Samba
Integrazione UNIX-NT

Questa unità didattica descrive le modalità di integrazione di un sistema *UNIX* all'interno di una rete in tecnologia *Windows*. In particolare viene presentato il *software* Samba, che implementa in *UNIX* la parte *server* del protocollo **SMB** (*Session Message Block*).

SMB, (utilizzato anche con il significato di *Server Message Block*) è un protocollo utilizzato per condividere risorse *hardware* (*file*, stampanti, periferiche in genere) e risorse *software* di un sistema di elaborazione (*pipe*, *mailbox*, eccetera).

L'idea del protocollo SMB nasce in ambito IBM verso la metà degli anni '80 e successivamente è stata ripresa da *Microsoft* fin dal 1987. Il protocollo è stato successivamente sviluppato ulteriormente da *Microsoft* e altri.

I dati SMB possono essere incapsulati e trasportati in datagrammi TCP/IP, oppure NetBEUI e IPX/SPX.

Al fine di collegare quanto analizzato nei moduli didattici in cui sono state affrontate le architetture e le infrastrutture per trasmissione dati ed i protocolli della famiglia TCP/IP, si include qui uno schema grafico che evidenzia la posizione del protocollo SMB nell'ambito dell'architettura di comunicazione.

Samba

Samba è una implementazione del protocollo *Session Message Block*, utilizzato dalle reti *Windows*. Samba è disponibile come *software Open Source* per molti sistemi *UNIX*. Oltre alla distribuzione ufficiale, esistono anche alcuni prodotti commerciali derivati da Samba.

Attualmente il pacchetto supporta solamente il protocollo SMB incapsulato all'interno di pacchetti IP (in *Windows* è infatti possibile utilizzare altri protocolli di trasporto come NetBEUI o IPX/SPX). Rispetto ad un *server* NT vi sono inoltre alcune differenze nei meccanismi di *locking* dei *file*, di gestione della autenticazione, una diversa gestione dei permessi ed un diverso formato nei *file* di testo.

Samba implementa in modo efficiente e sufficientemente completo la parte *server* del protocollo, e può essere utilizzato per fornire da un *server UNIX* i seguenti servizi ad una rete di *client Windows*:

- Condivisione di *directory* da *UNIX* verso PC.
- Condivisione di servizi di stampa verso PC.
- *Primary Domain Controller*.
- *Nameserver* compatibile NetBIOS utilizzabile come *master browser* e *server WINS*.
- Supporto per *Common Internet Filesystem* (CIFS).
- Gestione grafica mediante *browser Web* delle principali funzionalità (*Swat*).

La parte *client* invece comprende:

- un *client* a linea di comando per l'accesso a volumi condivisi (*smbclient*) o la stampa su stampanti *Windows*; la maggior parte delle distribuzioni di *Linux* è già predisposta per stampare attraverso *smbclient* su una stampante remota residente su un *server* di rete *Windows*.
- Un comando (*smbtar*) per eseguire il *backup* di PC via rete.
- I programmi per montare su *Linux* volumi condivisi da un *server Windows*; il supporto necessario da parte del *kernel* è compreso nella distribuzione standard di *Linux*.

I principali componenti di Samba sono i seguenti:

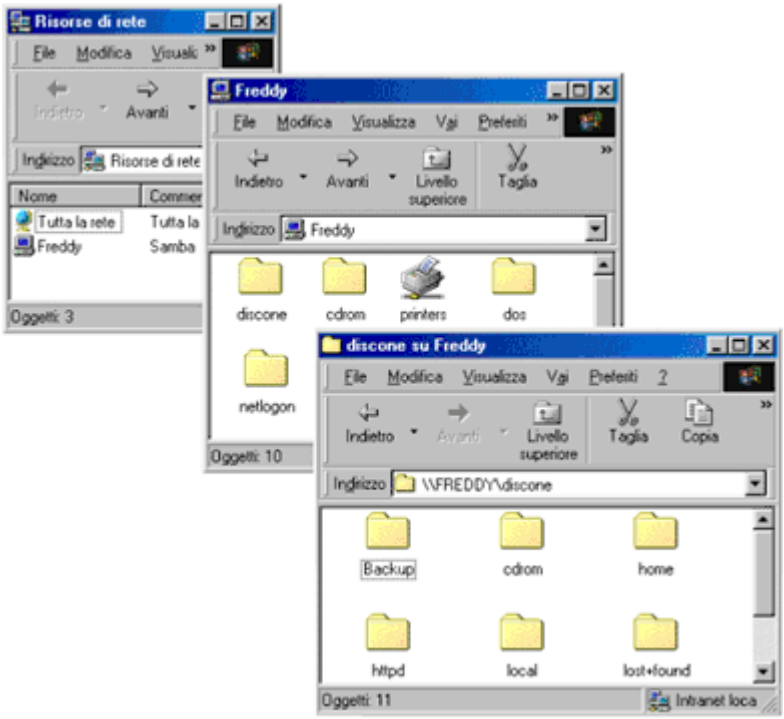
- *smbd*: *server* SMB;
- *nmbd*: *nameserver* NetBIOS (rfc1001/1002);
- *smbclient*, *smbprint*, *smbmount*, *smbtar*: *client* SMB;
- *smbpasswd*, *convert_smbpasswd*, *smbadduser*, *mksmbpasswd.sh*, *testparm*, *smbstat*, *nmbdlookup*: programmi di amministrazione;
- *swat*: interfaccia grafica (*web based*).

SAMBA versione 2.2

La versione 2.2 di Samba, a cui faremo riferimento, ha introdotto le seguenti novità:

- **Stampanti**. È stata introdotta la possibilità di fornire automaticamente i *driver* delle stampanti ai *client*. I *driver* devono essere prima installati ed assegnati alle stampanti sul *server* Samba mediante l'*Add Printer Wizard* (APW) di *Windows* oppure mediante il *software Imprints* (*Installation Manager of Printer driver Retreival and Installation for Samba*), disponibile su http://imprints.sourceforge.net/.
- ***Access Control Lists* (ACL)**. Viene effettuato una mappatura fra le ACL di NT e le ACL fornite dal *filesystem UNIX*. Tale funzione viene supportata limitatatmente ad alcuni sistemi operativi e *filesystem* (esempio: *Linux* + ext2). Le ACL sono modificabili direttamente tramite la *shell* grafica di *Windows WinNT Explorer Security Tab*.
- ***Locking***. Vengono risolte le limitazioni delle versioni precedenti, offrendo diversi meccanismi di *locking* dei *file*. Tali funzioni dovrebbero essere utilizzati con attenzione, in quanto potrebbero avere conseguenze significative sia sull'integrità dei *file* che sulle prestazioni del sistema.
- **Domini *Windows***. È possibile utilizzare Samba per gestire le funzionalità tipiche di un *server* di rete NT:
  - liste utenti per *Windows* 9x;
  - supporto completo dei *client* NT 4.0 SP3+;
  - supporto completo dei *client Windows* 2000 in modalità *legacy*.

  Le *System Policy* funzionano in modo analogo a quanto avviene nei domini NT 4.0, eccetto i gruppi, che verranno supportati in una prossima versione di Samba. Non sono inoltre supportate le *Trust Relationship* con altri domini ed il protocollo di replica (ovvero non è possibile utilizzare Samba come BDC).



Installazione di Samba

Il programma è già presente di serie in molte distribuzioni di *Linux* ed in alcuni sistemi *UNIX*. Nel caso non fosse presente, è possibile prelevare i sorgenti oppure i binari precompilati da http://www.samba.org/.

È possibile avviare Samba sia come *server* a sé stante, che mediante il supervisore `inetd/xinetd`. Nel primo caso è necessario creare uno *script* `rc` di avvio che faccia partire come demoni (opzione -D) i due programmi *smbd*, che implementa il protocollo vero e proprio, e *nmbd*, che si occupa della risoluzione dei nomi:

```
smbd -D
nmbd -D
```

Volendo utilizzare `inetd` si devono invece inserire in `/etc/inetd.conf` due linee simili alle seguenti:

```
netbios-ssn stream tcp nowait root /usr/sbin/smbd smbd
netbios-ns dgram udp wait root /usr/sbin/nmbd nmbd
```

L'utilizzo di `inetd` permette eventualmente di proteggere ulteriormente l'accesso ai servizi rispetto alle *access list* di Samba utilizzando un *TCP wrapper*.

Il protocollo NetBIOS sopra TCP/IP utilizza le seguenti porte

- UDP/137: risoluzione dei nomi e registrazione (*nmbd*);
- UDP/138: *browsing* e annuncio (*nmbd*);
- TCP/139: condivisione *file* e stampanti (*smbd*).

che devono essere opportunamente definite in `/etc/services`:

```
netbios-ns 137/tcp nbns # NetBIOS Name Service
netbios-ns 137/udp nbns
```

```
netbios-dgm 138/tcp nbdgm # NetBIOS Datagram Service
netbios-dgm 138/udp nbdgm
netbios-ssn 139/tcp nbssn # NetBIOS session service
```

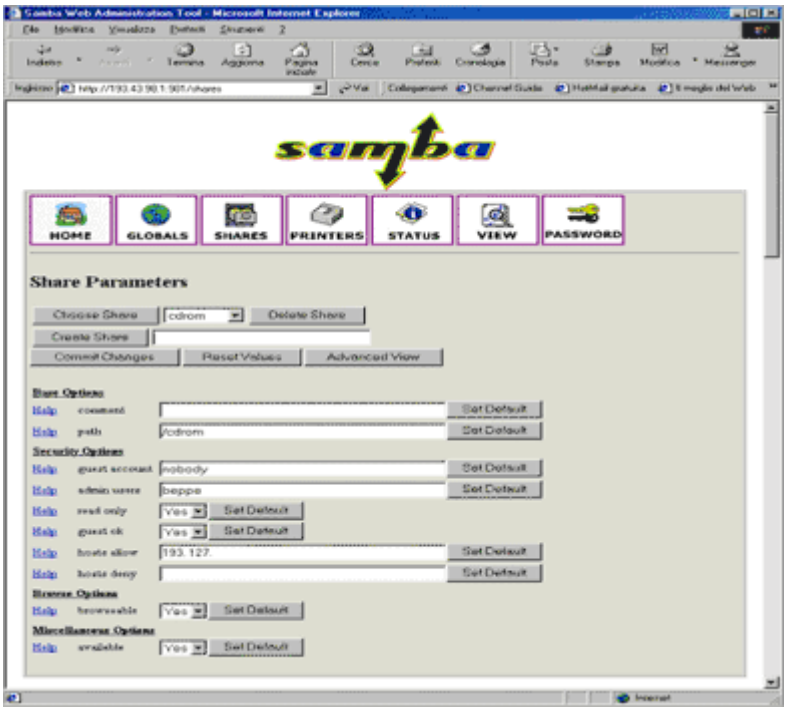
La configurazione di Samba avviene mediante il *file* `smb.conf` (generalmente in `/etc`) e può essere effettuata mediante la modifica diretta del *file*, che ha formato simile ad un *file* INI di *Windows*. Una volta modificato il *file* è necessario far ripartire il servizio oppure inviare un segnale di tipo HUP sia a *smbd* che a *nmbd*.

È buona norma, quando si apportano delle modifiche a `smb.conf`, verificare la correttezza della configurazione utilizzando il comando *testparm*.

Una volta attivato il servizio, è possibile tenerne sotto controllo il funzionamento mediante i *file* di log (generalmente in `/var/log/samba/`) e mediante il programma `smbstatus`.

Swat

Se è stato installato il programma *Swat*, è possibile accedere ad una interfaccia grafica collegandosi con un *browser* alla porta 901 del *server* (http://indirizzo:901/). L'utilizzo di *Swat* non è incompatibile con la modifica diretta di `smb.conf`.



Per installare il programma è sufficiente aggiungere a `/etc/services` la linea

```
swat 901/tcp
```

e configurare opportunamente `inetd`

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

Anche in questo caso è consigliabile utilizzare il *TCP wrapper* per limitare l'accesso al servizio.

Oltre a *swat* esistono anche altre interfacce grafiche che aiutano la configurazione di Samba. Volendo effettuarla direttamente da un *client Windows* si può utilizzare il programma SmbEdit.

Schema di autenticazione

Quando l'utente di un *client* accede ad una condivisione, Samba tenta di associarlo ad un utente *UNIX*, con i cui permessi verranno poi effettuati gli accessi alle risorse *UNIX* legate alla condivisione.

Samba utilizza diverse tecniche per determinare l'utente associato alla condivisione in base al nome della stessa. Nel caso non fosse possibile determinare l'utente, è possibile permettere comunque l'accesso utilizzando i permessi di un utente fittizio (*guest*). Questo è utile ad esempio per creare delle condivisioni pubbliche.

Come questa associazione venga effettuata dipende dallo schema di autenticazione prescelto. In Samba sono possibili i seguenti metodi di autenticazione:

- ***Share* (*security = share*)**. È lo schema di autenticazione utilizzato nelle versioni di Samba precedenti la 2.0. L'utente *UNIX* viene associato alla condivisione in fase di definizione della stessa.
- ***User* (*security = user*)**. È il metodo di autenticazione predefinito a partire dalla versione 2.0 di Samba. L'utente deve effettuare il *logon* per venire associato ad un corrispondente utente *UNIX* ed ottenere accesso alla risorsa condivisa.
- ***Server* (*security = server*)**. In questo schema si utilizza un altro *server* SMB (ad esempio un *server* NT) per l'autenticazione. Se questa fallisce, allora viene utilizzato il metodo "*security = user*".
- ***Domain* (*security = domain*)**. Valida gli utenti allo stesso modo di *Windows* NT, usando un PDC o un BDC. Richiede che i *client* vengano aggiunti al *domain* mediante il comando *smbpasswd*. Accetta solamente *encrypted password*.

Encrypted password

Allo scopo di non fare transitare *password* in chiaro attraverso la rete, a partire dalla versione 2.0 di Samba vengono utilizzate per *default* delle *password* codificate. Esse vengono mantenute in un *file* separato e sono codificate in modo diverso rispetto a quelle degli utenti *UNIX* in `/etc/passwd`. Per facilitare la transizione è prevista la creazione automatica della *password* codificata nel caso l'utente esegua il *logon* in chiaro.

Nel caso non si desideri utilizzare le *password* codificate, si deve specificare in `smb.conf` l'opzione *encrypt passwords* = No. Tuttavia le *password* in chiaro non sono supportate dai *client Windows* recenti e probabilmente non verranno supportate nelle prossime versioni di Samba.

Nota: volendo, è possibile far accettare ai nuovi *client* le *password* in chiaro utilizzando una *entry* speciale nel *registry*. I *file* `.reg` necessari sono inclusi per convenienza nella *directory* `doc` di Samba.

File di configurazione

Sezione	Descrizione
[*global*] *security=share* *workgroup=WORKGROUP* *netbios name=SERVER*	Parametri globali e valori di *default*
[*homes*] *comment=Home Directories*	*Home director* degli utenti *UNIX*: //*SERVER*/*USERNAME*

read only=No
create mask=0755
browseable=No

[*printers*]
comment=lista stampanti
path=/var/*spool*/samba Condivisione stampanti di sistema: //*SERVER*/*PRINTERNAME*
guest ok=YES
print ok=YES

[disco2]
comment=Disco2
path=/disk2
read only=No
guest ok=No

[cdrom]
comment=CD-ROM
path=/mnt/cdrom Definizione esplicita di servizi e condivisioni
read only=Yes
guest ok=Yes

[tmp]
path=/tmp
read only=No
create mask=0755
guest ok=Yes

Il *file* di configurazione `/etc/smb.conf` ha un formato simile ad un *file* INI di *Windows* ed è suddiviso in due tipologie di sezioni:

- sezioni speciali
  - [*global*];
  - [*homes*];
  - [*printers*];
- sezioni che definiscono servizi
  - [nomeservizio];

Sezioni speciali

- **[*global*]**. Le opzioni definite in questa sezione si applicano al *server* nella sua interezza. Generalmente viene utilizzato per il *tuning* del *server* (*dead time*, *keep alive*, *widelinks*, *getwd cache*, *socket options*, ...) e per definire i valori di *default* per i servizi.
- **[*homes*]**. È una sezione opzionale, che, se definita, permette di associare automaticamente una condivisione del tipo `//nomeserver/utente` con la *home directory* e con i permessi dell'utente *UNIX* corrispondente. Ad esempio, tentando di aprire `//nomeserver/rossi`, se non è stato definito esplicitamente un servizio di nome [rossi], viene condivisa la *home directory* per l'utente *UNIX* rossi. Questo permette di non dover definire e mantenere aggiornate in `smb.conf` tutte le condivisioni corrispondenti ai singoli utenti. Specificando nella definizione del servizio il valore *browseable = Yes*, è possibile rendere sfogliabile la lista degli utenti.
- **[*printers*]**. Definendo questa sezione, è possibile condividere automaticamente tutte le stampanti presenti nel *server UNIX* senza dover definire le singole condivisioni. È possibile rendere sfogliabile la lista delle stampanti specificando nella definizione del servizio *browseable = Yes*.

La regola di ricerca per associare il nome di una condivisione (esempio: `//nomeserver/nomevol`) con la corrispondente risorsa nel sistema è la seguente:

- viene cercato fra i servizi definiti se ne esiste uno con etichetta nomevol;
- se non viene trovato, ed è definita la sezione [*homes*], allora viene verificato se esiste l'utente *UNIX* nomevol;
- se non viene trovato, ed è definita la sezione [*printers*], allora viene verificato se nel sistema esiste una stampante di nome nomevol.

Esempio di definizione di un servizio

```
[nomeservizio]
comment = sample share
path = /disk2/test
writable = yes
printable = no
public = no
valid users = name1, name 2, @group2
invalid users = name3, name5, @group1
write list = name1, @group2
force create mode = 0660
force directory mode = 0775
```

Questo esempio di definizione di servizio mostra come rendere la *directory* `/disk2/test` del *server UNIX* accessibile dai *client Windows* come `//nameserver/nomeservizio`. Per far ciò è necessario creare una nuova sezione in `smb.ini` col nome che si vuole assegnare alla condivisione. Seguono un commento opzionale e il percorso della *directory* che si desidera condividere.

La riga *printable*=no indica che non si tratta di una stampante, mentre *writable = yes* identifica un servizio a cui è possibile accedere anche in scrittura.

La riga *public*=no restringe la leggibilità della condivisione ai soli utenti definiti come *valid users*, ad eccezione di quelli definiti come *invalid users*, mentre *write list* regolamenta l'accesso in scrittura.

Le liste possono essere costituite da un insieme di *username* di utenti *UNIX* oppure da scritture del tipo @gruppo, che identificano tutti gli utenti appartenenti ad un determinato gruppo *UNIX*.

Le due opzioni *force create mode* e *force directory mode* controllano i permessi assegnati dal sistema ai nuovi *file* ed alle *directory* che vengono create da Samba. La prima riga forza il permesso 0660 per ogni nuovo *file* che viene creato, in modo da permettere agli altri utenti dello stesso gruppo *UNIX* del proprietario di modificare il *file*. La seconda controlla invece il permesso da assegnare alle *directory* (775 permette la lettura e scrittura a tutti gli utenti dello stesso gruppo del proprietario e l'accesso a tutti gli utenti). La gestione dei permessi da parte di Samba comprende anche una maschera, con cui viene eseguita una operazione di *and* binario con i permessi DOS/*Windows*. I valori predefiniti sono 0744 per i *file* e 0755 per le "*directory*".

Questo metodo permette comunque una mappatura abbastanza limitata dei permessi, in quanto non esiste una corrispondenza biunivoca fra come vengono interpretati dal mondo *Windows* e da quello *UNIX*. Ad esempio in *UNIX* non esiste un meccanismo standard di gestione delle ACL, ma i diversi sistemi operativi lo implementano ciascuno a proprio modo. La versione 2.2 di Samba introduce dei notevoli miglioramenti in questo campo, che tuttavia sono disponibili solamente per certe combinazioni particolari di sistema operativo/*filesystem*.

Esempio di utilizzo di Samba come PDC

```
[global]
security = user
workgroup = GRUPPO
netbios name = NOME
server string = Samba
encrypt passwords = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *password* %n\n *password* %n\n *successfull*
unix password sync = Yes
log level = 2
logon script = scripts\%U.bat
logon path = \\netlogon\%U\profiles
logon home = \\netlogon\%U
domain logons = Yes
preferred master = Yes
domain master = Yes
wins support = Yes
admin users = beppe
hosts allow = 10.10.1. 213.215.88.138
[Profiles]
comment = Windows-User-Profiles
path = /home/%U/profiles
read only = No
guest ok = Yes
browseable = No
[homes]
comment = Home Directories
read only = No
create mask = 0755
browseable = No
[netlogon]
path = /home/samba/netlogon
create mask = 0755
[cartelle]
comment = Cartelle Condivise
path = /disk2/cartelle
force group = utenti
read only = No
create mask = 0777
directory mask = 0777
guest ok = Yes
hosts allow = 10.10.
[tmp]
path = /tmp
read only = No
create mask = 0755
guest ok = Yes
[printers]
comment = All Printers
path = /var/spool/samba
guest ok = Yes
print ok = Yes
```

Questo esempio, da intendersi come punto di partenza per realizzare una propria configurazione, illustra come Samba possa essere utilizzato per implementare un *server* di rete con funzione di *Primary Domain Controller*. Le diverse opzioni utilizzate sono descritte in dettaglio nella documentazione di Samba.

Creazione *account* per i *client*

È necessario creare un *account* per ognuno dei *client* a cui si desidera offrire accesso al sistema. Per far ciò si deve creare un utente *UNIX* corrispondente, avendo cura di far terminare il nome con il

carattere $. Per far questo si può utilizzare il comando

```
# useradd pc001$
```

Non è necessario assegnare una *password*, così come non sono importanti la *home directory* e gli altri campi in `/etc/passwd`, in quanto il controllo sugli accessi viene gestito da Samba mediante il *file* separato `/etc/smbpasswd`. Occorre pertanto aggiungere un record relativo al *client* anche in questo *file*, utilizzando il comando

```
# smbpasswd -a -m pc001
Added interface ip=193.43.98.1 bcast=193.43.98.255 nmask=255.255.255.0
Added user pc001$.
Password changed for user pc001$.
```

Non occorre specificare il $ alla fine del nome, in quanto viene aggiunto direttamente dal programma.

Creazione degli *account* per gli utenti

A questo punto si deve creare gli *account* per gli utenti che possono effettuare il *logon* sui *client*. Anche in questo caso deve essere creato sia l'*account UNIX* che quello nel *file smbpasswd*:

```
# adduser utente1
# smbpasswd -a utente1
Added interface ip=193.43.98.1 bcast=193.43.98.255 nmask=255.255.255.0
New SMB password:
Retype new SMB password:
Added user utente1.
Password changed for user utente1.
```

Per la creazione degli utenti può essere utile ricorrere allo *script mksmbpasswd.sh*, che permette di popolare il *file* `/etc/smbpasswd` con i record degli utenti definiti in *UNIX*.

Una volta creato l'utente, la modifica di una *password* può essere effettuata sia da *UNIX* che direttamente dal *client windows*. Non è necessario che le *password* usate da *UNIX* e da Samba coincidano.

Una volta configurati in modo opportuno i *client*, sarà possibile accedere alle risorse condivise utilizzando lo *username* appena creato.

Smbclient

Consiste in un *client* a linea di comando, che può essere utilizzato anche all'interno di *script*, e che permette di accedere a volumi condivisi da un *server* SMB. Permette di trasferire *file* da e verso *server Windows*, di spedire messaggi *WinPopUp* e di stampare su *server Windows*. Risulta inoltre un utile strumento diagnostico.

Lo *script smbtar* permette di eseguire il *backup* automatizzato di una rete di PC su un *server UNIX*.

Smbfs

Linux consente di accedere al volume condiviso da un *server Windows* o Samba come se si trattasse di un *filesystem UNIX*. Il *software* necessario è costituito da un modulo del *kernel*, compreso di serie in *Linux*, e dai programmi di gestione (*smbmount*), i quali si trovano all'interno della distribuzione di Samba.

Smbfs sfrutta solamente un sottoinsieme delle possibilità di SMB.

Il *mounting* del *filesystem* avviene mediante il comando *smbmount* specificando direttamente sulla linea di comando le *password* necessarie

```
# smbmount //ntserver/test /mnt4/ -U test
Added interface ip=193.43.98.1 bcast=193.43.98.255 nmask=255.255.255.0
Password:
```

oppure utilizzando il classico *mount* con l'opzione -t smbfs

```
# mount -t smbfs -o
username=test,password=test123,netbiosname=linuxserv //ntserver/JAZZ /backupdir/
```

È disponibile, come pacchetto a parte, l'interfaccia grafica Gnomba, che permette di sfogliare una rete e montare *filesystem* in modo simile a quanto avviene nei *client Windows*.

Maggiori informazioni sono disponibili all'interno della documentazione del *kernel* di *Linux* nel *file* `/usr/src/linux/Documentation/filesystems/smbfs.txt`.

Modulo PAM per autenticazione mediante server SMB

Si tratta di un modulo di autenticazione che permette l'integrazione di *workstation UNIX* in reti *Windows* NT. È utilizzabile anche come metodo di autenticazione per offrire servizi Intranet a reti *Windows*.

Esiste anche un modulo che permette autenticazione attraverso un *server* SMB per il *Web server Apache*.