Playing with AD Domains (not the Windows Way)

-

SambaXP 2017

- *Denis Cardon, Vincent Cardon*

Tranquil IT Systems

- IT support company
- since 2002, in Nantes, FRANCE
- 15 employees
- both small (outsourcing) and large (contracting) clients

TIS and SaMBa

- a long love story
  - 2004 first client on SaMBa3 PDC NT4
  - 2011 first client on SaMBa-AD
  - leading SaMBa-AD integrator in France (it's google.fr that says it :-)
- SaMBa very popular in France
  - free as in beer syndrom ?
  - free as in speech syndrom ?
  - Général de Gaulle syndrom ?

- some feedback

Our experience 1/4

- Installation and configuration is now soooo easy (IMHO :-)
- You are doing too much of a good job
- The main issues for simple deployments
  - basic networking skills → fire the sysadmin
  - basic AD skills → fire the sysadmin
  - basic linux skills → make samba AD run on windows ? → fire the sysadmin

Our experience 2/4
Bridging Windows and Linux...

- SaMBa is not only a bridge
  - AD integration for BOTH Windows and Linux
  - SMB protocol from Linux TO Linux
- no more
  - Nightmare File System
  - basic ldap bind auth
  - NIS...
- Better identity management

Our experience 3/4
SaMBa-AD and security

- Cisco Anyconnect 802.1x OK
- LAPS : OK
- Rights delegation : OK
- Software Restriction Policies (SRP/AppLocker) : OK
- RODC almost there, 4.7 ?
- KRB5 encryption type restriction:
- DCE-RPC port restriction:

Our experience 4/4
Samba and scalability

- 5000+ desktops
- 90 domain controlers
- Huge performance improvements in 4.6
- Even more improvements coming in 4.7...

- ex. : French Ministry of Culture : almost finished from 170 large and small domains to consolidated 13 domains. 170 sites

- Samba is ready for most domain
- We need to migrate them

SaMBa standard migration strategies 1/2

- SaMBa classicupgrade great for NT4 to AD
  - Simple and effective scripts
  - Easy to use

But

- Sometime takes to many attributes (arrrgh! mungeddial)
- 1 shot migration only

SaMBa standard migration strategies 2/2

- MS AD to Samba AD through join
  - Easy to setup

But

- Tricky for win2k / doesn't work for win2k12
- Migrate all what you want,
  - AND all the junk accumulated...
- Cannot rename domain
  - VIPs like rebranding

- need to go further

Server Side
Migration «LDB style» 1/3

- Domain rename
- Domain merge
- Win2k12 forest level migration
  - clone-dc-database
  - re-inject users !
- We cannot use most of Microsoft migration tools

Server Side
Migration «LDB style» 2/3

- Samdb and python-ldb are your friends
  - APIs are not hidden
- Scriptable with python
- Migration with same SID
  - recreate domain with same SID
  - re-create user
  - inject SID
  - set-nt-hash
  - rejoin / move computers to the new domain

Server Side Migration «LDB style» 3/3

- Merge domB in existing domA
  - recreate users
  - set-ntlm-hash
  - rejoin / move computers
  - migrate user profiles (hardest part)
- No need for ADMT or SID History

Client side
User profile migration

- In a fairy land, you'll just have to
  - change ACLs on user profile, ntuser.dat, userclass.dat
  - repoint SID from profileList in HKLM
- In the depressing reality, you have
  - locking problems
  - organisational problems
  - timing problems
  - Desktop availability is transient, and they have their own life and diversity.

- We need a tool for migrating users profiles

GPO are nice, but not good for everything

- People switching from NT4 to AD have big hopes about GPOs
- GPO concepts date back to the 90's
- Microsoft added SCCM : software deploiement / configuration management
- GPO still useful for security features (SRP, etc.)
- We need a tool to complement GPO...

WAPT

- Distribute, update and remove software applications and configurations
- WAPT is a powerful ingredient to manipulating AD domains on client side
- Python scripting like on SaMBa AD

DEMO

At last there is competition !

- not so much evolution in AD since 2000
- Times change, AD creativity booming
  - ADinternals -> MSAD has NTLM hash injection too (albeit not officially)
  - Mimikatz : lsass.exe inception, pass the hash/over pass the hash attack, golden ticket
  - People using samba4 for security auditing
- Microsoft does great software.
  - Sometimes some competition helps :-)

Whishlist 1/2

- DNS consistancy checker.
- AD DNS registering still has some black magic
- GPO manipulation (import/export)
- sysvolsync part of the project (people mess up when reading the wiki)
- smbd downgrade to ntlm auth if krb5 auth fails

whishlist 2/2

- Make /etc/krb5.conf site aware (easily)
- Commercial SaMBa/CUPS driver support from copier vendors
- Improve bind-DLZ integration (or internal DNS :-)
- human friendly « samba-tool ntacl get »
- Smaller smbd footprint on DCs
- SaMBa DC process state checker

And tomorrow?

- larger domains, tdb 64bits
- inter domain trust

- kerberos everywhere
- why keep kerberos on the LAN?

- make SaMBa be the innovator

Questions ?