Reti miste

Giovanni Franza

Contenuti

- Scenario attuale
- Introduzione server Linux
- Strumenti
- Più forte e più allegro
- Condivisione dati
- Sicurezza

Scenario attuale

- Molte tecnologie
- Molte topologie
- Poche applicazioni
- Carenze note

Molte tecnologie

- Poco NFS da vecchi server Unix
- Decrescente NetWare da server anni '80/'90
- Poco AFS in realtà Apple
- Molto SMB da mondo Windows

Molte topologie

- Poco client/server (Unix, NetWare ed NT)
- Molto Peer to Peer (W95/W98/WME)

Poche applicazioni

- Molta condivisione dischi (disordinata)
- Non molta condivisione stampanti
- Poca condivisione internet

Carenze note

- Non diffusa gestione utenti/accessi/permessi
- Backup non diffuso ed a cura utente
- In grandi realtà problema propagazione virus

Introduzione server Linux

- Inizio nascosto
- Condivisione dischi
- Accesso ad internet

Inizio nascosto

- Aziende 'terrorizzate' da Linux percepito come difficile
- Necessità di server quindi compromesso 'hidden blackbox'

Condivisione dischi

- Centralizzazione dei dischi
- Politica di backup automatico
- Implementazione controllo accessi
- Topologia client/server
- Vendor independence

Accesso ad Internet

- Sostituisce sovente embedded proxy
- Inizia a realizzare filtri

Potenzialità

- Servire macchine differenti (Windows/Macintosh)
- Implementare una politica degli accessi
- Realizzare backup centralizzati

Strumenti

- Per piattaforma Windows: *Samba*
- Per piattaforma Macintosh: *Netatalk*

Usare Samba

- Installazione quasi di default con Linux
- Configurazione semplice: sia testo che web
- Opzioni globali ed opzioni di share

Opzioni globali

- Nome del server
- Gruppo di lavoro
- Crittografia
- Livello di browsing
- Server di dominio
- Wins server
- Usare dominio Windows

```
[global]
   workgroup = MGENG
   guest account = nobody
   keep alive = 30
   os level = 99
   kernel oplocks = false
   security = user
   encrypt passwords = yes
```

Crittografia

- Serve per le 'nuove' versioni di Windows
- Comandi per disabilitarli nella registry
- Comandi per gestire (**smbpasswd**)

```
[global]
   workgroup = MGENG
   guest account = nobody
   keep alive = 30
   os level = 99
   kernel oplocks = false
   security = user
   encrypt passwords = yes
```

Livello di browsing

- Tipo di imbustamento di SMB: in TCP/IP o in Ethernet
- Tutti i PC tendenzialmente cercano di divenire master browser
- Al cambio del master browser succede il finimondo
- Samba configurato per vincere: sui client o anche sui server

Usare il dominio (NT/2000)

- Configurare Samba per usare la validazione di NT

```
; Uncomment the following, if you want to use an existing
; NT-Server to authenticate users, but don't forget that
; you also have to create them locally!!!
;  security = server
;  password server = 192.168.1.10
; Uncomment this, if you want to integrate your server
; into an existing net e.g. with NT-WS to prevent nettraffic
;  local master = no
; If you want Samba to act as a wins server, please set to yes
   wins support = no
; If you want Samba to use an existing wins server,
; please uncomment the following line and replace
; the dummy with the wins server's ip number.
;   wins server = 192.168.1.1
; Do you wan't samba to act as a logon-server for
; your windows 95/98 clients, so uncomment the
; following:
;   logon script =%U.bat
;   domain logons = yes
;   domain master = yes
; [netlogon]
;   path = /netlogon
```

Utenti

- Disabilitare le shell
- La conversione di più utenti in uno solo con **`smbuser`**
- Utente guest

Accessi

- Validazione con user
- Validazione con Host
- Permessi sui file creati
- Mangle case / Preserve case

```
[Deposito]
   path=/salva
   comment = Salvataggi di ogni tipo
   browseable = yes
   read only = no
   create mode = 0777
```

Usare Netatalk

- Da installarsi a parte (opzione in installazione)
- Demoni che operano (**afpd**, **papd**)
- Configurazione dei volumi
- Configurazione delle stampanti

```
# volume format:
# :DEFAULT: [all of the default options except volume name]
# path [name] [casefold:x] [codepage:y] [options:z,l,j] \
#   [allow:a,@b,c,d] [deny:a,@b,c,d] [dbpath:path] [password:p] \
#   [rwlist:a,@b,c,d] [rolist:a,@b,c,d] [limitsize:value in bytes]
#
~
/home/Documents Documenti
```

Più forte e più allegro

- PC server attualmente usati come file e print/server
- Limite ma anche potenzialità
- Emergere di nuovi strumenti

Appliances (1)

- Computer con 'singola missione'
- Più performanti
- Meno esigenti su hardware
- Più sicuri

Appliances (2)

- Realizzabili facilmente con Linux
- Amministrabili da browser
- Esempi già in commercio (FileZerver Microtest e Lightning Multicom)

Home Made Appliances

- Esempio classico: LRP (*Linux Router Project*)
- Fa solo da router/firewall
- Altro esempio: LTSP (*Linux Terminal Server Project*)

Condivisione dati

- Come per i database: poca scrittura e molta memorizzazione / lettura
- Soluzioni come SMB/CISF/Appleshare richiedono autenticazione
- Stesse soluzioni bloccano le risorse

Problematiche

- Impegno di memoria
- Lock su dischi
- Definizione di molti utenti (problema di sicurezza)
- Necessità del montaggio di risorse condivise sul desktop del client

Soluzione

- Compromesso: solo chi deve scrivere utilizza SMB/Appleshare
- Tutti gli altri usano accesso via web

Risultati

- Meno risorse impegnate (=meno RAM necessaria)
- Meno utenti da impostare sul server
- Nessuna necessità di montaggio di risorse condivise
- Web server limitabile a fornire pagine e quindi molto più sicuro (niente cgi)

Sicurezza

- Server proxy
- Filtri e-mail

Server proxy

- Evita di richiedere più volte la stessa pagina quindi aumenta le prestazioni
- Può filtrare pagine pericolose (`.eml`, `.nwl`) per parare alcuni meccanismi di attacco
- Può tenere traccia dei collegamenti effettuati

Filtri e-mail

- Bonus: *open source* è visibile per definizione, quindi i meccanismi sono semplici da verificare
- Implementabili filtri che parcheggiano file eseguibili o che azzerano estensioni pericolose