Veille Technologique – Serveur DNS sous Windows Server 2025

Nov 27, 2026 · @Serge Martins

Sujet et enjeux

En 2026, le serveur DNS de Windows Server 2025 a gagné sa plus grosse nouveauté depuis des années : le **chiffrement des requêtes en HTTPS (DoH)**. Il a aussi corrigé plusieurs failles d'exécution de code à distance. Le DNS étant le cœur de l'Active Directory, ces deux sujets concernent directement DC01.

Rubrique	Contenu
Thème	Rôle DNS de Windows Server 2025 intégré à l'Active Directory
Technologies suivies	DNS Windows, zones intégrées à l'AD, DNSSEC, DNS over HTTPS (DoH)
Contexte	DNS du domaine `martinscie.lan` porté par DC01
Bloc BTS SIO	SISR – services réseau, cybersécurité des services
Période couverte	Février à novembre 2026

La nouveauté 2026 : DNS over HTTPS

Le DNS classique circule **en clair** sur le port 53 : n'importe qui sur le réseau peut lire ou modifier les réponses. DoH les transporte dans une connexion HTTPS chiffrée par TLS, selon la norme RFC 8484.

Étape	Date	Détail
Préversion publique	Février 2026 (KB5075899)	Sur inscription, non supportée en production
Disponibilité générale	Juin 2026 (KB5094125)	Intégré au rôle DNS, aucun résolveur séparé
Commande	`Set-DnsServerEncryptionProtocol`	Active DoH et définit le modèle d'URI

Limites : DoH concerne le trafic **entre les clients et le serveur** ; le DNS classique continue en parallèle, et il faut un certificat TLS valide sur le serveur.

Actualité sécurité 2026

Date	Faille	À retenir
11 août 2026	CVE-2026-62820	Exécution de code à distance sur le serveur DNS (CVSS 8,1), exploitation difficile (situation de concurrence)
2026	CVE-2026-62817	Écriture hors limites : exécution de code depuis le réseau local (CVSS 8,8)
14 juil. 2026	CVE-2026-50426	Exécution de code à distance sur le serveur DNS
12 mai 2026	CVE-2026-41096	Faille critique du **client** DNS : une réponse forgée exécute du code sur le poste

Un serveur DNS compromis donne accès au contrôleur de domaine qui l'héberge : ces correctifs sont à installer en priorité.

Recommandations

- [ ] Appliquer chaque mois les mises à jour de sécurité sur les DC/DNS, après test.
- [ ] Garder des zones intégrées à l'AD avec mises à jour **sécurisées uniquement**, et refuser les transferts de zone.
- [ ] Ne jamais exposer le port 53 d'un DC sur Internet ; filtrer avec pfSense.
- [ ] Tester DoH en lab : certificat interne sur DC01, postes Windows 11 en « HTTPS uniquement ».
- [ ] Activer le nettoyage des enregistrements obsolètes et prévoir un second DNS (DC02).

Intérêt pédagogique (SISR) : le DNS relie réseau et annuaire (enregistrements SRV de l'AD) ; DoH illustre le chiffrement d'un protocole historique en clair.

Sources

- Microsoft – DoH disponible sur Windows DNS Server
- Microsoft – Activer DNS over HTTPS sur le serveur
- Microsoft – Chiffrement DNS avec DoH

- Microsoft – Set-DnsServerEncryptionProtocol
- Petri – Windows Server 2025 et DoH
- Action1 – CVE-2026-62820
- Action1 – CVE-2026-62817
- Vulners – CVE-2026-50426
- K7 Labs – CVE-2026-41096