Tranquil IT DevSecOps

SAMBA EXPERIENCE

A journey from 170 Samba3-NT4 domains to 1 unified Samba-AD domain with 8000 users

Denis Cardon, 6th June 2016

« They did not know it was impossible so they did it »

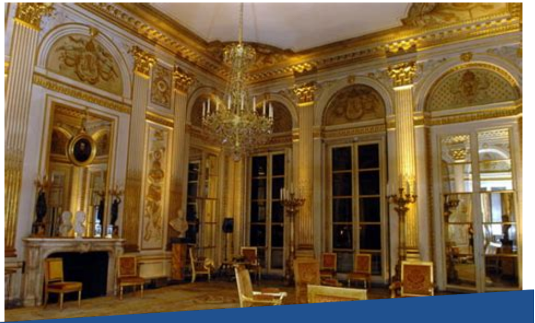
- Mark TWAIN

Tranquil IT

- IT company in Nantes, France, since 2002
- Largest Samba-AD integrator in France
- Editor of Wapt software deployment solution
- Good beer drinkers

Culture in France

- In France all is about culture
  - Wine, Cheese, Castles, Museum, Litterature, Philosophy, etc.
- So we have a Ministry in charge of that !
- Not mission critical, but important anyway !



Emmental

Ministry of Culture Migration

- Working with regional branches for 12 years
- Collaboration with IT team to restructure whole identity management starting 2016
- Architecture historically based on
  - Central LDAP for business applications
  - 170 domains for workstation authentication

Why Samba ?

Samba in France, French stereotype

Some say French people are...

- chauvinistic
- greedy
- anti-English/American
- self indulgent
- arrogant, etc.

Samba in France, a Fertile Ground

- What a better place for Samba to foursish!
  - free as in beer, free as in speech, anti Microsoft zealot
  - (General de Gaulle syndrom)
- Samba3-NT4 historically strong
  - administrations, schools, universities, research labs, hospitals, private companies, etc.
- Fertile ground for Samba-AD

Ministry of Culture Migration

- state of affairs in 2013 :
  - mostly Samba3-NT4 domains
  - some Microsoft AD 2k3, 2k8 (and 1 NT4)
  - IT management mostly de-centralized
  - No strict specification for domain management

Regional Initiative, 2013

- Regional initiative in early 2013
- migrating the « Pays de Loire » regional branch
- from Samba3-NT4
- Samba-AD 4.0
  - great minefield
  - In Samba team we trust !

Regional initiative, 2014

- Regional initiative, 2014
- Migrating Limousin regional branch
- Aging Windows NT4 domain…
- same setup, works great !

January 4th 2016

- First incoming business call of the year 2016...
- « we want the same thing »
- regional initiative become a national one
- one big domain, all merged !

Samba 4.3 Everywhere !

Ministry of Culture Migration

- Samba 4.3 not ready for large domains
- intermediate step : 16 domains
  - 1 central administration
  - 15 regional branches
- IMHO, the best choice
  - from a technical perspective
  - from a human perspective
  -

Ministry of Culture Migration

- Cyberspace landscape evolving rapidly
  - Many more threats everyday
  - Local Area Network / Endpoints are the new target
- Local Area Network security is Lame !
- Same network → same security level

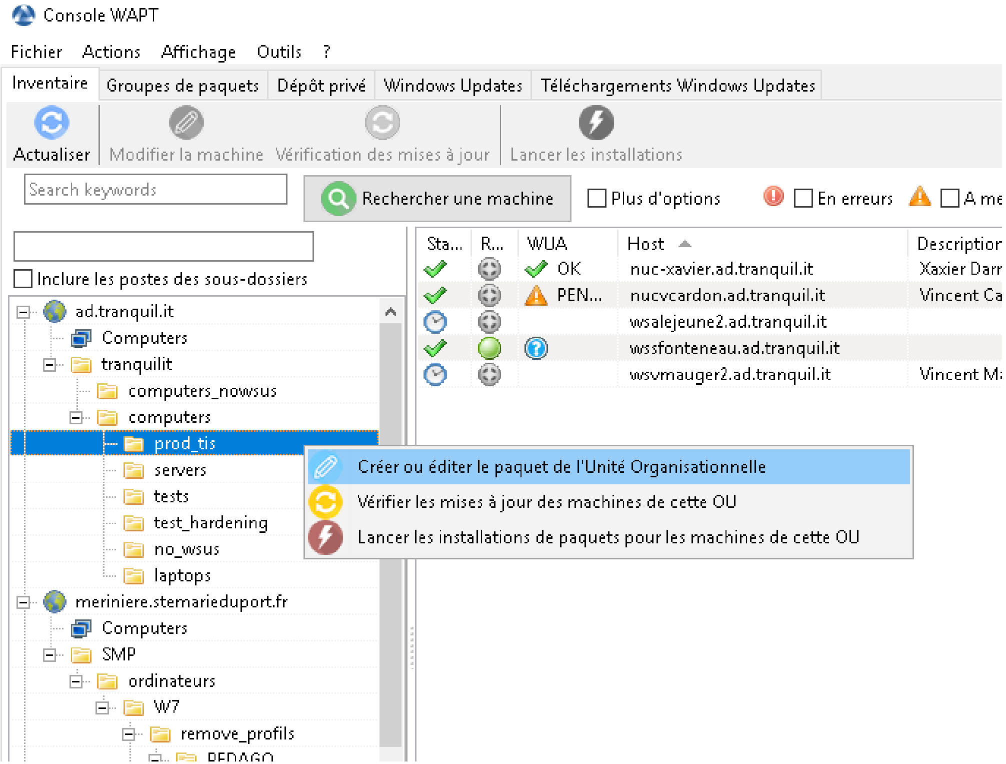
Ministry of Culture Migration Phase1

- Phase 1 :
  - Merge into 16 domains, cleanup, normalisation
  - 170 physical sites : France, Corsica, Martinique, Guadeloupe, Guyane, Réunion, etc.
  - a lot of travel, many souvenirs !
- at the same time
  - normalise username and groups, linux distribution, virtualization, etc.

- Server side migration automation
  - ansible playbook for creating / preconfiguring CentOS VM
  - ansible playbook for creating / join new DC
  - ansible playbook for normalizing SID on fileserver

Ministry of Culture Migration, Phase 1

- Client side migration automation
  - WAPT inventory
  - profile migration
  - WAPT scripting
  - Python rocks !



☐ Plus d'options ☐ En erreurs ☐ A me

☐ Inclure les postes des sous-dossiers

Sta...	R...	WUA	Host	Descriptior
✓	⚙	✓ OK	nuc-xavier.ad.tranquil.it	Xaxier Darr
✓	⚙	⚠ PEN...	nucvcardon.ad.tranquil.it	Vincent Ca
🕑	⚙		wsalejeune2.ad.tranquil.it	
✓	●	?	wssfonteneau.ad.tranquil.it	
🕑	⚙		wsvmauger2.ad.tranquil.it	Vincent M:

Migration tools

- Scripting, scripting, scripting...
  - python-ldb
  - samdb
- set-nt-hash hack
- Wapt
- Talking, talking, talking…
  - human cannot yet be scripted :-)

Ministry of Culture Migration, Phase 2

- Phase 2 :
  - samba 4.7 ready for 8k users domain
  - Merge 16 domains into 1 domain
  - More cleanup, more normalization
  - Less travel (only going to main sites)
  - Automatic AD user management directly from HR system

Ministry of Culture Migration, Phase 2

- Almost finished !
  - 166 sites merged, only 4 left
  - merging finished at the end of the month
  - One directory to rule them all !

Ministry of Culture Migration, Security Hardening

- Security Hardening
  - disabling NetBIOS, SMB1, NTLMv1, etc.
  - more RODC
  - lesser right policy on AD objects
- more automation
  - Ansible for servers, decrease « time to patch »
  - Wapt for Clients

Herding the Flock

- Many other already following suit
  - Ministry of Finance (1 domain, already 35k desktop migrated, 1k per week, aim at 150k desktops)
  - Ministry of Environment (46 domains, 25k desktops)
  - Ministry of Agriculture central administration (1 domain, 2k desktops)
  - French navy

- And many other catching up !
  - interministries regional branches (DDI)
  - Education ministry
    - academic region of new Aquitaine, Britanny, Normady, Centre, etc.

Samba Everywhere !

What’s Next ?

- Financing model not easy
- Being as good as MS-AD not sufficient
- Need to find revenue stream
  - SaaS (Samba-AD as a Service?)
  - Packaged product with support ?
  - have more sensible defaults ?

The end !

- a big thank to
  - Samba team
  - Ministry of Culture team
  - Tranquil IT team
  - To you all, no tomatoes thown yet...

Tranquil IT DevSecOps

SAMBA EXPERIENCE

- Any question ?
- dcardon@tranquil.it
- #tranquil_it