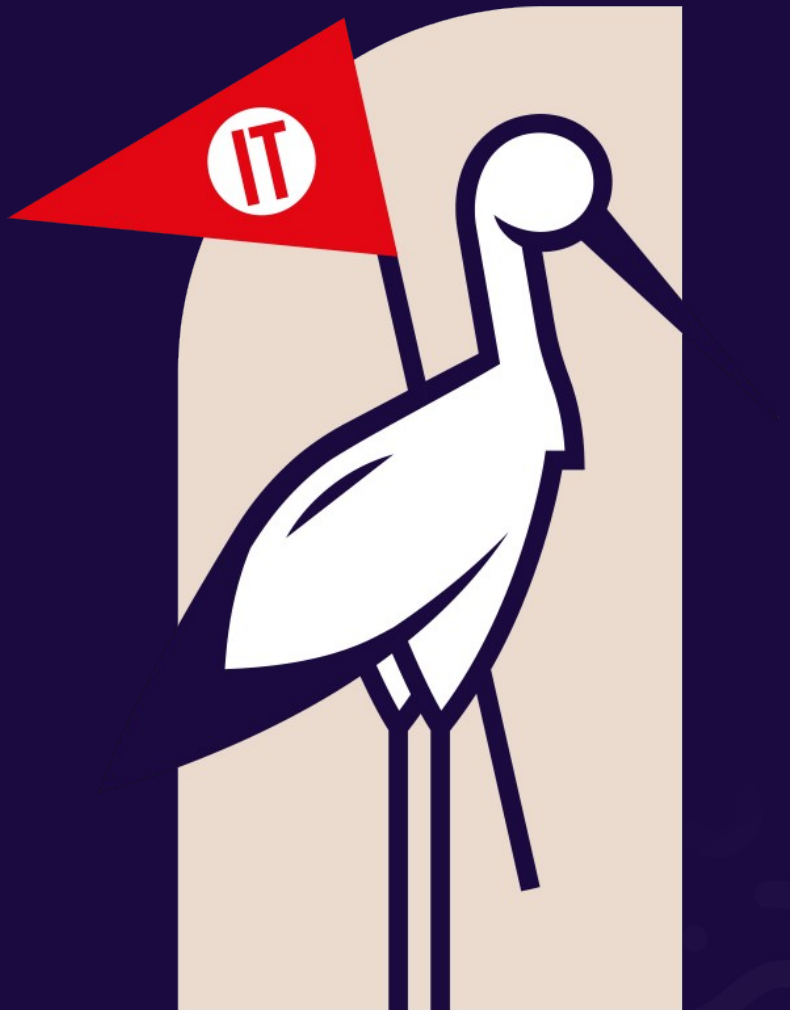

INTEGRATING SAMBA-AD IN REAL NETWORKS FROM A TECHNICAL POV

DENIS CARDON – TRANQUIL IT

21/04/2026

Active Directory is here to serve

- Active Directory does not live by itself
- It is the corner stone of on-premise IT systems
- The standard is Microsoft-AD
- Samba-AD is a re-implementation
  - But not a 100 % copycat
- Most of the time life is easy
  - Sometimes life needs hard work

SOME AREA WE'LL COVER

- Integrating with other Identity management tools
- Integrating with security audit tools
- Hardening with smartcard and ADCS Certificate Services
- Fighting hostile endpoints
- AD and Linux clients

Integrating with other IdM

Samba-AD and Google workspace

- GApps is very common in French Junior high and High schools
  - The dealers technique, the first sniff is free
- Google provides a DLL for synching MS-AD to Gapps
  - Nah...
- Samba provides extra hashes support
  - Password hash userPassword schemes = CryptSHA256 CryptSHA512
- A little python scripting and you get Samba-AD to Gapps sync !
  - Only one DC needs the scripted configuration
- This one was easy ...
- https://github.com/tranquilit/samba4-gaps

Samba-AD and EntraID

- O365 is common in France (unfortunatly)
  - People are addicted to Word and Outlook
- Now AzureADConnect works fine with Samba-AD
  - Needs a Windows server
  - And an account with DCSync rights
- Before that, we developped and still have AzureADConnect_Samba4
  - EntraID hash derived from NT Hash
- A little python scripting and you get Samba-AD to EntraID sync !
  - Have fun with Microsoft Binary XML format python-wfcbin
- https://github.com/tranquilit/AzureADConnect_Samba4
- No password writeback
  - Is it a bug or a feature ?

Samba-AD and OpenLDAP

- Many large entities have 2 sets of users
  - Internal users → in AD
  - External users → somewhere else
- For instance : universities, ministries
- Samdb and python scripting is king
- Sync password Samba-AD → OpenLDAP
  - password hash userPassword schemes = CryptSHA256 CryptSHA512
  - Playing with supplementalCredentials
- Sync password OpenLDAP → Samba-AD
  - Sam-R ? Used to be ok, but not anymore

Integrating with security audit tools

AD audit tools

- Now it's very common
  - Samba-AD needs to get good grades !
- Common real issues with Samba-AD setups
  - Missing some default groups in FL2016
  - Wrong default ACLs in schema (some hardcoded SID)
  - Etc.
- Most issues can be dealt with
  - By fixing The Samba-AD setup, or communicating with tool vendors
- But Samba-AD user base may not be large enough for them to care
  - eg. Tools flag a big security flaw because WMI RPC server is not there
    - If the tool can't get the info, then Samba-AD must be poorly configured !

AD audit tools

- ORADAD
  - ANSSI tool to do broad checks on AD security practices
    - For French administrations and Critical Infrastructure Operators
  - Used to have a few false positives on Samba, but now Samba-AD behaves well
  - Samba-AD user base is large enough in France for ANSSI to care :-)

- PingCastle / Netwrix
  - Used to be a one person army based in France
  - When there were false positives with Samba-AD
    - Used to be easy to have it fixed = a phone call to Vincent Le TOUX
  - Now it’s more complicated

SIEM integration

- (Security Information & Event Management)
- They are used to collect Eventlogs from AD servers
  - But it is not implemented in Samba-AD
- SIEM match EventIDs from AD server
  - But almost none of the events are mapped to an EventID
  - And they are not categorized (it is just a dsdb modify entry…)
- Logging could be improved in Samba-AD
  - Quiz : What is the highest logging level in Samba ?
- For now we can work with json logs (when they are available)
  - We can mostly provide what is asked
  - Then you send logs to rsyslog

Security Hardening with Smartcards and ADCS_python

Smartcards are getting trendy !

- More and more requests coming to Tranquil IT since last year
- Great timing : PKINIT has been much improved in latest Samba
  - Thanks to the French gov for financing
  - Thanks to Douglas BAGNALL and the Catalyst team for the implementation
- Now it works very well
- You just need a properly working PKI
  - And the proper OID configured

Distributing the certificates the Windows way

- ADCS (AD Certificate Services) provide the PKI and distribution server
  - PKI can be externalized
- Windows computers use CEP/CES protocol
  - Automatic discovery and delivery
  - Can store on disk or on TPM or on smartcard
- ADCS licencing not clear if CAL is necessary or not
  - So let's do our own ADCS_python !
- ADCS_python :
  - Certificate templates are coded in python (rather than xml stored in AD)
  - ADCS-python makes the process more versatile
- Still missing : TPM attestation (we need help with the specs ! :-)
- https://github.com/tranquilit/adcs_python

Ticking the « smartcard only » tickbox

- Getting rid of passwords is not an easy task
- Keycloak Kerberos auth on AD is easy to set up
- Fixing all applications to support Kerberos, Oauth or SAML
  - Applying configurations to compatible systems
  - Fixing some legacy code
  - Getting rid of or replacing what cannot be fixed

- « Smartcard only » is achievable with Samba-AD

Fighting hostile endpoints and applications

Life is not always kind

- When a printer wreaks the remote site bandwith
  - Downloading the whole AD db in a loop…
    - (objectclass=*) scope=SUB base=DC=..,DC=…
- Applications asking for computed attributes
  - A little bit too often
  - By a little bit too many endpoints
    - TokengroupName, recursive group membership, etc.
- Applications asking « who am I ? »
  - In a loop, every few seconds
  - On the PDC
  - With 8000 endpoints doing that, it gets ugly…
- Webapps querying group memberships…
  - at every http request

Making Linux first class citizen in AD network

Preparing tomorrow

- sssd is very mature and works very well with Samba-AD
- We need to apply to Linux all the security practices
- Not only end users need to be convinced
  - Sysadmins are the first user group to convince
- Recycle current habits to lower barrier of adoption to Linux administration

Preparing tomorrow

- Bitlocker → LUKS
  - Send the master key in Bitlocker recovery key attribute in AD
  - A WAPT package is available for Linux hosts
- LAPS support
  - Rotate root password and send in LAPS attribute in AD
  - A WAPT package is available for Linux hosts
- Avoid secrets in Debian pre-seed files
  - Create djoin blob in WAPT Deployment Server during Linux desktop provisioning
- 802.1x EAP/TLS for wired and wireless networks
  - Distributing certificate with cepces / certmonger client

Preparing tomorrow

- France wants Linux desktops, Tranquil IT is ready ! :-)
- Cohabitation of Linux / Windows / macOS will last
  - Samba-AD to make every client happy

THANKS !
QUESTIONS ?