www.cnrs.fr

resinfo.org

Retour d'Expérience AD Bridging

Anne COMBET - ICMUB UMR 6302 CNRS UBE

JOSY « Retours d'expérience sur la gestion et l'administration d'un parc de machines sous mac OS »

3 Novembre 2026 - Nancy

Institut de Chimie Moléculaire
UNIVERSITÉ DE BOURGOGNE

UNIVERSITÉ BOURGOGNE EUROPE

Le contexte d'origine

ICMUB, UMR CNRS UBE

- Créé en 2007
- Localisé au sein de l'UFR Sciences & Techniques
- Laboratoire rattaché à l'Institut National de Chimie du CNRS
- Initialement : environ 130 membres (chercheurs, enseignants-chercheurs, personnels supports à la recherche et la formation, doctorants, post-doctorants et chercheurs associés)
- Actuellement : plus de 170 membres
  - Structurés en 2 départements correspondant aux 2 axes de recherche : Chimie de synthèse propre et Santé & imagerie médicale
  - Et 5 équipes de recherche dont l'une est rattachée à l'UFR Santé
- Laboratoire sous statut réglementaire ZRR dans le cadre du dispositif PPST

L’évolution du S.I.

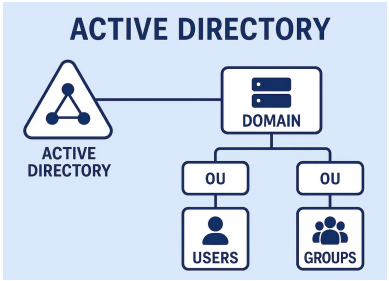
---------- **Avant 2015**

- Parc informatique hétérogène :
  - Mac OS
  - PC sous Windows
- Service d’annuaire Apple Open Directory sous Xserve Mac OS X 10.6 (basé sur OpenLDAP)
  - Gestion des utilisateurs et des groupes
  - Services assurés : AFP, SMB, FTP, MySQL, DHCP, DNS...



---------- **Mais, besoin accru de sécurité et de mise en conformité (PPST, PSSIO)**

- Passage à un réseau privé derrière un Firewall Netasq
  - DHCP
  - Filtrage et segmentation en VLAN
  - Isolation de certains réseaux, équipements
- Passage à un environnement Microsoft avec Active Directory (on-Premise)
  - DNS
  - Intégration des serveurs (fichiers, impression, virtualisation, sauvegardes, stockage, applications métiers)
  - Intégration du parc PC Windows

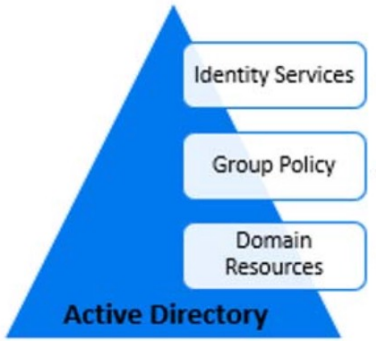


Mais, quid du parc Mac OS ?

Active Directory : élément clé du S.I.

Active Directory permet

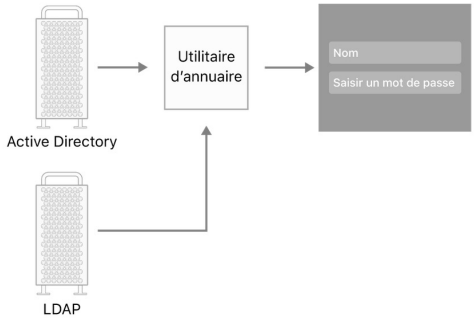
- l'authentification
- l'autorisation
- la gestion et stockage des informations (montage de partages SMB)
- le déploiement de services (PKI ADCS)
- le déploiement de stratégies de groupes (GPO)
- le management des utilisateurs, des postes de travail, des données, des applications
- la délégation d'administration



Quelle solution pour les Mac ?

- les GPO Windows ne s'appliquent pas nativement sur macOS

Les solutions possibles



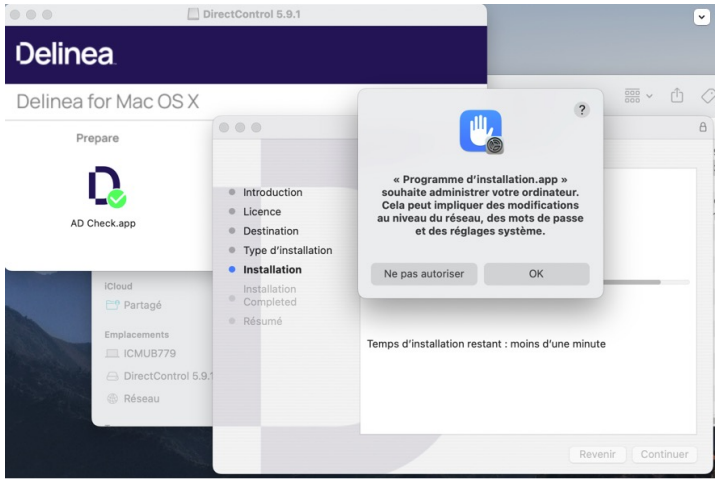
1. **Solution basique : connecteur AD intégré à l'utilitaire d'annuaire Apple (natif)**
   - permet de lier un Mac à un domaine Windows (via les protocoles LDAP et Kerberos)
   - Répond à la question = qui peut se connecter ?

--------- **Mais,**

   - Tous les besoins ne sont pas couverts (pas de gestion des GPO)
   - Pas d'audit (uniquement les connexions réussies)

2. **Profils de configuration et MDM (Mobile Device Management)**
   - Approche binding :
     - Le profil contenant les paramètres de liaison à l'AD (domaine, OU pour le Mac, Compte de service, l'option de création du compte mobile) va permettre au système de contacter le DC pour se lier
     - le MDM va appliquer des restrictions de sécurité (mais pas de gestion des GPO)
   - Approche sans binding (actuelle) :
     - le MDM utilise des extensions d'authentification unique (profil SSO)
     - le Mac ne fait pas partie du domaine AD (Objet ordinateur), seule l'identité de l'utilisateur est vérifiée
     - l'utilisateur accède de manière transparente aux partages de fichiers (SMB) et aux applications de l'entreprise sans jamais que le Mac ait eu besoin d'être "lié" techniquement au domaine Windows

Les solutions possibles



3. AD Bridging : solutions propriétaires

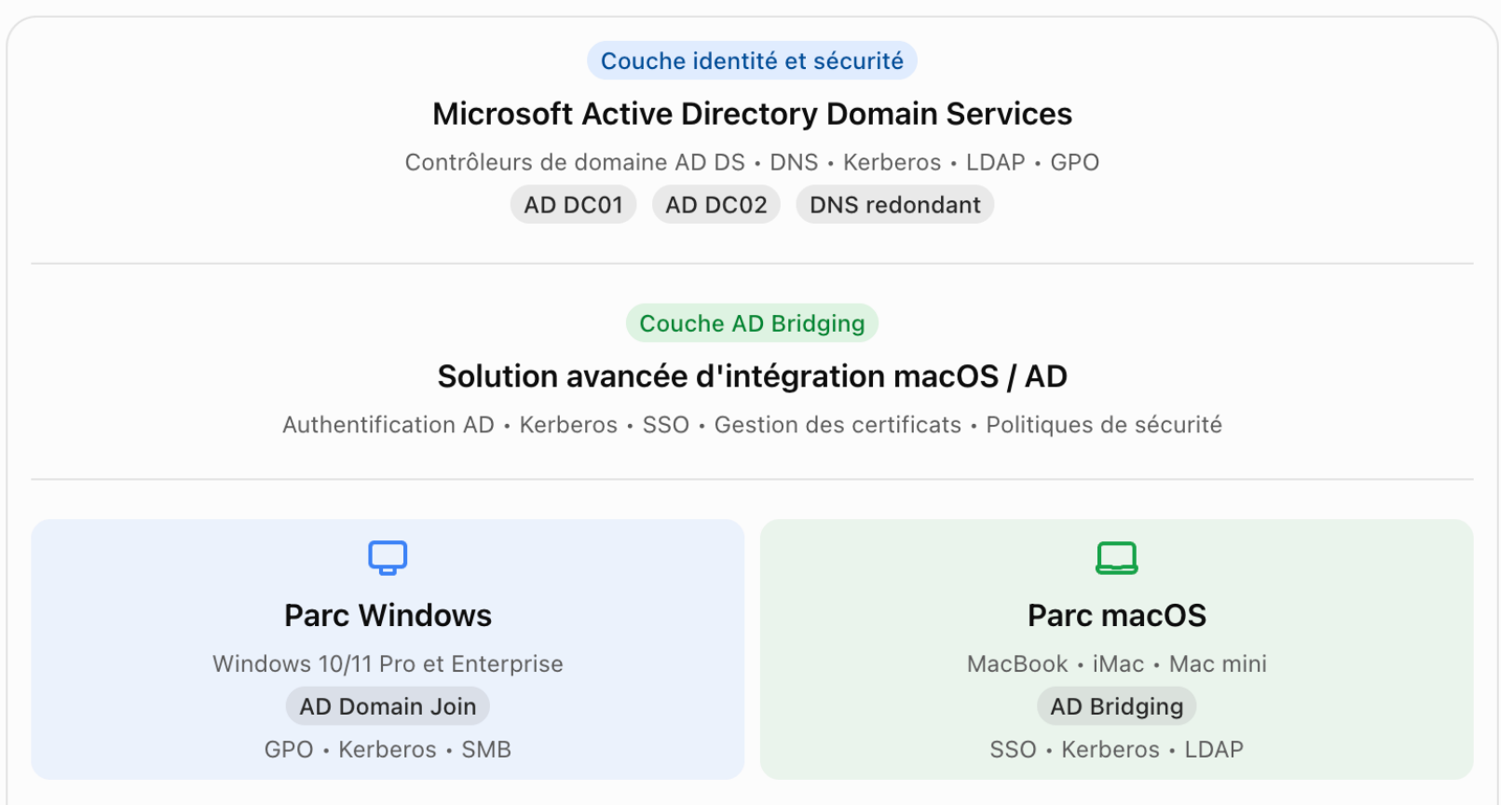
- Permet la gestion des identités et des accès (authentification et autorisation)
  - l'annuaire AD est la source d'authentification
  - et contrôle les droits des utilisateurs et des machines selon les stratégies appliquées
  - Une extension du schéma AD permet d'y ajouter des attributs UNIX/Linux (RFC 2307)

    (mac OS utilise le système POSIX basé sur UNIX avec UID et GID, alors qu'AD utilise des SID, identifiants uniques de sécurité)

- Nécessite l'installation d'un **agent logiciel** propriétaire sur le Mac
  - qui intercepte les requêtes d'authentification locales
  - qui communique avec les DC du domaine via les protocoles LDAP, Kerberos et DNS
  - quand un utilisateur se connecte sur le Mac, l'agent récupère le SID Windows et le convertit en UID/GID pour macOS

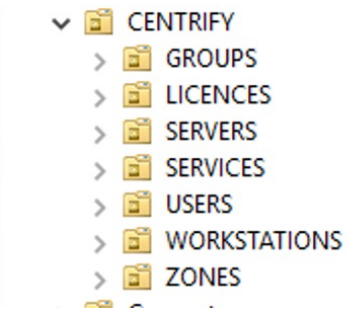
- Permet l'application des **Stratégies de groupes** qui ne fonctionnent pas nativement sur Mac

Architecture AD Bridging



Fonctionnement de l'AD Bridging

(Centrify / Delinea)

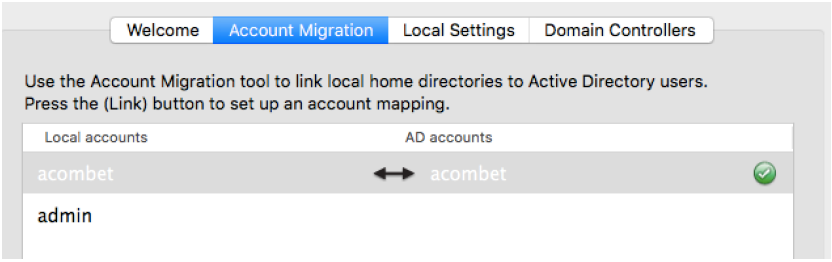


- **Le « bridge »** utilise les protocoles LDAP et Kerberos pour synchroniser les plateformes non Windows (Mac ou Linux) avec AD
  - Kerberos, basé sur la délivrance de tickets, permet de valider un utilisateur auprès d'autres applications et systèmes (sans jamais transmettre le mot de passe directement au service)
  - L'utilisateur tape ses identifiants sur l'écran de verrouillage, l'AD valide et renvoie un ticket Kerberos (TGT : Ticket-Granting Ticket)
  - L'agent ouvre la session locale et utilise un ticket de session (TGS) pour offrir un SSO natif (poste de travail, serveurs distants, partage réseau)
  - La commande klist sur Mac permet de lister les tickets en cours (TGT et TGS) dans le cache (/System/Library/CoreServices/Applications/Visualiseur de ticket)

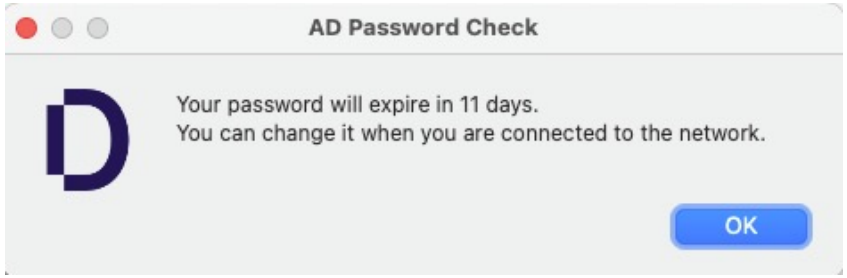
- **L'application des GPO** est le point fort de la solution :
  - L'agent Delinea télécharge les GPO applicables à l'utilisateur ou à la machine depuis le dossier SYSVOL de l'AD
  - Il traduit les GPO Windows en profils de configuration (.mobileconfig) ou en commandes lues par macOS
  - Cela permet de pousser des stratégies de sécurité (complexité des mots de passe, verrouillage de session, enrôlement des Mac pour les certificats PKI ADCS, …) basées sur les groupes

Avantages de l'AD Bridging

(Centrify / Delinea)



- **Centralisation dans AD**
  - ⇒ Fin des comptes locaux : tout utilisateur AD valide peut se connecter à un Mac joint au domaine
    - ⇢ Possibilité de convertir un compte local en compte de domaine (link)
  - ⇒ Renforce la sécurité globale par l 'extension des avantages de l'infrastructure AD aux systèmes non Windows
    - ⇢ Gestion des identités
    - ⇢ Management des GPO
  - ⇒ Améliore l'expérience utilisateur
    - ⇢ Exemple : expiration du mot de passe
  - ⇒ Facilite la gestion des accès
- **Bonnes pratiques SSI** :
  - ⇒ Principe du moindre privilège
    - ⇢ Gestion des comptes et des accès privilégiés (Dérogations)
    - ⇢ Conformité PSSIO
  - => Gestion des accès aux applications quel que soit le système (Windows ou non)
  - ⇒ Gestion par groupes de sécurité
  - ⇒ Gestion du cycle de vie des comptes utilisateurs (création, suppression, contrôles d'accès)
- **Traçabilité**
- **Interopérabilité facilitée**



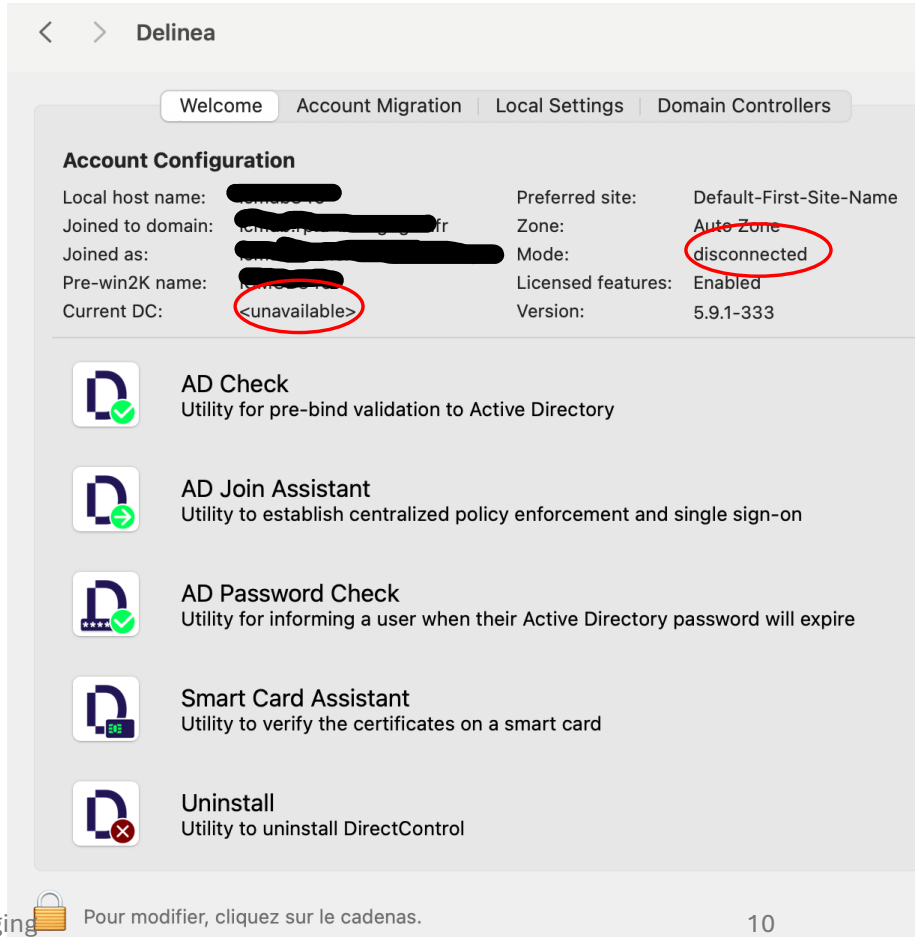
Problèmes rencontrés avec l'AD Bridging

- Maintenance et support
  - ⇢ Gestion des mises à jour
  - ⇢ Compatibilité des nouvelles versions de Mac OS
  - ⇢ Arrêt de la solution pour mac OS
- Dépendance à l'AD
  - ⇢ l'AD Bridging repose sur la disponibilité de l'infrastructure Active Directory

admin@XXXXX user % adgpupdate /force

Machine is running disconnect mode.

  - ⇢ Problème de la mobilité
- Limitations, incompatibilités de certaines applications
  - ⇢ Touch ID (échec de l'enregistrement de l'empreinte) (Big Sur)
  - ⇢ déverrouillage FileVault (Sonoma)
  - ⇢ interactions entre synchro mot de passe AD et Keychain



Evolution au fil du temps…

- Les usages ont évolué : mobilité, télétravail
- L'écosystème Apple a beaucoup évolué aussi :
  - ⇢ le binding simple à l'AD rend parfois les connexions instables
  - ⇢ Apple a progressivement abandonné le support optimal de cette architecture
  - ⇢ Quid des fournisseurs de solution d'AD Bridging ?
- Apple recommande aujourd'hui d'utiliser un **MDM couplé à l'identité fédérée** via un fournisseur d'identité Cloud (Microsoft Entra ID, Google Workspace) : Platform SSO (extension d'authentification unique) permet de lier la session locale du Mac à un identifiant Cloud
  - ⇢ Incompatible avec nos exigences de sécurité
- L'agent d'AD Bridging reste toutefois mieux supporté que l'outil de liaison natif de macOS
- **L'AD Bridging reste approprié pour les environnements centrés sur Active Directory et les réseaux isolés physiquement**

En conclusion

Avec un parc hétérogène, un S.I basé sur un annuaire AD central et de fortes contraintes de sécurité et de conformité, l'AD Bridging a permis de faciliter l'administration du laboratoire

- **Sécurité centralisée (authentification, autorisation, GPO)**
  - ⇢ Authentification unique
  - ⇢ Politiques de sécurité cohérentes
  - ⇢ Simplification de l'environnement

- **Conformité PSSIO / PPST pour les données sensibles**
  - ⇢ Contrôle d'accès aux systèmes et aux données