Tranquil IT

DevSecOps

Samba-AD : l'alternative méconnue pour aider à sécuriser son environnement Active Directory

Denis Cardon, Tranquil IT 2022

Tranquil IT
DevSecOps

- Présentation / historique Tranquil IT
- Courte histoire Active Directory et Samba
- Samba-AD aujourd'hui
- Samba dans la nature
- Sécurité de Samba
- Organisation projet Samba
- Avenir de la gestion de l'identité

- Tranquil IT : début 2002
  - Prestations d'expertise variées
- 2008 spécialisation sur l'infogérance
  - Développement d'outil/expertise interne pour l'infogérance
- 2016 Bascule Éditeur WAPT + Expert Samba
  - Fin bascule 2022

Courte Histoire Active Directory

- Année 80 : prémices du partage de ressources et de centralisation d'identité
- Année 90 : NT4
- Année 2000 : MS-AD
- Année 2020 : hybridation de la gestion de l'identité
- Futur de l'AD « on premise » ?

Courte histoire de Samba-AD (1/2)

- Années 90 : Samba partage de fichier
- 2002 : Samba3, domaine type NT4
- 2004 : lancement développement domaine type AD
- 2008 : condamnation antitrust Microsoft par EU
  - Obligation de partager les specs de protocoles
- 2012 : Samba 4.0.0, domaine type AD

Courte histoire de Samba-AD (2/2)

- Plusieurs parties de Samba
  - Samba serveur de fichier
  - Samba serveur d'impression
  - Samba Active Directory
- Ici on va parler de Samba-AD
  - AD en tant que techno

Serveur Active Directory

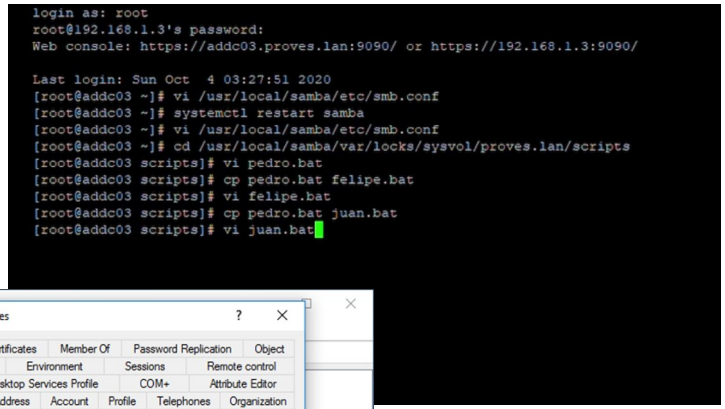
- Samba-AD = ré-implémentation libre des services MS-AD
  - Serveur DNS
  - Serveur LDAP
  - Serveur Kerberos
  - Serveur MS-RPC
    - Ouverture de session
    - Réplication entre serveurs
  - Serveur NTP

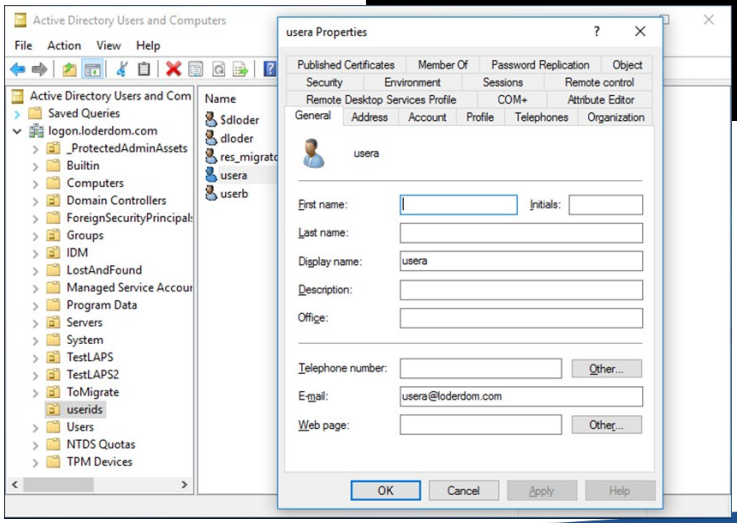
Samba-AD aujourd'hui (1/3)

- Différents composants, différents niveaux de support
  - ForestLevel 2k8r2
    - Plus Schema 2k12r2, Protected Users, Claims, etc.
  - Niveau crypto moderne
    - AES, etc.
  - Niveau protocole moderne
    - SMB3, etc.

Samba-AD aujourd'hui (2/3)

- Outils de management :
  - SSH
  - RSAT
  - Scripting LDAP
  - Scripting Python





Samba-AD aujourd'hui (3/3)

- Des limitations...
- Certains composants non développés, mais pas nécessaire dans la plupart des scénarios
  - Relations approbations interforêt partiellement supportées
  - Relations approbations intra non supportées
  - Protocole Eventlog / WMI
  - gMSA (normalement nécessaire pour Azure AD Connect)
  - Silos
  - AD web service
- Écosystème moins mature (Veeam, etc.), et peu de prestataires

Samba-AD dans la nature

- Ca fonctionne pour des grands réseaux multisites, par ex :
  - DGFiP 120k postes
  - Ministère de la culture 8k postes
  - Marine Nationale
- Et pour des réseaux plus modestes, par ex :
  - CH Tourcoing 1300 postes
  - Transport Ziegler 2600 postes
  - Université Paris8 1500 postes
  - BCEAO 2500 postes

Niveau de sécu Samba-AD (1/3)

- L'AD est de plus en plus attaqué
- FL2k8r2? WTF…
  - La sécurité c'est pas juste le ForestLevel, mais aussi comment c'est configuré
- Plus facile à sécuriser
  - Linux vs Windows Server vs Windows Core
  - Moins de composant, moins de surface d'attaque
    - Ex : spooler d'impression, jonction de machine par un Domain Users, etc.
    - Moins de légacy (LM, NTLMv1 non encapsulé, etc.)
  - Des valeurs par défaut plus sensées
  - Niveau de sécu ORADAD 3 plus facilement atteignable
-

Niveau de sécu Samba-AD (2/3)

- Ré-utilisation des habitudes de sécurisation Linux
  - Gestion des backups / automatisation Ansible, etc.
- Patching OS à la mode Linux
  - reboot seulement si besoin
- Patching Samba simple
  - maj RPM/Deb, pas de reboot nécessaire
- Side-Channel de management avec SSH
  - Possibilité de ne pas avoir de compte Domain Admins activé en temps normal
- Scripting avec Bash ou Python
  - Code Samba basé sur du C et du Python

Niveau de sécu Samba-AD (3/3)

- Samba est beaucoup déployé dans les administrations françaises
- « Accepté / toléré » comme alternative par l'ANSSI
  - depuis janvier 2021 dans les administrations publiques
  - à partir du moment où toutes les préconisations applicables sont appliquées
  - (petit) début de différentiation dans ORADAD
- Audit crypto commandé par l'ANSSI
  - Samba essaye de limiter la ré-écriture de crypto (mais nécessaire pour certains vieux proto)
- Facile d'auditer les objets directement sur le NTDS.DIT (bypass deny ACL)
- L'équipe Samba travaille avec Microsoft sur la sécu AD et tous les protocoles associés
  - ex. faille de fin 2021, failles de protocole, faille Channel Binding, etc.

Organisation du projet Samba (1/3)

- Projet open-source en GPLv3
- Pas vraiment de sponsor principal
- Plein d’acteurs avec des intérêts différents
  - Éditeur de NAS (Netgear, QNAP, etc.)
  - Éditeur de distrib (RedHat, SuSE, etc.)
  - Éditeur de solution (Univention, etc.)
  - Gros utilisateur (IBM, Google, Amazon, etc.)
  - Intégrateur (Tranquil IT, etc.)
  - Prestataire dev (Catalyst, SerNET)

Organisation du projet Samba (2/3)

- Avantage :
  - Une roadmap flexible en fonction des financements
  - Pas susceptible à des changements de stratégie commerciale
- Inconvénient :
  - Pas/peu d'évolution sans financement par un intégrateur/éditeur
- Modération :
  - Les bugs de sécu sont pris très au sérieux

Organisation du projet Samba (3/3)

- Samba en terme de manpower
  - Dev Samba-AD fulltime : entre 3 et 8
    - Principalement chez Catalyst et SerNET
  - Dev Samba fichiers fulltime : entre 10 et 20
    - Chez Redhat, SerNET, IBM, etc.
  - Commiteurs occasionnels : 80
- Une structuration projet très mature (CI/CD, etc.)
- Samba en tant qu'écosystème
  - Travail régulier avec Microsoft

L’avenir de la gestion de l’identité (1/2)

- Avenir de l’auth « on prem » ?
  - MS pousse pour la migration vers Azure-AD
  - Augmentation des coûts de licences « on prem »
  - Plus d’évolution sur le produit MS-AD
- Une auth hybride ?
  - 0auth, SAML, etc.

L’avenir de la gestion de l’identité (2/2)

- La techno AD montre ses limites
  - Limitation AD 2FA
  - Limitation sur les cartes à puces utilisables
    - Et contraintes techniques associées
  - Trop compliqué
- Et Microsoft ne fait plus évoluer MS-AD
- Samba peut devenir leader sur l’innovation AD

Conclusion

- Samba pour la cyber-souveraineté et pour garder votre auth « on prem »
- Testez Samba-AD
  - Site éditeur : https://samba.org
  - Documentation Tranquil IT : https://samba.tranquil.it/doc/

The end !

- Un grand merci
  - l'équipe Samba
  - L'équipe de l'OSSIR
  - l'équipe Tranquil IT
  - Et à vous tous !

Tranquil IT

DevSecOps

- Des questions ?
- @tranquil_it