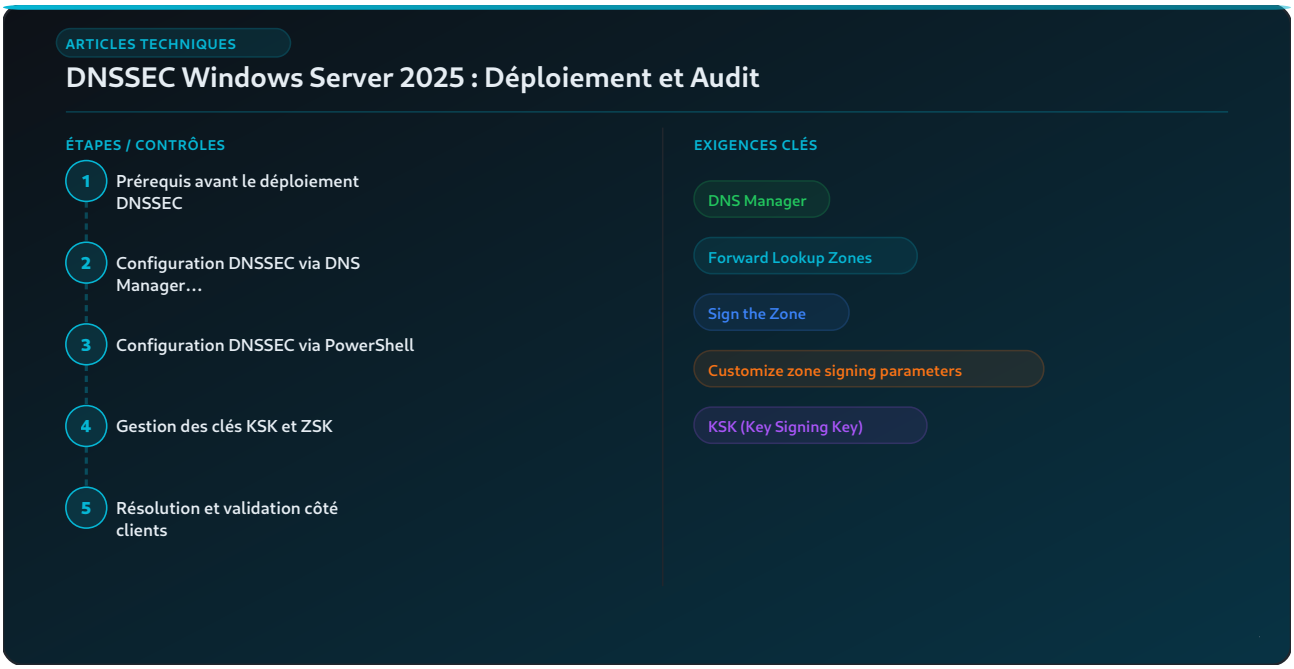
DNSSEC Windows Server 2025 : Guide Complet de Déploiement

> Déployer et auditer DNSSEC sur Windows Server 2025 : configuration via DNS Manager et PowerShell, zones signées, test de validation, conformité NIS2.

DNSSEC (DNS Security Extensions) est devenu un prérequis incontournable pour sécuriser l'infrastructure de résolution de noms des environnements Active Directory modernes. Sans DNSSEC, un attaquant positionné entre vos clients et vos serveurs DNS peut empoisonner le cache DNS (*cache poisoning*), rediriger les authentifications Kerberos vers des serveurs malveillants, ou intercepter les échanges LDAP. Windows Server 2025 marque une étape importante : la gestion des clés est simplifiée, le support NSEC3 est amélioré, et l'intégration avec les partitions AD est plus robuste qu'avec toutes les versions précédentes. Pour les RSSI et DSI des entités soumises à NIS2, DNSSEC n'est plus une option — c'est une exigence de conformité. Ce guide expert couvre l'intégralité du cycle de déploiement : des prérequis techniques à la gestion des clés KSK/ZSK en passant par les tests de validation et les particularités des zones AD-intégrées. Vous trouverez ici les commandes PowerShell exactes, les erreurs courantes et leurs solutions, ainsi qu'une checklist de déploiement opérationnelle pour vos DC Windows Server 2025. Que vous déployiez DNSSEC pour la première fois ou que vous migriez depuis une configuration existante, ce guide vous accompagne pas à pas avec des exemples issus de terrains réels.



Prérequis avant le déploiement DNSSEC

Avant de signer votre première zone DNS, il convient de valider l'environnement sur plusieurs dimensions. Un déploiement DNSSEC raté sur une zone AD-intégrée peut perturber la résolution DNS de tout votre domaine.

Niveau fonctionnel et rôle DNS

Windows Server 2025 supporte DNSSEC quel que soit le niveau fonctionnel de la forêt AD, mais les fonctionnalités avancées (distribution automatique des Trust Anchors) requièrent que tous vos DC tournent au minimum sous Windows Server 2012 R2. Vérifiez que le rôle DNS est bien installé sur vos DC cibles :

```
 Get-WindowsFeature DNS
Get-DnsServerSetting -ComputerName $env:COMPUTERNAME
```

DNS intégré AD vs. zones fichier

La grande majorité des entreprises utilisant AD Deploy utilisent des zones DNS intégrées à l'annuaire (Active Directory Integrated Zones). C'est la configuration recommandée et celle qui offre la meilleure expérience DNSSEC : les enregistrements de signature sont répliqués via AD plutôt que via AXFR/IXFR, et la gestion des clés peut être centralisée. Les zones fichier-based (.dns) supportent également DNSSEC mais nécessitent une gestion manuelle des transferts de zone incluant les enregistrements DNSSEC.

Support NSEC et NSEC3

NSEC (Next Secure) et NSEC3 (Next Secure version 3) sont les deux mécanismes de proof-of-nonexistence de DNSSEC. NSEC expose la liste des noms de votre zone (zone walking), ce qui peut être considéré comme une fuite d'information. NSEC3 résout ce problème via un hash SHA-1 des noms. Windows Server 2025 supporte les deux ; Microsoft recommande NSEC3 avec au moins 100 itérations de hachage pour les zones exposées publiquement.

Configuration DNSSEC via DNS Manager (interface graphique)

La console DNS Manager (dnsmgmt.msc) offre un assistant de signature de zone qui guide l'administrateur à travers toutes les étapes. C'est l'approche recommandée pour un premier déploiement — elle expose clairement les paramètres de clés et permet de valider visuellement chaque étape.

> ⚡ **Retour terrain**
>
> Pour un éditeur SaaS RH qui migrait vers Kubernetes, la première mise en production a révélé des pods qui consommaient 10× plus de mémoire que prévu — sans limits

configurées, ils saturaient les nodes. J'avais prévenu que les limits et requests devaient être calibrées avant le départ en production. La leçon retenue : dans un cluster mutualisé, un pod sans limite est une bombe à retardement pour les voisins.

Étapes de signature via l'assistant

Ouvrez **DNS Manager** (dnsmgmt.msc) sur votre DC principal (PDC Emulator de préférence).

Dans le panneau gauche, développez le serveur DNS, puis **Forward Lookup Zones**.

Clic droit sur la zone à signer → **DNSSEC** → **Sign the Zone**.

L'assistant DNSSEC Zone Signing Wizard s'ouvre. Choisissez **Customize zone signing parameters** pour contrôler les paramètres de clés.

Configurez la clé KSK (Key Signing Key) : algorithme RSA/SHA-256, longueur 2048 bits minimum. Activez la distribution automatique des Trust Anchors si tous vos DC sont ≥ 2012 R2.

Configurez la clé ZSK (Zone Signing Key) : RSA/SHA-256, 1024 ou 2048 bits, durée de vie DNSKEY 1 heure, durée de signature des enregistrements (validity period) 7 jours recommandé.

Sélectionnez **NSEC3** avec paramètres de hachage par défaut (SHA-1, 100 itérations).

Finalisez : l'assistant génère les clés, signe tous les enregistrements existants et crée les enregistrements DNSKEY, RRSIG, NSEC3, et NSEC3PARAM dans la zone.

Après signature, la zone apparaît avec un cadenas dans DNS Manager. Vous pouvez vérifier la présence des enregistrements DNSSEC dans les propriétés de la zone.

Configuration DNSSEC via PowerShell

PowerShell est indispensable pour l'automatisation, le déploiement multi-DC et la gestion des rollover de clés. Le module DnsServer inclus dans Windows Server 2025 expose toutes les cmdlets nécessaires.

```
# Signer une zone DNS avec DNSSEC
$zone = "corp.example.fr"
Invoke-DnsServerZoneSign -ZoneName $zone -SignWithDefault $true -Force

# Vérifier la signature
Get-DnsServerResourceRecord -ZoneName $zone -RRType DNSKEY
Get-DnsServerResourceRecord -ZoneName $zone -RRType RRSIG | Select Name, TimeToLive, RecordData

# Configurer le rollover KSK automatique
$ksk = Get-DnsServerSigningKey -ZoneName $zone | Where { $_.KeyType -eq "KeySigningKey" }
Set-DnsServerSigningKey -ZoneName $zone -KeyId $ksk.KeyId -KeyRolloverStatus $true -RolloverPerio

# Tester la résolution DNSSEC
Resolve-DnsName -Name "corp.example.fr" -Type SOA -DnssecOk -Server "8.8.8.8"
# AD bit = True si DNSSEC validé

# Vérifier depuis un client Windows
Resolve-DnsName "_kerberos._tcp.corp.example.fr" -Type SRV -DnssecOk | Select Name, Type, QueryTy
```

Le paramètre `-SignWithDefault $true` utilise les paramètres par défaut de Microsoft pour Windows Server 2025 : RSA/SHA-256, KSK 2048 bits, ZSK 1024 bits, rollover annuel pour KSK, rollover mensuel pour ZSK. Pour les environnements à haute exigence, customisez via `Invoke-DnsServerZoneSign` avec les paramètres explicites.

Afficher l'état de signature d'une zone

```
# État global de la zone
Get-DnsServerZone -Name $zone | Select ZoneName, IsDsIntegrated, IsSignedWithNSEC3, ZoneType

# Toutes les clés de signature
Get-DnsServerSigningKey -ZoneName $zone | Select KeyType, KeyId, KeyLength, CryptoAlgorithmId, Ac

# Statistiques de signature
Get-DnsServerStatistics -ZoneName $zone | Select *Sign*
```

Gestion des clés KSK et ZSK

La gestion du cycle de vie des clés est l'aspect le plus critique d'une infrastructure DNSSEC. Une mauvaise gestion du rollover KSK peut rendre votre zone inaccessible pour les résolveurs validants.

Architecture KSK / ZSK

DNSSEC utilise deux types de clés avec des rôles distincts :

KSK (Key Signing Key) : clé de longue durée (typiquement 1 à 2 ans). Elle signe uniquement les enregistrements DNSKEY. Son empreinte (DS record) est publiée chez le registrar parent. La rotation KSK est l'opération la plus délicate car elle nécessite une coordination avec le registrar.

ZSK (Zone Signing Key) : clé de courte durée (typiquement 30 à 90 jours). Elle signe tous les autres enregistrements de la zone (A, AAAA, MX, CNAME, etc.). La rotation ZSK est transparente et entièrement gérée par Windows Server.

Rollover KSK sur Windows Server 2025

Windows Server 2025 supporte le rollover KSK automatique via le mécanisme RFC 5011 (automatic trust anchor update) lorsque tous les DC et clients supportent ce mécanisme. Pour les environnements mixtes, le rollover manuel reste nécessaire :

```
 # Déclencher un rollover KSK manuel
$ksk = Get-DnsServerSigningKey -ZoneName $zone | Where { $_.KeyType -eq "KeySigningKey" }
Invoke-DnsServerSigningKeyRollover -ZoneName $zone -KeyId $ksk.KeyId -Force

# Surveiller l'état du rollover
Get-DnsServerSigningKey -ZoneName $zone | Select KeyType, KeyId, NextRolloverAction, NextRollover
```

Après un rollover KSK, vous devez mettre à jour le DS record chez votre registrar avec la nouvelle empreinte. Windows Server affiche la nouvelle empreinte via :

```
Get-DnsServerResourceRecord -ZoneName $zone -RRType DS | Select Name, RecordData
```

Durées de vie recommandées

Paramètre	Valeur recommandée (ANSSI)	Windows Server 2025 par défaut
KSK — longueur	2048 bits RSA ou ECDSA P-256	2048 bits RSA
KSK — durée de vie	12 à 24 mois	12 mois
ZSK — longueur	1024 à 2048 bits RSA	1024 bits RSA
ZSK — durée de vie	30 jours	30 jours
Signature RRSIG validity	7 à 14 jours	7 jours
NSEC3 itérations	≥ 100 (public), 0 suffisant (interne)	0

Résolution et validation côté clients

DNSSEC ne sert à rien si les clients ne valident pas les signatures. La chaîne de validation doit être configurée depuis le résolveur jusqu'au Trust Anchor de la zone racine.

Trust Anchors et forwarders

Pour les zones internes (corp.example.fr), vos DC font office de résolveurs autoritaires et validants. Les clients Windows qui pointent sur vos DC pour la résolution DNS bénéficient automatiquement de la validation DNSSEC si elle est configurée sur le DC.

Pour les zones externes, configurez vos DC en forwarders vers des résolveurs validants (8.8.8.8, 1.1.1.1, ou votre résolveur récursif interne validant DNSSEC) :

```
 # Configurer les forwarders DNSSEC-validants
Set-DnsServerForwarder -IPAddress "8.8.8.8","1.1.1.1" -UseRootHint $false

# Activer la validation DNSSEC sur le résolveur local
Set-DnsServerRecursion -Enable $true
Set-DnsServerCache -LockingPercent 100
```

Distribution des Trust Anchors

Pour les zones AD-intégrées signées, Windows Server gère automatiquement la distribution des Trust Anchors aux DC membres via la partition d'annuaire ForestDnsZones. Vérifiez la distribution :

```
 Get-DnsServerTrustAnchor -ZoneName $zone
# Les Trust Anchors doivent apparaître sur tous vos DC
```

Test et audit DNSSEC

La validation post-déploiement est critique. Ne considérez pas votre zone DNSSEC comme opérationnelle tant que vous n'avez pas testé la chaîne de confiance complète.

Tests PowerShell

```
 # Test de base — flag AD (Authenticated Data) doit être True
Resolve-DnsName -Name "corp.example.fr" -Type SOA -DnssecOk -Server "127.0.0.1"

# Tester un enregistrement spécifique
Resolve-DnsName -Name "_ldap._tcp.corp.example.fr" -Type SRV -DnssecOk

# Vérifier les enregistrements DNSKEY directement
Resolve-DnsName -Name "corp.example.fr" -Type DNSKEY -Server "127.0.0.1"
```

Tests avec dnscmd

```
 # Vérifier l'état de signature de la zone
dnscmd /zoneinfo corp.example.fr

# Lister les enregistrements DNSSEC de la zone
dnscmd /enumrecords corp.example.fr @ /type DNSKEY
dnscmd /enumrecords corp.example.fr @ /type RRSIG
```

Outils externes gratuits

zonemaster.net : teste la délégation DNSSEC complète (DS, DNSKEY, RRSIG, chaîne de confiance). Idéal pour les zones publiques.

dnsviz.net : visualisation graphique de la chaîne de délégation DNSSEC. Identifie visuellement les ruptures de chaîne.

Nmap DNS scripts : `nmap -sU -p 53 --script dns-nsec-enum --script-args dns-nsec-enum.domains=example.fr <dns-server>`

dig (sur Linux/WSL) : `dig +dnssec +multi corp.example.fr SOA`

DNSSEC sur zones AD-intégrées : particularités multi-DC

Le déploiement DNSSEC sur des zones AD-intégrées dans un environnement multi-DC présente des particularités importantes que les guides généralistes ignorent souvent.

Réplication des enregistrements DNSSEC

Les enregistrements DNSSEC (DNSKEY, RRSIG, NSEC3, NSEC3PARAM, DS) sont stockés dans la partition d'annuaire AD (ForestDnsZones ou DomainDnsZones) et répliqués via la réplication AD standard. La latence de réplication AD (typiquement <15 minutes en intrasite)

peut créer une fenêtre pendant laquelle certains DC servent des réponses non signées après une mise à jour de clé.

DC maître de signature

Un seul DC est désigné comme *Key Master* — c'est lui qui génère et gère les clés DNSSEC. Par défaut, Windows Server choisit le PDC Emulator. Si le Key Master tombe, les signatures peuvent expirer si les ZSK ne sont pas renouvelées. Vérifiez et transférez le rôle si nécessaire :

```
 # Identifier le Key Master actuel
Get-DnsServerZone -Name $zone | Select ZoneName, KeyMasterServer

# Transférer le Key Master vers un autre DC
Set-DnsServerPrimaryZone -Name $zone -KeyMasterServer "dc02.corp.example.fr"
```

Cohérence des Trust Anchors entre DC

Après un rollover KSK, vérifiez que le nouveau Trust Anchor est bien distribué sur tous vos DC avant d'envoyer le nouveau DS record au registrar. Un DS record mis à jour chez le registrar mais non distribué aux DC internes causera des échecs de validation pour les clients utilisant ces DC comme résolveurs.

Problèmes courants et résolution

Fragmentation UDP et EDNS0

Les réponses DNSSEC sont volumineuses — un enregistrement DNSKEY RSA 2048 bits fait environ 300 octets, et une réponse complète avec RRSIG peut dépasser 1500 octets. Si vos pare-feux bloquent les fragments UDP ou limitent UDP à 512 octets (RFC 1035 original), les clients tomberont en TCP fallback. Ce comportement ralentit la résolution et peut causer des timeouts.

Solutions :

Autoriser UDP 53 sans limite de taille sur les pare-feux entre DC et clients.

Autoriser TCP 53 pour le fallback.

Configurer EDNS0 buffer size approprié : `Set-DnsServerCache -MaxNegativeTtl (New-TimeSpan -Hours 1)`

Réduire la taille des clés ZSK à 1024 bits si les réponses sont trop volumineuses (compromis sécurité/performance).

Clients legacy sans support EDNS0

Les systèmes très anciens (Windows XP, certains équipements réseau) ne supportent pas EDNS0 et échouent sur les grandes réponses DNS. La solution recommandée est de les isoler derrière un résolveur récursif qui intercepte les requêtes et retourne des réponses tronquées si nécessaire — mais en pratique, ces systèmes devraient être remplacés.

Signatures expirées

Si le Key Master est hors ligne pendant une période supérieure à la durée de validité des signatures RRSIG (7 jours par défaut), les enregistrements signés deviennent invalides et la résolution échoue pour les clients validants. Surveillez l'expiration des signatures :

```
Get-DnsServerResourceRecord -ZoneName $zone -RRType RRSIG |
    Where { $_.RecordData.SignatureExpiration -lt (Get-Date).AddDays(7) } |
    Select Name, @{N="Expiration";E={$_.RecordData.SignatureExpiration}}
```

Conformité NIS2 et recommandations ANSSI

La Directive NIS2 (2022/2555), transposée en droit français par la loi du 26 mars 2024, impose aux entités essentielles et importantes des mesures de sécurité pour leur infrastructure DNS. L'ANSSI précise ces exigences dans ses guides de sécurité des systèmes d'information.

Exigences NIS2 applicables au DNS

Article 21.2.d NIS2 : sécurité de la chaîne d'approvisionnement, incluant les services de résolution DNS fournis à des tiers.

Article 21.2.h NIS2 : sécurité des ressources humaines, politiques et procédures (inclut la gestion du cycle de vie des clés DNSSEC).

Guide ANSSI "Recommandations pour la sécurisation des zones DNS" : DNSSEC est explicitement recommandé pour tous les domaines exposés publiquement des entités régulées.

Domaines .fr et registrar

L'Afnic propose DNSSEC sur l'ensemble de ses TLD (.fr, .re, .pm, .yt, .wf, .tf, .bzh, .alsace, .corsica, .paris). Pour activer DNSSEC sur votre domaine .fr, vous devez soumettre le DS record (Delegation Signer) à votre registrar accrédité Afnic après avoir signé votre zone sur votre serveur autoritaire.

Pour les organisations utilisant des DNS hébergés (OVH, Gandi, Azure DNS), vérifiez que votre prestataire supporte la délégation DNSSEC et le dépôt de DS records chez l'Afnic.

Audit de conformité DNSSEC

Pour une infrastructure Active Directory soumise à NIS2, documentez les éléments suivants dans votre politique de sécurité DNS :

Algorithmes de signature utilisés (RSA/SHA-256 minimum, ECDSA P-256 recommandé par ANSSI).

Procédures de rollover KSK et ZSK avec délais et responsables.

Procédure de mise à jour DS record chez le registrar après rollover KSK.

Surveillance des expirations de signatures (alertes J-7 minimum).

Tests périodiques de la chaîne de confiance (mensuel recommandé).

En complément de DNSSEC, consultez notre guide de sécurisation Active Directory pour une approche complète de la défense en profondeur de votre infrastructure d'annuaire.

Pour aller plus loin sur le durcissement AD selon les recommandations Microsoft, notamment les paramètres de stratégie de groupe applicables à la résolution DNS sécurisée, consultez notre article dédié.

Si votre environnement inclut une PKI interne, l'architecture DNSSEC se combine naturellement avec les certificats ADCS — consultez notre guide sur la PKI d'entreprise et le déploiement ADCS.

À RETENIR

Points clés à retenir

DNSSEC signe les enregistrements DNS mais ne les chiffre pas — complémentaire à DoH/DoT.

Déployez sur le PDC Emulator en premier ; la réplication AD propage les signatures aux autres DC.

NSEC3 est préférable à NSEC pour éviter le zone walking sur les zones publiques.

Surveillez l'expiration des signatures RRSIG — une panne du Key Master peut invalider votre zone.

Soumettez le DS record à votre registrar uniquement après avoir vérifié la propagation complète sur vos DC.

Checklist déploiement DNSSEC Windows Server 2025

Retrouvez la checklist interactive DNSSEC pour Windows Server 2025 pour valider chaque étape de votre déploiement.

[ ] Vérifier le niveau fonctionnel AD (tous DC ≥ Windows Server 2012 R2)

[ ] Confirmer que les zones DNS sont de type AD-integrated

[ ] Identifier le PDC Emulator comme Key Master DNSSEC

[ ] Signer la zone via DNS Manager ou PowerShell (RSA/SHA-256, KSK 2048 bits)

[ ] Configurer NSEC3 avec ≥ 100 itérations pour les zones publiques

[ ] Vérifier la présence des enregistrements DNSKEY, RRSIG, NSEC3 dans la zone

[ ] Configurer le rollover automatique KSK (90 à 365 jours) et ZSK (30 jours)

[ ] Distribuer les Trust Anchors à tous les DC (vérifier via Get-DnsServerTrustAnchor)

[ ] Tester la validation via Resolve-DnsName -DnssecOk (flag AD = True)

[ ] Valider via zonemaster.net et dnsviz.net

[ ] Ouvrir UDP/TCP 53 sans restriction de taille sur les pare-feux internes

[ ] Soumettre le DS record au registrar (zones publiques)

[ ] Configurer une alerte sur l'expiration des signatures RRSIG (J-7)

[ ] Documenter les procédures de rollover dans la politique de sécurité DNS

[ ] Planifier un test mensuel de la chaîne de confiance

FAQ — DNSSEC Windows Server 2025

DNSSEC est-il supporté sur les zones DNS intégrées à Active Directory ?

Oui. Windows Server 2008 R2 a introduit le support DNSSEC, et Windows Server 2025 le perfectionne. Les zones DNS intégrées à AD peuvent être signées via DNS Manager ou PowerShell (Invoke-DnsServerZoneSign). La signature est stockée dans les partitions d'annuaire

AD et répliquée automatiquement entre tous les DC portant le rôle DNS. Toutefois, contrairement aux zones fichier-based, la gestion des Trust Anchor Distribution Points (TADP) requiert une attention particulière pour les zones AD-integrated.

Quelle est la différence entre DNSSEC et DNS over HTTPS ?

DNSSEC (DNS Security Extensions) est un mécanisme d'intégrité et d'authenticité : il signe cryptographiquement les enregistrements DNS pour garantir qu'ils n'ont pas été falsifiés. Il ne chiffre pas le trafic DNS. DNS over HTTPS (DoH) est un protocole de confidentialité : il encapsule les requêtes DNS dans HTTPS pour chiffrer le trafic et masquer les requêtes aux observateurs réseau. Ces deux mécanismes sont complémentaires : DNSSEC protège l'intégrité des données, DoH protège la confidentialité des échanges. NIS2 et les recommandations ANSSI préconisent DNSSEC pour les domaines critiques ; DoH est davantage un choix de politique de confidentialité.

Comment tester que DNSSEC est bien configuré sur Windows Server 2025 ?

Plusieurs méthodes : (1) PowerShell : Resolve-DnsName -Name 'votre.domaine.fr' -Type SOA -DnssecOk — vérifiez que le flag AD (Authenticated Data) est True ; (2) dnscmd /zoneinfo votre.zone pour confirmer l'état de signature ; (3) outils en ligne gratuits : zonemaster.net (teste la chaîne de confiance complète) et dnsviz.net (visualisation graphique de la délégation DNSSEC) ; (4) Nmap avec le script dns-nsec-enum pour énumérer les enregistrements NSEC/NSEC3 ; (5) vérifier la présence des enregistrements DNSKEY, RRSIG, NSEC/NSEC3 et DS dans votre zone parent.

DNSSEC casse-t-il la résolution DNS pour les clients legacy ?

Pas directement, mais des problèmes peuvent survenir. Les clients qui ne supportent pas EDNS0 (extension requise pour les grandes réponses DNSSEC) peuvent échouer si les réponses dépassent 512 octets. Les anciens pare-feux bloquant UDP > 512 octets causent des timeouts. Les clients legacy ignorent simplement les enregistrements DNSSEC — ils reçoivent les

réponses DNS normales sans validation. Le risque réel est côté infrastructure réseau : assurez-vous que UDP 1232+ et TCP 53 (fallback) sont autorisés entre vos DC et vos clients.

NIS2 impose-t-il DNSSEC pour les organisations françaises ?

NIS2 (Directive 2022/2555, transposée en France) impose aux entités essentielles et importantes des mesures de gestion des risques incluant explicitement la sécurité de la résolution de noms. L'ANSSI préconise fortement DNSSEC pour les domaines critiques. Pour les domaines en .fr, l'Afnic propose DNSSEC sur tous ses TLD. Bien que NIS2 ne cite pas DNSSEC nommément, son absence pour une entité essentielle gérant des services critiques sera difficilement justifiable lors d'un audit de conformité.

Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory