Serveur DNS sous Windows Server 2025

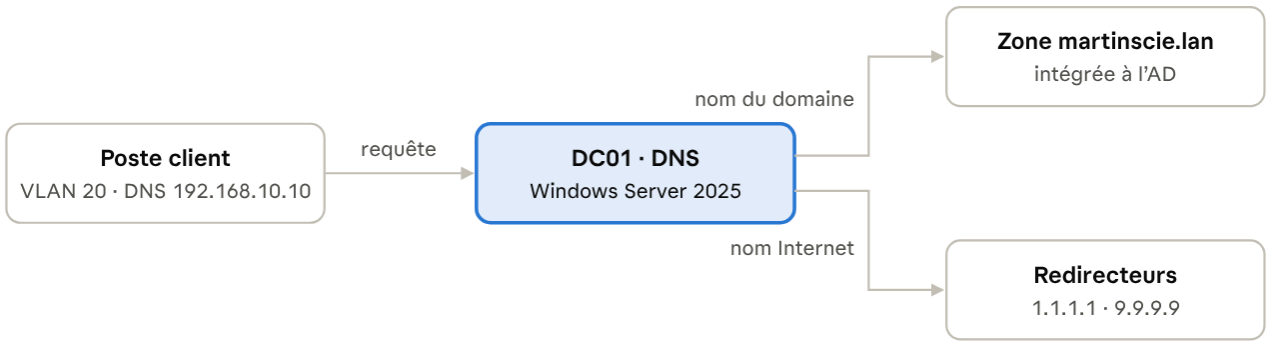
Nov 27, 2026 · @Serge Martins

Objectif et architecture

Le DNS traduit les noms (`dc01.martinscie.lan`) en adresses IP. Dans un domaine Active Directory, il est indispensable : les postes trouvent les contrôleurs de domaine grâce aux enregistrements SRV. Ce guide configure le rôle DNS de **DC01** (Windows Server 2025), installé lors de la promotion, et explique comment l'installer sur un autre serveur.

Élément	Valeur (à adapter)
Serveur DNS	`DC01` – `192.168.10.10` (contrôleur de domaine)
Zone directe	`martinscie.lan` (intégrée à l'Active Directory)
Zones inverses	`10.168.192.in-addr.arpa` , `20.168.192.in-addr.arpa`
Redirecteurs	`1.1.1.1` , `9.9.9.9`
Clients	Postes du VLAN 20 (DNS distribué par DHCP, option 006)

DC01 répond pour martinscie.lan et relaie le reste vers Internet



Résolution DNS par DC01

1. Installation du rôle

Sur un contrôleur de domaine, le rôle DNS est déjà installé (case « Serveur DNS » de la promotion). Sur un autre serveur membre :

```
Install-WindowsFeature DNS -IncludeManagementTools
Get-Service DNS
```

La console s'ouvre par Gestionnaire de serveur > Outils > **DNS** (`dnsmgmt.msc`).

2. Zones

2.1 Zone directe intégrée à l'AD : `martinscie.lan` est créée par la promotion. Elle est stockée dans l'annuaire et répliquée vers tous les DC. Vérifier qu'elle n'accepte que les **mises à jour sécurisées** :

```
Get-DnsServerZone
Set-DnsServerPrimaryZone -Name martinscie.lan -DynamicUpdate Secure
```

2.2 Zones inverses (adresse → nom) :

```
Add-DnsServerPrimaryZone -NetworkId "192.168.10.0/24" -ReplicationScope
Forest -DynamicUpdate Secure
Add-DnsServerPrimaryZone -NetworkId "192.168.20.0/24" -ReplicationScope
Forest -DynamicUpdate Secure
```

Interface : console DNS > Zones de recherche inversée > Nouvelle zone > Zone principale, stockée dans l'AD > IPv4 > ID réseau `192.168.20` .

3. Enregistrements

```
# Hôte (A) + pointeur (PTR) en une commande
Add-DnsServerResourceRecordA -ZoneName martinscie.lan -Name parc01 -
IPv4Address 192.168.10.20 -CreatePtr

# Alias (CNAME) : glpi.martinscie.lan -> parc01
Add-DnsServerResourceRecordCName -ZoneName martinscie.lan -Name glpi -
HostNameAlias parc01.martinscie.lan

# Messagerie (MX)
Add-DnsServerResourceRecordA -ZoneName martinscie.lan -Name mail01 -
IPv4Address 192.168.10.25 -CreatePtr
Add-DnsServerResourceRecordMX -ZoneName martinscie.lan -Name "." -
MailExchange mail01.martinscie.lan -Preference 10

Get-DnsServerResourceRecord -ZoneName martinscie.lan
```

Type	Rôle	Exemple
A	Nom → adresse IPv4	`parc01` → `192.168.10.20`
PTR	Adresse → nom	`20` → `parc01.martinscie.lan`
CNAME	Alias	`glpi` → `parc01`
MX	Serveur de messagerie du domaine	`mail01`, priorité 10
SRV	Service (LDAP, Kerberos)	`_ldap._tcp.dc._msdcs` (créé par l'AD)

4. Résolution des noms Internet

```
# Redirecteurs : les requêtes externes partent vers ces serveurs
Set-DnsServerForwarder -IPAddress 1.1.1.1, 9.9.9.9 -UseRootHint $true

# Redirecteur conditionnel : la zone sambalab.lan est demandée au DC Samba
Add-DnsServerConditionalForwarderZone -Name sambalab.lan -MasterServers
192.168.10.11 -ReplicationScope Forest
```

5. Maintenance et sécurité

```
# Nettoyage des enregistrements obsolètes (postes disparus)
Set-DnsServerScavenging -ScavengingState $true -ScavengingInterval 7.00:00:00
-ApplyOnAllZones
Set-DnsServerZoneAging -Name martinscie.lan -Aging $true

# Interdire les transferts de zone (aucun serveur secondaire autorisé)
Set-DnsServerPrimaryZone -Name martinscie.lan -SecureSecondaries NoTransfer

# Consulter le journal du service
Get-WinEvent -LogName "DNS Server" -MaxEvents 20
```

- Ne jamais exposer le port 53 du DC sur Internet.
- Optionnel : signer la zone avec DNSSEC (console DNS > clic droit sur la zone > DNSSEC > Signer la zone).

6. DNS over HTTPS (DoH)

Depuis la mise à jour de juin 2026, Windows Server 2025 peut chiffrer les requêtes des clients en HTTPS. Il faut un certificat TLS sur le serveur, puis :

```
Set-DnsServerEncryptionProtocol -EnableDoh $true -UriTemplate
"https://dc01.martinscie.lan/dns-query"
Get-DnsServerEncryptionProtocol
```

Côté Windows 11 : Paramètres > Réseau > Ethernet > Attribution du serveur DNS > Chiffrement DNS **HTTPS uniquement**, avec le même modèle d'URI. Le DNS classique (port 53) continue de fonctionner en parallèle.

7. Tests et dépannage

```
Resolve-DnsName dc01.martinscie.lan
Resolve-DnsName 192.168.10.10                        # résolution inverse
Resolve-DnsName _ldap._tcp.dc._msdcs.martinscie.lan -Type SRV
Resolve-DnsName www.debian.org                       # redirecteurs
dcdiag /test:dns
ipconfig /flushdns ; ipconfig /registerdns           # sur un poste
Clear-DnsServerCache                                  # sur le serveur
```

Symptôme	Cause probable	Correction
Les postes ne joignent pas le domaine	DNS du poste = box ou DNS public	DNS = `192.168.10.10` (DHCP option 006)
Pas de résolution Internet	Redirecteurs absents ou bloqués par pfSense	Vérifier les redirecteurs et l'UDP/TCP 53 sortant
`nslookup` affiche « Serveur : UnKnown »	Pas de zone inverse ou de PTR pour le DNS	Créer la zone inverse et le PTR de DC01
Anciens noms qui répondent encore	Enregistrements obsolètes	Activer le nettoyage (§ 5)
Un poste n'apparaît pas dans le DNS	Mise à jour dynamique en échec	`ipconfig /registerdns`, vérifier « Sécurisé uniquement »