Samba/ Active Directory

Samba/Active Directory

...una esperienza concreta di migrazione multidominio da Samba/NT a Samba/AD

Dott. Marco Gaiarin
SIR Associazione La Nostra Famiglia, Polo FVG
marco.gaiarin@lanostrafamiglia.it

IRCCS EUGENIO MEDEA

ASSOCIAZIONE la Nostra Famiglia

L'Associazione la Nostra Famiglia si dedica alla cura e alla riabilitazione delle persone con disabilità, soprattutto in età evolutiva.
Dispone di una vasta rete di strutture di riabilitazione: è presente in 6 Regioni italiane e collabora con l'Organismo di Volontariato per la Cooperazione Internazionale (OVCI) in 5 Paesi del mondo;
Si prende cura di bambini e ragazzi, sia con quadri patologici di estrema gravità (come gli stati vegetativi e le pluriminorazioni), sia con situazioni meno gravi, a rischio psicopatologico o di svantaggio sociale.

La Nostra Famiglia si occupa di:

- ricerca scientifica e studio delle problematiche mediche, psicologiche e psicoeducative delle varie disabilità, attraverso l'attività dell'Istituto Scientifico "Eugenio Medea";
- accoglienza di bambini con grave disagio familiare in attesa di affido o adozione, bambini e adolescenti soli o con disagio socio-ambientale in piccole comunità o in nuclei di tipo familiare;
- gestione di centri diurni e residenziali per persone adulte con disabilità;
- formazione professionale e universitaria di operatori dei servizi alle persone;
- sensibilizzazione e promozione della cultura dell'inclusione sociale

http://www.lanostrafamiglia.it/

Ringraziamenti

- LNF
- Rowland, Louis e tutta la lista samba
- Andrea Zwirner/LinkSpirit

Menù

- Il punto di partenza...
- Breve intro storico/tecnologica
- Come installare un dominio AD con Samba
- Cosa ho fatto io
- Sitografia

Situazione...

- Samba3
  - ottima documentazione
  - aderenza totale alla filosofia UNIX
  - ottimo supporto nella lista italiana di Samba
- Samba4
  - wiki, di difficile fruibilità senza punti di riferimento (come tutti i wiki...)
  - alcune scelte di fondo (che sembrano) in totale rottura alla filosofia UNIX
  - lista samba italiana silente...
- Il coraggio di (ri)allacciare alcuni **collegamenti** e ridare **spirito** a un povero sysadmin affranto...

SMB

- Servizi di condivisione file e stampanti, risoluzione in rete locale, IPC
- SMB/CIFS/SMB 1
  - SMB (IBM, 1983) + LAN Manager (MS + 3Com per OS/2, 1990)
  - Inizialmente con un protocollo di rete a se (NetBEUI), ora sostanzialmente solo su TCP/IP (NetBIOS over TCP/IP, NBT)
  - Altamente inefficiente, specie non in LAN
- SMB 2 (2006, Vista/Server 2008)
  - Profonda revisione, molto più efficiente, protocollo proprietario ma con specifiche pubbliche (grazie Europa!)
- SMB 3 (2012, 8/Server 2012)
  - Cifratura

Dominio (di autenticazione)

- Workgroup
  - Ogni scelta è locale
  - Qualche automatismo (del client)
- Dominio di tipo NT
  - 1993, SMB 1 + estensioni, successore di LAN Manager (NTLM)
  - Flat (LAN: broadcast o WINS), single master
- Dominio Active Directory
  - In buona sostanza: CIFS + Kerberos + LDAP + DNS + NTP
  - Completamente gerarchico, multimaster
- Samba ovviamente supporta tutte queste modalità.

Dominio (di gestione)

- NT aveva le Policy
  - Dismesse da Vista+
  - Tattoo effect
- AD ha le GPO
  - Attivamente utilizzate, molto anche da terze parti, anche FLOSS
  - Distinzione Policy/Preferenze
  - Meccanismo di applicazione molto articolato (utente/host/sito, filtri sui gruppi, …)
  - Anche se può fare molte cose, solitamente usato per le impostazioni
- Meccanismi di applicazione locali: MLGPO
- In generale io resto scettico
  - Preferisco sistemi autodocumentanti, come Ansible/WPKG

Per chi viene da Samba3...

- Samba3/NT: Samba come tecnologia gateway tra POSIX e Windows
  - Rapporto 1=1 tra utenti e gruppi
  - Molte feature ottenute solo con backend LDAP
- Samba4/AD: L'approccio in un qualche modo *ribaltato*, POSIX appoggiato a Samba
  - Alcune differenze non facilmente colmabili (ID_BOTH *transgender*, nested group, forte gerarchizzazione, ...)
  - Molto complicato l'utilizzo diretto di LDAP(+Kerberos)...
  - Differenza tra DC e DM estremamente marcata
- Richiesto un cambio di mentalità

Perché?

- Il supporto a NT è ufficialmente dismesso da Microsoft, lo sarà a breve da Samba
- Microsoft ripetutamente rompe il supporto a NT con le sue patch (poi sistema, ma...)
- Per poter utilizzare i dominii di tipo NT è necessario abilitare SMB1 negli SO client Microsoft
  - SMB1 è insicuro
  - SMB1 è lento
- Gestire una rete senza GPO non è facile
- Si imparano tante cose nuove...

Punto sulle feature di Samba

- Supporto completo ad AD
  - Domain level a Windows Server 2008R2
  - Schema level a Windows Server 2012R2
- Feature mancanti o incomplete
  - DFS (ma serve un altro FS replicato a Linux?)
  - Foreste (join tra dominii OK, il problema dell'enumerazione dei gruppi)
- Noticine
  - Essendo una gestione multidominio, le login sono domainful…
  - Utenti e gruppi che è meglio che *non esistano…* AD, RID e xID, ID_BOTH e ACL/ATTR: NIENTE PANICO! ;-)

Ipotesi

- Dominio: ad.iononesisto.it/IONONESISTO
- DC e DM separati
  - Il codice è molto diverso, sono quasi due cose diverse...
  - Anche Microsoft lo consiglia, anche per questioni di efficienza (il traffico verso un DC è cifrato)
- Questo implica la virtualizzazione!
  - Ovviamente proxmox, i DC in Container LXC
- La migrazione *in place* (classicupgrade) ha delle controindicazioni (mapping da rivedere, unicità tra utenti e gruppi, ...) e induce una forte discontinuità (*o la va o la spacca* ;); poi, abbiamo 4 dominii da trasformare in uno solo...

  Procediamo per sovrapposizione...

Ipotesi/2

- Usiamo RFC2307, ovvero il mapping degli ID in LDAP
  - Pro: posso alla bisogna usare utenti che non hanno dati POSIX (lo facevo anche prima...)
  - Con: devo stare attento a **NON** mappare ID_BOTH
- In alternativa: RID
- Usiamo come backend DNS bind (BIND9_DLZ) e non il DNS interno (INTERNAL_DNS)
  - Utilizziamo come dominio un sottodominio dell'attuale (stile: ad.iononesisto.it)
  - Configuriamo correttamente il sottodominio integrandolo nell'attuale (la risoluzione DNS **DEVE** funzionare!)
- Per ora lasciamo fuori DHCP (supponiamo esista e non sia coinvolto)
- Usiamo i repository Debian di Louis (comunque, **non** RH-based)

Installazione

```
apt-get install samba winbind libnss-winbind libpam-
winbind libpam-krb5 acl attr krb5-config krb5-user krb5-
doc ldb-tools smbclient
```

- Spegnamo e riconfiguriamo i servizi:

```
systemctl stop samba smbd nmbd winbind samba-ad-dc
systemctl mask samba smbd nmbd winbind
systemctl disable samba smbd nmbd winbind
systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc
```

- Eliminiamo la configurazione di default (a voi il backup):

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.dist
rm /var/cache/samba/printing/*
rm /var/cache/samba/*
rm /var/lib/samba/*.tdb
mv /etc/krb5.conf /etc/krb5.conf.dist
```

Installazione/bind

```
apt-get install bind9 bind9utils dnsutils
```

- Configurare la coerenza con il DNS esistente (esercizio...)
- Modificare **`/etc/bind/named.conf.local`**:

```
// Includo la configurazione per Samba in modo AD
//
include "/var/lib/samba/private/named.conf";

// Per la modifica dinamica del DNS via Kerberos,
// è necessario aggiungere la chiave.
//
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
```

- Modificare **`/var/lib/samba/private/named.conf`** di modo che carichi la corretta versione della libreria dinamica, rispetto alla versione di bind
- Permettere query e recursion a piacere

Installazione/NTP

```
apt-get install ntp ntpdate
```

- Configuare la coerenza con eventuali gerarchie interne di server (esercizio...)
- Creare la pipe:

```
mkdir -p /var/lib/samba/ntp_signd/
chmod 750 /var/lib/samba/ntp_signd
chown root:ntp /var/lib/samba/ntp_signd
```

- In **`/etc/ntp.conf`**:
  - Aggiungere alle righe "`restrict -4 default …`" e "`restrict -6 default …`" l'opzione "`mssntp`"
  - Aggiungere:

```
# Location of the samba ntp_signed directory
#
ntpsigndsocket /var/lib/samba/ntp_signd
```

Nuovo dominio/Primo DC

```
samba-tool domain provision \
  --server-role=dc --use-rfc2307 \
  --dns-backend=BIND9_DLZ \
  --realm=AD.IONONESISTO.IT \
  --domain=IONONESISTO
```

- In buona sostanza specifico il nome del dominio, l'utilizzo di RFC2307 e il backend BIND9_DLZ per il dns
- Se tutto procede come deve essere, alla fine il sistema sputa la configurazione del dominio (nome, SID, password di Administrator)
- Di default, si cucca tutti i ruoli FSMO

Join a un dominio/Ulteriori DC

- Ovviamente il primo DC deve essere funzionante!
- Se ho già abilitato le verifiche di complessità delle password, meglio disabilitarle:
  `samba-tool domain passwordsettings set --complexity=off`
  e ovviamente riabilitarle in seguito
- `samba-tool domain join ad.iononesisto.it DC \`
  `-U 'IONONESISTO\Administrator' --dns-backend=BIND9_DLZ \`
  `--option='idmap_ldb:use rfc2307 = yes'`
- Notare che:
  - Non specifico un altro dc, il dns deve funzionare!
  - Esplicito BIND9_DLZ, ovviamente (ha poco senso avere alcuni DC su bind e altri su INTERNAL...)
  - Esplicito RFC2307, non c'è modo di saperlo interrogando altri DC!
  - L'aggiunta di un DC comporta il reload di bind su tutti gli altri DC, ma... il reload non funziona! ;-)

Join/2

- È necessaria la replica del SYSVol tra tutti i DC.
  - Di default i tool che operano in scrittura sul sysvol, lo fanno sempre sul DC con i ruoli FSMO
  - Non serve in tempo reale! Un rsync con le opzioni `-XAazq --delete-after` basta ed avanza...
  - Più che altro, se si spostano i ruoli FSMO...
- Occorre anche replicare, una tantum, gli xID per evitare rogne nell'applicazione delle ACL:

```
# Sul DC con ruoli FSMO
tdbbackup -s .bak /var/lib/samba/private/idmap.ldb
# …copia del file idmap.ldb.bak sull'altro DC…
cp idmap.ldb.bak /var/lib/samba/private/idmap.ldb
net cache flush
```

- Ovviamente si può automatizzare il tutto (esercizio per casa)

Abbiamo finito!

- Configurazione di Kerberos
  `cp /var/lib/samba/private/krb5.conf /etc/krb5.conf`
- Configurazione di NSS/PAM:
  - PAM: autoconfigurato
  - NSS: un DC legge da RFC2307 solo UID/GID; necessario aggiungere in `/etc/samba/smb.conf`:

    ```
    # Aggiungo i parametri di default per winbindd
    template shell = /bin/bash
    template homedir = /home/%U
    ```

    Oltre ovviamente aggiungere `winbind` come provider per i contesti `passwd` e `group` in `/etc/nssswitch.conf`.
- (ri)avvio del servizi (reboot...)
- Test:
  - `samba-tool dbcheck --cross-ncs`
  - `samba-tool drs showrepl`
  - Join e logon da una workstation

Gestione

- smbpasswd/pdbedit/wbinfo/net: in disarmo
- samba-tool: the swiss army knife!
- ldb* (abituarsi a usare query LDAP…)
- Microsoft RSAT
  - ADUC, GPMC, ADSS
  - .Net, PowerShell, ...
- LAM (LDAP Account Manager)

Percorso/1

- Letto molto, in particolare molta teoria per farsi un quadro…
- Con l’aiuto di un consulente esterno, pianificato l’aggiornamento e risolto qualche problema *di base…*
- Tirati su i nuovi DC
  - A meno di scelte scellerate, i due dominii possono convivere tranquillamente…
- Importata la base utenti
  - Normalizzata
  - Creato script di importazione (si, trovo errori ancora oggi ;-)
  - Grazie agli hook `check password script` (NT) e `samba-tool user syncpasswords` (AD) è stata realizzata una sincronia delle password quasi in tempo reale
- Ricreati e riassociati i gruppi d’utenza
  - L’occasione fa l’uomo ladro ;-)

Percorso/2

- Tirato su un DM per Home e Profili (e WPKG)
- Laboratorio
  - Testing del dominio (logon, profilo, autenticazione, …)
  - Testing delle GPO
    - Configurati come share i vecchi server!
    - Creazione dei siti
  - Testing di WPKG
- Predisposizione script di migrazione dei dati degli utenti (Home; Profilo al solito si sta prima a mano…)
- (Finito di) Tirato su un DM per sito

Percorso/3

- Pianificazione e spostamento lotti di PC/Utenti dal vecchio al nuovo domino, per gruppi uniformi o siti
  - Maledetto antivirus!
- Spostamento/migrazione dell'autenticazione dei sistemi da LDAP ad AD/Kerberos
  - Uno alla volta, con tutta calma…
- Tirato su, ove necessario, eventuali altri DM
- Migrazione dati da vecchi a nuovi server/share principali
- Spostamento dei servizi di base allocati sui vecchi server: DNS, DHCP, Proxy, Radius, …
- Spento i vecchi server

Documentazione/1

- AD
  - What is Active Directory?
  - Pianificazione e progettazione di Active Directory Domain Services
- Kerberos
  - Designing an Authentication System: a Dialogue in Four Scenes
  - How the Kerberos Version 5 Authentication Protocol Works
- GPO
  - Criteri di gruppo per principianti
  - Group Policy Planning and Deployment Guide

Documentazione/2

- Samba
  - Samba Wiki
  - Lista internazionale samba (non mordono! ;-)
  - Lista italiana samba-it
- Debian
  - Repository di Louis
  - Script e documentazione di Louis
- Per i deboli di cuore c’è sempre Zentyal o Univention Corporate Server

Domande?