

samba : in rete con Windows

Marco Prandini

14 maggio 2005





A cosa serve?

- A fornire i servizi tipici delle reti Microsoft
- Ad utilizzare i servizi tipici delle reti Microsoft





Perchè usarlo?

- Eliminare il costo di un server Windows e delle Client Access Licenses (CALs)
- In ambienti con stazioni Windows e Unix
 - Fornire aree comuni di scambio dati
 - Condividere stampanti
 - Predisporre un singolo sistema di autenticazione





Origini

- IBM propone NetBIOS
 - Un set di API per accedere a risorse remote
 - Il trasporto sulla rete è implementato da NetBEUI
 - Piccole reti locali, fino a 255 nodi identificati da stringhe di lunghezza fino a 15 caratteri
- RFC 1001/1002
 - NetBIOS su TCP/IP (NBT)
 - Conversione nomi NetBIOS / indirizzi IP
 - Modalità di trasporto dei pacchetti dati





Elementi essenziali del protocollo

- Server Message Block (SMB)
 - Protocollo a richiesta/risposta
 - Invio di comandi e ricezione di risultati, es:
 - Aprire e chiudere file
 - Creare e cancellare file e directory
 - Leggere e scrivere file
 - Cercare file
 - Inserire e rimuovere file in una coda di stampa





Elementi essenziali del protocollo

- Modalità di comunicazione
 - Sessioni (affidabile, peer-to-peer)
netbios-ssn 139/TCP
 - Datagrammi (non affidabile, broadcast)
netbios-dgm 138/UDP
 - Naming
netbios-ns 137/UDP
 - Nuova implementazione (W2K)
microsoft-ds 445/TCP&UDP

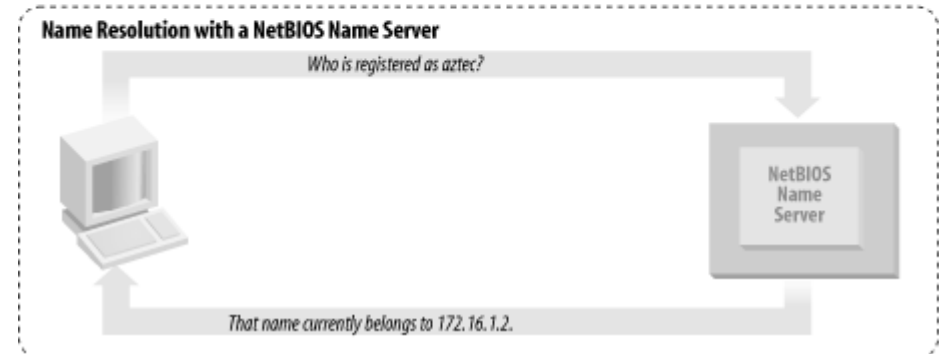
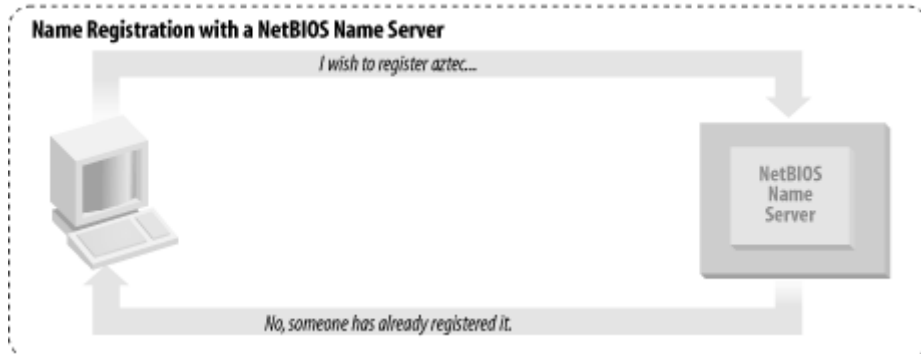
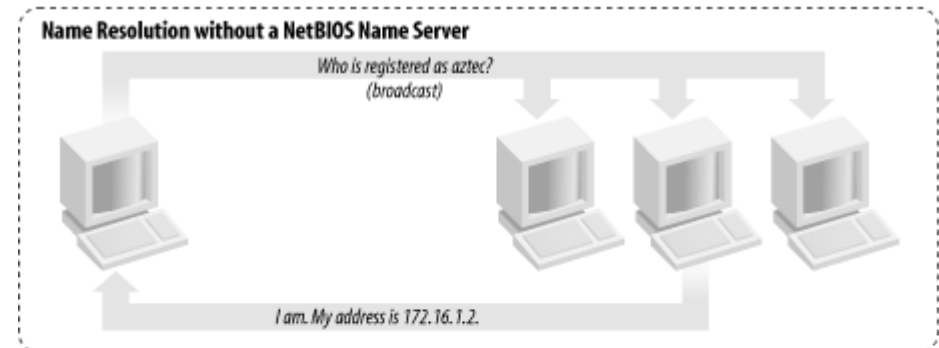
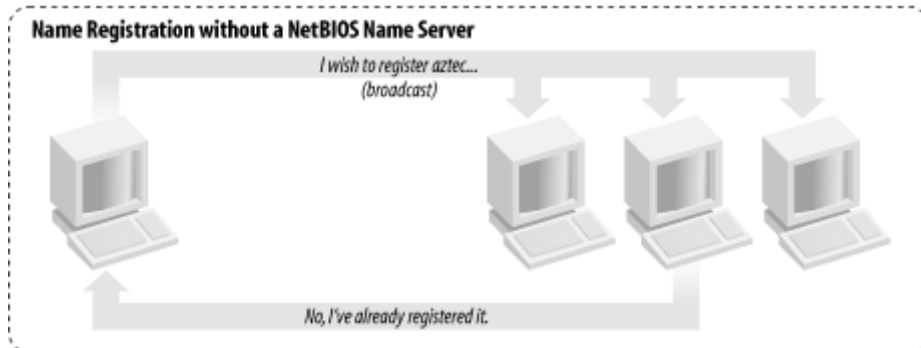




Naming (processi)

Registrazione

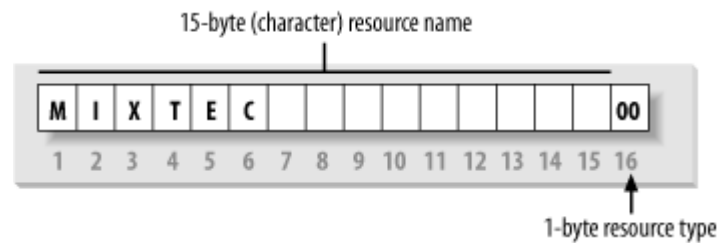
Risoluzione





Naming (informazioni)

- Nome registrato = Nome host + Tipo risorsa
- Registrazione multipla (1 entry per risorsa)



```
smbclient -L <host>  
nbtstat -a <host>
```





Browsing e workgroup

- Il *Local Master Browser* (LMB) svolge in parte il ruolo di NBNS: per sapere quali computer sono disponibili si chiede al LMB la *browse list*
- Per facilitare il browsing, ogni computer annuncia al LMB anche la propria appartenenza ad un *workgroup*
 - MA per conoscere le risorse offerte da un computer bisogna contattarlo direttamente
- Il LMB viene eletto tra tutti i computer





... e tanto altro

- Domini e domain controller
 - Un dominio è un “contesto di sicurezza”
 - Il Domain Controller gestisce l'autenticazione e l'autorizzazione (distribuzione delle ACL)
- Risoluzione dei nomi al di fuori della rete locale: WINS e DNS
- Active Directory





Cosa può e non può fare

Role

File server

Printer server

Microsoft Dfs server

Primary domain controller

Backup domain controller

Active Directory domain controller

Windows 95/98/Me authentication

Windows NT/2000/XP authentication

Local master browser

Local backup browser

Domain master browser

Primary WINS server

Secondary WINS server

Can perform?

Yes

Yes

Yes

Yes

No

No

Yes

Yes

Yes

Yes

Yes

Yes

No





Installazione

- Compreso nella maggior parte delle distribuzioni
- Scaricabile in forma sorgente da <http://www.samba.org/>
- Utile tool di terza parte: LinNeighborhood
 - Interfaccia grafica simile alle “Risorse di rete”
 - <http://www.bnro.de/~schmidjo/>





Componenti essenziali (lato client)

- smbclient
Un client ftp-like per connettersi a risorse remote ed operare su di esse
- smbmount / smbmount
Permette di montare dischi condivisi via SMB come parte del proprio filesystem

Vediamoli in azione...





Componenti essenziali (lato server)

- **nmbd** Svolge il ruolo di WINS e LMB (se eletto)
- **smbd** Eroga le risorse condivise e gestisce l'autenticazione degli utenti
- **smbpasswd** Definisce le password di rete degli utenti SMB e li mappa sugli utenti Unix
- **winbindd** Coopera con nmbd per l'autenticazione degli utenti su domain controller NT/2000





Configurazione del server

- Nella directory di configurazione
 - Il file di testo principale
 - smb.conf – definisce i parametri di funzionamento e le risorse da condividere
 - Con nomi definibili in smb.conf, ma tipicamente come segue, gli altri due file essenziali
 - smbpasswd – contiene gli account e le password
 - smbusers – contiene la mappatura tra nomi utente SMB ed i corrispondenti username Unix





Configurazione manuale

- Esempio di smb.conf essenziale

[global] ← Identificatore della sezione speciale
contenente i parametri globali

```
workgroup = METRAN
```

[test] ← Identificatore di una sezione che
definisce una risorsa condivisa

```
comment = For testing only, please
```

```
path = /usr/local/samba/tmp
```

```
read only = no
```

```
guest ok = yes
```





Configurazione manuale

- Creazione di un utente

```
[root@itsi root]# smbpasswd -a pippo
```

New SMB password:

Retype new SMB password:

User pippo does not exist in system password file (usually /etc/passwd). Cannot add account without a valid local system user.
Failed to modify password entry for user pippo

(deve già esistere sul sistema!)



samba Configurazione con SWAT

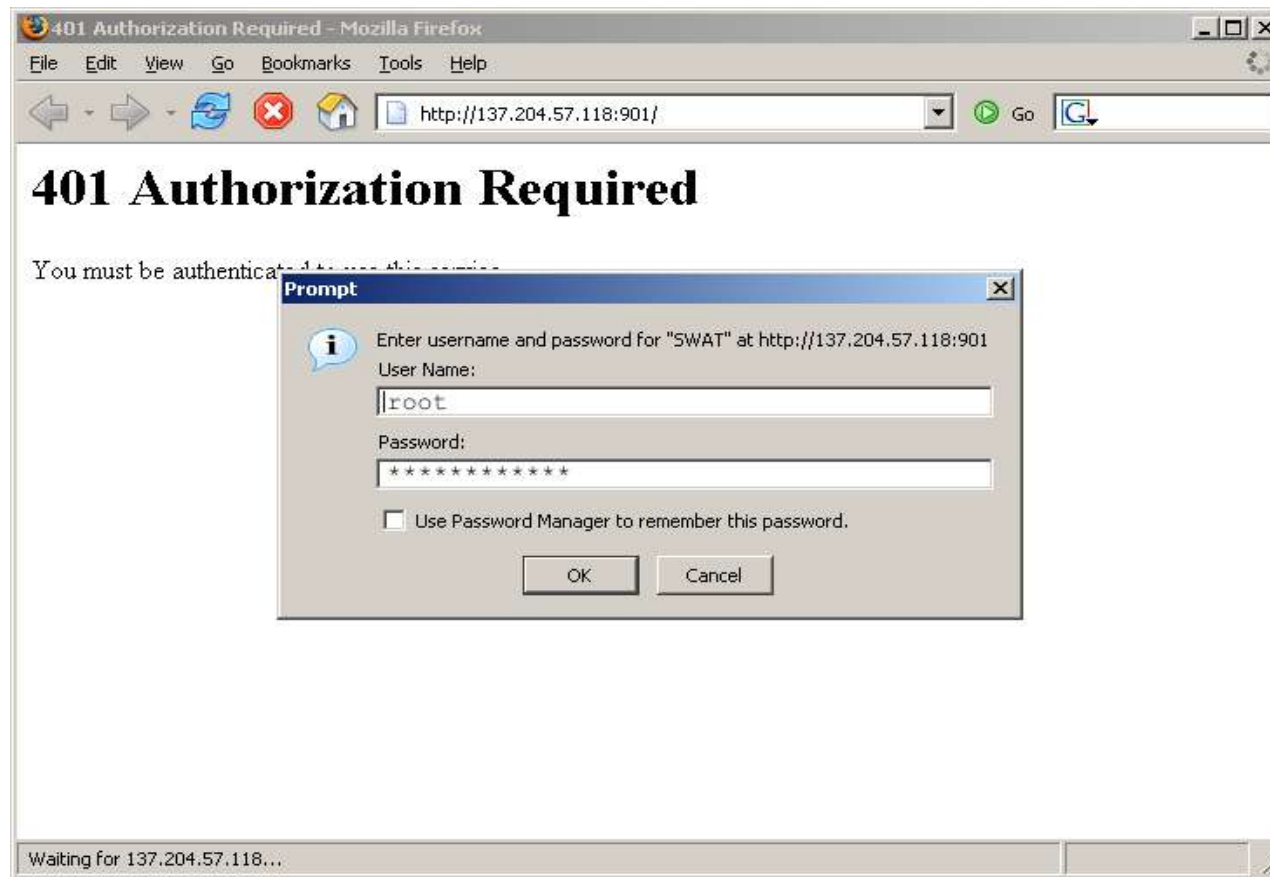
- Abilitazione del servizio: in `/etc/xinetd.d/` aggiungere il file *swat* contenente

```
service swat
{
    socket_type           = stream
    wait                 = no
    protocol             = tcp
    only_from            = localhost
    user                 = root
    log_on_failure       += USERID
    server               = /path/to/swat
    port                 = 901
    disable              = no
}
```



Configurazione con SWAT

- Login via web (porta 901) come root





Configurazione

- Parametri globali essenziali



- workgroup
- netbios name
- security

Guest mapping



Eventuali ACL per share

In ogni caso permessi Unix

- **SHARE** - autenticazione legata alla risorsa
- **USER** - autenticazione dei singoli utenti
 - SERVER - validazione degli utenti su altro server
 - DOMAIN - idem, ma il server Samba deve essere aggiunto ad un dominio con il comando *net*
 - ADS - idem, ma in AD (richiesto Kerberos)





Configurazione

- Parametri riguardanti directory condivise
 - path (directory locale da rendere accessibile)
 - elenchi di utenti ammessi/banditi/super
 - elenchi di client ammessi/banditi
 - accessibilità come utente guest
 - protezione dalla scrittura





Configurazione

- Parametri riguardanti stampanti condivise



- path (directory di spool)
- elenchi di client ammessi/banditi
- accessibilità come utente guest
- nome della stampante (come definita localmente)

- Nota: se esiste una sezione `[printers]` in `smb.conf`, le stampanti sono automaticamente importate dal file di configurazione del demone di stampa installato





Gestione



- Ogni modifica va inviata usando il pulsante “Commit changes” della relativa sezione
 - Effetto: aggiornare smb.conf
 - Le modifiche non sono attive finchè non si riavvia smb

Server Status

Auto Refresh

Refresh Interval:

version: 3.0.2-7.FC1

smbd: running	<input type="button" value="Stop smbd"/>	<input type="button" value="Restart smbd"/>
nmbd: running	<input type="button" value="Stop nmbd"/>	<input type="button" value="Restart nmbd"/>
winbindd: not running	<input type="button" value="Start winbindd"/>	<input type="button" value="Restart winbindd"/>
	<input type="button" value="Stop All"/>	<input type="button" value="Restart All"/>





Gestione



- Tutte le connessioni al server sono controllabili dal pannello Status ...

Active Connections

PID	Client	IP address	Date	Kill
4122	smbd	0.0.0.0	Fri May 13 18:47:50 2005	X

Active Shares

Share	User	Group	PID	Client	Date
prova	prandini	prandini	4126	deis121	Fri May 13 18:47:51 2005

- ... o con le utilità a riga di comando `smbstatus` e `smbcontrol`





Cos'altro (non) dire?

- Questa presentazione copre forse il 10% delle potenzialità di Samba 3! Ci sarebbe molto da dire su:
 - Realizzazione di un PDC con Samba
 - Gestione di filesystem distribuiti (NFS/DFS)
 - Gestione avanzata di autenticazione e ACL
 - Server virtuali, sincronizzazione, gestione della messaggistica Windows...





Risorse

- Il libro Open Source su Samba!
<http://www.oreilly.com/catalog/samba2/book/toc.html>
- Il sito ufficiale
<http://www.samba.org/samba/>
 - con un documento che insegna per esempi (molti e sofisticati):
<http://www.samba.org/samba/docs/man/Samba-Guide/>
 - e innumerevoli altri link, tra cui questo per approfondire il funzionamento di SMB
<http://www.samba.org/cifs/docs/what-is-smb.html>

