Veille Technologique – Contrôleur de domaine Samba AD sous Debian

Nov 27, 2026 · @Serge Martins

Sujet et enjeux

Samba permet de faire tourner un contrôleur de domaine Active Directory sur Linux, sans licence Windows Server. En 2026, le projet est très actif (versions 4.24 puis 4.25), mais il a aussi corrigé plusieurs failles graves propres au rôle de contrôleur de domaine. Un DC Samba doit donc être mis à jour aussi vite qu'un DC Windows.

Rubrique	Contenu
Thème	Contrôleur de domaine Active Directory libre : Samba AD DC sous Debian
Technologies suivies	Samba 4.22 à 4.25, Kerberos, LDAP, DNS interne, Debian 13
Contexte	Serveur `debdc01`, alternative libre à DC01 (Windows Server 2025)
Bloc BTS SIO	SISR – administration des systèmes, gestion des identités, logiciels libres, cybersécurité
Période couverte	Octobre 2025 à novembre 2026

Samba AD en 2026

Versions. Samba 4.25.0 est sorti le 12 octobre 2026 ; il passe notamment les types de chiffrement du domaine en AES par défaut. La branche 4.24 (mars 2026) est en maintenance. Debian 13 fournit Samba **4.22**, branche que l'équipe Samba ne maintient plus qu'en correctifs de sécurité ; Debian y intègre les correctifs via ses avis DSA.

Niveau fonctionnel. Samba crée un domaine au niveau 2008 R2 par défaut ; depuis la 4.19, le niveau **2016** s'active avec l'option `ad dc functional level = 2016`. Samba ne gère pas le niveau Windows Server 2025.

Critère	Samba AD DC (Debian 13)	Windows Server 2025
Coût	Gratuit, logiciel libre (GPL)	Licence serveur + licences d'accès client (CAL)
Niveau fonctionnel maximal	2016	2025
Administration	`samba-tool` en ligne de commande + outils RSAT depuis Windows	Consoles graphiques sur le serveur + PowerShell
GPO	Oui (stockées dans SYSVOL, éditées avec RSAT)	Oui
Ressources	2 Go de RAM suffisent	4 Go conseillés (interface graphique)
Réplication SYSVOL entre DC	Non automatique (à scripter)	Automatique (DFS-R)
Nouveautés sécurité 2025 (dMSA, LDAP signé par défaut sur nouvelle forêt…)	Non, ou partiellement	Oui
Support	Communauté + Debian (sécurité), offres commerciales tierces	Microsoft jusqu'en 2034

Actualité 2025-2026

La faille la plus grave de 2026 pour Samba AD permet à un simple utilisateur du domaine d'en prendre le contrôle. Debian 13 l'a corrigée dès le lendemain de sa publication.

Date	Événement	À retenir
12 oct. 2026	Samba 4.25.0 et 4.24.8	Nouvelle branche stable ; AES par défaut pour le chiffrement du domaine
28 juil. 2026	Versions de sécurité 4.24.5, 4.23.10, 4.22.11	Cinq failles corrigées ; Debian 13 corrigée par DSA-6401-1 (Samba 4.22.10+dfsg-0+deb13u2)
→	CVE-2026-58221	Un utilisateur authentifié peut modifier des enregistrements internes via LDAP et **prendre le contrôle du domaine** (CVSS 8,8), sans contournement possible

Date	Événement	À retenir
→	CVE-2026-58222	Lecture d'attributs confidentiels par un simple utilisateur ; critique si des comptes gMSA sont utilisés
→	CVE-2026-6949, 58216, 58218	Plantage du DNS ou du KDC, déni de service sur la signature DNS
26 mai 2026	CVE-2026-3238 (Samba 4.24.3)	Déni de service du serveur WINS d'un DC
26 mai 2026	CVE-2026-4408	Exécution de code à distance via le « check password script » ; concerne les serveurs de fichiers et les anciens DC NT4, **pas** un DC Active Directory
18 mars 2026	Samba 4.24.0	Gestion des mots de passe à distance, audit des authentifications
15 oct. 2025	CVE-2025-10230	Exécution de code sans authentification (CVSS 10) sur un DC, **seulement** si WINS et le paramètre `wins hook` sont activés

Côté Microsoft, le retrait de RC4 dans Kerberos (2026) et la future désactivation de NTLM concernent aussi les domaines Samba : les postes Windows récents attendent AES, d'où le passage d'AES par défaut dans Samba 4.25.

Impact et recommandations

Samba AD convient bien à un lab, une école ou une petite structure sans licence Windows Server. Pour un domaine qui doit suivre les nouveautés de Microsoft (niveau 2025, dMSA), Windows Server 2025 reste nécessaire.

- [ ] Installer les mises à jour de sécurité Debian dès leur parution (`unattended-upgrades` pour la sécurité) et suivre les avis DSA de Samba.
- [ ] Laisser WINS désactivé et ne jamais définir `wins hook` sur un DC.
- [ ] Activer le niveau fonctionnel 2016 pour bénéficier des dernières fonctions disponibles.
- [ ] Prévoir deux DC Samba et une sauvegarde `samba-tool domain backup` régulière.
- [ ] Ne pas mélanger un DC Samba avec une forêt Windows au niveau 2025 : Samba ne peut pas la rejoindre.
- [ ] Pour des fonctions plus récentes, évaluer Samba 4.24 ou 4.25 (rétroportages ou paquets tiers) en lab avant la production.

Intérêt pédagogique (SISR) : comparer un DC Samba et un DC Windows sur le même scénario montre que les clients ne voient pas la différence (Kerberos, LDAP, DNS, GPO), et illustre le choix entre logiciel libre et propriétaire.

Outils de veille et sources

Outil	Ce qu'il surveille
Samba – Latest News et page Security	Nouvelles versions et avis de sécurité
Liste samba-announce	Annonces envoyées par l'équipe Samba
Debian Security Tracker (paquet `samba`)	État des CVE dans Debian 12 et 13
Liste debian-security-announce	Avis DSA
CERT-FR (ANSSI)	Alertes de sécurité en français

Sources

- Samba – Latest News
- Samba 4.24.5 – notes de version (sécurité)
- Samba – CVE-2026-58221
- Samba – CVE-2026-58222
- Samba – CVE-2026-3238
- Samba – CVE-2026-4408
- Samba – CVE-2025-10230
- Debian Security Tracker – CVE-2026-58221
- Phoronix – Samba 4.25
- LWN – Samba 4.24.0
- Samba 4.19 – niveau fonctionnel 2016
- Microsoft – Niveaux fonctionnels Active Directory