



Éric Seigne
<erics/at/rycks.com>

L'autore:

Ho lavorato per il mondo del software libero e tra le altre cose sviluppo applicazioni per il web con accesso a database usando tools come PostGreSQL, MySQL e PHP. Per mantenere un po' di libertà nel mio modo di lavorare (per poter fare qualcos'altro di tanto in tanto... come iniziare un nuovo progetto in C) ho avviato di recente una mia società. Per peggiorare le cose, sono –ancora– un membro ABUL www.abul.org (e non ho ancora pagato la mia quota di iscrizione!)

Tradotto in Italiano da:
Stefano Gorgoni ([homepage](#))

Configurazione di Samba



Premessa:

Proverò a spiegare qui il lavoro che abbiamo fatto per implementare un server linux con samba usato come domain controller per una rete Windows. La gestione dei permessi utenti, i profili... saranno spiegati in dettaglio. Questo documento si basa su Debian GNU/Linux 2.2, il che potrebbe significare che il vostro file smb.conf di default potrebbe presentare alcune differenze dipendenti dalla vostra distribuzione. La versione di samba usata per questo articolo è la **2.0.7**

Installare Samba

Suppongo che tu conosca già un minimo su samba e che sia installto sul tuo server. Se così non fosse, per una veloce installazione, prova:
Debian: `apt-get install samba`
RedHat(Mandrake): `rpm -vih /mnt/cdrom/RedHat(Mandrake)/RPMS/samba*`

Il file di configurazione: impostazioni generali

Samba usa un unico file di configurazione nel quale trovi blocchi come [global].

Solo un file di
configurazione
per samba!

```
<un smb.conf minimalista>
[global]
  printing = bsd
  printcap name = /etc/printcap
  load printers = yes
  guest account = pcguest

  log file = /usr/local/samba/log.%m

[tmp]
  comment = Temporary file space
  path = /tmp
  read only = yes
  public = yes
</file>
```

Se lanci samba con questo file di configurazione, le macchine windows nella tua rete locale saranno in grado di vedere, in Risorse di rete, che una macchina chiamata (il nome della linuxbox) condivide una directory temp nella quale hai il permesso di scrittura.

ATTENZIONE: quando aggiorni il file di configurazione di samba, devi far ripartire samba usando lo script */etc/init.d/samba restart* (per debian)

Il file di configurazione, parametri "avanzati"

Proviamo i seguenti parametri:

- Sezione [global]
 - ◆ **netbios name:**
Si può specificare il nome netbios del server samba. Puoi vedere il nome netbios in Risorse di rete dalle macchine windows. Se non ne assigni uno, il server linux userà il proprio hostname come nome netbios.
 - ◆ **invalid users:**
Lista di utenti che non possono accedere al server samba. Per esempio l'utente root non dovrebbe avere il permesso.
 - ◆ **interfaces:**
Se il server linux ha più di una scheda di rete e vuoi restringere la sua attività ad una sola rete.
 - ◆ **security:**
Selezione della modalità di autenticazione da usare. Usando security=user è necessario che ogni utente abbia un account sul server linux.
Se non vuoi che samba gestisca gli utenti e vuoi condividere le stesse risorse per tutti, puoi selezionare security=share.

- ◆ **workgroup:**
Nome del workgroup al quale appartiene il server linux.
 - ◆ **server string:**
Una descrizione della linuxbox (una qualunque stringa).
 - ◆ **socket options:**
Una lista di opzioni per "ottimizzare" samba e renderlo più veloce, per esempio.
 - ◆ **encrypt passwords:**
Devi usare password criptate? E' importante sapere che ogni sistema windows (quasi) usa uno schema differente!
 - ◆ **wins support:**
Il server linux deve fungere da server wins?
 - ◆ **os level:**
Livello di priorità da conoscere per sapere quale computer verrà "eletto" domain master, local master, etc...
 - ◆ **domain master:**
Imposta samba come domain master
 - ◆ **local master:**
Imposta samba come local master server
 - ◆ **preferred master:**
Deve essere preferito samba ad altri server se presenti?
 - ◆ **domain logons:**
Samba deve gestire il controllo delle connessioni per l'intero dominio?
 - ◆ **logon script:**
Quale script lanciare per l'utente quando questo inizia una sessione?
 - ◆ **logon path:**
Dove sono gli script di avvio?
 - ◆ **logon home:**
Dove conservare i profili utenti?
 - ◆ **name resolve order:**
Qual è l'ordine delle risorse da seguire per trovare il nome della macchina nella rete?
 - ◆ **dns proxy:**
Il server samba deve essere usato anche come DNS proxy?
 - ◆ **preserve case:**
Per mantenere maiuscole e minuscole dei nomi dei file.
 - ◆ **short preserve case:**
Come sopra ma anche per i nomi MS DOS (8 + 3).
 - ◆ **unix password sync:**
Le password unix e windows devono essere sincronizzate?
 - ◆ **passwd program:**
Che programma usare per cambiare le password?
 - ◆ **passwd chat:**
Qual è il "protocollo" chat per cambiare le password?
 - ◆ **max log size:**
Dimensione massima per i file di log.
- Sezione [netlogon]
 - Specifica dove si trova netlogon.
 - Sezione [profiles]
 - Profili degli utenti.
 - Sezione [homes]

Variabili di Samba

Variabile	Definizione
Variabili client	
%a	Architettura dei client Esempio: Win95, WfWg, WinNT, Samba ...
%I	Indirizzo ip del client
%m	Nome netbios del client
%M	Nome dns del client
Variabili utenti	
%g	Gruppo primario dell'utente %u
%H	Home directory dell'utente %u
%u	Utente unix
Variabili condivisioni	
%P	Root della condivisione corrente
%S	Nome della condivisione corrente
Variabili server	
%h	Nome DNS del server Samba
%L	Nome netbios del server Samba
%v	Versione Samba
Variabili varie	
%T	Data e ora corrente

Esempio con queste variabili: se le macchine della tua rete hanno windows 3.11 e windows 98, puoi creare due file di configurazione, una per ciascun sistema, utilizzando la variabile %a.

Risultato: il nostro file di configurazione

<smb.conf file>

```
[global]
printing = bsd
printcap name = /etc/printcap
load printers = yes
guest account = nobody
invalid users = root
```

```
; metti il nome netbios della tua macchina
netbios name = pantoufle
; la rete su cui deve stare in ascolto samba
; (non mettere samba in ascolto sull'interfaccia di rete collegata a internet!)
interfaces = 192.168.0.1/255.255.255.0
```

; security user richiede che ogni utente abbia un account unix sul server samba
security = user

; Il nome del workgroup al quale appartiene il server
workgroup = rycks
; Descrizione del server
; %h indica il nome dns del server e %v la versione di samba
server string = %h server (Samba %v)

; Vogliamo usare il log di samba, non solo syslog
syslog only = no

; il minor numero di informazioni vengono scritte su syslog,
; le altre informazioni si trovano i /var/log/smb(nmb)/
syslog = 0;

; ottimizzazioni
socket options = IPTOS_LOWDELAY TCP_NODELAY \
SO_SNDBUF=4096 SO_RCVBUF=4096

; Usiamo le apssword criptate. Attenzione,
; ogni client W95 deve essere patchato con la MS SMB
; security patch.
; NT4 deve essere patchato con il SP3 o superiore...
; wfg probabilmente non supporta le password criptate:(
encrypt passwords = yes

; Questo server funziona anche da server wins.
wins support = yes

; Livello Sistema Operativo. Dato che il nostro server funge da domain master, local logons, etc...
; diamogli un livello piú alto di un server NT, se presente!
os level = 34

; Gestione dominio
domain master = yes
local master = yes
preferred master = yes

; Gestione delle connessioni al dominio
domain logons = yes

; Che script eseguire quando il client si connette?
; %g corrisponde al nome del gruppo primario dell'utente che si connette
logon script = %g.bat
; In quale directory troviamo gli script di avvio?
; %L é il nome netbios del server samba
logon path=\\%L\netlogon
; Dove conservare i profili utenti?
; %U indica il login utente
logon home=\\%L%\%U\winprofile

```
; In quale ordine devono essere controllate le risorse per trovare
; il nome della macchina?
name resolve order = lmhosts host wins bcst

; Samba deve essere utilizzato come dns proxy?
dns proxy = no

; Mantieni i nomi dei file e maiuscole/minuscole
preserve case = yes
short preserve case = yes

; Sincronizzare le password windows e unix?
unix password sync = yes

; Cosa usare per la sincronizzazione delle password
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\sUNIX\spassword:* \
%n\n *Retype\snew\sUNIX\spassword:* %n\n .

; Dimensione massima del file di log,
; per evitare di riempire la directory /var
max log size = 1000

; Samba funge da time server: buona cosa per sincronizzare
; l'ora dei client.
; Useremo questa feature dal file logon .bat
time server = yes

; Specifichiamo dove si trovano i netlogon.
; Viene usato solo alla connessione,
; quindi non abbiamo bisogno di renderlo pubblico.
[netlogon]
path = /home/netlogon/%g
public = no
writeable = no
browseable = no

; La Home per tutti gli utenti
[homes]
comment = Home Directories
browseable = no

; Ci possono scrivere, no?
read only = no

; La mask Unix per la creazione di file
create mask = 0700

; Per motivi di sicurezza, anche la mask delle
; directory viene impostata a 0700!
directory mask = 0700
```

```
;Condividiamo l'FTP. È più facile trovarlo  
; nelle Risorse di Rete piuttosto che lanciare  
; un programma apposito.
```

```
[ftp]  
path = /home/ftp/pub  
public = yes  
printable = no  
guest ok = yes
```

```
; La directory temporanea
```

```
[tmp]  
path = /tmp  
public = yes  
printable = no  
guest ok = yes  
writable = yes
```

```
; Un'altra directory temporanea speciale  
; per un utente che ha bisogno di molto spazio!
```

```
[bigtemp]  
path = /home/bigtemp  
public = yes  
printable = no  
guest ok = yes  
valid users = erics  
writable = yes
```

```
</smb.conf file>
```

Cos'abbiamo sul server

In breve, sul server dovremmo avere:

- un account per ogni utente
- il file smb.conf
- una directory /home/netlogon (nel mio esempio)
- un file .bat per ogni gruppo di utenti in questa directory (tra breve ci sarà un esempio)
- un file CONFIG.POL per le strategie di sicurezza del sistema (anch'esso in questa directory).
- Per creare il file config.pol file, cercate il programma poledit.exe sul CD di Windows

```
<file /home/netlogon/admin.bat>  
net use P: \\pantoufle\homes  
net use T: \\pantoufle\tmp  
net time \\pantoufle /SET /YES  
</file admin.bat>
```

```

<file /home/netlogon/teachers/teachers.bat>
net use P: \\pantoufle\homes
net use T: \\pantoufle\tmp
net time \\pantoufle /SET /YES
regedit /s \\pantoufle\netlogon\teachers.reg
</file teachers.bat>

<file /home/netlogon/pupils/pupils.bat>
net use P: \\pantoufle\homes
net use T: \\pantoufle\tmp
net time \\pantoufle /SET /YES
regedit /s \\pantoufle\netlogon\pupils.reg
</file pupils.bat>

<file /home/netlogon/teachers/teachers.reg>
[HKEY_CURRENT_USER\Software\Microsoft\Windows
\CurrentVersion\Explorer\User Shell Folders]
"Personal"="P:\\"
</file teachers.reg>

<file /home/netlogon/pupils/pupils.reg>
[HKEY_CURRENT_USER\Software\Microsoft\Windows
\CurrentVersion\Explorer\User Shell Folders]
"Personal"="P:\\"
</file pupils.reg>

```

Questo file permette di montare automaticamente la directory personale di ogni utente come drive P: e la directory temporanea come drive T:. Anche l'orario di sistema viene preso dal server samba.

NOTA: Il file .bat deve avere le linee terminate alla maniera del DOS. Il modo più semplice di crearlo è di usare il Blocco Note, per esempio, e poi mandarlo sul server.

Definire le politiche di sicurezza del sistema (C) (TM) (R)

Rendere sicuro
Windows è
quasi possibile,
usando un
domain
controller.

È un titolo! Beh, l'ho preso in prestito dalla documentazione MS riguardante i loro tool di politica di sistema.

Per creare una politica di sistema in Windows, per esempio per impedire a certi utenti (tutti?) di lanciare regedit, un programma DOS, ecc. dovete usare POLEDIT che si trova sul CD di Windows 98.

Lanciate PoEdit, date un'occhiata al suo help, scrivetevi le informazioni... questo articolo non è fatto per insegnarvi come funziona un software proprietario.

Una volta che il vostro file .POL è pronto, copiatelo sul vostro server samba, nella directory specificata dal PATH nel gruppo [netlogon].

ATTENZIONE: Per i client W9x il file per le strategie di sistema è CONFIG.POL... per WindowsNT ha un altro nome, e visto che non conosco NT non ve lo so dire :(
No, non mandatemi una versione di NT per provare. Grazie comunque, siete molto gentili :o)

NOTA: PolEdit consente di creare gruppi e utenti, ma non ci siamo ancora riusciti. Solo l'utente di default viene preso in considerazione.

Per esempio, se creo il gruppo "admin" con PolEdit, a cui consento di lanciare regedit, quando mi connetto come "erics" (che ha "admin" come gruppo primario), non posso lanciare regedit :(

Per contro, create un utente "erics" con poledit... e funziona.

Visto che non siamo in vena di creare i 1056 utenti con poledit e che un'amministrazione globale degli utenti è più interessante, vi "offriamo" il seguente trucco:

Per riuscirci abbiamo aggirato il problema: abbiamo preparato 3 config.pol con i soli utenti di default, quindi sul server linux abbiamo:

```
/home/netlogon/teachers/CONFIG.POL
/home/netlogon/teachers/teachers.bat
/home/netlogon/pupils/CONFIG.POL
/home/netlogon/pupils/pupils.bat
/home/netlogon/admin/CONFIG.POL
/home/netlogon/admin/admin.bat
```

E abbiamo cambiato il file smb.conf per tenerne conto:

```
<smb.conf file>
[netlogon]
; abbiamo aggiunto %g per fare in modo che netlogon punti a una directory diversa
; in base al gruppo, dentro la quale c'è un file config.pol corrispondente a
; ogni gruppo di profili utente.
path = /home/netlogon/%g
public = no
writeable = no
browseable = no
</smb.conf file>
```

Configurazione delle Macchine Windows

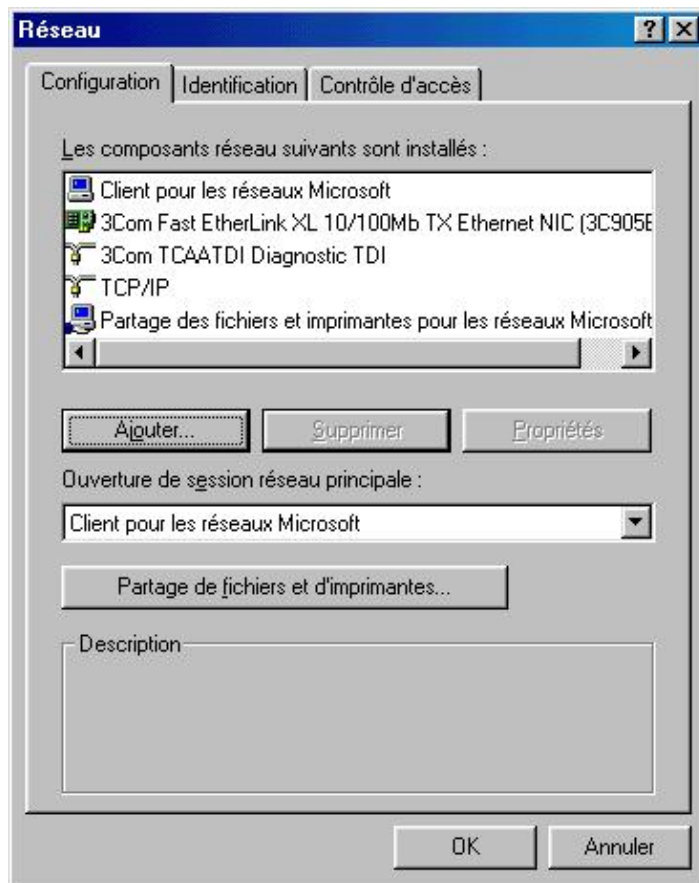
Con un po' di fortuna, 20 click del mouse e un riavvio dovrebbero essere

Per un client di tipo Win98

Clickate su Avvio/Impostazioni/Pannello di Controllo e fate doppio click su Rete

Installate:

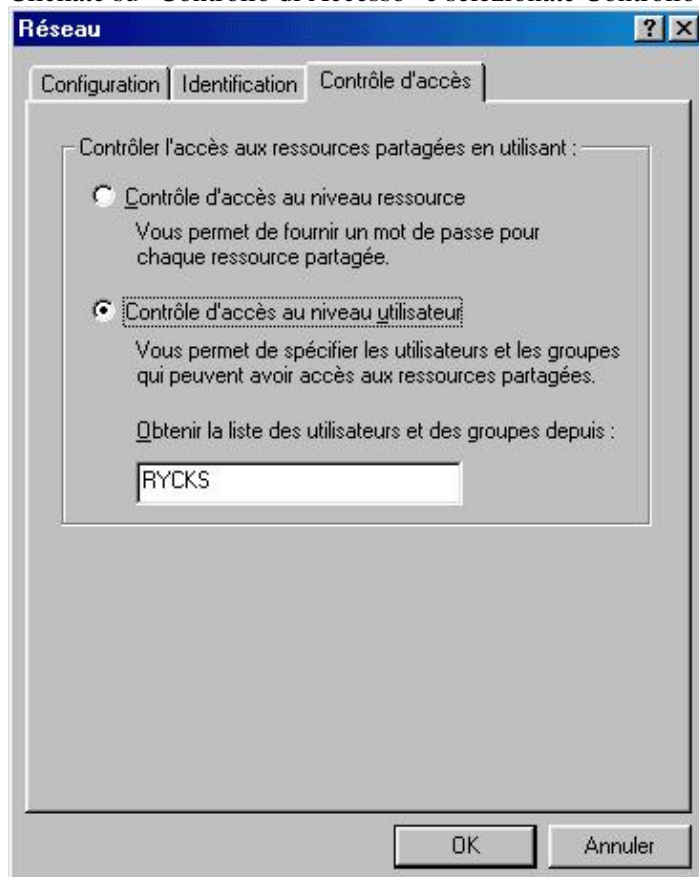
- Client per reti Microsoft
- Il driver della scheda di rete
- Protocollo TCP/IP e SOLO TCP/IP (niente ipx o netbios)
- Condivisione di File e Stampanti



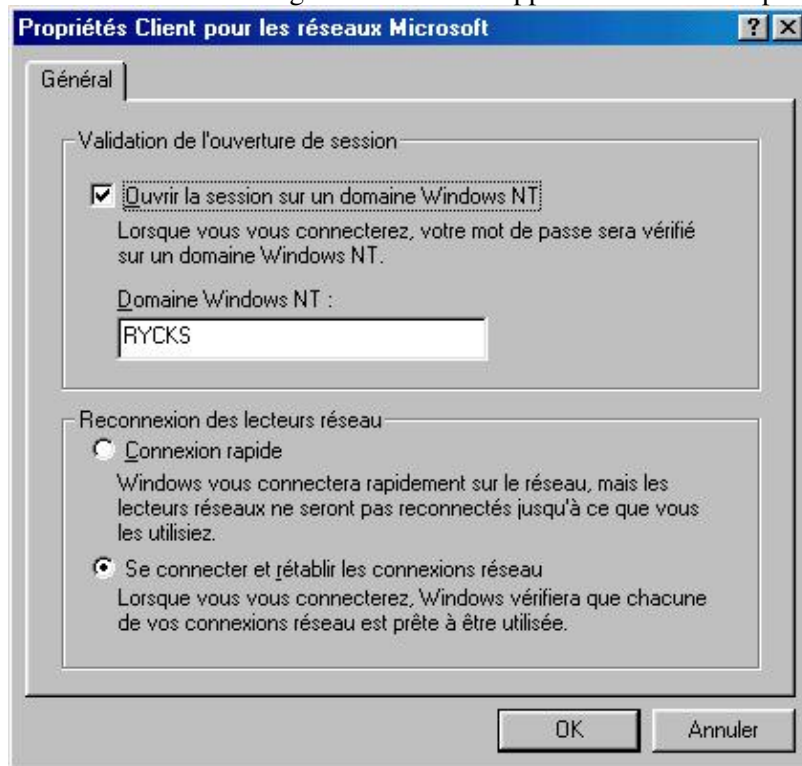
Quindi clickate sul tab "Identificazione" e date un nome e il corrispondente gruppo di lavoro al computer.



Clickate su "Controllo di Accesso" e selezionate Controllo di Accesso a Livello Utente



Tornate alla tab di configurazione e fate doppio click su "Client per reti Microsoft"



Non dimenticate di configurare il supporto TCP/IP:

Doppio click su TCP/IP

Indirizzo IP:

- l'indirizzo IP che volete per questa macchina (es.: 192.168.0.2)
- Maschera di rete (es.: 255.255.255.0)

Configurazione WINS:

- Attivate la Risoluzione WINS
- Aggiungete un server WINS, IP 192.168.0.1 (se questo è l'indirizzo del server samba)
- Gateway: se avete un gateway, configuratelo qui
- Configurazione DNS: configurate l'accesso al vostro DNS

Note "tuning/performance/buon senso?"

Durante il lavoro si nota subito un collo di bottiglia a causa dell'uso dei profili di windows.

È un dato di fatto che i profili siano pieni di roba che MS ha deciso essere importante, come la cache di IE, quella di Outlook, ecc.

In breve, questo significa che a ogni collegamento alla macchina verranno scaricati circa 10 Mb (comunque il mio è un profilo "classico", un'immagine di sfondo, ie e outlook...) a 10 Mb saranno mandati al server alla disconnessione.

10 Mb per ogni utente, in una stanza di 15 macchine (una dimensione "normale" per un laboratorio, per esempio), fanno 150 Mb e, se il palazzo contiene 10 stanze... potete solo calcolare gli utenti che si scollegano alla fine della giornata.

Dovreste quindi anticipare e sconnettervi prima delle 5... (beh, devo ammettere che è quello che facevo quando ero studente)... piuttosto che dopo le 5. È un po' come gli ingorghi del traffico delle grandi città: meglio partire 10 minuti prima oppure 2 ore dopo!

Quindi, in base alla politica che implementate, potrebbe essere una buona idea montare la home come drive P: (per esempio, P come Personale) per tutti, e spiegarli: "salvate i documenti in P e non in "Documenti", altrimenti li perderete per sempre".

A questo punto dovrete trovare un software in grado di essere configurato per avere i bookmark in P:\bookmarks.html, e lo stesso per la configurazione.

Non so nemmeno se esista nel mondo windows!

Se conoscete la soluzione, scriveteci un articolo, è una cosa degna di essere condivisa!

Domande e suggerimenti per un seguito

È possibile avere diversi workgroup sullo stesso dominio, come possono essere gestiti, è possibile suddividere i problemi tra vari server samba con GNU/Linux>

Come usare sia server NT che Samba>

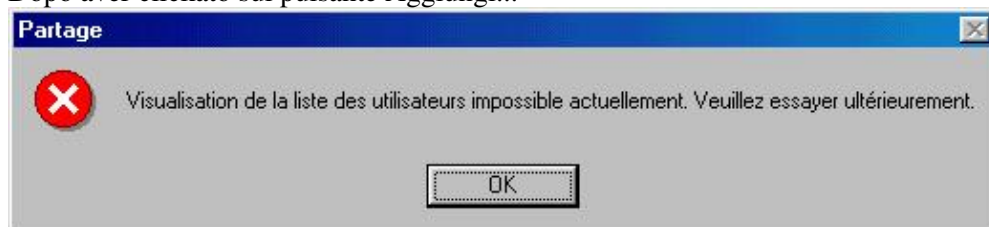
Configurazione di client NT: l'equivalente di CONFIG.POL ha un altro nome sotto NT.

Un problema usuale quando si ha solo un server Samba (e nessun NT): sto lavorando sotto W98 e voglio condividere una risorsa locale, per esempio la mia stampante:

Visualizzate il pannello della stampante



Dopo aver clickato sul pulsante Aggiungi...



ULTIM'ORA: qualcuno mi ha dato la soluzione. È sufficiente selezionare "Controllo di accesso a livello condivisione" al passo 3 della configurazione di Windows.

Riconoscimenti

Bruno <bcarrere(at)asp-france.fr> per la rilettura di questo articolo e per il prezioso aiuto :o)

John Perr per avermi convinto a scrivere il mio primo articolo per LinuxFocus e per averlo tradotto in inglese.
michel Billaud aka MiB per tutte le soluzioni che ha trovato ai nostri problemi; ci ha insegnato trucchi come strace ecc. :o)

Etienne, Éric, e l'uomo invisibile di cui ho dimenticato il nome, scusami! Grazie per aver condiviso le tue conoscenze apprese dai corsi MS sui server NT.

Jean Peyratout, dobbiamo dire perché? Sarebbe troppo lungo.

L'Abul in generale

Rycks per avermi dato l'opportunità e il tempo di sviluppare e documentare free software.

Risorse

Il libro online della O'Reilly: <http://www.oreilly.com/catalog/samba/chapter/book/index.html>

In italiano lo si può trovare sul sito di [Hops Libri](#)

Questo articolo sarà aggiornato nella [sezione sulla documentazione di rycks.com](#)

<p>Webpages maintained by the LinuxFocus Editor team © Éric Seigne "some rights reserved" see linuxfocus.org/license/ http://www.LinuxFocus.org</p>	<p>Translation information: fr --> -- : Éric Seigne <erics@rycks.com> fr --> en: Georges Tarbouriech <georges.t@linuxfocus.org> en --> it: Stefano Gorgoni (homepage)</p>
--	---

2005-03-31, generated by lfparsr_pdf version 2.51