Veille Technologique – Jonction des postes Windows 11 et Linux à Active Directory

Nov 27, 2026 · @Serge Martins

Sujet de la veille

Joindre un poste à un domaine Active Directory est un geste quotidien de l'administrateur. En 2026, il évolue : Microsoft désactive progressivement NTLM, durcit Kerberos et pousse Entra ID, tandis que les postes Linux rejoignent AD avec realmd et SSSD, non sans difficultés face aux contrôleurs Windows Server 2025.

En bref

Élément	Situation au 27/11/2026
Windows 11	Jonction AD native (éditions Pro, Entreprise, Éducation)
Linux (Debian 13)	realmd + SSSD + adcli, ou Samba/Winbind
Authentification	Kerberos privilégié ; NTLM en voie de désactivation
Mot de passe admin local	Windows LAPS intégré à Windows 11 et Windows Server 2025
Alternatives cloud	Jonction Microsoft Entra ID ou hybride

Actualité côté Microsoft

- **Fin programmée de NTLM (janvier 2026)** : Microsoft a annoncé un plan en trois phases. Audit renforcé de NTLM dès maintenant sur Windows Server 2025 et Windows 11 24H2+ ; au second semestre 2026, nouvelles fonctions **IAKerb** et **KDC local** pour utiliser Kerberos là où NTLM était obligatoire ; enfin, dans la prochaine version majeure de Windows Server et du client, **NTLM réseau désactivé par défaut** (réactivable par stratégie).
- **NTLMv1** : supprimé de Windows 11 24H2 et Windows Server 2025, il en reste des traces dans les connexions MS-CHAPv2 (PEAP) en environnement de domaine.

- **Durcissement Kerberos (avril 2026)** : les contrôleurs de domaine utilisent par défaut le chiffrement AES-SHA1 pour les comptes sans type de chiffrement explicite ; les systèmes qui ne savent faire que RC4 peuvent échouer à s'authentifier.

Actualité côté Linux

- **realmd + SSSD** reste la méthode standard sur Debian, Ubuntu et RHEL : `realm join` découvre le domaine, crée le compte ordinateur et configure SSSD, Kerberos et PAM.
- **Contrôleurs Windows Server 2025** : des administrateurs signalent l'erreur *Message stream modified* lors de la définition du mot de passe du compte ordinateur par adcli ; la jonction réussit avec `--membership-software=samba`.
- **Stratégies de groupe** : SSSD sait appliquer le contrôle d'accès des GPO Windows (`ad_gpo_access_control`), et des outils comme ADSys (Ubuntu) étendent les GPO aux postes Linux.

Comparatif des méthodes

Méthode	Postes	Points forts	Limites
Jonction AD classique	Windows	GPO, Kerberos, gestion centralisée	Nécessite le réseau interne ou un VPN
Microsoft Entra ID	Windows	Gestion cloud, Intune, Windows Hello	Pas de GPO classiques
Jonction hybride	Windows	Les deux mondes	Synchronisation Entra Connect à maintenir
realmd + SSSD	Linux	Simple, cache hors ligne, mapping automatique des UID	GPO partiellement appliquées
Samba Winbind	Linux	Partages et intégration Samba	Configuration plus lourde

Recommandations

1. Joindre les postes avec un compte délégué sur une OU dédiée, jamais avec l'administrateur du domaine en production.
2. Auditer dès maintenant l'usage de NTLM (journaux NTLM, stratégies *Restrict NTLM* en mode audit) pour préparer sa désactivation.

3. Définir explicitement les types de chiffrement Kerberos (AES) des comptes de service.
4. Déployer Windows LAPS sur les postes Windows.
5. Sur Linux, restreindre les connexions à un groupe AD (`realm permit -g`) et tester la jonction contre un DC Windows Server 2025 avant généralisation.

Sources

- Windows IT Pro Blog — *Advancing Windows security: Disabling NTLM by default* (janvier 2026)
- Neowin — Durcissement Kerberos d'avril 2026
- freedesktop.org — Guide realmd de jonction Active Directory
- Microsoft Tech Community — jonction Debian/Ubuntu à un domaine Windows Server 2025