
Samba/
Active
Directory

Samba/Active Directory

...ovvero sul come abbandonare la nostra comoda casa ed entrare in terre inesplorate...

Marco ‘gaio’ Gaiarin
Pordenone Linux User Group
gaio@linux.it

Ringraziamenti

- Rowland, Louis e tutta la lista samba
- Andrea Zwirner/LinkSpirit
- Pordenone Linux User Group
- Associazione La Nostra Famiglia, polo FVG
- ISIS Mattiussi-Pertini di Pordenone
  - 1100 studenti, 120 docenti
  - 150 PC

Menù

- Home UNIX home...
- Breve intro storico/tecnologica
- Nelle terre inesplorate...
- Installare un controller di dominio
- Installare un membro di dominio
- Note di gestione
- Classicupgrade?
- Sitografia

Home UNIX home...

- Samba3
  - ottima documentazione
  - aderenza totale alla filosofia UNIX
  - sviluppo *lento*
  - ottimo supporto nella lista italiana di Samba
- Samba4
  - wiki, di difficile fruibilità senza punti di riferimento (come spesso capita ai wiki...)
  - alcune scelte di fondo (che sembrano) in totale rottura alla filosofia UNIX: il mio caro OpenLDAP...
  - sviluppo rapidissimo!
  - lista samba italiana silente...

Home UNIX Home.../2

- *Modo NT*: Samba come tecnologia gateway tra POSIX e Windows
  - Singolo dominio (+ relazioni di trust)
  - Rapporto 1=1 tra utenti e gruppi
  - Molte funzionalità ottenute solo con backend LDAP (spirito UNIX!)
- *Modo AD*: L'approccio in un qualche modo *ribaltato*, POSIX appoggiato a Samba
  - Alcune differenze non facilmente colmabili:
    - Multidominio, gerarchia, nested groups, ...
    - ID_BOTH, gli oggetti transgender...
  - Molto complicato l'utilizzo diretto di LDAP(+Kerberos)...
  - Differenza tra DC e DM estremamente marcata

Tech: SMB

- Servizi di condivisione file e stampanti, risoluzione in rete locale, IPC
- SMB/CIFS/SMB 1 (History of SMB Project)
  - SMB (IBM, 1983) + LAN Manager (MS + 3Com per OS/2, 1990)
  - Inizialmente con un protocollo di rete a se (NetBIOS over ethernet Framed, NBF o anche NBX), 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

Tech: 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 (ma Flexible Single Master Operation)

Tech: 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

Nelle terre inesplorate?

- Il supporto a NT è ufficialmente dismesso da Microsoft (server), lo sarà a breve da Samba
- Microsoft (client) 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 un dominio con le GPO è più facile
- Molte cose *funzionano* con AD…
- È sempre bello imparare cose nuove!

Nelle terre inesplorate!

- 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)
- E il browsing?
  - Rimosso da SMB2+, WSDD

Nelle terre inesplorate!/2

- Nella gestione di utenti e gruppi…
  - Essendo una gestione multidominio, le login sono per definizione domainful…
  - Namespace condiviso tra utenti e gruppi…
  - Posso mappare esplicitamente (AD/RFC2307) o implicitamente (RID)
  - Per certi share è impossibile usare il mapping tra ACL Windows e ACL POSIX
    - gli oggetti in crisi di identità, ID_BOTH
    - acl windows salvate come attributi estesi, direttamente in formato SDDL
  - Nei domain controller deve esistere una sorta di mappa implicita automatica, gli xID
  - Questo implica che alcuni utenti e gruppi **non devono essere mappati**!

Nelle terre inesplorate!/3

- 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)
  - Facile per il backup!
- Questo implica la virtualizzazione!
  - Ovviamente ProxmoxVE, i DC **NON** in Container LXC (gli Unprivileged container NON supportano alcuni attributi estesi)!
- NIENTE PANICO! ;-)

DC/Intro

- 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; nome del dominio IONONESISTO)
  - 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)

DC/samba

```
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
```

DC/bind

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

- Configurare l'integrazione con il DNS esistente (esercizio...)
- Modificare **`/etc/bind/named.conf.local`** (alla fine del file):

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

  e invece in **`options{}`**:

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

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

DC/NTP

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

- Configuare l'integrazione 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
```

DC/bootstrap

```
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

DC/ulteriori

- 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! ;-)

DC/ulteriori/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)
- Se schema/domain leve sono compatibili, posso convivere/migrare da/verso un DC Microsoft

DC/fine

- 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

DM/intro

- Un domain member è qualsiasi cosa che non è un DC, dalla workstation al fileserver. Sarò generico.
- Occorre installare le stesse cose di un DC, ma i servizi sono configurati già correttamente (i vecchi smbd, nmbd e winbind).
- Occorre avere DNS e sincronizzazione oraria (client) funzionante.
- Occorre inserire in `smb.conf` una mappa degli ID coerente con il dominio, ad esempio in `[globals]`:

```
idmap config * : backend = tdb
idmap config * : range = 5000-9999
idmap config IONONESISTO : backend = ad
idmap config IONONESISTO : range = 10000-49999
idmap config IONONESISTO : schema_mode = rfc2307
idmap config IONONESISTO : unix_nss_info = yes
idmap config IONONESISTO : unix_primary_group = yes
winbind use default domain = yes
```

DM/Join

- Occorre configurare Kerberos (basta il realm in fase di installazione)
- Ancora in smb.conf in `[globals]`:

```
security = ADS
workgroup = IONONESISTO
realm = AD.IONONESISTO.IT
```

- Join!

```
net ads join -U Administrator
```

- Occorre configurare winbind in PAM/NSS
- Poi ovviamente occorre configurare gli share e le stampanti, ma li la vecchia documentazione va ancora bene.

Kerberos

- Keytab, Service Principal Name
- Molti servizi sono *Kerberizzabili*...
- Un territorio ancora più inesplorato... ma agli effetti pratici non indispensabile (si può usare winbind/PAM).

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)

Classicupgrade?

- 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* ;); e permette di migrare un dominio solo...
- Ma i dominii possono convivere nella stessa rete... possibile procedere per sovrapposizione...
- Parallelo: questa è l'esperienza di migrazione completata al lavoro, e in corso a scuola. La consiglio senz'altro.

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, Univention Corporate Server o NethServer.

Domande?