GNU/Linux
Amministrazione di rete mista con Samba

Michele Baldessari

Revision : 1.1
2003

Indice

1 Introduzione

1.1 Natura di Samba

Samba utilizza il protocollo SMB (Server message block) definito per reti MS-Windows e a sua volta basato sull'interfaccia di rete NetBIOS (Network basic input output system). SMB è stato progettato originariamente per reti molto piccole. Per permettere la connessione a reti più estese ed eterogenee, Microsoft ha sviluppato il sistema CIFS (Common internet file system) ancora basato su NetBIOS.

Samba può essere a tutti gli effetti considerato una versione libera e gratuita di CIFS; con esso, una macchina GNU/Linux, può accedere alle risorse condivise di un elaboratore MS-Windows ma anche mettere a disposizione proprie risorse a clienti MS-Windows o GNU/Linux.

Più in dettaglio ecco quali sono i servizi offerti da Samba:

- server per offrire la condivisione di file system e stampanti
- client per l'accesso a risorse NetBIOS su macchine Unix, MS-Windows, Novell remote
- master browser sia locale che di dominio
- server WINS (Windows internet name service)
- server per l'autenticazione di clienti di un dominio MS-Windows
- server DFS (Distributed file system).

A livello di protocolli è necessario far presente che MS-Windows può incapsulare messaggi SMB sui protocolli IPX/SPX, NetBEUI e TCP/IP mentre invece Samba può dialogare con macchine MS-Windows solo attraverso il TCP/IP. Questa non è comunque una grande limitazione vista la diffusione ormai universale di tale protocollo.

La descrizione di come NetBIOS debba operare all'interno di una rete TCP/UDP è contenuta nei documenti RFC 1001/1002. Lo standard descritto in questi documenti è noto come NBT (NetBIOS over TCP/IP) ed è alla base del funzionamento sia delle reti NetBIOS che di Samba.

1.2 Storia di Samba

Il progetto Samba nasce nel 1991 da Andrew Tridgell che scrive un programma per gestire da una macchina SUN la condivisione di file gestita da un programma chiamato Pathworks, che veniva usato per far dialogare una macchina DEC e una DOS. Nasce così una prima implementazione del protocollo SMB (Short Message Block). Il progetto

rimane sostanzialmente fermo fino al 1993 quando avviene il porting su un sistema Linux. A questo punto viene annunciato per la prima volta sotto il nome di *NETBIOS for Unix*. Nel 1994 il progetto cambia il proprio nome in *Samba*. (La leggenda narra che tale nome sia stato ottenuto tramite il comando: `grep ‘‘s*m*b’’ /usr/share/dict/words`). Sempre nello stesso anno viene fondato il newsgroup *comp.protocols.smb*, la prima homepage e mailinglist su `http://www.samba.org` e così via. Da lì in poi il progetto ha suscitato sempre maggiore interesse presso sviluppatori e aziende varie. Al giorno d'oggi *Samba* viene supportato anche commercialmente da diverse aziende come: *IBM*, *HP*, *SGI*, *Cobalt Networks* e molte altre.

1.3 Protocolli e terminologie

Diamo qui una breve descrizione dei vari protocolli e delle terminologie che stanno dietro al funzionamento di *Samba* (o più precisamente delle reti Windows-based)

1.4 NetBios

NetBIOS (che sta per Network Basic Input Output System) è un protocollo sviluppato da IBM e Sytec agli arbori della storia dei PC. Più propriamente il software, che venne appunto chiamato NetBios, era un interfaccia che veniva caricata nella memoria del DOS, per fare in modo che le applicazioni fossero in grado di comunicare con l'hardware sottostante. Questo protocollo è stato progettato fin dall'inizio per gestire reti piuttosto piccole con un numero massimo di nodi di circa 70/80 unità. Viene descritto nel *Network Technical Reference Manual* di IBM. Fornisce tre servizi:

- Name services (udp/137)
- Message services (udp/138)
- Session services (tcp/139)

NetBios di suo non fornisce la condivisione di risorse.

1.5 NETBEUI

Il protocollo *NETBEUI* (NetBios Extended User Interface) rappresenta un'estensione di NetBios per permettere ai messaggi di essere spediti su Ethernet e Token Ring. Come per *NetBios* anche in questo caso non ci sono informazioni di routing e il protocollo è progettato solo a livello di LAN di modeste dimensioni. È da notare che Samba non implementa questo protocollo, che può anche essere utilizzato per condividere file.

1.6 NBT

Il *NetBios over TCP/IP* é il meccanismo che ha sostanzialmente permesso la nascita di Samba. Nasce grazie agli RFC 1001/1002 che descrivono i meccanismi per emulare una LAN NetBios su una rete TCP/IP. Rimane tutt'ora la strada perferibile per far girare pacchetti NetBios in rete. Mentre i client Windows sono in grado di encapsulare NETBios su diversi protocolli (IPX/SPX, TCP/IP, NETBeui), Samba utilizza solo la modalità *NBT*. Rimane sconsigliato utilizzare NetBios su più protocolli contemporaneamente.

1.7 NBNS - WINS

L'rfc 1001 tra le altre cose definisce l'implementazione e l'utilizzo di *NBNS* (NetBios Name Service). In sostanza si tratta di gestire la risoluzione dei nomi NetBios in modo centralizzato per risolvere i problemi legati a più sottoreti e al traffico broadcast. Nel mondo Windows l'implementazione del NetBios Name Service viene chiamata *WINS*.

1.8 Workgroups and NT Domains

I workgroup sono nati per classificare gli utenti in gruppi logici, affinchè un amministratore di rete non debba essere obbligato a gestire i permessi per ogni singolo utente. I domini NT espandono ulteriormente questo concetto e forniscono un server centrale che gestisce l'autenticazione degli utenti.

1.9 Browsing

Il *Browsing* permette di tenere traccia dei vari servizi SMB offerti dalle varie macchine in rete. Tali liste di servizi erogati viene chiamate *Browse List* e viene gestita dal demone NBD, che vederemo più nel dettaglio successivamente.

1.10 CIFS

Il protocollo *CIFS* (Common Internet File Sharing) é sostanzialmente il protocollo per gestire

- Condivisione dei file
- Condivisione delle stampanti
- Permessi sulle condivisioni
- Permessi sui file/stampanti

- Locking sui file

Nel 1997 la specifica di tale protocollo è stato sottoposta all'IETF.

2 Concetti di Network Services

2.1 Concetti di base dei servizi di rete

In linea generale,i servizi di rete in una rete TCP/IP vengono associati ad una porta specifica (80 per HTTP, 443 HTTPS ecc.) e Samba, in quanto gestisce il protocollo NetBios su TCP/IP non è da meno. Chiaramente nulla vieta di gestire un servizio su una porta qualsivoglia, ma così facendo una rete diverrebbe sostanzialmente inutilizzabile. Il file che di norma gestisce le porte associate ad un servizio è: `/etc/services`. Il contenuto di questo file, cioè l'associazione di un protocollo ad un numero specifico di una porta viene gestito dall'Internet Assigned Numbers Authority (`http://www.iana.org/`) Un programma che gestisce un particolare servizio viene anche chiamato *Demone* (in quanto in teoria non dovrebbe morire mai ;) Generalmente ci sono due modalità in cui un demone gestisce il proprio servizio. Vediamone brevemente le caratteristiche:

2.2 Demoni standalone

Un demone si dice *standalone* quando gestisce da solo il servizio. Esiste quindi un processo che si mette in ascolto sulla porta e quando arrivano le connessioni le gestisce man mano, o creando processi figli per gestirle o gestendole direttamente o tramite altri meccanismi come i thread.

2.3 Demoni non-standalone

Un demone che è sempre attivo e in attesa di gestire i propri servizi è anche uno spreco di risorse, nel momento in cui tale servizio viene utilizzato saltuariamente. Una possibile soluzione a tale spreco di risorse sono i cosiddetti *Superdemoni* che non fanno altro che attendere le connessioni su diverse porte e nel momento in cui ne arriva una, il servizio associato viene lanciato e i dati gli vengono rigirati. Sono sostanzialmente due i *Superdemoni* più utilizzati:

- `ftp://ftp.uk.linux.org/pub/linux/Networking/base` Si trova ancora in Debian Woody, ma non viene mantenuto da diverso tempo e si preferisce utilizzare il suo "successore". (File di configurazione `/etc/inetd.conf`)
- `http://www.xinetd.org` Ormai è alla lunga il più utilizzato in quanto più flessibile rispetto a inetd e molto più ricco in quanto a funzionalità come ad esempio

(Access Control, libwrap, logging esteso, limitazione del numero e del tipo di connessioni, ecc.)

È importante sottolineare che è altamente sconsigliato lanciare Samba (in particolare il demone NMBD) tramite inetd o xinetd, in quanto devono essere mantenuti degli stati e particolari timeout, cosa che non è fattibile se non in modalità standalone.

2.4 Tcpwrapper

Citiamo brevemente anche il TCP Wrapper (`ftp://ftp.porcupine.org/pub/security/index.html`) che è un sistema per limitare e controllare gli accessi basandosi sugli indirizzi o sugli hostname di provenienza delle connessioni. Molti servizi in certe distribuzioni (xinetd su Red Hat ad esempio) vengono compilati utilizzando tale supporto. Quando attivato entrano in gioco due file di configurazione per limitare gli accessi basandosi su IP e Host ad un certo servizio: `/etc/hosts.deny` e `/etc/hosts.allow`

3 Installazione di Samba

3.1 Installazione da pacchetti binari

All'interno di queste dispense faremo riferimenti in particolare a due distribuzioni: Debian e Red Hat. La prima utilizza come sistema di gestione dei pacchetti *dpkg* ed eventualmente *apt* e si appoggia al formato .deb, mentre la seconda utilizza *RPM*. Tutto ciò che verrà detto qui si dovrebbe poter applicare senza grosse difficoltà a tutte le distribuzioni basate rispettivamente su *dpkg* e *rpm*

3.2 Componenti di Samba - Red Hat


I pacchetti che gestiscono le diverse funzionalità offerte da Samba sono i seguenti (`<x.y.z>` rappresenta il numero di versione):

- `samba-<x.y.z>.i386.rpm`
- `samba-client-<x.y.z>.i386.rpm`
- `samba-common-<x.y.z>.i386.rpm`
- `samba-swat-<x.y.z>.i386.rpm`

Vediamo brevemente i contenuti dei singoli pacchetti:

- Nel pacchetto `samba` si trovano i demoni nmbd e smbd che sono alla base del funzionamento di un server Samba e alcuni programmi di servizio come smbadduser, smbstatus
- `samba-client` contiene altri programmi di servizio come `nmblookup`, `smbclient`, `smbmount`, `smbumount`, `smbtar`, `findsmb`, `testparm`
- Nel pacchetto `samba-common` si trovano tra altri elementi il programma smbpasswd e il file di configurazione di Samba `/etc/samba/smb.conf` precompilato con alcune impostazioni predefinite.
- `samba-swat` contiene i file necessari per poter amministrare un server Samba via web

Diamo uno sguardo breve alle varie versioni di Samba incluse negli ultimi rilasci di Red Hat:

Red Hat 7.3 Samba 2.2.3a-6 - (Samba 2.2.7-3.7.3 ultimo update)

Red Hat 8.0 Samba 2.2.5-10 - (Samba 2.2.7-5.8.0 ultimo update)

Red Hat 9 Samba 2.2.7a-7.9.0 - (Samba 2.2.7a-8.9.0 ultimo update)

3.3 Componenti di Samba - Debian

- `samba` - I demoni che gestiscono il servizio vero e proprio
- `samba-common` - File in comune sia al server che al client
- `smbclient` - I client per accedere a risorse di tipo CIFS
- `swat` - Samba Web Administration Tool
- `samba-doc` - Documentazione su Samba
- `smbfs` - I comandi per montare e smontare una condivisione Samba (kernel 2.0.x o superiori).
- `libpam-smbpass` - Moduli Pam per l'autenticazione via SMB
- `libsmbclient` - Libreria condivisa utilizzata da applicazioni per accedere a server SMB
- `libsmbclient-dev` - Librerie per lo sviluppo di applicazioni che necessitano di accedere a risorse SMB
- `winbind` - Servizio per ottenere le informazioni su utenti e gruppo da un server NT/Samba

3.4 Installazione su Red Hat

Su distribuzioni Red Hat (o comunque basate su RPM) è sufficiente installare samba con il comando:

```
rpm -ivh samba-common-2.2.7a-7.9.0.i386.rpm \
         samba-2.2.7a-7.9.0.i386.rpm \
         samba-client-2.2.7a-7.9.0.i386.rpm \
         samba-swat-2.2.7a-7.9.0.i386.rpm
```

In realtà è possibile installare il tool *apt* anche su distribuzioni basate su rpm. Per maggiori informazioni si veda:

`http://www.freshrpms.net`

Una volta installato *apt* per RPM basterà semplicemente digitare:

```
apt-get install samba samba-swat samba-client
```

Così facendo, vengono scaricati i pacchetti in modo automatico e inoltre vengono scaricate e installate eventuali altre dipendenze necessarie per il corretto funzionamento del servizio.

3.5 Installazione su Debian

A differenza di Red Hat, la suddivisione in pacchetti di Samba è molto più granulare. Per cui risulta necessario specificare tutti i vari componenti che si vuole installare: Installazione tramite: `apt-get install samba samba-client swat`

Con Debian è possibile gestire una minima parte della configurazione di Samba tramite *debconf*: `dpkg-reconfigure samba`

3.6 Compilazione da sorgenti

Diamo ora uno sguardo alla compilazione di Samba dai sorgenti. Per prima cosa è necessario scaricare la versione di Samba che siamo interessati a compilare `http://www.samba.org` Una volta scaricato e scompattato l'archivio, il primo passo da eseguire è lanciare

`./configure --help` e vedere così quali sono le opzioni a disposizione per la compilazione.
Prima di procedere con la compilazione è necessario accertarsi di avere installato tutti i pacchetti di sviluppo necessari come ad esempio : `glibc-devel, readline-devel, fileutils` (Red Hat).
La lista dei pacchetti necessari cambia chiaramente a seconda delle opzioni passate al `./configure`.

Diamo un veloce sguardo a come viene compilato Samba su Red Hat e su Debian:

Red Hat 7.3 Samba 2.2.3a-6

```
./configure --libdir=/etc/samba --with-fhs
--with-privatedir=/etc/samba
--with-lockdir=/var/cache/samba
--with-swatdir=/usr/share/swat --with-utmp
--with-codepagedir=/usr/share/samba/codepages
--with-automount --with-smbmount --with-pam
--with-pam_smbpass --with-mmap --with-quotas
--without-smbwrapper --with-libsmbclient
```

Red Hat 8.0 Samba 2.2.5-10

```
./configure --libdir=/etc/samba
--with-fhs --with-privatedir=/etc/samba
--with-lockdir=/var/cache/samba
--with-swatdir=/usr/share/swat
--with-codepagedir=/usr/share/samba/codepages
--with-automount --with-smbmount --with-pam
--with-pam_smbpass --with-mmap --with-quotas
--without-smbwrapper --with-libsmbclient
--with-utmp
```

Red Hat 9 Samba 2.2.7a-7.9.0

```
./configure --libdir=/etc/samba
--with-fhs --with-privatedir=/etc/samba
--with-lockdir=/var/cache/samba
--with-swatdir=/usr/share/swat
--with-piddir=/var/run/samba --with-utmp
```

```
--with-codepagedir=/usr/share/samba/codepages
--with-automount --with-smbmount --with-pam
--with-pam_smbpass --with-mmap --with-quotas
--without-smbwrapper --with-libsmbclient
--with-acl-support --with-vfs --with-msdfs
```

Debian Woody Samba 2.2.3a

```
./configure --with-fhs --prefix=/usr \
--sysconfdir=/etc --with-privatedir=/etc/samba \
--localstatedir=/var --with-netatalk \
--with-smbmount --with-pam \
--with-syslog --with-sambabook \
--with-utmp --with-readline \
--with-pam_smbpass --with-libsmbclient \
--with-winbind --with-msdfs
```

4 Configurazione di Samba

4.1 I demoni di Samba

Un server Samba si basa su due demoni:

smbd che fornisce i servizi di condivisione di file stampanti per i clienti SMB (che possono essere macchine MS-Windows o altre macchine GNU/Linux) e si occupa della gestione delle sessioni di comunicazione e delle autenticazioni necessarie all'accesso alle risorse che vengono offerte in condivisione dal server; il demone avvia una copia di se stesso per ogni richiesta di servizio da soddisfare

nmbd che gestisce la distribuzione dell'elenco delle risorse condivise alle altre macchine della rete, può mantenere la lista delle risorse condivise (scansione della rete) ed eventualmente risolvere i nomi NetBIOS della rete (server WINS)

4.2 Attivazione di un server Samba

Entrambi i demoni smbd e nmbd possono essere attivati in modo autonomo, o gestiti dal supervisore dei servizi di rete (come Xinetd); qui viene presa in esame solo la prima alternativa che è di gran lunga la più praticata e anche quella predefinita in molte distribuzioni GNU/Linux.

In quasi tutte le distribuzioni si trovano infatti degli script preconfezionati per l'attivazione e la disattivazione di determinati servizi; nel caso della Red Hat si attivano entrambi i demoni con il comando:

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

e si disattivano con il comando:

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

ci sono poi anche i comandi:

```
/etc/rc.d/init.d/smb restart
```

e

```
/etc/rc.d/init.d/smb status
```

il cui significato dovrebbe essere ovvio.

4.3 Configurazione di un server Samba

La configurazione di un server Samba si basa su di un file di testo; nella distribuzione Red Hat (ma anche per altre) è /etc/samba/smb.conf.

Solitamente viene fornito preconfezionato e commentato, con una configurazione di base già pronta all'uso; ovviamente è possibile intervenire sul file per adattare il comportamento del server alle proprie esigenze.

Prima di esaminare la struttura del file e i parametri principali di configurazione è opportuno sottolineare alcuni importanti aspetti generali:

- È indifferente usare maiuscole o minuscole a meno che tale uso non vada a interferire con le regole del sistema operativo sottostante. Se ad esempio si indica il percorso di una directory condivisa su una macchina GNU/Linux con l'opzione (che verrà descritta più avanti) PATH=/USR/LOCAL, Samba non ha alcun problema ad accettare la direttiva ma al momento di collegarsi alla risorsa fallisce in quanto in GNU/Linux quella directory al 99 % non esiste, mentre esiste /usr/local/. è quindi consigliabile l'uso delle minuscole.
- Le righe di commento iniziano con i simboli `#` oppure `;`.
- Il carattere di continuazione riga è .
- Alcune direttive di configurazione di Samba, per ragioni di compatibilità, sono ridondanti; per questo motivo uno stesso risultato si può ottenere in modi diversi.

- Per rendere effettive le variazioni fatte al file di configurazione non è necessario riavviare i demoni di Samba in quanto il file viene riletto automaticamente ogni 60 s; se si vuole forzare la rilettura basta impartire il comando: `kill -SIGHUP <n>` dove `<n>` 'e il numero del processo corrispondente al demone smbd in funzione (per individuarlo si può eseguire `ps afx | grep smbd`). Occorre comunque notare che non tutti i cambiamenti alla configurazioni vengono necessariamente attuati subito; in particolare le variazioni della configurazione di risorse condivise rimangono congelate finch c'è qualche utente connesso a tali risorse.

Il file di configurazione è suddiviso in sezioni i cui nomi sono racchiusi tra parentesi quadrate.

Ogni sezione corrisponde a una risorsa condivisa a eccezione della sezione global usata per le configurazioni globali. Altre sezioni con un ruolo un po' particolare sono homes e printers.

Sezione [global]

In essa si impostano le informazioni che condizionano tutto il sistema ed eventualmente quei parametri che se non specificati vengono assunti in modo predefinito, ad esempio il nome del gruppo di lavoro (workgroup).

Sezione [homes]

In essa si regolano i parametri di configurazione delle directory personali degli utenti che si collegano al server Samba.

Sezione [printers]

Consente di impostare le caratteristiche della condivisione di tutte le stampanti installate nella macchina GNU/Linux senza dover definire una condivisione separata per ognuna di esse.

All'interno del file di configurazione è possibile usare alcune variabili il cui nome viene sostituito dal rispettivo valore quando il file di configurazione viene utilizzato dai demoni smbd e nmbd.

Segue una lista delle variabili più importanti con una breve descrizione:

Variabile	Descrizione
%S	nome del servizio corrente ([tmp], [homes], ecc.)
%P	directory principale del servizio corrente
%u	nome dell'utente (GNU/Linux) del servizio corrente
%g	nome del gruppo primario di %u
%U	nominativo-utente della sessione
%D	nome del dominio MS-Windows in cui il server Samba si integra
%G	nome del gruppo primario di
%H	directory personale assegnata a %u
%v	versione in uso di Samba
%h	nome del nodo che ha avviato il servizio Samba
%m	nome NetBIOS della macchina cliente
%L	nome NetBIOS assegnato al server
%M	nome Internet della macchina cliente
%N	nome della directory personale ottenuta dal servizio NIS del server
%p	percorso della directory personale ottenuto dal servizio NIS
%d	numero identificativo del processo corrente
%a	architettura software della macchina remota (Samba, MS-Windows 95/98/Me/NT), diversamente sarà assegnata la parola UNKNOWN
%I	indirizzo IP della macchina cliente
%T	data e ora corrente.

4.4 smb.conf: sezione global

È la sezione che appare in tutte le configurazioni di Samba, anche se non è obbligatoria. Le opzioni in essa contenute vengono applicate a tutte le altre sezioni.

Viene mostrato un esempio comprendente alcune direttive di uso comune suddivise in blocchi in base alla funzione svolta e intervallate da brevi descrizioni del loro significato:

```
[global]
;
; identificazione del server
;
    workgroup = INF
    netbios name = pippo
    server string = Samba Server
```

La voce più importante è workgroup che assegna a Samba il dominio o il gruppo di appartenenza. Occorre assegnarla correttamente, pena conflitti nella rete paritetica (peer-to-peer).

La voce netbios name è di utilizzo meno frequente e serve ad assegnare al server Samba un nome NetBIOS a piacere. Il nome NetBIOS viene infatti assegnato in modo definito pari a quello ottenuto dal DNS. Ad esempio se il nome DNS del server fosse muscolis.inf.besta il nome NetBIOS sarebbe muscolis. Uno dei casi in cui è utile poter impostare un nome NetBIOS diverso da quello predefinito è quello in cui la rete è suddivisa in due o più domini DNS diversi; in questo caso potrebbe infatti anche esistere una macchina con nome muscolis.mat.besta che verrebbe quindi ad avere lo stesso nome NetBIOS. Ovviamente il valore di netbios name deve essere assegnato seguendo le regole dei nomi NetBIOS (unica stringa senza punti contenente i simboli alfabetici maiuscoli e minuscoli le cifre e i simboli !, @, ;, $, %, ˛ &, (,), -, é ˜).

Con server string si assegna semplicemente la descrizione dell'elaboratore server.

```
;
; opzioni di rete
;
    hosts allow = 192.168.1. localhost
    hosts deny  = 172.16.244.254
    interfaces  = 192.168.1.1/24 172.16.244.1/16
    bind interfaces only = yes
```

Le direttive Host allow e host deny servono rispettivamente a specificare quali nodi possono e non possono accedere alle risorse condivise dal server Samba. L'indicazione può essere fatta tramite il nome del nodo, il nome di dominio, il numero IP, il numero della sottorete. Nell'esempio viene concesso l'accesso a tutte le macchine della sottorete 192.168.1.* e al localhost (è opportuno che l'accesso a localhost sia sempre concesso pena possibili malfunzionamenti della scansione delle risorse del server) e viene negato alla macchina con indirizzo 192.168.1.3. Possono anche essere usate le parole chiave ALL, per designare qualsiasi elaboratore, e EXCEPT per indicare un'eccezione a una regola (ad esempio host allow 192.168.1. EXCEPT 192.168.1.3). Si deve inoltre notare che in caso di assenza delle direttive host allow e host deny, l'accesso è concesso a tutti in modo predefinito. Infine si tenga presente che tali direttive possono essere inserite anche in specifiche condivisioni ma con grado di priorità inferiore rispetto a quanto specificato nella sezione global.

La direttiva interfaces è utile in caso il server Samba risieda in più di una sottorete. Se sull'elaboratore sono presenti più interfacce di rete, in modo predefinito, Samba si mette in ascolto di richieste provenienti dagli indirizzi di rete corrispondenti alla rete della prima interfaccia che trova (di solito eth0). Per fare in modo che invece risponda alle richieste provenienti da più sottoreti si deve impostare questa opzione. Nell'esempio Samba si pone in ascolto dalle sottoreti 192.168.1.* e 172.16.*.* (si può usare anche una notazione con maschera di rete: 192.168.1.1/255.255.255.0 172.16.244.1/ 255.255.0.0).

Ponendo bind interfaces only = yes (l'alternativa è ovviamente no oppure si può evitare di inserire questa opzione), si forza il server a rispondere soltanto alle sottoreti

corrispondenti alle interfacce indicate in interfaces. In tal caso si deve inserire tra le interfacce anche 127.0.0.1 per permettere al programma smbpasswd di potersi collegare al localhost e funzionare correttamente.

```
;
; opzioni per la stampa
;
    printing = bsd
    printcap name = /etc/printcap
    load printers = yes
```

La direttiva printing permette di specificare il sistema di stampa in uso nel server; per i sistemi GNU/Linux il valore da indicare è di solito bsd, l'alternativa più diffusa è sysv.

Le altre due opzioni permettono di caricare automaticamente tutte le stampanti configurate nel sistema senza descriverle singolarmente, indicando a tale scopo il percorso del file printcap contenente la definizione di tali stampanti. La loro configurazione relativamente a Samba viene poi indicata nell'apposita sezione printers descritta più avanti.

```
;
; opzioni per il log
;
    log file = /var/log/samba/%m.log
    max log size = 100
    log level = 3
```

La direttiva log file permette di indicare il file delle registrazioni per gli eventi Samba; tale file può essere unico oppure, come nell'esempio, diverso per ogni cliente che si collega al server (il nome del file sarà `<nome\_host>.log`). Altra possibilità è quella di avere un file di registrazioni per ogni utente usando opportunamente la variabile %U o %u.

Con max log size si specifica la grandezza in kibibyte del file delle registrazioni, raggiunta la quale il file stesso viene rinominato con estensione .old e reinizializzato; il file .old eventualmente già esistente viene cancellato. Il valore predefinito di questo parametro è 5 000; il valore zero significa nessun limite di ampiezza (scelta non consigliabile per evitare una crescita abnorme del file o dei file delle registrazioni).

La direttiva log level indica il livello di dettaglio dei messaggi annotati nel registro; il valore predefinito è zero e corrisponde a nessun messaggio. Aumentando questo valore si hanno messaggi sempre più dettagliati; è comunque sconsigliabile un livello superiore a 3.

```
;
; opzioni per l'accesso alle condivisioni
;
    encrypt password = yes
    null password = yes
    guest account = utentesmb
    security = share
; in alternativa
;  security = user
;  security = server
;  security = domain
; altri parametri nel caso di security = user
;  smb passwd file = /etc/samba/smbpasswd
;  username map = /etc/samba/smbusers
; altri parametri nel caso di security = server o domain
;  password server = SERVER_NT
```

La direttiva encrypt password = yes è praticamente obbligatoria se il server Samba deve convivere con macchine equipaggiate con sistemi operativi MS-Windows 98/NT o più recenti che usano le parole d'ordine cifrate.

La direttiva null password = yes permette di avere utenti Samba con parola d'ordine nulla (il valore predefinito è no.)

La direttiva guest account indica il nome di un utente generico al quale può essere consentito l'accesso alle condivisioni (da usare nel caso di security = share, come dettagliato più avanti). Tale utente deve essere definito nel sistema GNU/Linux senza directory personale e senza shell, aggiungendo al file /etc/passwd la riga:

```
utentesmb::499:499:utente generico samba:/dev/null:/dev/null.
```

Il valore predefinito è nobody.

Il parametro security è di importanza fondamentale e richiede una trattazione leggermente più ampia.

4.5 Livello di sicurezza share

Con l'impostazione security = share si ha il controllo di accesso a livello di condivisione: il cliente che vuole accedere a una risorsa invia ogni volta una parola d'ordine e nessun nominativo-utente. Samba tenta di dedurre il nominativo-utente dalla direttiva valid users eventualmente inserita nella sezione di condivisione di quella risorsa (come illustrato in seguito), oppure dal nome dell'elaboratore cliente, o, in caso di insuccesso,

da quanto indicato con il parametro guest account (questo solo se fra i parametri di condivisione è indicato guest ok = yes e guest only = yes).

Questo livello di sicurezza si usa, soprattutto nel caso di utenti MS-Windows e GNU/Linux non coincidenti, per condividere porzioni di file system quando si ha interesse a far s che tutti gli utenti abbiano gli stessi diritti sui file condivisi (con l'impostazione `guest account = utentesmb` il proprietario delle risorse condivise sarà sempre l'utente GNU/Linux `utentesmb` qualunque sia il nominativo dell'utente MS-Windows che si connette).

4.6 Livello di sicurezza user

Con l'impostazione security = user, che è quella predefinita, si ha il controllo di accesso a livello di utente: il cliente che vuole accedere a una risorsa invia al momento della connessione una coppia utente-parola d'ordine in base alla quale avviene l'autenticazione da parte del server. Se la connessione viene accettata il cliente può accedere a tutte le risorse condivise senza doversi autenticare nuovamente a ogni accesso.

Il controllo delle utenze viene effettuato dal server Samba in base al contenuto del file dei suoi utenti che solitamente è /etc/samba/smbpasswd (si può cambiare il nome del file o il percorso tramite il parametro smb passwd file =).

Gli utenti Samba vengono aggiunti con il comando smbpasswd illustrato in un paragrafo successivo.

È di fondamentale importanza notare che comunque il nome utente Samba deve coincidere con il nome di un utente definito nel sistema GNU/Linux, in quanto quest'ultimo deve essere sempre in grado di assegnare un proprietario valido agli eventuali file creati o copiati dall'utente conneso all'interno della risorsa condivisa.

Questa esigenza può costituire un problema, ad esempio per la limitazione a otto caratteri dei nominativi-utente di GNU/Linux, che viene in parte superato grazie all'uso di un file di corrispondenza tra utenti GNU/Linux e utenti MS-Windows, il cui nome è indicato con la direttiva username map =. Un valore abbastanza comune di tale parametro è /etc/samba/smbusers. Tale file conterrà delle righe cos formate:

```
nome_linux = <nome_smb_1> <nome_smb_2>...
```

Per ovvi motivi di sicurezza, entrambi i file smbusers e smbpasswd, devono essere accessibili sia in scrittura che in lettura dal solo utente root.

4.7 Livello di sicurezza server

Con l'impostazione `security = server` si ha lo stesso controllo di accesso visto nel caso di user con la differenza che l'utenza viene controllata su un server esterno (solitamente un PDC MS-Windows) il cui nome (NetBIOS) viene indicato con la direttiva `password server =`

4.8 Livello di sicurezza domain

Con l'impostazione `security = domain` si ha ancora lo stesso controllo di accesso visto nel caso di user, ma questa volta il server Samba va a inserirsi in un dominio MS-Windows NT/2000.

Per ottenere questo risultato occorre fermare i demoni di Samba, quindi aggiungere il server Samba al dominio NT sul PDC usando il server manager di MS-Windows NT oppure a una active directory sul server MS-Windows 2000 con la MMC (Microsoft management console) attraverso lo strumento Utenti e computer di Active Directory. A questo punto si deve eseguire il comando:

```
smbpasswd -j <nome_dominio> -r <nome_server> -U<nome_utente>%<parola_d'ordine>
```

Il `<nomedominio>` deve essere lo stesso indicato nella direttiva workgroup di smb.conf; il `<nomeserver>` deve coincidere con il valore di password server. `<nomeutente>` e relativa `<parolad'ordine>` devono rappresentare un'utenza con privilegi sufficienti ad aggiungere un'utenza nuova nella macchina MS-Windows NT/2000.

Ultimate queste operazioni occorre naturalmente riavviare il servizio Samba.

Il vantaggio principale dell'impostazione domain rispetto a quella server consiste nel fatto che il PDC risulta meno carico, in quanto non è più necessaria una connessione di rete permanente tra esso e il server Samba. Quest'ultimo infatti effettua una chiamata RPC (Remote procedure call) solo al momento dell'autenticazione e non necessita di essere costantemente connesso al PDC come avviene nel caso del livello di sicurezza server.

Per concludere occorre notare che comunque anche con questo tipo di impostazione (come pure per quella server) è necessario tenere allineati gli elenchi degli utenti dal lato MS-Windows e dal lato GNU/Linux (il motivo è stato illustrato nel paragrafo del livello user). Ci sono però due direttive della sezione global che permettono di automatizzare l'aggiornamento degli utenti GNU/Linux:

```
add user = <script1> %u
delete user = <script2> %u
```

La prima entra in azione quando, a seguito di una connessione di un cliente MS-Windows, Samba si rivolge al server di dominio per l'autenticazione con esito positivo ma l'utente GNU/Linux corrispondente non esiste; ovviamente lo script `<script1>` deve essere scritto in modo adeguato affinch crei l'utente ricevendolo come parametro dalla variabile %u.

In modo speculare si usa l'altra direttiva che entra in azione quando, a seguito di una connessione di un cliente MS-Windows, Samba si rivolge al server di dominio per l'autenticazione con esito negativo ma il corrispondente utente GNU/Linux esiste; in questo caso `<script2>` deve provvedere a cancellare l'utente in questione.

4.9 smb.conf: sezioni generiche di condivisione

Una sezione indicante una risorsa condivisa può avere un nome a piacere purch sempre racchiuso tra parentesi quadrate.

Vengono adesso illustrati alcuni esempi allo scopo di descrivere almeno le direttive più importanti:

```
;
; condivisione 1: una directory accessibile solo a certi utenti
;
[Pagine WWW]
   comment = Dir per le pagine web
   browseable = yes
   public = no
   path = /var/www
   writable = yes
   valid users = utente1 utente2
```

La direttiva comment serve ad associare una descrizione alla risorsa condivisa.

L'opzione browseable permette di rendere visibile o no la risorsa agli utenti che si connettono al server.

public è un sinonimo di guest ok; in questo esempio non si vuole che la risorsa sia accessibile per l'utente generico.

path permette di indicare il percorso della risorsa sul sistema GNU/Linux.

writable serve a concedere o negare l'accesso in scrittura (un sinonimo è writeable.

valid users indica quali sono gli utenti che possono accedere alla risorsa. è anche possibile indicare gruppi di utenti GNU/Linux con la sintassi + `<nomegruppo>` e gruppi di utenti NIS (ovviamente deve essere presente in rete un server NIS) con la sintassi `&<nomegruppo>` e anche entrambi con la sintassi `+&<nomegruppo>` o `&+<nomegruppo>`, o ancora `@<nomegruppo>`.

```
;
; condivisione 2: una directory pubblica = accessibile a tutti
;
[public]
   comment = Dir pubblica
   browseable = yes
   guest ok = yes
   path = /usr/local/public
   writable = yes
```

```
;
; condivisione 3: una directory pubblica = accessibile a tutti in cui tutti
; gli utenti possano creare, modificare, cancellare tutti i file
;
[temp]
   comment = Dir pubblica plus
   browseable = yes
   guest ok = yes
   guest only = yes
   path = /tmp
   writable = yes
```

La differenza tra le due condivisioni è molto sottile ma anche interessante. La presenza di guest ok = yes permette le connessioni anonime; eventuali file creati o copiati nella directory sarebbero di proprietà dell'utente indicato in guest account in caso di accesso anonimo, oppure dell'utente effettivo in caso esso fosse registrato in GNU/Linux. Se è presente anche guest only = yes invece il proprietario è sempre l'utente fittizio ospite anche nel caso l'utente collegato fosse riconosciuto regolarmente da GNU/Linux; in questo caso quindi tutti gli utenti possono fare tutte le operazioni con qualsiasi file presente nella directory condivisa.

Un modo alternativo per ottenere lo stesso risultato è quello di usare la direttiva force `user = <nomeutente>`; in questo modo Samba assegna lo stesso nominativo-utente a chiunque si connetta alla risorsa.

```
;
; condivisione 4: un cd-rom
;
[cd]
   comment = CD-ROM
   preexec = mount /mnt/cdrom
   postexec = umount /mnt/cdrom
   browseable = yes
   public = yes
   path = /mnt/cdrom
   writable = no
```

Il significato delle impostazioni è ovvio compreso quello delle due opzioni preexec e postexec. In caso si tema che possano connettersi utenti sprovvisti dei privilegi per montare e smontare il CD, si possono sostituire le due direttive rispettivamente con root preexec e root postexec che svolgono lo stesso compito ma con i privilegi dell'utente root.

```
;
; condivisione 5: una directory privata con permessi preimpostati
;
[privata]
   comment = Dir privata
   browseable = yes
   path = /usr/local/private
   writable = no
   public = no
   write list = pippo pluto
   create mask = 0644
   directory mask = 0644
```

In questo esempio nella directory non sarebbe possibile scrivere, ma la presenza della direttiva write list permette di impostare permessi di scrittura, per gli utenti indicati, indipendentemente da quanto specificato negli altri parametri. Si deve però notare che i permessi impostati a livello di sistema su quella risorsa hanno sempre il sopravvento su quanto specificato nel file di configurazione di Samba (in altre parole, se /usr/local/private è di proprietà dell'utente root e i permessi sono impostati a (600), gli altri utenti non possono n leggere n scrivere alcunch in quella directory condivisa).

Le ultime due direttive, infine, servono a indicare i permessi con cui verranno creati file e directory all'interno della risorsa condivisa; il valore predefinito è (0755)

Altre direttive importanti sono:

```
admin users = tizio
follow symlinks = no
```

Con la prima si indica che l'utente tizio ha gli stessi privilegi dell'utente root sulla condivisione e quindi non risente di eventuali limitazioni dovute ai permessi sui file; con la seconda si impedisce che vengano seguiti i collegamenti simbolici evitando che chi accede alla condivisione possa accedere anche a file che si trovano all'esterno di questa.

4.10 smb.conf: sezione [homes]

La sezione homes viene utilizzata affinch ogni utente possa avere accesso a una propria directory personale sul server Samba che potrà anche coincidere con la directory personale GNU/Linux di quell'utente. Un esempio di definizione può essere il seguente:

```
;
; directory personali degli utenti
;
```

```
[homes]
    comment = directory home
    browseable = no
    writable = yes
    path = usr/local/samba/%S
```

Qui è importante l'impostazione che impedisce la scansione della risorsa in modo che essa non appaia con il nome homes a tutti gli utenti.

La presenza di path serve a fare in modo che questa directory non coincida con quella GNU/Linux dell'utente (cosa che sarebbe l'impostazione predefinita).

La logica di funzionamento è la seguente: quando l'utente si connette, se l'utenza è accettata, viene creata dal server Samba una condivisione con le caratteristiche specificate nella sezione homes ma con un nome uguale a quello dell'utente connesso.

4.11 smb.conf: sezione [printers]

Con questa sezione si impostano i parametri di configurazione di tutte le stampanti definite nel sistema GNU/Linux a patto che nella sezione global siano state inserite le direttive seguenti:

```
load printers = yes
printcap name = /etc/printcap
```

L'alternativa, che consiste nel definire le varie stampanti come singole risorse condivise, non viene presa in esame in questa sede.

Un esempio di configurazione per le stampanti è il seguente:

```
;
; Stampanti
;
[printers]
   comment = stampanti
   path = /var/spool/samba
   browseable = no
   printable = yes
   public = yes
   writable = no
```

Qui occorre notare che il parametro path serve a impostare una directory per la coda di stampa, diversa da /tmp/ che è quella predefinita.

Altra direttiva da segnalare è printable con la quale si attiva la coda di stampa.

5 Samba dal lato client

Da una macchina GNU/Linux è possibile connettersi a un server Samba o a macchine MS-Windows per accedere alle risorse che queste condividono grazie a una serie di strumenti che costituiscono il lato cliente di Samba.

5.1 smbclient

Il primo programma da esaminare è smbclient che si usa fondamentalmente in due maniere:

```
smbclient -L <nome_server_samba>
```

per avere la lista delle risorse condivise dal server; oppure:

```
smbclient <nome_servizio> [-U <nominativo_utente>]
```

per connettersi alla risorsa `<nomeservizio>` (ad esempio //serversamba/public). Se la connessione ha successo si ha a disposizione un'interfaccia testuale del tutto simile a quella del programma ftp tradizionale, dove si possono eseguire più o meno gli stessi comandi (get, put, cd, pwd, ecc.).

Un'opzione importante è -I seguita da un numero IP, con la quale si può appunto indicare il numero IP del server a cui ci si vuole connettere.

5.2 smbmount

Sicuramente l'interfaccia messa a disposizione da smbclient non è il massimo della comodità; sarebbe molto meglio poter disporre della risorsa condivisa da un'altra macchina come se fosse una risorsa locale. Anche questo si può ottenere con Samba, in particolare grazie a smbmount.

La sintassi è:

```
smbmount <nome_servizio> <punto_di_innesto> [-o <opzioni>]
```

Ad esempio:

```
smbmount //serversamba/public /mnt/dirsamba -o username=tizio\%<parola_d'ordine>
```

Per smontare la risorsa si può usare il comando:

```
smbumount <mountpoint>
```

È anche possibile ottenere l'inserimento automatico della risorsa all'avvio di GNU/Linux con la riga seguente nel file /etc/fstab:

```
//serversamba/public    /mnt/dirsamba    smbfs    username=tizio%<parola_d'ordine>
```

> È importante ribadire che in questa sede non viene illustrata la sintassi completa dei vari comandi con l'elenco di tutte le opzioni possibili. Per avere queste informazioni si deve consultare la documentazione dei vari pacchetti e il manuale in linea (per esempio smbpasswd(8)).

5.3 Altri comandi utili

Altri comandi presenti nel pacchetto samba-client sono:

`nmblookup` che permette di trovare il numero IP di una macchina fornendo il nome NetBIOS

`findsmb` che fornisce informazioni sui serventi Samba presenti in rete

`smbtar` che permette di effettuare copie di sicurezza di risorse SMB su unità a nastro installate sul server GNU/Linux.

Per i dettagli di uso di questi comandi si rimanda ai rispettivi manuali in linea.

6 Stampa

Il codice contenuto in Samba per gestire tutto il sottosistema di stampa è sicuramente tra i più complessi. Questo perché esistono, a seconda delle varie versioni di Windows, almeno tre modalità diverse di gestione della stampa. Basti ricordare che in NT4 i driver di stampa girano in "kernel space" e che quindi un crash del driver di stampa porta a un crash del sistema intero (BSOD).
A partire dalla versione 2.2.0 di Samba il supporto per la stampa è piuttosto completo e sono state aggiunte le seguenti funzionalità:

- Supporto per fare il download dei driver di stampa su client Windows 95/98/NT/2000
- Supporto dell'upload dei driver di stampa tramite l'NT Add Printer Wizard (NPW) o tramite Imprints (`http://imprints.sourceforge.net`)
- Supporto per ACL sulle stampanti

6.1 Uso con Samba di stampanti MS-Windows

Per usare su una macchina GNU/Linux una stampante condivisa da una macchina MS-Windows, occorre impostare in modo opportuno il file di definizione delle stampanti GNU/Linux: `/etc/printcap`.

Ecco un esempio di righe di configurazione da aggiungere a tale scopo:

```
stsamba:\
  :mx=0:\
  :sh:\
  :sd=/var/spool/lpd/stsamba:\
  :lp=/dev/null:\
  :af=/var/spool/lpd/stsamba/acct:\
  :if=/usr/bin/smbprint:
```

Una breve spiegazione sul significato di queste righe è necessaria, anche se lo studio del file di configurazione delle stampanti in GNU/Linux esula dallo scopo di questo documento:

- mx=0 indica nessun limite di grandezza dei file da stampare
- sd= indica la directory della coda per questa stampante
- lp=/dev/null indica che la stampante non è collegata ad alcuna porta (non è locale)
- af= indica il nome del file per registrare le transazioni
- if= indica il nome del filtro da usare per la stampa; quello usato nell'esempio è un filtro fornito in modo predefinito con la distribuzione Red Hat all'interno del pacchetto samba-client.

Affinchè il tutto funzioni è poi necessaria la presenza del file .config nella directory della coda indicata con la riga sd=. Un esempio del suo contenuto è il seguente:

```
share="//<server_smb>/<nome_stampante_condivisa>"
user="tizio"
password="blablabla"
```

Data la complessità della configurazione manuale di una stampante SMB in GNU/Linux (e anche di una stampante in generale), può essere consigliabile l'uso di strumenti appositi come printconf-gui che semplificano molto queste operazioni.

6.2 Samba e LPRng

Vediamo in questa sezione come configurare Samba per gestire le code di stampa quando il demone di stampa è LPRng. LPRng è sicuramente meno innovativo rispetto a CUPS, ma ha tutt'ora un numero di installazioni piuttosto considerevole; basti pensare che Red Hat installa CUPS di default solamente dalla versione 9.

Vediamo brevemente un esempio della sezione `[printers]` nel file di configurazione di Samba:

```
[printers]
    path = /var/spool/lpd/samba
    print ok = yes
    printing = lprng
    load printers = yes
    guest ok = no
    printcap name = /etc/printcap
    print command =      /usr/bin/lpr  -P%p -r %s
    lpq command   =      /usr/bin/lpq  -P%p
    lprm command  =      /usr/bin/lprm -P%p %j
    lppause command =    /usr/sbin/lpc hold %p %j
    lpresume command =   /usr/sbin/lpc release %p %j
    queuepause command = /usr/sbin/lpc  stop %p
    queueresume command = /usr/sbin/lpc start %p
```

La directory specificata con la voce `path` andrà a contenere una copia dei file che devono andare in stampa e nel caso di operazioni di stampa fallite rimarranno nella directory. È quindi opportuno effettuare la rimozione dei file più vecchi di un certo numero di giorni. Ad esempio è possibile aggiungere in `/etc/cron.daily` uno script di questo tipo:

```
find /var/spool/lpd/samba -type f -mtime 2d -exec rm -f {} \;
```

La voce più importante nel file di configurazione di Samba è quella che setta il backend di stampa a LPRng e cioè: `printing = lprng`. Quest'opzione consente a Samba di interpretare l'output del comando `lpq` in modo corretto.

La sezione `[printers]` è una share particolare che permette di esportare in un unico passaggio tutte le stampanti definite nel file `/etc/printcap`.

6.3 Samba e CUPS

Il demone di stampa CUPS (`http://www.cups.org`) è il sistema di stampa che recentemente ha riscosso una diffusione imponente (con Red Hat 9, CUPS è diventato il demone di stampa di default.

Una delle feature di rilievo di CUPS è senz'altro il supporto al protocollo IPP (Internet Printing Protocol), che si sta delineando come il protocollo di stampa del futuro (Windows 2000 con le IPP ISAPI DLL è in grado di comunicare nativamente con un server o con una stampante che supporti IPP).

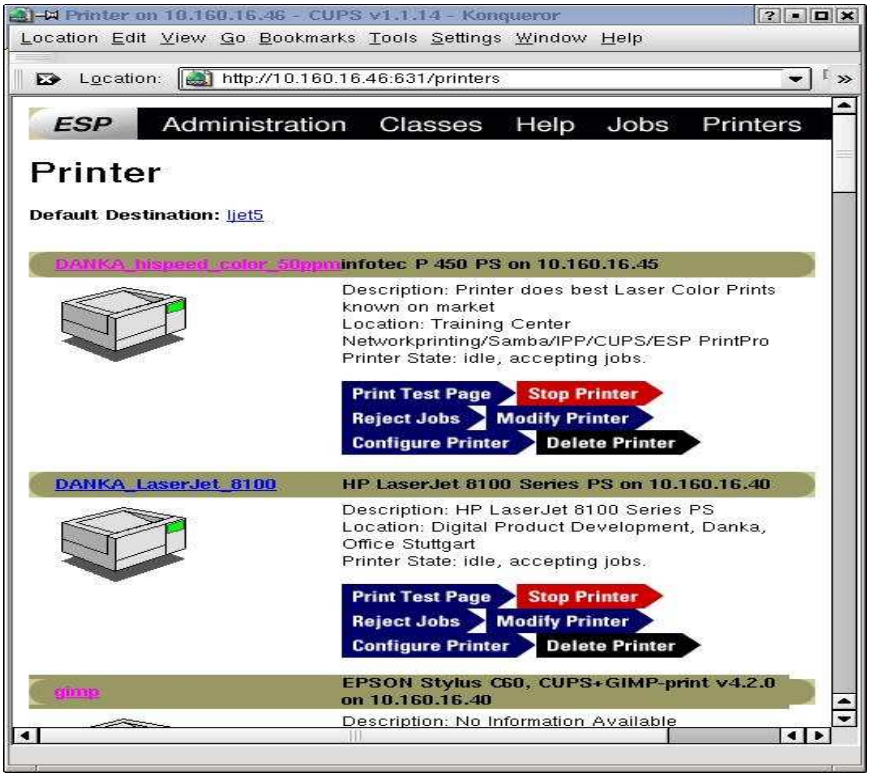
Se il demone SMB è stato compilato con le librerie cups presenti nel sistema (lo si verifica con `ldd 'which smbd\`), verranno utilizzate le API di CUPS per ottenere le informazioni sulle stampanti, per inviare un job in coda e così via, altrimenti vengono utilizzati i soliti comandi System V, come per LPRng.

Il settaggio:

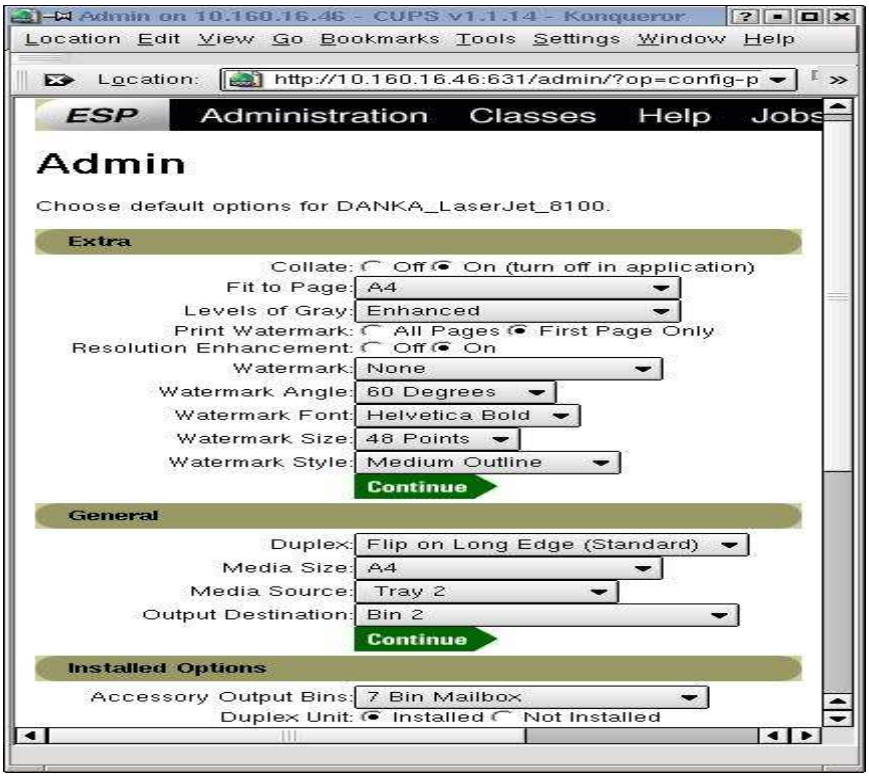
```
printing = CUPS
printcap = CUPS
```

è quello che attiva l'utilizzo dell supporto CUPS da parte di Samba.

La configurazione del demone CUPS è piuttosto intuitiva in quanto sono presenti diversi tool grafici. CUPS, di suo, viene fornito con un'interfaccia di gestione via web (`http://localhost:631`) piuttosto completa:



Vediamo qui la gestione della singola stampante:



7 Samba e i FAX

Diamo uno sguardo brevemente come configurare Samba per poter creare una stampante virtuale che prende dei documenti in coda e li spedisce via FAX ad un numero contenuto all'interno del documento. È necessario innanzitutto installare Hylafax (`http://www.hylafax.org`) e configurarlo in modo appropriato per il proprio dispositivo di Fax. Gli script di riferimento per spedire i fax si trovano a:

`http://www.purpel3.com/sambafax`

7.1 LPRng

La procedure per configurare l'invio dei Fax usando LPRng come backend di stampa è la seguente :

1. Vanno aggiunte in `/etc/printcap` le seguenti righe:

```
### /etc/printcap
### salsafax printer
...

SalsaFax:\
  :lp=/dev/null:\
  :sd=/usr/spool/lpd:\
  :if=/var/spool/fax/bin/salsafax.pl:\
  :sh:ff_separator:bkf:mx#0:

...
```

2. Lo script `salsafax` va decompresso e poi messo in `/var/spool/fax/bin/` o comunque nella directory degli eseguibili di Hylafax

3. Vanno verificati all'inizio dello script alcuni settaggi, tra i quali alcuni Path.

4. Il file di configurazione di Samba dovrà avere un sezione di stampa simile a questa:

```
; /etc/samba/smb.conf
...
 [printers]
        comment = All Printers
        path = /var/spool/lpd/lp
        browseable = no
        printable = yes
        public = yes
        writable = no
        create mode = 0700
        directory = /tmp
...
```

5. Va riavviato sia Samba che il demone di stampa lpd

6. Va testato il funzionamento dello script (come utente root):

```
echo foo | ./salsafax.pl
```

   In questo modo si potrà verificare che tutti i moduli Perl necessari allo script siano installati correttamente. (Getopt-Long e Mail-Sendmail)

7. A questo punto la stampante virtuale è in grado inviare Fax

7.2 CUPS

Come per LPRng si assume che Hylafax sia stato installato correttamente e che l'utility `sendfax` stia funzionando in modo corretto.

1. Lo script `salsafax` va decompresso e messo in `/usr/lib/cups/backend` o comunque nella directory dei backend di CUPS.

2. La directory e i settaggi all'inizio di questo script vanno verificate

3. Si aggiunge una nuova stampante con il seguente comando:

   ```
   lpadmin -p SalsaFax -E -v salsafax.pl
   ```

4. Si assume che Samba mostri tutte le stampanti, altrimenti sarà necessario configurare `smb.conf` in modo appropriato. Ad esempio:

   ```
   ;;/etc/smb.conf (or etc/samba/smb.conf)
   ...
   [global]
   printcap name = lpstat
   printing = cups
   use client driver = Yes
   print command = lp -d%p -oraw %s; rm %s
   lpq command = lpstat -o%p
   lprm command = cancel %p-%j
   queuepause command = disable %p
   queueresume command = enable %p
   printer admin = yourloginname

   [printers]
   path = /tmp
   printable = Yes
   browseable = No
   show add printer wizard = yes

   ...
   ```

5. Dopo aver riavviato Samba, si verifichi il funzionamento dello script:

   ```
   echo foo | ./salsafax.pl
   ```

In questo modo si potrà verificare che tutti i moduli Perl necessari allo script siano installati correttamente. (Getopt-Long e Mail-Sendmail)

6. A questo punto la stampante virtuale è in grado inviare Fax

7.3 Utilizzo

Dal punto di vista del client è necessario installare un driver postscript (come ad esempio un Apple Laserwriter 12/640 PS) che punti alla stampante virtuale configurata come Fax sul server :

```
\\SERVER-SAMBA\StampanteFax
```

Si crea un documento che contenga una riga (in qualsiasi punto del documento) con la seguente sintassi :

```
Fax-Nr : 012-345-6789
```

Se il faxserver non è in grado di spedire il fax si riceverà comunque una notifica della spedizione non riuscita.

Esiste anche la possibilità di inviare lo stesso Fax a più numeri. Per fare ciò è necessario attivare il supporto Multifax in `salsafax` cambiando la riga:

```
my $ALLOWMULTIFAX = 0;
```

in

```
my $ALLOWMULTIFAX = 0;
```

Per inviare il Fax a più numeri basterà semplicemente separare i numeri nella riga `Fax-Nrs` (non `Fax-Nr`) con un `;` :

```
Fax-Nrs : 12345678; 123456433; 1298376132; 129387612; 2873692817
```

8 Domain Logons

È la direttiva che permette di configurare Samba come PDC in quanto lo imposta come server di autenticazione di dominio.

8.1 Logon script

Samba consente l'esecuzione degli script di accesso di MS-Windows (.BAT o .CMD). Tali script vengono eseguiti sul cliente al momento della connessione di un utente al dominio ma sono memorizzati sul server e vengono quindi trasferiti attraverso la rete. Ovviamente sono molto utili per impostare dinamicamente le configurazioni di rete per gli utenti quando si connettono.

L'opzione logon script permette appunto di indicare il nome dello script da eseguire quando l'utente si collega; come si vede dall'esempio può essere uno script unico, valido per tutti, oppure dipendente dal cliente o dal nome utente.

Sul server GNU/Linux questi script vengono memorizzati nella directory indicata nella condivisione netlogon, che viene descritta più avanti.

Una cosa importante da ricordare è che gli script di accesso vengono eseguiti in ambiente MS-Windows e devono essere quindi scritti con righe terminanti con i caratteri di `<CR>` e `<LF>`, invece del solo `<LF>` di un sistema GNU/Linux.

L'esempio seguente di script di accesso, definisce un disco di rete W: su una condivisione di Samba:

```
echo Connette disco di rete
net use w: \\ServerSamba\dati
```

8.2 Logon path

In MS-Windows 95/98 ciascun utente può avere il proprio profilo comprendente informazioni sull'aspetto della scrivania grafica, sulle applicazioni che appaiono nel menù Start, sullo sfondo e altre ancora. Tale profilo può essere memorizzato direttamente su un elaboratore cliente e si chiama allora profilo locale, oppure sul server e si chiama profilo di roaming, in quanto l'utente ha a disposizione sempre lo stesso ambiente anche spostandosi da un cliente all'altro.

La direttiva logon path viene usata per indicare dove vengono memorizzati i profili dei vari utenti.

8.3 Logon home e logon drive

Con logon home si indica la posizione della directory personale di un utente, che può essere diversa da quella indicata nella sezione homes.

Con logon drive, da usare solo in caso di clienti MS-Windows NT, si indica la lettera del disco su un client in cui vengono abbinate le directory personali indicate con logon home.

8.4 Sezione [netlogon]

In questa sezione viene configurata una condivisione speciale che serve a contenere gli script di accesso. La configurazione scelta nell'esempio (sola lettura, pubblica, non visibile alla scansione delle risorse) è dettata dal ruolo particolare che svolge.

8.5 Definizione delle utenze per macchina

Nel caso nella rete siano presenti dei clienti MS-Windows NT, per essi devono essere creati sul PDC i cosiddetti machine account in aggiunta alle utenze normali. Ovviamente, tali utenze speciali devono essere inserite sia come utenti Samba che come utenti del sistema GNU/Linux che ospita il server. Tale operazione può essere fatta in modo automatico (direttiva add user illustrata in precedenza) oppure manualmente, con i seguenti comandi:

```
/usr/sbin/useradd -d /dev/null -g 100 -c"<descrizione_dell'elaboratore_client>"
  -s /bin/false <nome_elaboratore>
passwd -l <nome_elaboratore>
smbpasswd -a -m <nome_elaboratore>
```

È necessario prestare attenzione al carattere $ alla fine del nome della macchina nel primo e nel secondo comando. Il secondo comando permette di bloccare la parola d'ordine di quell'utente fittizio. Con il terzo comando si definisce l'utente `<nomeelaboratore>` per Samba grazie all'opzione -m.

9 Servizi di Naming

9.1 DNS - Concetti di base

Domain Name Service è il sistema che gestisce la risoluzione dei nomi in Internet. È un servizio assolutamente cruciale per il corretto funzionamento della rete. In linea generale avvengono dei ritardi piuttosto consistenti nel momento in cui la risoluzione IP non è funzionante.
Ad esempio diversi servizi come telnet, ssh ecc. subiscono dei delay iniziali molto elevati quando la risoluzione inversa dei nomi (da IP a Nome) non è funzionante. La posta elettronica in particolare non è nemmeno in grado di funzionare correttamente quando la risoluzione dei nomi non è funzionante.
Vediamo qui brevemente i concetti di base che stanno dietro al corretto funzionamento del DNS:

- `Forward lookup`: risolve un nome (foo.bar.org) in un indirizzo IP. La configurazione di base della risoluzione dal punto di vista client avviene nei file `/etc/resolv.conf`, `/etc/host.conf` e `/etc/hosts`.

- `Reverse Lookup`: risolve un indirizzo IP in un nome di dominio. Ll'iter di questa risoluzione viene specificato negli stessi file della risoluzione diretta.
- `Root name servers`: Sono i server DNS di riferimento che contengono gli indirizzi dei Name server autoritativi per i TLD (Top Level Domains .org .net ecc.)
- `Zone authoritative name server`: Sono i server che contengono le informazioni "autoritative" della zona. In generale esiste il Master Server che contiene le informazioni originali del dominio e lo Slave Server che ne mantiene una copia e che va a sincronizzarsi con il Master Server.
- `Domain` Un dominio è un sottoalbero completo della gerarchia ad albero dei nomi. (Il dominio `gnome.org` contiene tutti i sottodomini come `www.gnome.org`, `mail.gnome.org` ecc.)

9.2 DNS - Configurazione

Vediamo brevemente la configurazione del server DNS più utilizzato in assoluto e cioè *Bind* (`http://www.isc.org/products/BIND/`).
La configurazione di *Bind* avviene nei seguenti file:

- Red Hat: `/etc/named.conf` e `/var/named/*`
- Debian: `/etc/bind/named.conf` e `/etc/bind/*`

Vediamo brevente un esempio di `named.conf`:

```
options {
        directory "/etc/bind";
        /*
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
        // query-source address * port 53;

        // Facendo solamente da caching nameserver si settano qui
// i DNS a cui girare le richieste.
        //forwarders { 212.216.112.112;  212.216.172.62; };
};
```

```
// named.ca punta ai Root nameserver (FTP.RS.INTERNIC.NET)
zone "." IN {
        type hint;
        file "named.ca";
};

zone "example.com" IN {
        type master;
        file "example.com.zone";
        allow-update { none; };
};

zone "0.168.192.in-addr.arpa" IN {
        type master;
        file "0.168.192.reverse";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
```

Ecco un esempio di uno dei file di dati che contiene il mapping diretto da Nome ad IP:

```
// Default Time To Live
$TTL 86400

// Start of Authority Record
// @ Dominio contenuto in /etc/bind/named.conf
// SOA Tipo di Record
// Dominio
// Email dell'amministratore di rete
```

```
@       SOA     example.com. root.example.com. (
                        2001050101 ; Serial
                        21600      ; Refresh
                        1800       ; Retry
                        604800     ; Expire
                        900 )      ; Negative Cache TTL

// La sintassi dei RR (Resource Records) e' la seguente:
// [domain] [ttl] [class] <RR type> <Dati del record>
// [domain] Si specifica il dominio o si utilizza quello corrente
// [ttl] Si specifica il Time To Live per il record o si usa quello di default
// [class] Generalmente si lascia vuoto oppure IN (Internet)
// <RR type> E' il tipo di record: A, MX, NS, PTR, CNAME
// SOA - Ne esiste uno per ogni zona e ne configura gli aspetti di base
// NS - Mappa i nameserv della zona
// A - Mappa un nome di un host in IP
// CNAME - Definisce degli alias
// PTR - Mappa un IP in host
                NS      pippo.example.com.
                NS      ns.example.com.

                MX      10 mail1.example.com.
                MX      20 mail2.example.com.

workstation     A       192.168.0.1
server1         A       192.168.0.2
server2         A       192.168.0.3
pippo           A       192.168.0.4
ns              A       192.168.0.5
mail1           A       192.168.0.6
mail2           A       192.168.0.10
test            CNAME   server2
```

9.3 WINS - Configurazione

In una rete basata su NetBIOS la risoluzione dei nomi è basata sull'invio di messaggi circolari; quando un elaboratore con MS-Windows si collega in rete invia un messaggio a tutti informando sul proprio nome e sul proprio indirizzo. è ovvio che un sistema di questo tipo può essere efficiente solo su piccole reti e in assenza di sottoreti multiple (i router di solito sono configurati per bloccare i messaggi circolari).

La soluzione a questo problema proposta da Microsoft consiste nell'introduzione di un server WINS allo scopo di gestire una tabella contenente le associazioni tra nomi NetBIOS e indirizzi IP. I clienti della rete hanno impostata l'indicazione del numero IP del server WINS in modo che, quando devono qualificarsi o chiedere informazioni circa l'identità di altre macchine, si rivolgono direttamente al server senza generare traffico superfluo.

Un server Samba può essere configurato sia per svolgere la funzione di server WINS sia per essere cliente di un server WINS già presente in rete (ovviamente non sono possibili entrambe le impostazioni contemporaneamente).

Nella sezione global si deve aggiungere il seguente parametro per attivare il server WINS:

```
wins support = yes
```

Invece per indicare a Samba qual è il server WINS già attivo in rete si usa:

```
wins server = 192.168.1.1
```

10 Samba e la scansione della rete

In una rete locale le macchine hanno sempre una lista delle altre macchine attive che si chiama lista di browse. Il server che la gestisce si chiama master browser locale se riveste questo ruolo solo per una sottorete, se invece mantiene la lista per tutta la rete locale diviene un master browser di dominio.

Siccome in una rete le macchine possono essere collegate e scollegate in ogni momento, il master browser locale aggiorna continuamente la lista e la invia alle macchine che ne fanno richiesta. Il master browser di dominio invece raccoglie le liste di ogni sottorete e le mette a disposizione dei master browser locali.

Un elaboratore diventa master browser locale a seguito di una elezione che può essere effettuata in qualunque momento (ad esempio quando un nuovo elaboratore si presenta in rete). Riguardo a tale elezione Microsoft assegna ai suoi sistemi operativi un valore, detto livello, che cresce sempre di più per i sistemi operativi più recenti (ad esempio una macchina con MS-Windows 98 ha livello 2, una con MS-Windows NT 4 Workstation ha livello 17, una con MS-Windows NT 4-Server ha livello 32, una con MS-Windows 2000-Server ha livello 64).

L'elezione avviene sulla base di questo valore; in caso di parità viene esaminata la funzione svolta dalla macchina (senza entrare in dettagli eccessivi, basti sapere che un PDC diviene sempre anche PDM); in caso di ulteriore parità viene scelta la macchina che è da più tempo in rete.

Con Samba il livello per la partecipazione all'elezione può essere scelto in sede di configurazione. Nell'esempio seguente vengono mostrate le direttive da inserire nella

sezione global affinch il server Samba sia master browser locale prevalendo su macchine MS-Windows equipaggiate fino a NT-server:

```
local master = yes
os level = 34
preferred master = yes
```

La terza direttiva serve ad attivare il preferred master bit del server Samba, in modo che il proprio server prevalga al momento dell'elezione su macchine con uno stesso sistema operativo.

Se si vuole che il server Samba divenga master browser di dominio occorre inserire anche:

```
domain master = yes
```

In caso però che il server partecipi a un dominio NT è preferibile che il ruolo di master browser di dominio sia lasciato al PDC (che comunque, come viene descritto nel prossimo capitolo, può essere lo stesso server Samba).

A proposito della scansione della rete, nel caso siano presenti sottoreti multiple, è opportuno ricordare le seguenti regole generali:

- ci deve essere una macchina MS-Windows o Samba che faccia da master browser locale per ciascuna sottorete (se nella sottorete c'è gia un master browser di dominio non è necessario anche il master browser locale);
- almeno una macchina MS-Windows o Samba deve essere master browser di dominio per il gruppo di lavoro;
- ogni master browser locale deve sincronizzarsi con il master browser di dominio.

In caso nella rete non sia presente un master browser di dominio e ci siano però delle sottoreti multiple, Samba mette a disposizione due direttive utili per la sincronizzazione (da inserire sempre nella sezione global):

```
remote announce = 192.168.1.255/INF  192.168.2.255/INF
remote browse sync = 192.168.3.255 192.168.4.255
```

Con remote announce il server Samba fornisce l'elenco di scansione anche ad altre sottoreti. Se si conoscono i numeri IP dei master browser locali si possono indicare tali numeri, altrimenti (come nell'esempio) si indicano degli indirizzi broadcast. In pratica con i valori indicati, il server Samba segnalerà la sua presenza a tutte le macchine delle sottoreti 192.168.1.* e 192.168.2.* (del gruppo di lavoro INF) e quindi anche ai relativi master browser locali.

L'altra direttiva ha uno scopo simile nel caso però i master browser locali delle sottoreti siano altri serventi Samba (anche in questo caso si possono indicare gli indirizzi precisi dei server o degli indirizzi broadcast). Nell'esempio, un server Samba contatta altri serventi Samba delle sottoreti 192.168.3.* e 192.168.4.*, con i quali sincronizza le liste di scansione.

A proposito della possibilità di usare gli indirizzi broadcast ci si deve sincerare che i router della rete non siano configurati per bloccare il traffico broadcast tra sottoreti diverse.

11 SWAT

SWAT è il Samba Web Administration Tool, che permette di configurare Samba comodamente via web senza dover modificare a mano i file di configurazione.

11.1 Installazione

SWAT, generalmente viene lanciato tramite un Internet Superserver. Con Inetd nel file di configurazione `/etc/inetd.conf` ci sarà una riga simile a questa:

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

Con Xinetd invece in `/etc/xinetd.d`, ci dovrà essere un file `swat` tipo:

```
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#              to configure your Samba server. To use SWAT, \
#              connect to port 901 with your favorite web browser.
service swat
{
        port            = 901
        socket_type     = stream
        wait            = no
        only_from       = 127.0.0.1
        user            = root
        server          = /usr/sbin/swat
        log_on_failure  += USERID
        disable         = no
}
```

L'installazione è piuttosto immediata:

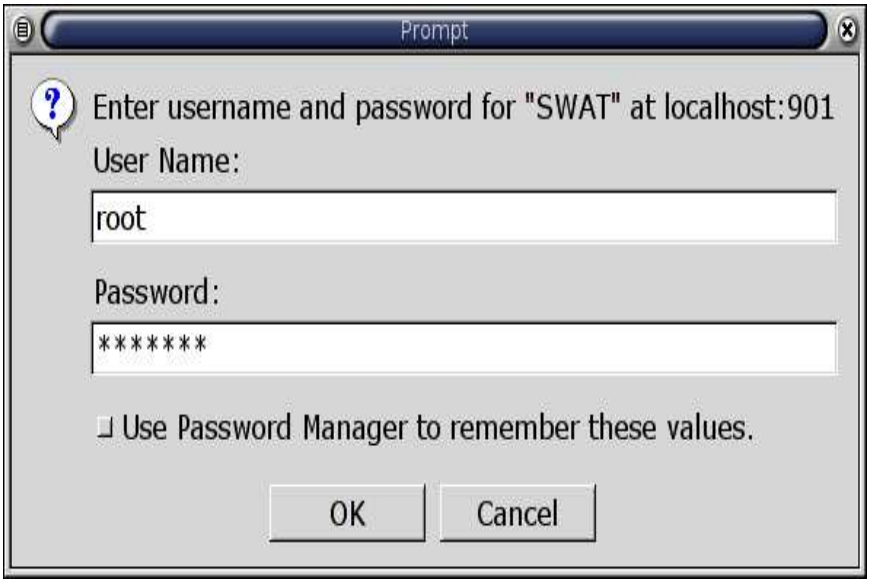
- Red Hat - `rpm -Uvh samba-swat-<x.y.z>.i386.rpm`

- `Debian - apt-get install swat`

Una volta installati i pacchetti basta attivare in inetd o xinetd il servizio.

11.2 Utilizzo

Una volta puntato il proprio browser verso `http://nomemacchina:901`, basta autenticarsi come root :



Dopodichè è possibile accedere a tutte le funzionalità offerte da SWAT:

11.3 Swat e SSL

Per un'amministrazione remota più sicura è possibile utilizzare SWAT tramite SSL. Qui di seguito i passi necessari per la configurazione:

- Si installi Openssl (`http://www.openssl.org`, di norma si trova già installato) e Stunnel (`http://www.stunnel.org`)
- Si generino le chiavi pubbliche e private con:

  ```
  /usr/bin/openssl req -new -x509 -days 365 -nodes -config \
    /etc/stunnel/stunnel.conf -out /etc/stunnel/stunnel.pem -keyout \
    /etc/stunnel/stunnel.pem
  ```

- Si rimuova la entry relativa a Swat di inetd o xinetd
- Si attivi l'stunnel

  ```
  stunnel -p /etc/stunnel/stunnel.pem -d 901 -l /usr/bin/swat swat
  ```

- A questo punto basta puntare il proprio browser su `https://nomehost:901`, accettare il certificato SSL e procedere all'utilizzo.

Ad ogni modo. volendo evitare la configurazione di SSL, è sempre possibile accedere in modo sicuro a SWAT abilitando il Forwarding X11 di ssh e collegarsi via ssh alla macchina con `ssh -X <nomemacchina>` e da lì lanciare un browser.

12 Winbind

12.1 Accesso a GNU/Linux da parte di utenti di un dominio MS-Windows con Winbind

In precedenza, nel capitolo sull'impostazione di un server Samba, è stato illustrato come integrare quest'ultimo in un dominio MS-Windows NT o in una active directory di MS-Windows 2000. In particolare si è visto come questo sia possibile impostando il livello di sicurezza al valore domain ed eseguendo un opportuno comando smbpasswd.

Grazie a Winbind, un nuovo strumento di Samba presente dalla versione 2.2.2, diventa addirittura possibile l'autenticazione degli utenti GNU/Linux (attenzione: utenti GNU/Linux, non utenti Samba) presso il domain controller windows. Ciò può essere molto utile in quei contesti in cui si vogliano inserire elaboratori con GNU/Linux in reti già consolidate su piattaforma MS-Windows, utilizzando le informazioni su utenti e gruppi preesistenti senza essere costretti a ridefinirle anche per le macchine GNU/Linux.

Winbind è costituito da un piccolo gruppo di componenti disponibili all'interno del pacchetto samba-common; in dettaglio ne fanno parte:

- una libreria per il NSSwitch (Name service switch)
- una libreria per i moduli PAM (Pluggable authentication modules)
- un programma di servizio, wbinfo, e un demone, winbindd.

Il servizio NSSwitch è presente in tutte le moderne librerie C e permette di ottenere i dati relativi a utenti, gruppi e nodi, da varie fonti (ad esempio NIS, DNS, ecc.); Winbind diventa un'ulteriore fonte di informazioni per NSSwitch relativamente a utenti e gruppi di un dominio MS-Windows.

Il PAM è un sistema generalizzato per la gestione dei metodi di autenticazione per molteplici servizi (quelli per cui esistono le librerie PAM relative); grazie all'apposita libreria PAM, Winbind fornisce anche il servizio di autenticazione.

12.2 Configurazioni necessarie

Per configurare il servizio Winbind occorre intervenire innanzitutto nel file smb.conf inserendo le direttive seguenti:

```
workgroup name = nome_dominio_NT
encrypt password = yes
security = domain
password server = nome_PDC_WIN
```

```
;  impostazioni per il demone winbindd
   winbind separator = +
   template shell = /bin/bash
   template homedir = /home/%D/%U
   winbind uid = 10000-20000
   winbind gid = 10000-20000
   winbind enum users = yes
   winbind enum groups = yes
```

Con winbind separator si imposta il carattere usato per ottenere il nome utente GNU/Linux dall'unione di nome di dominio e nome utente NT; il valore predefinito corrisponde a ma è sconsigliabile, in quanto ha un significato speciale nella shell di GNU/Linux; invece, la scelta del carattere + dovrebbe essere quella migliore.

Con template shell si imposta la shell degli utenti.

Con template homedir si definisce la directory personale degli utenti; nell'esempio si usano le variabili %D e %U in modo che ogni utente abbia come directory `/home/<nomedominiont>/<nomeutentent>`.

winbind uid e winbind gid permettono di impostare gli intervalli di numeri di identificazione per utenti e gruppi che Winbind utilizza per riabbinare gli utenti e i gruppi MS-Windows a utenti e gruppi GNU/Linux.

winbind enum users e winbind enum groups permettono di attivare l'enumerazione di gruppi e utenti.

12.3 Modifiche ai file di configurazione dei moduli PAM

Le modifiche ai file di configurazione dei moduli PAM devono essere effettuate con molta attenzione in quanto errori in questa fase possono causare anche l'impossibilità di accedere. Può quindi essere opportuno fare una copia dei file interessati alle modifiche in modo da poter ripristinare la situazione precedente in ogni momento.

Maggiori informazioni sul funzionamento dei moduli PAM non possono essere fornite in questa sede; eventualmente si può consultare il capitolo 56.

Nel file /etc/pam.d/system-auth deve essere aggiunta la riga:

```
auth   sufficient   /usr/lib/security/pam_winbind.so
```

dopo la prima riga auth già presente e trasformata la riga:

```
auth   sufficient   /lib/security/pam_unix.so   likeauth   nullok
```

in:

```
auth  sufficient  /lib/security/pam_unix.so  likeauth  nullok  use_first_pass
```

Nel file /etc/pam.d/login devono essere aggiunte le seguenti due righe, rispettivamente come prima riga account e come ultima riga session required:

```
account  sufficient /lib/security/pam_winbind.so
...
session  required   /lib/security/pam_mkhomedir.so  skel=/etc/skel/  umask=0022
```

L'ultima è molto importante in quanto permette la creazione automatica della directory personale dell'utente al primo accesso alla macchina GNU/Linux.

Riguardo la modifica al file system-auth occorre osservare che, essendo la sua configurazione usata, attraverso il modulo pam-stack, in molti altri file di configurazione dei moduli PAM (e non solo in login), sarebbe più opportuno lasciarlo invariato definendone uno nuovo con le modifiche e con nome leggermente diverso. Se si opta per questa scelta è ovvio che si devono modificare opportunamente i riferimenti al file system-auth contenuti nel file login.

12.4 Modifiche alla configurazione di NSSwitch

Nel file /etc/nsswitch.conf, contenente la configurazione del servizio NSSwitch, è necessario aggiungere Winbind tra le fonti dei dati relativi a utenti e gruppi. Ad esempio:

```
passwd:     files winbind
group:       files winbind
```

L'ordine con cui vengono elencate le fonti è significativo e quindi è opportuno lasciare la priorità a files in modo che per primi siano interrogati i file di sistema (/etc/passwd e /etc/group).

12.5 Attivazione

Per prima cosa occorre inserire la macchina GNU/Linux nel dominio MS-Windows operando come illustrato nel capitolo relativo alla configurazione di un server Samba, nel paragrafo sul livello di sicurezza domain (207.3.1.4).

Occorre poi avviare i servizi smb e winbind:

```
/etc/rc.d/init.d/smb start
/etc/rc.d/init.d/winbind start
```

Si può verificare il buon funzionamento di Winbind con i comandi:

```
wbinfo -u
wbinfo -g
```

con i quali si elencano rispettivamente utenti e gruppi del dominio MS-Windows.

Si possono usare anche i comandi:

```
getent passwd
getent group
```

per ottenere gli elenchi di tutti gli utenti e gruppi utilizzabili, sia quelli del dominio che quelli propri di GNU/Linux.

Infine si può procedere all'accreditamento sulla macchina GNU/Linux di un utente del dominio MS-Windows ricordando che il nome utente è dato da `<nomedominiont>+<nomeutentente>` e la parola d'ordine è ovviamente la stessa utilizzata in ambiente MS-Windows.

13 Samba e DFS

Il DFS (Distributed file system), introdotto con MS-Windows 2000, permette di organizzare le condivisioni di rete in una struttura ad albero svincolando gli utenti di tali risorse dalla conoscenza della reale collocazione delle stesse sui vari serventi. Con MS-Windows 95/98/NT è invece necessario, quando si deve connettere una risorsa, conoscere esattamente la sua collocazione in rete; si può ovviare in parte a questo inconveniente connettendo permanentemente la risorsa all'avvio dell'elaboratore cliente, ma in caso di spostamento della risorsa il problema si ripresenta.

Con il DFS si vengono a creare dei volumi di rete che possono essere ispezionati come fossero residenti fisicamente su un solo server. La struttura può poi essere duplicata, tutta o in parte, per ottenere maggiori garanzie contro le perdite di dati accidentali.

Ogni struttura DFS ha una radice comune a tutte le condivisioni e numerose diramazioni (foglie), tutte di primo livello. Un server può ospitare una sola radice mentre le foglie possono anche essere ospitate su macchine diverse. Sarebbe anche possibile ottenere strutture più complesse annidando radici di DFS come foglie di altri DFS ma qui non si considera tale possibilità.

Samba può assumere il ruolo di server DFS e ospitare una radice di un volume DFS grazie alla seguente direttiva nella sezione global:

```
   host msdfs = yes
```

e alla definizione di questa nuova sezione:

```
[dfs]
   path = /dir-expo/dfs
   msdfs root = yes
```

Nella directory /dir-expo/dfs del server GNU/Linux si dovranno poi impostare i collegamenti simbolici agli altri serventi della rete procedendo come nell'esempio seguente:

```
cd /dir-expo/dfs
chown root /dir-expo/dfs
chmod 755 /dir-expo/dfs
ln -s msdfs:serverA\\shareA coll-a
ln -s msdfs:serverB\\shareBC,serverC\\shareBC coll-bc
```

Il secondo collegamento dell'esempio associa a un solo nome di risorsa DFS, due condivisioni: queste saranno in fault tolerance tra di loro e l'allineamento dei dati al loro interno sarà assicurato dal server DFS.

Grazie alla definizione dei collegamenti simbolici, quando un cliente si collega a una risorsa DFS, viene ridiretto, in modo del tutto trasparente e automatico, verso la macchina che ospita fisicamente i dati condivisi.

14 Programmi ausiliari per un server samba

Un primo strumento molto utile è testparm con il quale si verifica la correttezza sintattica delle impostazioni scritte nel file smb.conf.

Il comando da eseguire è:

```
testparm /etc/samba/smb.conf
```

si ottiene una risposta suddivisa in due parti: prima il resoconto del controllo sintattico del file di configurazione, poi l'elenco delle risorse condivise descritte in esso.

Altro programma di fondamentale importanza è smbpasswd, già visto in precedenza a proposito della connessione di Samba a un dominio MS-Windows NT, ma che si usa principalmente per definire utenti e parole d'ordine relative. La sintassi in questo caso è:

```
smbpasswd [-a] [-x] [<nominativo>]
```

L'opzione -a permette di inserire un nuovo utente e poi di definirne la parole d'ordine; l'opzione -x permette invece di eliminarlo; se non si indica alcuna opzione si esegue solo il cambio della parole d'ordine per l'utente. Il nominativo-utente che si può inserire alla fine della riga di comando è quello sul quale il comando opera (se non viene indicato, si fa riferimento in modo predefinito all'utente GNU/Linux che esegue il comando).

Altro strumento utile è lo script smbadduser che permette di definire un nuovo utente Samba e contemporaneamente l'associazione con utenti GNU/Linux corrispondenti. La sintassi è:

```
smbadduser <utente_linux>:<utente_smb> [<utente_linux>:<utente_smb>]...
```

In pratica questo comando aggiorna i file smbpasswd e smbusers, permettendo di definire la parola d'ordine per i nuovi utenti Samba.

Infine può essere molto utile anche il comando smbstatus per avere un rapporto (con l'opzione -d anche dettagliato) delle connessioni Samba attive.

> Maggiori dettagli sulla configurazione di un server Samba si possono trovare anche nella documentazione fornita insieme al pacchetto in /usr/share/doc/samba-x.y.z, oppure consultando la pagina di manuale smb(5).

15 Autenticazione di utenti MS-Windows con Samba (PDC)

A partire dalla versione 2.0 è possibile configurare Samba come domain controller e autenticare gli utenti degli elaboratori clienti MS-Windows 95/98 sostituendo un server MS-Windows NT/2000.

Con la versione 2.1 è stata data la possibilità di accreditare anche clienti MS-Windows NT.

Dalla versione 2.2, che è la più recente, Samba può accreditare anche clienti MS-Windows 2000/XP, partecipare a una ADS (Active directory service) ed è stato aggiunto il demone winbind che consente di usare un domain controller MS-Windows come server per le utenze, allineando del tutto le utenze di GNU/ Linux con quelle di MS-Windows e centralizzando la loro gestione su un solo sistema.

È sicuramente anche il caso di elencare ciò che Samba non può fare (almeno per il momento):

- utilizzo di BDC (Backup domain controller) in domini NT e Active directory replication con MS-Windows 2000;
- partecipazione ad alcun tipo di trust relationship
- sostituzione di un MS-Windows 2000-Server.

In questa sede viene presa in esame solo la configurazione di Samba come PDC per l'accreditamento di clienti MS-Windows 95/98/Me/NT.

Di seguito viene presentato un possibile file smb.conf con le definizioni necessarie affinch Samba sia un PDC:

```
[global]
   netbios name = ServerSamba
```

```
   workgroup = INF
   server string = Samba Server NT
   log file = /var/log/samba/%m.log
   max log file = 50
   security = user
   encrypt password = yes
   smb password file = /etc/samba/smbpasswd
   local master = yes
   preferred master = yes
   os level = 33
   domain master = yes
;
   domain logons = yes
;
;  script di accesso fisso per tutti
   logon script = logon.bat
;  oppure uno per ogni cliente
;  logon script = %m.bat
;  oppure uno per ogni utente
;  logon script = %U.bat
;
;  profili utenti
   logon path =  \\ServerSamba\profile\%U


[netlogon]
   comment = Directory degli script di inizializzazione
   path = /home/netlogon
   read only = yes
   guest ok = yes
   browseable = no

[home]
   comment = Dir utente
   path = /home/%U
   browseable = yes
   writable = yes

[public]
   comment = Dir pubblica
   path = /home/public
```

```
browseable = yes
writable = yes
public = yes
create mask = 0777
```

16 Argomenti avanzati

16.1 ACL

Con le ultime release di Samba è diventato possibile supportare le **Access Control Lists** (o piu' brevemente **ACL**). In sostanza Samba diventa in grado di mappare le ACL di Windows (ACL Win32) in quelle POSIX.
È importante sottolineare come sia necessario disporre di un kernel, o più propriamente di un filesystem che supporti le ACL. Effettueremo le nostre prove utilizzando il filesystem ext3 con il supporto per le ACL. Oltre al supporto nativo nel kernel, è inoltre necessario di disporre di alcune librerie per gestire queste liste di accesso. Sono diversi i filesystem che supportano le ACL e gli EATTR (Extended Attributes). Uno dei filesystem più utilizzati per questo scopo è XFS, in quanto è stato tra i primi ad implementare su Linux queste funzionalità. In questa sezione vedremo come utilizzare le EA e le ACL su EXT3: Per poter disporre delle ACL e delle AE è innanzitutto necessario patchare il kernel in quanto tale funzionalità non sono ancora state incluse nei kernel ufficiali.

Le patch per Ext3 si trovano all'indirizzo: `http://acl.bestbits.at`

È necessario scaricare due patch e applicarle al codice sorgente del kernel:

```
cp linux-a.b.cea-x.y.z.diff.gz /usr/src
cp linux-a.b.cacl-x.y.z.diff.gz /usr/src
cd /usr/src/linux-2.4
zcat ../linux-a.b.cea-x.y.z.diff.gz ../linux-a.b.cacl-x.y.z.diff.gz | \
patch -p1 --dry-run
```

Una volta verificato che le patch si applicano senza errori:

```
zcat ../linux-a.b.cea-x.y.z.diff.gz ../linux-a.b.cacl-x.y.z.diff.gz | \
patch -p1
```

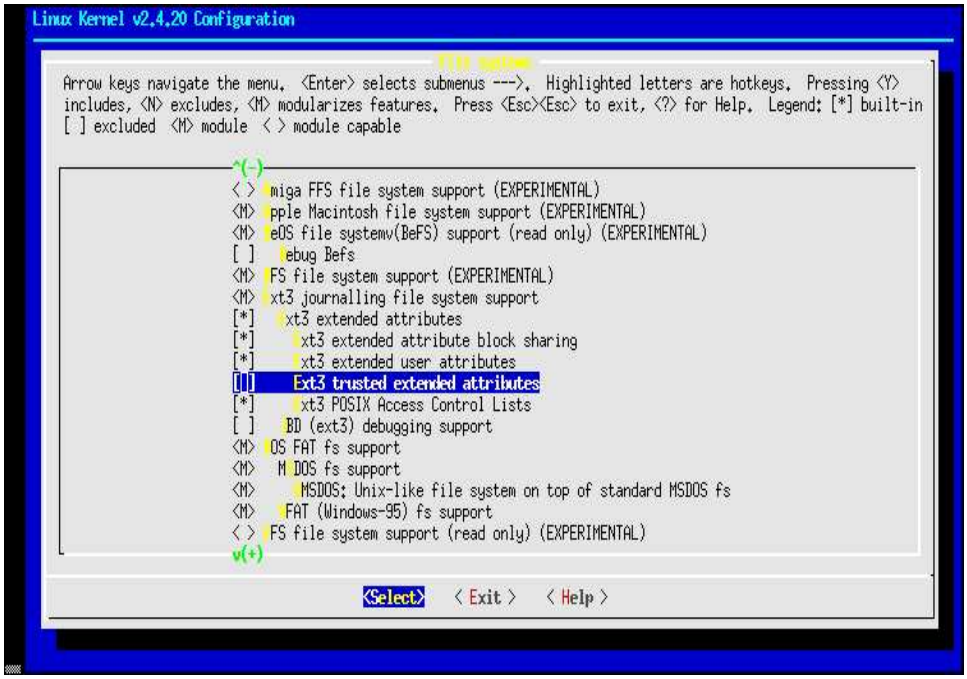
Nota: sotto Debian e' possibile semplicemente lanciare:

```
apt-get install kernel-source-2.4.x kernel-patch-acl
```

Una volta aggiunto il supporto ai sorgenti del kernel, si procede alla attivazione di tale funzionalita':

Le opzioni da attivare sono: `CONFIG_FS_POSIX_ACL`, `CONFIG_EXT3_FS_XATTR`, `CONFIG_EXT3_FS_POS` (per il filesystem ext3), `CONFIG_EXT2_FS_XATTR` e `CONFIG_EXT2_FS_POSIX_ACL` (per il filesystem ext2).

Dal `make menuconfig` queste opzioni si trovano sotto File System Menu e sono:



- `POSIX Access Control Lists`
- `Ext3 extended attributes (NEW)`
- `Ext3 POSIX Access Control Lists`
- `Ext2 extended attributes (NEW)`
- `Ext2 POSIX Access Control Lists`

Dopodiché si procede normalmente alla ricompilazione del kernel:

```
...
make dep bzImage modules
cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.x-foo
cp System.map /boot/System.map-2.4.x-foo
make modules_install
...
```

Una volta completata la ricompilazione e l'installazione del nuovo kernel e' necessario installare le librerie e le utility necessarie:

- Debian `apt-get install libattr1 libacl1 acl`
- Red Hat è necessario prima scaricare gli rpm che si trovano sul sito ufficiale `http://acl.bestbits.at`

Nota: Nelle ultime release di Red Hat questo passaggio non è necessario, in quanto tali librerie sono già presenti. Manca solamente il supporto a livello di kernel.

A questo punto è sufficiente montare il filesystem con l'opzione `''attr=acl''`, semplicemente aggiungendo `''attr=acl''\ nelle opzioni del file \verb`/etc/fstab—.

I due comandi per settare e modificare le ACL su un file sono:

`setfacl` La sintassi di questo comando è la seguente:

```
setfacl <opzioni> <permessi> <file>
```

Alcune opzioni di `setfacl` sono:

- `-m` modifica i permessi correnti sul file
- `-s` sostituire i permessi correnti
- `-x` rimuove una entry delle ACL

La sintassi dei permessi è la seguente:

- `[d[efault]:][u[ser]:]<uid>[:<perms>]` Permessi di un utente. Se il campo uid viene omesso ci si riferisce all'utente proprietario del file.
- `[d[efault]:]g[roup]:<gid>[:<perms>]` Permessi di un gruppo. Anche in questo caso omettendo il gruppo di si riferisce al gruppo proprietario.
- `[d[efault]:]m[ask][:][:<perms>]` Setta i permessi di mask.
- `[d[efault]:]o[ther][:][:<perms>]` Setta i permessi di 'tutti gli altri'

Utilizzando `getfacl` è invece possibile visualizzare le ACL di un file:

```
getfacl <file>
```

Per visualizzare altre opzioni aggiuntive è necessario fare riferimento alle pagine man dei due comandi.

A questo punto basta solamente ricompilare Samba con l'opzione `--with-acl-support`, se necessario (Red Hat 9 è al momento una delle poche distribuzioni che ha quest'opzione attiva nei propri pacchetti).

Un possibile `./configure` è il seguente:

```
./configure --host=i386-linux --build=i386-linux --with-fhs --prefix=/usr/local \
--sysconfdir=/etc --with-privatedir=/etc/samba --localstatedir=/var \
--with-netatalk --with-smbmount --with-pam --with-syslog \
--with-sambabook --with-utmp --with-readline --with-pam_smbpass \
--with-libsmbclient --with-winbind --with-msdfs --with-acl-support
```

Una volta compilato e installato Samba è pronto per supportare le **ACL**. Non è nemmeno necessario attivare l'opzione `nt acl support` in quanto è attiva di default.

16.2 Sicurezza

Per quel che riguarda la sicurezza di Samba non c'é molto da aggiungere se non che il protocollo non è nato con l'idea di essere utilizzato in reti di una certa dimensione. Per cui in linea generale una rete CIFS non viene mai esposta esternamente, ma viene sempre tenuta a livello locale. I motivi dietro a questa scelta sono molteplici e non ultimo è il fatto che il protocollo SMB/CIFS è assolutamente molto complesso e per questo motivo non certamente facile da gestire in modo sicuro.
Si ricorda che a tale scopo è possibile utilizzare le direttive `hosts allow`, `hosts deny` e `interfaces`/`bind interfaces only` nel file di configurazione per limitare l'ascolto dei servizi su interfacce specifiche o su sottoreti definite. Anche in luce ai recenti molteplici Advisory di sicurezza relativi a Samba, è assolutamente importante avere una policy di gestione per gli upgrade rilasciati dalla propria distribuzione.

- `Debian` - `http://www.debian.org/security/`
- `Red Hat` - `http://www.redhat.com/errata/`

Per avere un'idea di fondo sulle vulnerabilità conosciute relativamente a Samba, diamo uno sguardo a `http://cvs.mitre.org` (Common Vulnerabilities ed Exposures). Si possono notare 4 vulnerabilità (di cui 3 remote) rilasciate nei soli primi mesi del 2003:

- `CAN-2003-0085` Buffer overflow in the SMB/CIFS packet fragment re-assembly code for SMB daemon (smbd) in Samba before 2.2.8, and Samba-TNG before 0.3.1, allows remote attackers to execute arbitrary code.
- `CAN-2003-0086` The code for writing reg files in Samba before 2.2.8 allows local users to overwrite arbitrary files via a race condition involving chown.
- `CAN-2003-0196` Multiple buffer overflows in Samba before 2.2.8a may allow remote attackers to execute arbitrary code or cause a denial of service, as discovered by the Samba team and a different vulnerability than CAN-2003-0201.

- `CAN-2003-0201` Buffer overflow in the call-trans2open function in trans2.c for Samba 2.2.x before 2.2.8a, 2.0.10 and earlier 2.0.x versions, and Samba-TNG before 0.3.2, allows remote attackers to execute arbitrary code.

Per questo motivo è importante utilizzare sempre le versioni di Samba con le patch di sicurezza più recenti.

16.3 Samba e LDAP

È possibile utilizzare LDAP come backend di Samba per ottenere un *Single Sign On* verso cui autenticare sia utenti Unix/Linux che utenti Samba/Windows.
Un architettura di rete di questo tipo offre una serie di vantaggi piuttosto importanti nel momento in cui una rete raggiunge un certo tipo di dimensioni:

- Gestione centralizzata degli utenti
- Possibilità tramite *OpenLDAP* di replicare il database delle informazioni.
- Accesso granulare via ACL a tutti i dati
- Possibilità di conservare dati aggiuntivi oltre a User Id/PassWord/Gruppi ecc.
- L'accesso alle informazioni è ottimizzato in lettura

Non scendiamo qui nei dettagli dell'implementazione di un sistema e facciamo riferimento ad un documento libero molto completo sull'argomento e che è reperibile qui:

`http://samba.idealx.org/index.en.html`

17 Tuning

Il discorso relativo al Tuning di un server Samba è estremamente delicato in quanto entrano in gioco un numero di variabili più o meno indipendenti tra di loro. In linea generale è importante iniziare dalle ottimizzazioni più semplici e ovvie, quali il tuning del kernel, dei dischi e delle interfacce di rete. È altresì importante effettuare le misurazione delle performance relativamente ad ogni singolo sottosistema. Includiamo qui alcune parti rilevanti di un documento abbastanza completo sul tuning reperibile presso: `http://people.redhat.com/alikins/`

Incluso nell'appendice, si possono trovare le sezioni più pertinenti al tuning di un server Samba.

18 Samba 3.0

18.1 Novità

Diamo uno sguardo alle novità attese per il la versione 3 di Samba:

- Active Directory: Ci sarà la possibilità di diventare membri di un realm ADS come server partecipante e autenticare gli utenti utilizzando LDAP/Kerberos.
- Unicode: Supporto on-the-wire per *UNICODE*. Una gestione interna migliorata per set di carattere multi-byte e Unicode
- Autenticazione: Il sistema di autenticazione è stato riscritto quasi completamente e sarà molto più configurabile.
- Comando "net': È stato aggiunto un nuovo comando `net` molto simile al comando analogo di Windows.
- Analisi più completa dei codici errore per una gestione migliore delle situazioni di errore.
- Supporto per la stampa da Windows 2000 migliorato, inclusa la gestione degli attributi della stampante su Active Directory.
- Nuovo backend VFS modulare. Permetterà di aggiungere e configurare moduli VFS per ogni share.
- Performance migliorata di Winbind
- Supporto per la migrazione da un dominio NT 4.0
- Supporto per le relazioni trust con Domain Controllers NT 4

A Tuning

A.1 Server Oriented System Tuning Info

This page is about optimizing and tuning Linux based systems for server oriented tasks. Most of the info presented here I've used myself, and have found it to be beneficial. I've tried to avoid the well tread ground (hdparm, turning off hostname lookups in apache, etc) as that info is easy to find elsewhere.
Some cases where you might want to apply some of benchmarking, high traffic web sites, or in case of any load spike (say, a web transfered virus is pegging your servers with bogus requests)

A.2 File and Disk Tuning

Benchmark performance is often heavily based on disk I/O performace. So getting as much disk I/O as possible is the real key.
Depending on the array, and the disks used, and the controller, you may want to try software raid. It is tough to beat software raid performace on a modern cpu with a fast disk controller.
The easiest way to configure software raid is to do it during the install. If you use the gui installer, there are options in the disk partion screen to create a md or multiple-device, linux talk for a software raid partion. You will need to make partions on each of the drives of type linux raid, and then after creating all these partions, create a new partion, say /test, and select md as its type. Then you can select all the partions that should be part of it, as well as the raid type. For pure performance, RAID 0 is the way to go.
Note that by default, I belive you are limited to 12 drives in a MD device, so you may be limited to that. If the drives are fast enough, that should be sufficent to get ¿ 100 MB/s pretty consistently.
One thing to keep in mind is that the position of a partion on a hardrive does have performance implications. Partions that get stored at the very outer edge of a drive tend to be significantly faster than those on the inside. A good benckmarking trick is to use RAID across several drives, but only use a very small partion on the outside of the disk. This give both consistent performance, and the best performance. On most moden drives, or least drives using ZCAV (Zoned Constant Angular Velocity), this tends to be sectors with the lowest address, aka, the first partions. For a way to see the differences illustrated, see the (`http://www.coker.com.au/bonnie++/zcav/`) ZCAV page.

This is just a summary of software RAID configuration. More detailed info can be found elsewhere including the (`http://www.linuxdoc.org/HOWTO/Software-RAID-HOWTO.html`)

Software-RAID-HOWTO, and the docs and man pages from the raidtools package.

A.3 File System Tuning

Some of the default kernel paramaters for system performance are geared more towards workstation performance that file server/large disk io type of operations. The most important of these is the bdflush value in

```
/proc/sys/vm/bdflush
```

These values are documented in detail in `/usr/src/linux/Documenation/sysctl/vm.txt`
A good set of values for this type of server is:

```
echo 100 5000 640 2560 150 30000 5000 1884 2 > /proc/sys/vm/bdflush
```

(you change these values by just echo'ing the new values to the file. This takes effect immediately. However, it needs to be reinitilized at each kernel boot. The simplest way to do this is to put this command into the end of `/etc/rc.d/rc.local`)
Also, for pure file server applications like web and samba servers, you probably want to disable the atime option on the filesystem. This disabled updating the atime value for the file, which indicates that the last time a file was accessed. Since this info isnt very useful in this situation, and causes extra disk hits, its typically disabled. To do this, just edit `/etc/fstab` and add notime as a mount option for the filesystem.
For example:

```
/dev/rd/c0d0p3          /test                   ext2    noatime         1 2
```

With these file system options, a good raid setup, and the bdflush values, filesystem performace should be suffiecent.

The disk i/o elevators is another kernel tuneable that can be tweaked for improved disk i/o in some cases.

A.4 SCSI Tuning

SCSI tuning is highly dependent on the particular scsi cards and drives in questions. The most effective variable when it comes to SCSI card performace is tagged command queueing.
For the Adaptec aic7xxx seriers cards (2940's, 7890's, *160's, etc) this can be enabled with a module option like:

```
aic7xx=tag_info:{{0,0,0,0,}}
```

This enabled the default tagged command queing on the first device, on the first 4 scsi ids.

```
options aic7xxxaic7xxx=tag_info:{{24.24.24.24.24.24}}
```

in `/etc/modules.conf` will set the TCQ depth to 24.
You probably want to check the driver documentation for your particular scsi modules for more info.

A.5 Disk I/O Elevators

On systems that are consistently doing a large amount of disk I/O, tuning the disk I/O elevators may be useful. This is a 2.4 kernel feature that allows some control over latency vs throughput by changing the way disk io elevators operate.
This works by changing how long the I/O scheduler will let a request sit in the queue before it has to be handled. Since the I/O scheduler can collapse some request together, having a lot of items in the queue means more can be cooalesced, which can increase throughput.

Changing the max latency on items in the queue allows you to trade disk i/o latency for throughput, and vice versa.

The tool `/sbin/elvtune` (part of util-linux) allows you to change these max latency values. Lower values means less latency, but also less thoughput. The values can be set for the read and write queues seperately.

To determine what the current settings are, just issue:

```
/sbin/elvtune /dev/hda1
```

substituting the approriate device of course. Default values are 8192 for read, and 16384 for writes.

To set new values of 2000 for read and 4000 for example:

```
/sbin/elvtune -r 2000 -w 4000 /dev/hda1
```

Note that these values are for example purposes only, and are not recomended tuning values. That depends on the situation.

The units of these values are basically sectors of writes before reads are allowed. The kernel attempts to do all reads, then all writes, etc in an attempt to prevent disk io mode switching, which can be slow. So this allows you to alter how long it waits

before switching.

One way to get an idea of the effectiveness of these changes is to monitor the output of `isostat -d -x DEVICE`. The avgrq-sz and avgqu-sz values (average size of request and average queue length, see man page for iostat) should be affected by these elevator changes. Lowering the latency should cause the avqrq-sz to go down, for example.

See the `elvtune` man page for more info. Some info from when this feature was introduced is also at (`http://lwn.net/2000/1123/kernel.php3`) Lwn.net.

This info contributed by Arjan van de Ven.

A.6 Network Interface Tuning

Most benchmarks benifit heavily from making sure the NIC's in use are well supported, with a well written driver. Examples include eepro100, tulip's, newish 3com cards, and acenic and sysconect gigabit cards.
Making sure the cards are running in full duplex mode is also very often critical to benchmark performace. Depending on the networking hardware used, some of the cards may not autosense properly and may not run full duplex by default.
Many cards include module options that can be used to force the cards into full duplex mode. Some examples for common cards include

```
alias eth0 eepro100
options eepro100 full_duplex=1
alias eth1 tulip
options tulip full_duplex=1
```

Though full duplex gives the best overall performance, I've seen some circumstances where setting the cards to half duplex will actually increase thoughput, particulary in cases where the data flow is heavily one sided.

If you think your in a situation where that may help, I would suggest trying it and benchmarking it.

A.7 TCP tuning

For servers that are serving up huge numbers of concurent sessions, there are some tcp options that should probabaly be enabled. With a large number of clients doing their best to kill the server, its probabaly not uncommon for the server to have 20000 or

more open sockets.
In order to optimize TCP performace for this situation, I would suggest tuning the following parameters.

```
echo 1024 65000 > /proc/sys/net/ipv4/ip_local_port_range
```

Allows more local ports to be available. Generally not a issue, but in a benchmarking scenario you often need more ports available. A common example is clients running ‘ab‘ or ‘http-load‘ or similar software.

In the case of firewalls, or other servers doing NAT or masquerading, you may not be able to use the full port range this way, because of the need for high ports for use in NAT.

Increasing the amount of memory associated with socket buffers can often improve performance. Things like NFS in particular, or apache setups with large buffer configured can benefit from this.

```
echo 262143 > /proc/sys/net/core/rmem_max
echo 262143 > /proc/sys/net/core/rmem_default
```

This will increase the amount of memory available for socket input queues. The wmem-* values do the same for output queues.

Note: With 2.4.x kernels, these values are supposed to autotune fairly well, and some people suggest just instead changing the values in:

```
/proc/sys/net/ipv4/tcp_rmem
/proc/sys/net/ipv4/tcp_wmem
```

There are three values here, min default max.

These reduce the amount of work the TCP stack has to do, so is often helpful in this situation.

```
echo 0 > /proc/sys/net/ipv4/tcp_sack
echo 0 > /proc/sys/net/ipv4/tcp_timestamps
```

A.8 File Limits and the like

Open tcp sockets, and things like apache are prone to opening a large amount of file descriptors. The default number of available FD is 4096, but this may need to be

upped for this scenario.

The theorectial limit is roughly a million file descriptors, though I've never been able to get close to that many open.
I'd suggest doubling the default, and trying the test. If you still run out of file descriptors, double it again.
For example:

```
echo 128000 > /proc/sys/fs/inode-max
echo 64000 > /proc/sys/fs/file-max
```

and as root:

```
ulimit -n 64000
```

Note: On 2.4 kernels, the inode-max entry is no longer needed.

You probabaly want to add these to `/etc/rc.d/rc.local` so they get set on each boot.
There are more than a few ways to make these changes sticky. In Red Hat Linux, you can you `/etc/sysctl.conf` and `/etc/security/limits.conf` to set and save these values.

If you get errors of the variety Unable to open file descriptor you definately need to up these values. You can examine the contents of `/proc/sys/fs/file-nr` to determine the number of allocated file handles, the number of file handles currently being used, and the max number of file handles.

A.9 NFS

A good resource on NFS tuning on linux is the (`http://nfs.sourceforge.net/nfs-howto/performan`
Linux NFS HOW-TO. Most of this info is gleaned from there.

But the basic tuning steps include:

Try using NFSv3 if you are currently using NFSv2. There can be very significant performance increases with this change.

Increasing the read write block size. This is done with the `rsize` and `wsize` mount options. They need to the mount options used by the NFS clients. Values of 4096 and 8192 reportedly increase performance alot. But see the notes in the HOWTO about experimenting and measuring the performance implications. The limits on these are

8192 for NFSv2 and 32768 for NFSv3.

Another approach is to increase the number of nfsd threads running. This is normally controlled by the nfsd init script. On Red Hat Linux machines, the value RPCNFSDCOUNT in the nfs init script controls this value. The best way to determine if you need this is to experiment. The HOWTO mentions a way to determin thread usage, but that doesnt seem supported in all kernels.

Another good tool for getting some handle on NFS server performance is 'nfsstat'. This util reads the info in /proc/net/rpc/nfs[d] and displays it in a somewhat readable format. Some info intended for tuning Solaris, but useful for it's description of the (`http://www.princeton.edu/%7Eunix/Solaris/troubleshoot/nfsstat.html`) nfsstat format.

A.10 Samba Tuning

Depending on the type of tests, there are a number of tweaks you can do to samba to improve its performace over the default. The default is best for general purpose file sharing, but for extreme uses, there are a couple of tweaks.

The first one is to rebuild it with mmap support. In cases where you are serving up a large amount of small files, this seems to be particularly useful. You just need to add a –with-mmap to the configure line.

You also want to make sure the following options are enabled in the /etc/smb.conf file:

```
read raw = no
read prediction = true
level2 oplocks = true
```

One of the better resources for tuning samba is the Using Samba book from O'reily. The (`http://k12linux.mesd.k12.or.us/using_samba/appb_02.html`) Chapter on performance tuning is available online.

A.11 Openldap tuning

The most important tuning aspect for OpenLDAP is deciding what attributes you want to build indexes on.

I use the values:

```
cachesize 10000
dbcachesize 100000
```

```
sizelimit 10000
loglevel 0
dbcacheNoWsync

index cn,uid
index uidnumber
index gid
index gidnumber
index mail
```

If you add the following parameters to `/etc/openldap/slapd.conf` before entering the info into the database, they will all get indexed and performance will increase.

B GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that

they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

Terms And Conditions For Copying, Distribution And Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   (a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   (b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   (c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most

ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   (a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   (b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   (c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit

royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Riferimenti bibliografici

[1] Robert Eckstein, David Collier-Brown, Peter Kelly: *Using Samba* Novembre 1999

[2] Adrian Alikins: *System Tuning for Linux Servers* Marzo 2003

[3] Samba Team: *Samba HOWTO Collection* Aprile 2003

[4] Fulvio Ferroni: *Appunti di Informatica libera - Samba* Gennaio 2003