DNS

Le DNS traduit un **nom** en **adresse IP** (et l'inverse). Dans un domaine Active Directory, **le DNS est indispensable** : les clients trouvent les contrôleurs de domaine grâce à des enregistrements DNS (SRV).

Fonctionnement d'une résolution

```
Client ──(récursive)──> SRV01 (DNS local)
                        │ pas dans ses zones ni dans son cache ?
                        ├──> serveur racine "."        → « demande à .be »
                        ├──> serveur TLD ".be"         → « demande à hugo-pierret.be »
                        └──> serveur faisant autorité   → « wiki = 1.2.3.4 »
Client <──── réponse ──── SRV01 (garde la réponse en cache pendant le TTL)
```

- **Requête récursive** : le client demande « donne-moi la réponse finale ».
- **Requête itérative** : le serveur DNS interroge les autres serveurs étape par étape.

Les serveurs racine (root servers)

- 13 **noms** de serveurs racine, de `a.root-servers.net` à `m.root-servers.net`, gérés par 12 organisations.
- Grâce à l'**anycast**, ce sont en réalité **plus de 1 500 instances** réparties dans le monde. Carte : https://root-servers.org/
- Windows Server connaît leurs adresses grâce aux **indications de racine** (*root hints*) : console DNS → propriétés du serveur → onglet **Indications de racine**.

Redirecteurs vs indications de racine

	Redirecteur (*forwarder*)	**Indications de racine**
Principe	« Je ne sais pas → je demande à **ce** serveur » (DNS de l'école, 1.1.1.1, 8.8.8.8…)	« Je ne sais pas → je fais moi-même la résolution itérative à partir des serveurs racine »
Avantage	Rapide, profite du cache du serveur amont, passe les pare-feu	Aucune dépendance à un autre serveur
Labo	Souvent nécessaire si le réseau de l'école bloque le DNS sortant	Utilisé si aucun redirecteur ne répond

Redirecteur conditionnel : « pour le domaine `ecole.local`, demande à `10.2.x.x` ». Utile entre deux domaines AD.

Zones

Type	Rôle	Exemple
Zone de recherche directe	Nom → IP	`hp.lan`
Zone de recherche inversée	IP → nom	`1.19.10.in-addr.arpa` (pour 10.19.1.0/24, octets à l'envers)

Types de stockage :

- **Principale** : copie modifiable.
- **Secondaire** : copie en lecture seule obtenue par transfert de zone.
- **Stub** : contient seulement les NS/SOA d'une autre zone.
- **Intégrée à Active Directory** : stockée dans AD, répliquée avec AD, **mises à jour dynamiques sécurisées**. C'est le choix par défaut sur un DC.

Enregistrements principaux

Type	Rôle	Exemple
A	Nom → IPv4	`srv01 → 10.19.1.254`
AAAA	Nom → IPv6	
PTR	IP → nom (zone inversée)	`254 → srv01.hp.lan`
CNAME	Alias vers un autre nom	`intranet → srv01.hp.lan`
MX	Serveur de mail du domaine	
NS	Serveurs faisant autorité pour la zone	
SOA	Infos de la zone : serveur principal, numéro de série, TTL...	
SRV	Localise un **service** : c'est ainsi que les clients trouvent le DC	`_ldap._tcp.dc._msdcs.hp.lan`

Installation et configuration (PowerShell)

Le rôle DNS s'installe **automatiquement** pendant la promotion du DC (`-InstallDns`). Sinon :

```
Install-WindowsFeature DNS -IncludeManagementTools

# Zone inversée pour le LAN, intégrée à AD
Add-DnsServerPrimaryZone -NetworkId "10.19.1.0/24" -ReplicationScope Domain

# Enregistrements
Add-DnsServerResourceRecordA     -ZoneName "hp.lan" -Name "rtrhp01" -IPv4Address 10.19.1.1 -
CreatePtr
Add-DnsServerResourceRecordCName -ZoneName "hp.lan" -Name "intranet" -HostNameAlias
"srv01.hp.lan"

# Redirecteur
Add-DnsServerForwarder -IPAddress 10.2.51.254      # ou le DNS de l'école, 1.1.1.1…
Get-DnsServerForwarder

# Vider le cache du serveur DNS
Clear-DnsServerCache
```

nslookup

```
C:\> nslookup
Serveur par défaut :   UnKnown
Address:  10.19.1.254
>
```

- **Sans argument**, `nslookup` passe en **mode interactif** et affiche **le serveur DNS utilisé** par la machine. Pratique pour vérifier rapidement la configuration DNS.
- `UnKnown` : nslookup essaie de résoudre l'**IP du serveur DNS en nom** (requête PTR). S'il n'y a **pas de zone inversée** (ou pas de PTR), il affiche `UnKnown`. Ce n'est pas grave, mais créer la zone inversée corrige l'affichage.

Commandes utiles :

```
nslookup srv01.hp.lan                # résolution A
nslookup 10.19.1.254                 # résolution inverse (PTR)
nslookup google.com 1.1.1.1          # interroger un serveur précis
nslookup -type=SRV _ldap._tcp.dc._msdcs.hp.lan   # trouver les DC du domaine
nslookup -type=MX gmail.com
```

En mode interactif : `server 1.1.1.1` (changer de serveur), `set type=ns`, `exit`.

PowerShell : `Resolve-DnsName srv01.hp.lan`, `Resolve-DnsName -Type SRV _ldap._tcp.dc._msdcs.hp.lan`.

Questions de révision

1. Quelle est la différence entre une requête récursive et une requête itérative ?
2. Combien y a-t-il de serveurs racine ? Et combien de machines réelles derrière ?
3. Pourquoi nslookup affiche-t-il `UnKnown` comme nom du serveur ? Comment corriger ?
4. Quel type d'enregistrement permet à un client de trouver un contrôleur de domaine ?
5. Quel DNS doit être configuré sur un poste membre du domaine : le DC ou 8.8.8.8 ? Pourquoi ?
6. Quand utilise-t-on un redirecteur plutôt que les indications de racine ?

Revision #1
Created 2 November 2026 13:51:04 by Hugo
Updated 2 November 2026 13:51:04 by Hugo