in grado di colloquiare con il server nella modalità di default. A questo punto è necessario presentare due comandi fondamentali per la fase di debugging di Samba: log level e log file.
Log level indica il livello di dettaglio (da 1 a 10) del file di log degli eventi accaduti durante l'esecuzione di Samba, compresi owiamente i possibili errori riscontrati. Si consiglia di settare sempre questo parametro almeno al suo valore più basso, cioè 1, per la verifica dei possibili problemi giornalieri che possono insorgere.
Il valore di riferimento per un buon equilibrio tra dettaglio e performance è 3, oltre il quale si rischia di incorrere in file di log molto grandi (che possono presto saturare lo spazio libero sull'hard disk) e utili solo ai programmatori del servizio. I creatori di Samba hanno comunque pensato anche a questa eventualità, fornendo il comando max log size per limitarne le dimensioni (in KB). Log file permette di definire la posizione dei file di log e il modo nel quale vengono rinominati; la directory di default è /var/log/samba.
Aggiungiamo quanto detto alla definizione global di *smb.conf*

 # Parametridi configurazione dei log
log level = 3
log file = /var/log/samba.log.%m
max log size = 50

2.7 Local Master Browser

Esaminiamo ora l'attivazione delle proprietà di master browsing, PDC e supporto Wins iniziando dal Local Master Browser. Per fare in modo che Samba partecipi a vari livelli all'elezione come Local Master Browser inserire sempre in [global]

#Parametri di elezione browsing
os level = 34
local master = yes
preferred master = yes

Analizziamo i nuovi parametri inseriti:
os level utilizza un numero intero (da O a 255) per stabilire in che modo partecipare all'elezione (vedere le tabelle 4 e 5). In prima istanza si verifica il livello dei sistemi operativi; in caso di parità si procede alla comparazione del ruolo di ciascuna macchina all'interno del workgroup. Nell'esempio qui citato, utilizzando anche il comando preferred master si associa il valore 8 al server Samba, permettendogli di battere una possibile macchina Windows con la quale ha ottenuto un pareggio con il valore os level.
local master informa il server Samba di partecipare all'elezione come local master browser.
preferred master fa in modo di forzare una elezione ogni volta che Samba si

connette al workgroup, anche se un local master browser è già attivo (con un valore di 4).

Tabella 3: Valori dei Sistemi Operativi

Sistema Operativo	Valore
Windows NT/2000 Server, funzionante come PDC	32
Windows NT/2000/XP, non PDC	16
Windows 95/98/Me	1
Windows for Workgroups	1

Tabella 4: Ruolo del computer nel workgroup

Ruolo	Valore
Domain master browser	128
WINS client	32
Preferred master	8
Running master	4
Recent backup browser	2
Backup browser	1

Per verificare la situazione di browsing nel network, è possibile dal prompt di MS-DOS lanciare il comando:

C:\>nbtstat -a LIGHTLORD

Si ottiene un output dei Nomi di Netbios del computer remoto confrontabile con la tabella:

Nome	*Tipo*		*Stato*
LIGHTLORD	<00>	UNICO	REGISTRATO
LIGHTLORD	<03>	UNICO	REGISTRATO
LIGHTLORD	<20>	UNICO	REGISTRATO
MSBROWSE	<O1>	GRUPPO	REGISTRATO
ESEMPIO	<00>	GRUPPO	REGISTRATO
ESEMPIO	<1D>	UNICO	REGISTRATO
ESEMPIO	<1E>	GRUPPO	REGISTRATO

La riga di nostro interesse è la quarta (MSBROWSE): comunica all'utente che la macchina interrogata possiede i privilegi di local master browser del workgroup ESEMPIO.

I valori esadecimali tra i segni di minore e maggiore indicano il ruolo ricoperto:

RisorsaNetBIOS	*Valore*	*Tipo*
Standard Workstation Service	<00>	UNICO
Messenger Service (WinPopup)	<03>	UNICO
RAS Server Service	<06>	UNICO
Domain Master Browser (con PC	<1B>	UNICO
Master Browser name	<1D>	UNICO
NetDDE Service	<1F>	UNICO
Fileserver (incluso printer server)	<20>	UNICO
RAS Client Service	<21>	UNICO
Network Monitor Agent	BE	UNICO
Network Monitor Utility	BF	UNICO
Standard Workstation	<00>	GRUPPO
Logon Serve	<1C>	GRUPPO
Master Browser name	<1D>	GRUPPO
Normal Group name	<1E>	GRUPPO
Internet Group name	<20>	GRUPPO

2.8 Primary Domain Controller

L'attivazione di Samba come Primary Domain Controller risulta abbastanza articolata; editare come già visto smb.conf e aggiungere a [global] i seguenti parametri (i comandi identici a quelli già trattati vanno sostituiti con i valori in corsivo qui esposti):

#Parametri PDC
domain master = yes
domain logons = yes
os level = 255
security = user
encrypt passwords = yes

Brevemente analizziamo i nuovi comandi
domain master = yes: attiva la funzione di domain master browser verificabile

con nbtstat e la comparsa del nome NetBIOS del dominio con il ruolo di <1B>
domain logons = yes: attiva la finestra di login nei client Windows per l'accesso al dominio
os level = 255: il massimo valore utilizzabile garantisce la vittoria di Samba come PDC;
security = user: ciascuna condivisione è assegnata ad utenti specifici
encrypt passwords = yes: attiva la transazione delle password in criptato tra client e server.

Il passo successivo è generare un utente in Linux e in Samba (nell'ordine):

#~adduser <utenteprova>
#~smbpasswd - a <utenteprova>

e aggiungere la macchine (client) del dominio:

#~useradd -s /bin/false -d /dev/null firefox/$
#~smbpasswd -a -m firefox

Si consiglia di evitare di assegnare password identiche sia per motivi di sicurezza che di amministrazione di sistema. Si può inoltre generare una password samba per l'utente root (responsabile delle possibili modifiche dei parametri di dominio)

#smbpasswd -a root

Infine, affinché Windows XP accetti Samba come PDC, intervenire sul registro (regedit.exe) modificando i seguenti valori:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Netlogon\Parameters]
"requiresignorseal"=dword:00000000
"signsecurechannel"=dword:00000000

e aprire in seguito da "Pannello di Controllo" la voce "Sistema". Nel sotto menu "Nome computer" scegliere l'opzione "Cambia" e attivare nella finestra che compare la voce (Membro di) "Dominio' digitando ESEMPIO. La conferma dei dati inseriti provoca la comparsa di una finestra di autorizzazione per le modifiche apportate: la prima volta che ci si collega inserire come nome utente root e la relativa password Samba. AI termine della procedura (disconnettersi e ricollegarsi) si dovrebbe essere in grado di connettersi al dominio ESEMPIO introducendo come login il nome dell'utente Linux e Samba precedentemente inseriti e come password quella impostata con smbpasswd.
La configurazione di un Windows Domain Controller coinvolge molti altri aspetti (primi tra i quali i roaming profiles) che saranno approfonditi più avanti.

2.9 WINS server

Il supporto di risoluzione dei nomi offerto da Samba può diventare molto utile laddove non si abbia a disposizione un server DNS. Per l'attivazione del server WINS, introdurre i seguenti comandi in [global]:

 # WINS server
wins support = yes
name resolve order = hosts bcast

Il parametro wins support è responsabile dell'avvio vero e proprio del supporto server WINS, mentre name resolve order indica l'ordine in cui Samba tenta la risoluzione. I valori possibili sono:

lmhosts: file localizzato in /etc/samba; il contenuto è simile a quello di /etc/hosts, con la differenza che all'indirizzo IP viene associato un nome NetBIOS (Es. 192.168.1.111 FIREWINS#OO)

wins: cerca di risolvere il nome avvalendosi di un server WINS sul network; questo comando si accompagna al parametro wins server = <IP wins server>;

hosts: utilizza il file /etc/hosts;

bcast: si avvia un broadcast per rilevare i nomi delle macchine presenti.

A questo punto editare il file */etc/hosts* e aggiungere:

192.168.1.111 firefoxsuwins

e riavviare Samba (operazione che si ricorda deve essere effettuata per qualunque modifica apportata a smb.conf).
Un semplice ping dal client FIREFOX ci informerà del funzionamento di WINS su Samba:

ping firefoxsuwins

3) Politiche di accesso e parametri di sicurezza

E' giunto il momento di sperimentare alcune soluzioni di accesso e le diverse modalità di autenticazione. A causa delle continue prove che verranno effettuate, si consiglia di volta in volta di resettare le connessioni di rete in esecuzione digitando dal prompt di MS-DOS del client il seguente comando:

C:\>net use * /delete /yes

3.1 Sicurezza e autenticazione

Riassumendo quanto è stato inserito nelle prove precedenti, il file smb.comf dovrebbe comparire come segue:

[global]
#Parametri di configurazione Server
netbios name = LIGHTLORD
server string = Samba %v on (%L)
workgroup = ESEMPIO

#Parametri di accesso security
security = share
encrypt passwords = yes

#Parametri di configurazione permessi di accesso globali hosts allow = 192.168.1. 127.0.0.1
hosts deny = all

#Parametri di scelta interfaccia
interfaces = 192.168.1.0/255.255.255.0 127.0.0.1
bind interfaces only = yes

#Parametri di configurazione log
log level = 2
log file = /var/log/samba/samba.log.%m.prova
max log siee = 50

#Parametri di elezione browsing
os level = 34
local master = yes
preferred master = yes

#Parametri PDC
#domain master = yes
#domain logons = yes

#WINS server
wins support = yes
name resolve order = hosts bcast

[test]
comment = Test di funzionamento
path = /prova
read only = no
guest ok = yes

Come si può notare è stato disattivato il supporto PDC dal momento che, per le prove che si andranno a eseguire, non è necessario. Il parametro di nostro interesse è security, attualmente impostato sulla modalità "share". Samba fornisce quattro diverse possibilità: sicurezza a livello condivisione (share-level security), a livello utente (user-level security),a livello server (server-level security) e a livello di dominio (domain-level security). Qualunque sia l'impostazione adottata, è fondamentale la presenza della direttiva encrypt passwords = yes che permette la transazione in criptato delle coppie login/password.

3.2 Share-level security

L'impostazione security = share istruisce Samba affinché controlli gli accessi a livello di condivisione: viene inviata esclusivamente una password e il nome dell'utente viene dedotto confrontandola con quelle rispettive
-- dei nominativi utenti indicati con la direttiva valid users se presente;
-- della macchina del client;
-- dei nominativi-utenti indicati con la direttiva guest account se presente (devono anche essere presenti all'interno dei parametri della condivisione i comandi guest ok = yes guest only = yes).

Questo livello di sicurezza viene adottato quando gli utenti Windows e Linux non coincidono e si desidera condividere delle porzioni di file system mantenendo gli stessi diritti sui file condivisi; il parametro guest account (se non indicato, di default "nobody") indica il nome dell'utente Linux grazie al quale i client Windows opereranno sulla condivisione, indipendentemente dalle loro rispettive identità. Impostiamo nuovamente la share "test" seguendo lo schema di funzionamento appena spiegato. Generiamo un nuovo utente Linux generico che verrà utilizzato dai client per l'autenticazione e la politica dei permessi di file e directory:

#~adduser samba

(verrà creato automaticamente anche il gruppo Samba)

#chsh /bin/false samba

(disattia la possibilità di login all'utente)

Ridefiniamo la maschera dei permessi della directiry /prova

#~chmod -R 0700 /prova
#~chown -R samba.samba /prova

Editiamo smb.conf per accettare qualunque accesso senza controllo di password:

[global]

#Definizidne dell'utente che accede alle condlvisioni
guest account = samba

[test]
comment = tst di funzionamento
path = /prova
read only = no
guest ok = yes
guest only= yes
create mask= 0600
directory mask = 0700

Come sempre, si riawia il server per l'attivazione delle modifiche; apparentemente non è cambiato nulla nell'utilizzo della share, ma in realtà sono state inseriti importanti politiche di sicurezza:
-- la directory "prova" non è più accessibile a chiunque ma solo all'utente generico "samba";
-- viene forzato, a scopo di autenticazione, l'utilizzo dell'utente definito in guest account attraverso la direttiva guest only (e nessuno altro);
-- create mask 0600: qualunque file creato all'interno della share [test] ha una maschera di permessi 600, leggibile e scrivibile solo dal proprietario (nel nostro caso "samba");
-- directory mask 0700: qualunque directory creata in [test] ha una maschera di permessi 700. Può essere aperta, cancellata e riscritta solo dal proprietario "samba".
Nel caso intendessimo richiedere una password per accedere a [test], dovremo intervenire su smb.conf con smbpasswd, fornito da Samba.

Editiamo nuovamente il file di configurazione:

[test]
comment = test di funzionamento
path = /prova
read only = no
#guest ok = yes
guest only = yes
valid users= samba
create mask = 0600
directory mask = 0700

Occorre disabilitare la direttiva per rendere pubblica la share e abilitare il controllo della password con l'opzione valid users. Quest'ultima funzione permette di definire gli utenti o gruppi (valid users = @group) in grado di accedere alla condivisione; se si intende adottare una politica di sicurezza

basata su utenti specifici si consiglia di utilizzare una security di tipo “user” molto più adatta allo scopo.
Un'osservazione di carattere generale: la validità di una password risiede nella sua segretezza; adottarne una in "condivisione" ne fa perdere l'efficacia. Di norma gli amministratori di rete evitano di impostare una security share sui loro server per avere maggiore controllo sui singoli utenti con una security user.
Passiamo alla creazione della password di Samba; quest'ultima è necessaria per l'autenticazione in fase di accesso e può essere generata solo se è già presente il rispettivo utente sul sistema Linux. Samba registra le sue password nel file /etc/samba/smbpasswd (smbpasswd -a il comando da usare).
Se visualizziamo il file /etc/samba/smbpasswd dovremmo vedere qualche cosa del genere:

samba:499:9720F5DDD2A634CEAAD3B435851404EE:D37EA50CSC784C33 FP6CBBC38499A5PB:[UX]:LCT.3EAE3937:

I due punti suddividono le varie sezioni: la prima indica il nome dell'utente inserito, la seconda la UID di riferimento, la terza la "LAN Manager Password Hash", sequenza esadecimale di 32 bit che rappresenta la password utilizzata da sistemi Windows 95 e 98, la quarta la "NT Password Hash" per le password Windows NT, l'ultima la rappresentazione in esadecimale del tempo intercorso in secondi dall'ultima modifica. La quinta parte, racchiusa tra i segni
[U/W I X I D I N] indicano:
U - tipo di account utente
W - tipo di account workstation
X - nessuna scadenza per la password dell'account
D - account disabilitato
N - l'account non ha password

Siamo in grado di verificare le impostazioni fino a qui inserite. Prima di tentare di accedere si consiglia di resettare la connessione precedentemente stabilita dal client con il comando net use accennato prima (altrimenti si incorre nel rischio di trasmettere i vecchi dati di autorizzazione, con il conseguente blocco dell'accesso).
Riavviamo il server e tentiamo la connessione; dovrebbe venire richiesto l'inserimento di una password quando si cerca di accedere a [test]: introducendo quella impostata con il comando smbpasswd, avremo il via libera a procedere.

3.3 User-level security

Il livello di sicurezza generalmente scelto (oltre che di default se non specificato) è quello utente: il client che desidera accedere alle condivisioni invia una login e una password (a differenza del livello share dove si manda esclusivamente una password) che vengono controllate da Samba con i dati inseriti in smbpasswd; se c'è corrispondenza l'utente ottiene i privilegi di accesso. L'elemento che contraddistingue questo tipo di configurazione consiste nella corrispondenza tra

l'utenza GNU/Linux e quella Samba: chi cerca di connettersi a una share deve essere registrato come utente anche su Linux, obbligo che può creare problemi nelle autenticazioni a causa del limite degli otto caratteri nel sistema Unix rispetto ai nomi estesi (fino a 255 caratteri) utilizzati da Windows. Può risultare quindi necessario avvalersi di un file che abbini gli utenti Linux a quelli Windows: smbusers.
Passiamo alla fase di configurazione; aprire smb.conf, commentare security = share, inserire una nuova direttiva security = user e commentare la direttiva guest account:

[global]

#Parametri di accesso security
#security = share
security = user
...
#guest account = samba

e condividiamo la home di un utente Linux sul server grazie
a Samba: nel nostro caso [marco]

[marco]
path = %H
comment = homedir dell'utente Marco
writable = yes
valid users = marco
create mask = 0664
directory mask = 0755

Come appena spiegato, dobbiamo ricordarci di inserire l'utente marco nel file delle password di Samba:

#~smbpassd -a marco
New SMB password:
Retype new SMB password:

Si può evitare di immettere una password identica a quella dell'account Linux per aumentare la sicurezza
Una volta riavviato il server (e resettato la connessione con net use), a differenza di quando si settava la security a livello di share, non appena si apre dalle risorse di rete il server Samba viene richiesta l'autenticazione con una login e una password. Terminata la procedura, si dovrebbe essere in grado di visualizzare le condivisioni [marco] e [test] a disposizione.
In realtà in questo momento non si hanno i privilegi di accesso per la share test che deve essere modificata per accettare i nuovi parametri introdotti, ma prima è necessario completare la panoramica dei parametri più importanti legati a questo

tipo di impostazione di sicurezza. Come accennato in precedenza, spesso il nome dell'utente è molto più lungo dei tradizionali otto caratteri degli username di Linux; in questo caso ci viene in aiuto la direttiva username map. Aprire il file smbusers (è anche possibile creare un file nuovo e mapparne l'indirizzo con username map) e aggiungere alle linee già presenti:

root = admin administrator
nobody = guest pcguest samba

la seguente:

marco = "utente marco"

Editare smb.conf e introdurre in [global] il pararnetro che informa Samba della presenza di un file di traduzione dei nomi:

...
#Mappa dei nomi-utente
username map = /etc/samba/smbusers

Riavviare Samba (si ricorda ancora il reset con net use) e tentare dal client Windows una connessione; come nome-utente digitare "utente marco" e a seguire la password impostata. Samba dovrebbe garantire l'accesso senza nessun problema. È giunto il momento di risolvere il problema dell'accesso a [test]: in questo momento viene rifiutata la connessione per problemi di autorizzazione. Per prima cosa è necessario impostare le diverse appartenenze ai gruppi degli utenti inseriti; aggiungiamo l'utente marco al gruppo samba

#~adduser marco samba

Si ricorda che anche i permessi della directory /prova devono essere modificati per accettare gli accessi degli utenti non proprietari:

#~chmod -R 770 /prova

Infine editiamo smb.conf affinché la share [test] accetti
le richieste di accesso di "marco":

[test]
...
valid users = samba, marco
create mask = 0660
directory mask = 0770

Dopo il riavvio del server (e solito net use), l'utente marco(o "utente marco") sarà in grado di creare, modificare e cancellare i file della propria home directory su Linux e di operare sulla condivisione comune [test] essendo appartenente al gruppo samba. La differente maschera dei permessi garantisce ad entrambi gli utenti di interagire reciprocamente con i file e le cartelle presenti nella directory. È importante notare che la proprietà dei file, a differenza della soluzione in security = share dove l'unico proprietario era "samba", rimane differente a seconda di chi accede alla share.

A completamento di quanto visto, diamo una rapida occhiata alla share speciale [homes], che non abbiamo ancora implementato in smb.conf. Il suo utilizzo torna utile quando sono presenti molti utenti che intendono accedere alla propria home di sistema, con il vantaggio di inserirvi tutte le direttive di funzionamento generiche. Un secondo aspetto è che viene interrogata quando un utente cerca di connettersi a una condivisione non specificata in smb.conf: in questo caso il nome immesso nell'UNC (barra degli indirizzi) in Windows Explorer verrà utilizzata per identificare l'utente Linux grazie a /etc/passwd. Per verificare quanto detto, si crei un nuovo utente Linux:

#***~adduser roberto***

Definita la password in GNU/Linux, si prepari quella in Samba:

#***~smbpasswd -a roberto***

L'utente "roberto" appena creato non compare con nessuna share nel file di configurazione; introduciamo la [homes]
che permetterà a chiunque possieda un account su Linux
di accedervi via Samba:

[homes]
browsable = no

writable = yes
create mask = 0600
directory mask = 0700

È stata inserita una nuova direttiva, browsable = no, che non permette la visualizzazione di questa particolare condivisione in fase di browsing. Si apra "risorse di rete" e si immetta direttamente l'UNC (barra deli indirizi) (barra che punta alla home dell'utente (*lightlord**roberto*); riferirsi alla' figura 3. In questomodo si ha a disposizione un metodo rapido ed efficace di fare accedere i nostri utenti alle rispettive home directory.

3.4 Server-level security

Il livello di sicurezza server è simile a quello utente. Questa opzione delega la fase di autenticazione delle password a un altro server SMB che può essere sia Samba che Windows NT Server con il ruolo di PDC. Quando un client tenta una connessione, il server di appoggio viene interrogato per convalidare la coppia username/password; in caso di conferma viene reso possibile l'accesso. In figura lo schema di autenticazione:

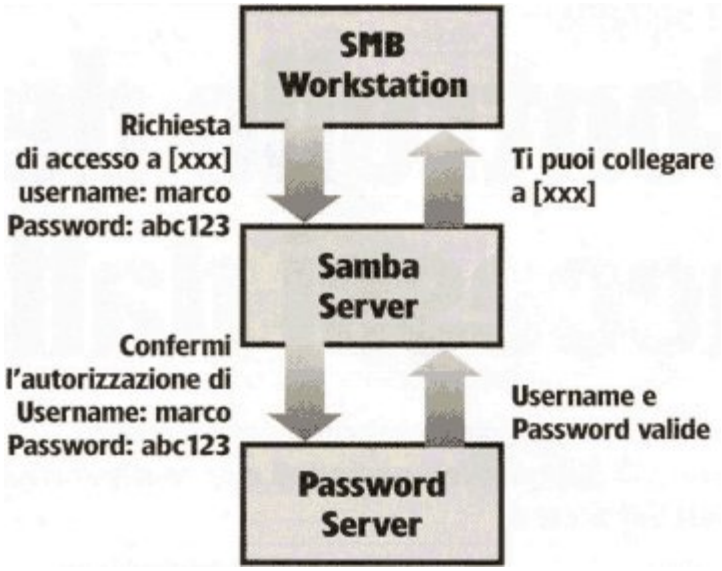

Fig 7 L'autenticazione secondo la modalità server-level security

La configurazione di smb.conf risulta semplice:

[global]
security = server
passwd server = NOMENETBIOS_SERVER1 NOMENETBIOS_SERVER2

Si noti come sia possibile specificare più di un server di appoggio; Samba procederà nella lista delle macchine elencate nel caso che la prima non sia raggiungibile. Un tentativo fallito di autenticazione terminerà la procedura d'interrogazione.

3.5 Domain-level security

Il livello di sicurezza dominio utilizza lo stesso meccanismo di autenticazione di quello utente, con l'importante differenza che il server Samba viene posizionato all'interno di un dominio Windows 2000/NT. Come accennato prima, un dominio è un workgroup con un domain controller normalmente un server Windows NT che copre il ruolo di PDC: in questo caso sarà proprio quest'ultimo a gestire il processo di autenticazione degli utenti (SAM) evitando che Samba copra tale ruolo non perfettamente compatibile (data la strutturazione delle password tipicamente Unix) con i network Microsoft.
I passi da compiere sono i seguenti:

-- fermare il demoni di Samba; (/etc/init.d/samba stop)
-- aggiungere il server Samba al dominio NT sul PDC con il server manager di Windows NT oppure ad una active directory sul server Windows 2000 con la MMC (Microsoft management console) con il tool "Utenti e computer di Active Directory";
eseguire:

#~smbpasswd -j nome_dominio -r nome_server -Unome_utente%password.

nome_dominio è lo stesso indicato nella direttiva workgroup in smb.conf;
nome_server coincide con quello indicato in password server;
nome_utente e password rappresentano la username e password dell'utente con i privilegi necessari ad aggiungere nuove utenze nel server Windows NT/2000;

riawiare Samba.

#~/etc/init.d/samba start

L'utilizzo di una sicurezza livello dominio rispetto a quella server evita un carico eccessivo di dati al PDC: infatti la seconda mantiene un collegamento di rete permanente tra i due server mentre la prima interroga il PDC solo quando è necessario autenticare un utente. Un aspetto importante da considerare quando si adotta la soluzione del dominio consiste nell'allineamento dell'elenco delle utenze tra il server Windows e quello GNU/Linux. In quest'ultimo caso vengono in aiuto due direttive che ne automatizzano l'aggiornamento:

[global]
add user = script1 %u
delete user = script2 %u

La prima direttiva si attiva quando un client Windows tenta l'autenticazione ma l'utente corrispondente GNU/Linux
non esiste: lo "script1:, adeguatamente scritto e testato, dovrà creare l'utente

ricevendolo come parametro dalla variabile %u. La seconda entra in funzione nel caso contrario, cioè quando un client Windows con il corrispondente utente GNU/Linux si connette e Samba chiede l'autorizzazione al PDC, ottenendo una risposta negativa: lo "script2" dovrà cancellare l'utente in questione.

4) Breve conclusione

Sono state trattate le differenti modalità di sicurezza fornite da Samba, evitando di entrare nel dettaglio nel caso di server-level security e domain-level security, a causa della loro complessità.
Consideriamo inoltre cheil panorama di Samba è in continua evoluzione, e il rilascio di Samba 3 ha introdotto nuove fubìnzionalità che non sono state quì trattate.