Veille Technologique – Windows Server 2025 et Active Directory

Nov 27, 2026 · @Serge Martins

Sujet et enjeux

Windows Server 2025 apporte le premier nouveau niveau fonctionnel Active Directory depuis 2016 et des réglages de sécurité plus stricts par défaut. En 2026, Microsoft a aussi commencé à retirer RC4 et NTLM, et Windows Server 2016 arrive en fin de support le 12 janvier 2027. Créer un nouveau domaine aujourd'hui, c'est donc partir directement sur Windows Server 2025.

Rubrique	Contenu
Thème	Contrôleurs de domaine Active Directory sous Windows Server 2025
Technologies suivies	AD DS, Kerberos, NTLM, LDAP, dMSA, Windows LAPS
Contexte	Contrôleur de domaine `DC01` de la forêt `martinscie.lan`
Bloc BTS SIO	SISR – administration des systèmes, gestion des identités, cybersécurité des services
Période couverte	Mai 2025 à novembre 2026
Support Windows Server 2025	Standard jusqu'en novembre 2029, étendu jusqu'au 14 novembre 2034

Nouveautés Active Directory de Windows Server 2025

Le nouveau niveau fonctionnel (valeur 10) n'accepte que des contrôleurs de domaine Windows Server 2025 ; une forêt neuve doit être au moins au niveau 2016. Selon Microsoft, les principaux changements sont :

Nouveauté	Ce qu'elle change	Effet sur le SI
Signature LDAP exigée	Toute nouvelle forêt exige par défaut la signature LDAP	Les applications en LDAP simple (port 389) doivent passer en LDAPS (636)

Nouveauté	Ce qu'elle change	Effet sur le SI
Kerberos sans RC4	Le KDC n'émet plus de tickets TGT en RC4	Les vieux équipements limités à RC4 ne s'authentifient plus
Credential Guard	Activé par défaut sur le matériel compatible	Vol d'identifiants en mémoire plus difficile
LDAP en TLS 1.3	LDAPS prend en charge TLS 1.3	Chiffrement plus moderne des requêtes d'annuaire
Mots de passe SAM	Les anciennes méthodes RPC de changement de mot de passe sont bloquées à distance	Anciens clients ou scripts à vérifier
dMSA	Nouveau type de compte de service géré, aux clés aléatoires	Remplace les comptes de service à mot de passe fixe
Windows LAPS	Phrases de passe, détection de restauration, gestion du compte local	Mots de passe des administrateurs locaux uniques et renouvelés
Base 32k (optionnelle)	Pages de base de données de 32 Ko, attributs multivalués 2,6 fois plus grands	Utile pour les très grands annuaires
NUMA	AD DS exploite tous les groupes de processeurs, au-delà de 64 cœurs	Performances sur gros serveurs

Actualité 2025-2026

Depuis sa sortie, Windows Server 2025 a connu une faille grave propre à sa nouveauté dMSA et plusieurs mises à jour qui ont perturbé les contrôleurs de domaine. Il faut donc tester chaque mise à jour cumulative avant de la déployer partout.

Date	Événement	À retenir
23 oct. 2026	Rappel de fin de support de Windows Server 2016	Dernière mise à jour de sécurité en janvier 2027 ; Microsoft recommande Windows Server 2025
14 oct. 2026	Problème réseau des DC 2025 après redémarrage	Contournement : tâche planifiée qui redémarre la carte réseau au démarrage

Date	Événement	À retenir
Juillet 2026	RC4 : phase d'application finale	Le mode audit disparaît ; RC4 n'est plus utilisé par défaut pour les tickets de service
14-19 avr. 2026	Mise à jour KB5082063 : DC qui redémarrent en boucle	Plantage de LSASS corrigé par la mise à jour hors bande KB5091157
14 avr. 2026	RC4 : phase 2	Les DC utilisent AES-SHA1 par défaut pour les comptes sans réglage explicite
29 janv. 2026	Feuille de route de désactivation de NTLM	NTLM réseau désactivé par défaut dans la prochaine version de Windows Server ; audit NTLM déjà disponible sous 2025
13 janv. 2026	RC4 : phase 1, audit (CVE-2026-20833)	Événements KDCSVC 201 à 209 pour repérer les comptes encore en RC4
12 août 2025	Correctif BadSuccessor (CVE-2025-53779)	La faille dMSA est corrigée ; mettre à jour tous les DC 2025
21 mai 2025	BadSuccessor révélée par Akamai	Un utilisateur ayant des droits sur une OU pouvait, via un dMSA, devenir administrateur du domaine ; il suffisait d'un seul DC 2025

Problèmes connus à surveiller : les mises à jour cumulatives de Windows Server 2025 ont aussi causé des erreurs de changement de mot de passe et des refus de connexion dans des domaines mixtes 2022 / 2025. Le tableau de bord Windows Release Health liste les problèmes ouverts.

Impact pour martinscie.lan et recommandations

Pour une forêt neuve comme `martinscie.lan`, Windows Server 2025 au niveau fonctionnel 2025 est le bon choix : support jusqu'en 2034, sécurité renforcée d'origine et aucun DC ancien à gérer.

À l'installation de DC01

- [ ] Installer toutes les mises à jour cumulatives avant la promotion (correctifs BadSuccessor et KB5091157 inclus).
- [ ] Choisir le niveau fonctionnel Windows Server 2025 (`-DomainMode 10 -ForestMode 10`).

- [ ] Prévoir LDAPS (certificat sur DC01) pour GLPI, le NAS et les autres applications.
- [ ] Restreindre qui peut créer des objets dans les OU : c'était la condition de l'attaque BadSuccessor.

En exploitation

- [ ] Activer l'audit NTLM et surveiller les événements KDCSVC 201-209 pour repérer les usages de NTLM et de RC4.
- [ ] Déployer Windows LAPS et placer les administrateurs dans le groupe Protected Users.
- [ ] Tester chaque mise à jour cumulative sur un DC de lab avant la production, et consulter Windows Release Health.
- [ ] Ajouter un second contrôleur de domaine (DC02) et sauvegarder l'état du système.

Intérêt pédagogique (SISR) : DC01 sert de base aux autres services du lab (xrdp avec SSSD, GLPI, Zabbix). Les durcissements de 2025-2026 illustrent la défense en profondeur et l'abandon des protocoles obsolètes.

Outils de veille et sources

Outil	Ce qu'il surveille
Windows Release Health (Windows Server 2025)	Problèmes connus et correctifs des mises à jour
Blog Windows Server et Windows IT Pro Blog	Annonces : NTLM, RC4, fins de support
Microsoft Security Response Center (MSRC)	CVE du Patch Tuesday mensuel
CERT-FR (ANSSI)	Avis de sécurité Microsoft en français
BleepingComputer, Help Net Security	Actualité des failles et incidents

Sources

- Microsoft – Nouveautés de Windows Server 2025
- Microsoft – Niveaux fonctionnels Active Directory
- Microsoft – Problèmes connus de Windows Server 2025
- Microsoft – Advancing Windows security: Disabling NTLM by default
- Microsoft – Beyond RC4 for Windows authentication
- Microsoft – Gestion de RC4 par le KDC (CVE-2026-20833)
- Microsoft – Phase 2 du durcissement RC4
- Microsoft – Planning ahead for Windows Server 2016 end of support

- Help Net Security – BadSuccessor (CVE-2025-53779)
- Akamai – Analyse du correctif BadSuccessor
- BleepingComputer – Correctifs d'urgence d'avril 2026
- BleepingComputer – Fin de support de Windows Server 2016