EUGENIO MEDEA

ASSOCIAZIONE la Nostra Famiglia

Gestione di una rete Windows con software libero: L'esperienza della associazione *La Nostra Famiglia*

Dott. Marco Gaiarin

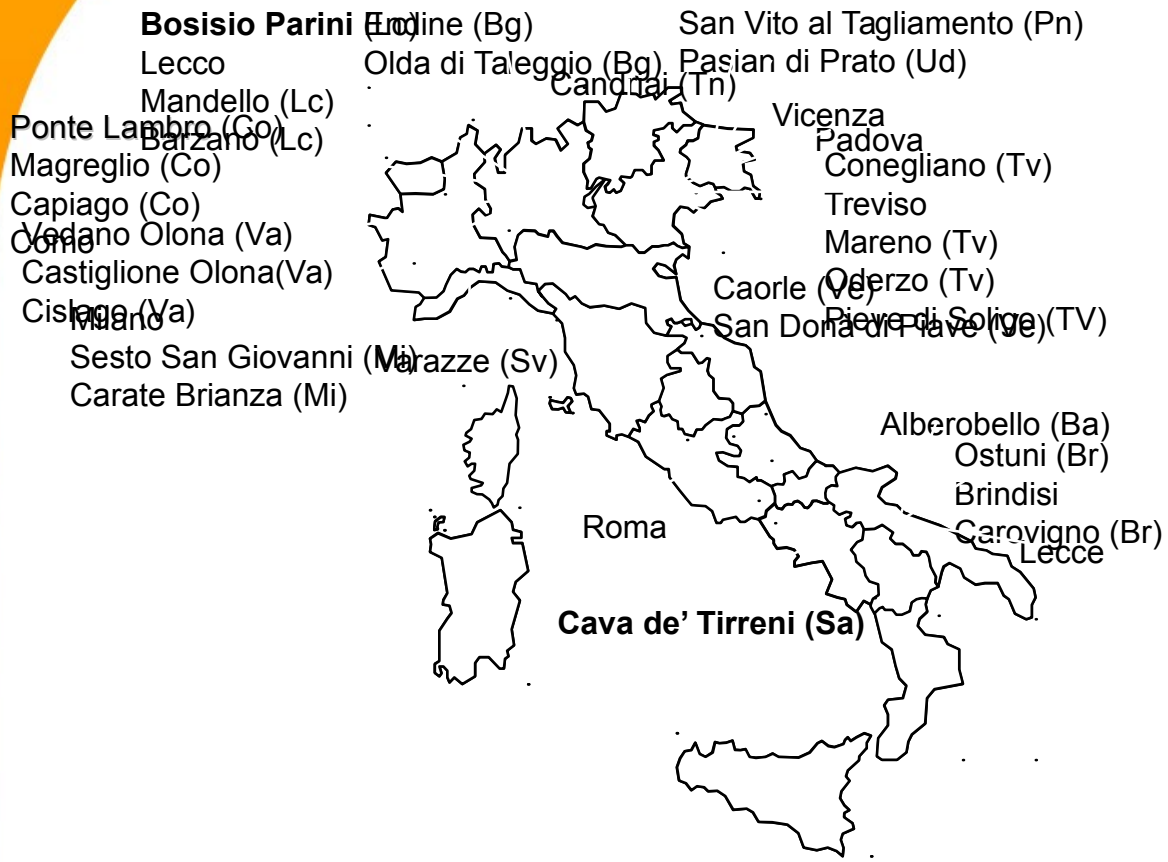
Responsabile Informatico Polo FVG

marco.gaiarin@lanostrafamiglia.it

La LNF

- Ci preoccupiamo che ad ogni bambino che parte in situazione di svantaggio sia data la possibilità di **sviluppare pienamente le sue potenzialità**.
- Obiettivo fondamentale di ogni nostro intervento è la **qualità della vita** della persona disabile e della sua famiglia.

LNF Dove?



- 36 sedi in Italia
- 3 sedi in FVG
- Presente nel mondo con la NGO *OVCI*
- IRCCS *Eugenio Medea*

LNF CED

- Un CED organizzato in 4 poli (FVG, Veneto, Lombardia, Puglia) fortemente coordinati tra loro
- Una forte tradizione UNIX, ottime competenze e ben distribuite
- La scelta dello sviluppo interno, e una naturale tendenza all'*hacking*
  - Postgres, PHP
  - Asterisk (Elastix)
  - Samba!
  - Contribuiamo alla comunità (esempio: WVIOLA)
- Non siamo piccoli!
  - Oltre 2000 PC con Windows
  - Oltre 50 server (Debian/CentOS/Fedora/…)

Menù

- Perché siamo qui?
- Un po' di teoria
- Dove eravamo rimasti? Dominî NT4
- Alcune note sui Dominî AD
- Alcune peculiarità di Windows 7
- Mettiamo assieme i pezzi
- Conclusioni

Perché?

Ma se funziona, perché cambiare?

- L'8/4/2014 scade il supporto a Windows XP: http://windows.microsoft.com/it-it/windows/end-support-help
- Il Decreto legislativo 30 giugno 2003, n. 196 (la *Privacy*), allegato B (disciplinare tecnico), punto 17, impone l'aggiornamento: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184
- Io tratto dati sensibili, quindi ho circa un anno di tempo per *fare le scarpe* a XP.
- Bisogna cambiare!!!

Teoria

- NetBIOS, NetBEUI, NetBIOS over TCP/IP (NBT)
  - Servizi di risoluzione a nomi: Broadcast, NetBIOS Name Server (NBS), o WINS
  - Servizi di trasporto: SMB o CIFS

  Servizi di base per una rete locale: risoluzione dei nomi, autenticazione (utente e computer), condivisione file e stampanti, RPC, gestione del *dominio* (flat): ridondanza, relazioni di trust, policy utente e macchina.
- Active Directory
  - Servizi di risoluzione a nomi: DNS, DHCP
  - SSO: Kerberos
  - Gestione: LDAP
  - Servizi di trasporto: SMB o CIFS

  Servizi avanzati per una rete locale, ma inserita in una contesto che può essere fortemente gerarchizzato; tutta la gestione avviene con il modello *Directory* (oggetto all'interno di un albero strutturato).
- Dominî *di tipo NT* e Dominî *di tipo AD*: ancora tutti i SO client (di classe professional) sono compatibili con entrambe le tipologie.

NT4

- Samba3 replica perfettamente (salvo qualche RPC) le funzionalità dei dominî di tipo NT
- Windows XP, pur supportando i dominî di tipo AD, è ancora perfettamente compatibile con quelli NT (e quindi con Samba3)
- Cosa era stato fatto?
  - DNS, DHCP e NTP a parte
  - LDAP come base account; sincronizzazione delle informazioni account (la scadenza!) per tramite di script, quasi un SSO. ;) *En passant*, fornisce gratis la ridondanza
  - Policy vecchio stile (NTConfig.POL), solo utente (alla fin fine: dimensione del roaming profile e screensaver)
  - Gestione delle macchine per altre strade (WPKG)
  - Wiki interno per documentare tutto

AD

- Praticamente tutto è cambiato, ma principalmente:
  - Permette di gestire realtà fortemente strutturate/gerachizzate in modo molto semplice, il salto dalle relazioni di trust è abissale
  - Anche la gestione ha fatto un salto di qualità abissale, dal meccanismo grezzo delle policy di tipo NT al nuovo meccanismo dei Group Policy Object (GPO)
- Samba4 supporta pienamente l'architettura dei dominî di tipo AD: perché non usarlo?
  - Le cose sono cambiate parecchio, non ho avuto il tempo di studiare bene; manca ad ogni modo documentazione
  - *Ha venduto l'anima al nemico*! Per poter raggiungere un livello di compatibilità decente ha dovuto reimplementare buona parte dei componenti (in particolare LDAP e DNS) violando la regola KISS! di UNIX
  - Per la gestione è necessario comunque utilizzare i tool Microsoft (o di terze parti con questi compatibili)

Win7

- Anche qui, parecchi cambiamenti sotto al cofano, ma in particolare:
  - Architettura 32 e 64bit: già presente da XP, ma ormai sta diventando lo standard
    - gioie e dolori del layer di compatibilità (SysWOW64)
    - *carinerie* dei driver di stampa 32/64bit
  - Passaggio ai profili in roaming *versione 2*: se qualcuno mi spiega come si usano i tool di migrazione…
  - Già da Vista, invero, è stata abbandonata la compatibilità alle policy di tipo NT: l'interessante presenza dei MLGPO, e qualche minimo tool di gestione
  - Curiosità: in Windows 7 non si può più cercare nel contenuto dei file nei dischi di rete (iFilter, Windows Search, …)
- E Windows 8?

Fatto

- L'esistente installazione di WPKG è stata estesa e rimaneggiata in modo da:
  - Essere compatibile a un ambiente misto 32/64bit
  - Applicare la parte di sistema delle GPO direttamente via script/patch al registry
  - Applicare la parte utente delle GPO via MLGPO (GPOPack) e netlogon script (marginalmente)
    - Limitazioni al profilo roaming e screensaver
  - Installare componenti aggiuntivi e di terze parti per aggirare le limitazioni/feature
- Microsoft fornisce una tabella di conversione tra GPO e registry
  http://www.microsoft.com/en-us/download/details.aspx?id=25250
  e il tool LocalGPO
  http://gallery.technet.microsoft.com/LocalGPOmsi-Excellent-MS-2593b2eb
  che permettono di fare queste cose.
- Alla fine quello che si ottiene è un dominio *di tipo NT*, ma che supporta le macchine Win7 per un insieme di funzionalità comparabili a quelle del vecchio sistema NTConfig.POL

LocalGPO

- La funzionalità Multiple Local Group Policy Object permette di definire delle GPO locali (LGPO) associate a utenti e gruppi **locali**.
- LocalGPO permette di *esportare* la LGPO, anche in modo *autoinstallante* (GPOPack) e applicarla selettivamente a utenti e gruppi locali (tra cui i gruppi Administrators e Users).
- In pratica:
  - Si prende una macchina campione, si definisce una LGPO, la si esporta in una GPOPack
  - Si ripete l'operazione per ogni utente/gruppo/macchina/…
  - Si applica selettivamente la GPO, e valgono ovviamente le regole di applicazione delle GPO (non c'è *tattoo effect*)

  L'applicazione selettiva è per gli utenti; per questo è preferibile usare altri metodi (patching diretto del registry e scripting) per le GPO macchina.
- Concretamente: ho una LGPO per Users e un override per l'utente Administrator (non il gruppo Administrators).

LocalGPO/Esempio

Una volta impostata una certa policy, l'esportazione può avvenire con i comando:

```
LocalGPO.wsf /path:%TEMP% /export /GPOPack:Esempio
```

questo comando crea nella cartella %TEMP% una cartella Esempio con dentro la policy (sia user che host, si badi bene) e i file necessari alla sua applicazione; una volta trasportata su un altro PC (può essere trasferita, zippata, … il tutto a piacere) è possibile applicare la policy (solo la parte utente) ad esempio con:

```
GPOPack.wsf /MLGPO:Users
```

ovvero la policy viene applicata a tutti gli utenti non-amministratori della macchina, oppure:

```
GPOPack.wsf /MLGPO:pippo
```

ovvero la policy viene applicata all'utente locale pippo.

Varie

- A parte l'aggiornamento ad una versione Win7 compatibile di Samba, quasi nulla è cambiato lato server
- Dopo aver provato i tool di migrazione del profilo di Microsoft, alla fine abbiamo optato per la copia manuale dei file (grazie Firefox e Thunderbird!), approfittando per redirezionare quante più cartelle possibili fuori dal profilo
- Il problema della ricerca nei file è stato alla fine risolto con un tool esterno, FileLocator Lite, purtroppo *free as in beer*
  - Eventualmente potrebbe essere interessante valutare un servizio, magari web-based…
- L'occasione fa il sysadmin libero: installazione di massa di LibreOffice in sostituzione di MSOffice 2003; in via *sperimentale*, ma inserito all'interno dell'*upgrade path*

Conclusioni

- L'obiettivo di *far funzionare* Windows 7 è stato raggiunto, e senza complicare troppo le cose
- Tutti i principali problemi sono stati affrontati e risolti, imparando molte cose nuove
- É stato fatto un passo ulteriore verso il software libero, anche se in modo molto opportunistico

- La gestione delle Isole/Sedi è sotto revisione, quindi nulla toglie che questo sia solo un passaggio (o un prendere tempo ;-) verso AD/Samba4

Quindi, alla prossima puntata…