Table des matières

1 Le fichier Hosts

Les machines traitent aussi aisément les chiffres que les lettres. Il n'en va pas de même pour les humains ! Nous avons beaucoup plus facile avec les noms qu'avec les enfilades de chiffres des adresses IP.

Le fichier hosts a vu le jour dès les débuts d'Arpanet, le précurseur d'Internet. Il était géré manuellement le Stanford Research Institute et disponible en téléchargement pour les membres d'Arpanet. Dans les années 70, le fichier contenait dans les 200 hosts. Il a commencé à montrer ses limites au début des années 80.

Le fichier hosts.txt est un simple fichier texte qui met en relation l'IP des hosts avec les hostsnames :

127.0.0.1 localhost

La gestion manuelle d'un fichier central a rapidement montré ses limites :

- Délais de mise à jour
- Nécessité de télécharger régulièrement le nouveau hosts.txt
- Taille du fichier (en Go !)

Même si le fichier central hosts.txt du Stanford Research Institute n'est plus utilisé, le fichier hosts hérité de cette époque reste présent dans les systèmes d'exploitation. Windows conserve le fichier HOSTS dans le dossier %SystemRoot%\System32\drivers\etc. Il est utilisé comme source primaire pour la résolution des noms.

2 NetBIOS

NetBIOS a été développé en 1983 par Sytek Inc. comme interface de programmation pour les communications entre ordinateurs IBM PC sur des petits réseaux locaux. NetBIOS est une API non un protocole réseau. Il repose sur le protocole de son époque : IPX/SPX. Ensuite, il a été adapté à TCP/IP.

Pour être en mesure d'utiliser NetBIOS sur le réseau Token Ring, IBM a conçu un émulateur appelé NetBEUI (NetBIOS Extended User Interface).

Le nom NetBEUI est aussi le nom retenu par Microsoft pour son implémentation du protocole réseau non routable NetBIOS Frames (NBF). Au final, NetBUI désigne donc :

- Un émulateur conçu par IBM.
- Un protocole réseau de Microsoft.

Dans les années 90, le protocole « NetBIOS Frames » est en vogue chez Microsoft ; il est notamment utilisé par Windows 3.1, Windows 3.11, Windows 95 et Windows NT. Il présente cependant de nombreux inconvénients : des noms codés en seulement 16 caractères dont 1 réservé pour définir le type de service et un fonctionnement en mode broadcast. De plus Il n'est pas hiérarchisé et est utilisé uniquement par Microsoft.

3 WINS

Windows Internet Name Service est l'implémentation Microsoft d'un serveur de noms NBNS (NetBIOS Name Service) qui fournit les services d'enregistrement et d'interrogation d'une base de données contenant un mapping des adresses IP et des noms NetBIOS.

Par rapport à tout ce qui a été conçu auparavant, WINS offres des avantages significatifs :

- Grâce à l'usage de NetBIOS over TCP/IP (NBT), il fonctionne dans les réseaux routés (ce qui n'était pas le cas de NBF).
- Dès le démarrage, un client WINS enregistre dynamiquement son nom et son adresse IP sur le serveur WINS (exit les soucis de maintien manuel d'un fichier).
- En l'absence de fichier à maintenir de façon manuelle ou statique, les clients peuvent recevoir une adresse IP dynamique distribuée par un DHCP.
- Les clients interrogent le serveur WINS pour résoudre les noms (plus de broadcast inutile).
- Via l'explorateur, il est possible de parcourir la liste des ordinateurs enregistré (y compris dans des domaines et des sous-réseaux différents).
- La base de données est distribuée et répliquée sur plusieurs serveurs assurant ainsi une redondance des informations.

En cas d'indisponibilité du serveur WINS, le fichier texte local Lmhosts contient le mappage des adresses IP (Internet Protocol) sur les noms NetBIOS des serveurs distants. Il se trouve dans %SystemRoot%\System32\Drivers\Etc. Le fichier LMhost.sam est un peu plus élaboré que hosts, il permet de pré charger des entrées (#PRE).

```
129.102.12.10   Paul            #PRE

148.107.16.45   Jacques
```

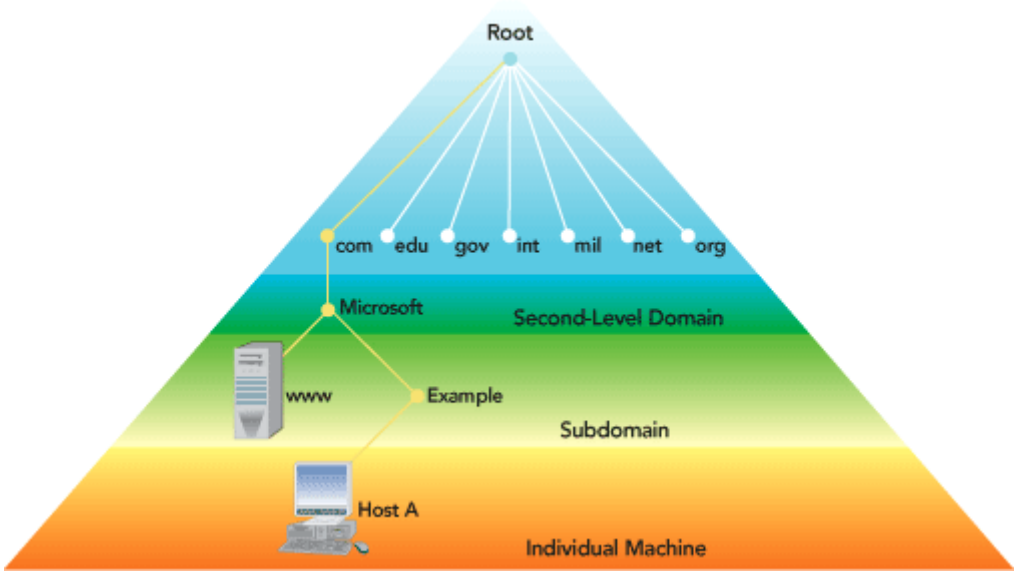
4 DNS

Même si WINS présentait déjà des avancées majeures, le système n'a pas été conçu pour une utilisation à grande échelle en outre, il n'est pas hiérarchisé. Le DNS ou Domain Name System est un système d'annuaire décentralisé et hiérarchisé permettant de retrouver l'adresse IP d'un ordinateur sur base du nom de la machine et du nom de domaine. Il a été conçu au début des années 80 à la demande de la DRAPA.

4.1 Principe du DNS

Le DNS consiste en une hiérarchie dont le sommet est appelé la racine. Un domaine peut contenir un ou plusieurs sous-domaines ainsi que d'éventuelles délégations. Les délégations permettent la prise en charge des informations des sous–domaines par d'autres serveurs. Les sous-domaines peuvent également déléguer de nouveaux sous-domaines vers d'autres serveurs...

Internet repose sur le principe du DNS et permet d'en comprendre facilement le fonctionnement.



1. La racine ou root est gérée par l'IANA (Internet Assigned Numbers Authority). Elle est représentée par le point : **.**
2. Le first level domain aussi appelé top level domain (TLD) constitue le premier niveau de la hiérarchie. Initialement, il n'existait que com, edu, gov, int, mil, net et org. De nouvelles zones sont ajoutées de manière limitée mais régulière. Elles sont gérées par des organismes locaux (AFNIC en France, CIRA au Canada). Le TLD utilise une répartition géographique (be, fr, de, etc) et une répartition générique (org, edu, mil, gov).
3. Le second level domain (SLD) est constitué de noms initialement destinés aux entreprises et organismes : Microsoft, IBM, Intel, wikipedia, etc. Ils sont depuis de nombreuses années accessibles aux particuliers. A ce niveau, on parle généralement de « nom de domaine ».
4. Les sous-domaines permettent une organisation dans un domaine : technet.microsoft.com ou news.google.com.
5. Les hosts, très souvent www mais aussi ftp, etc.

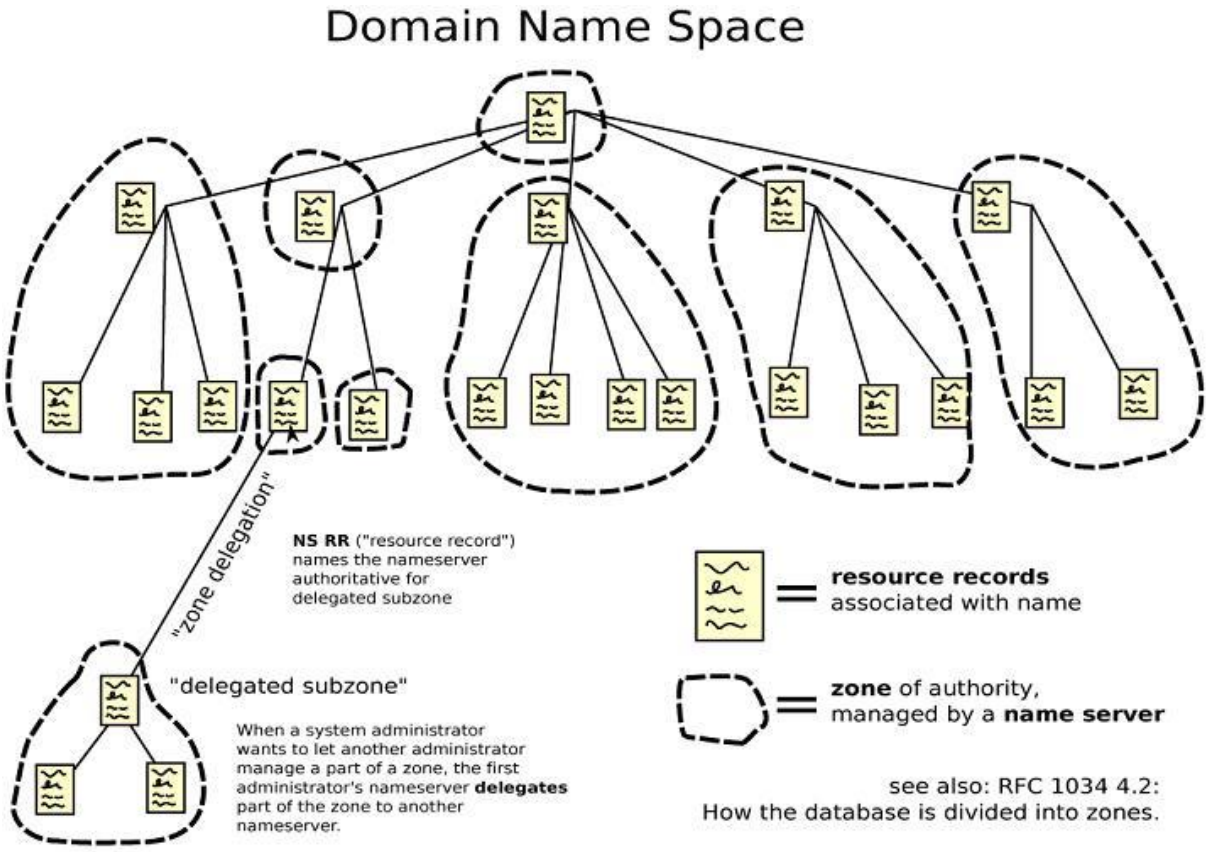
Exemple : ftp.msdn.microsoft.com

ftp = hostname, msdn = sub, microsoft = second, com = first

Où est donc le fameux point représentant la racine ? Il n'est tout simplement plus là. Mais au début d'Internet, une adresse d'écrivait ainsi : ftp.msdn.microsoft.com**.** Il y avait un « point » à la fin. Autre exemple : http://google.com**./**images

Le DNS n'est pas non plus sans rappeler l'organisation d'un disque dur avec une racine (c : en DOS ou / en Unix) une arborescence avec des sous-dossiers et au final, le fichier. Toutefois, contrairement aux chemins utilisés par les OS, qui se lisent de gauche à droite, dans le DNS, la lecture se fait de droite à gauche.

4.2 Les zones DNS



Les zones d'autorité (communément appelées zones) sont gérées par un name server. Vu dans l'autre sens, un name server (ou serveur DNS) est un serveur qui gère un ou plusieurs fichiers de zone.

- Pour chaque zone, il doit exister :
    - Au moins 1 primary server en lecture/écriture et de 0 à ∞ slave servers en lecture seule).
    - Un fichier de zone.
- Un name server peut gérer plusieurs fichiers de zone.
- Un fichier de zone peut être géré par plusieurs servers.

Dans le monde, il existe 13 name servers (de A à M) dont 10 aux USA, 2 en Europe et 1 au Japon. Ce sont les Root Hints dont l'adresse IP est déjà présente dans Windows. Les 13 Root Hints sont visibles dans les propriétés du DNS Manager.

4.3 FQDN Fully Qualified Domain Name

Le FQDN permet d'identifier un host sans ambiguïté. Il est composé de labels.

- Le FQDN est codé sur 256 octets dont un pour la longueur du nom ; 255 caractères sont donc utilisables.
- Au niveau des zones (labels), le codage se fait sur 64 octets avec un octet pour la longueur du nom ; 63 caractères sont exploitables.
- Le label nul est réservé à la racine.

Les caractères alphanumériques non accentués ainsi que l'hyphen (-) sont les seuls utilisables dans un FQDN.

5 DNS Namespace, Name server et resolver

Le DNS joue un rôle crucial autant sur Internent que dans l'Active Directory. Il est donc important de bien comprendre les rouages du système.

- DNS Namespace : Définit la structure hiérarchique en arbre dans laquelle chaque branche identifie un domaine
- Name server : Les serveurs DNS contiennent des informations sur la hiérarchie et, dans certains cas, des informations authoritatives de zone. Un serveur DNS offre un service de réponse aux requêtes des clients. Le service est capable de répondre de manière authoritative sur la zone mais aussi de « forwarder » les requêtes à d'autres name servers.
- Resolver : Le resolver est un client capable de générer des requêtes DNS qui sont envoyées directement à un ou plusieurs serveurs DNS.

Le client DNS est intégré à toutes les versions de Windows. Le rôle DNS peut être installé sur les systèmes d'exploitation Windows Server. Quand le rôle DNS est installé et configuré sur un serveur, il devient un serveur DNS.

Un client DNS n'est que client. Un serveur DNS est serveur ET client. Il joue le rôle de serveur DNS quand il répond aux requêtes des clients. Il joue le rôle de client quand il interroge d'autres serveurs DNS.

6 Mécanisme de résolution

La résolution DNS convertit un nom en adresse IP. Le processus fait appel à deux catégories de requêtes. La conversion d'une adresse IP en nom est le reverse DNS.

6.1 Requête récursive

Une requête récursive est une requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur de fournir une réponse complète. Une requête récursive ne peut pas être redirigée vers un autre serveur DNS. Le serveur DNS interrogé a trois options de réponse :

- Les informations demandées.
- Les informations demandées n'existent pas.
- Le nom de domaine demandé n'existe pas.

6.2 Requête itérative

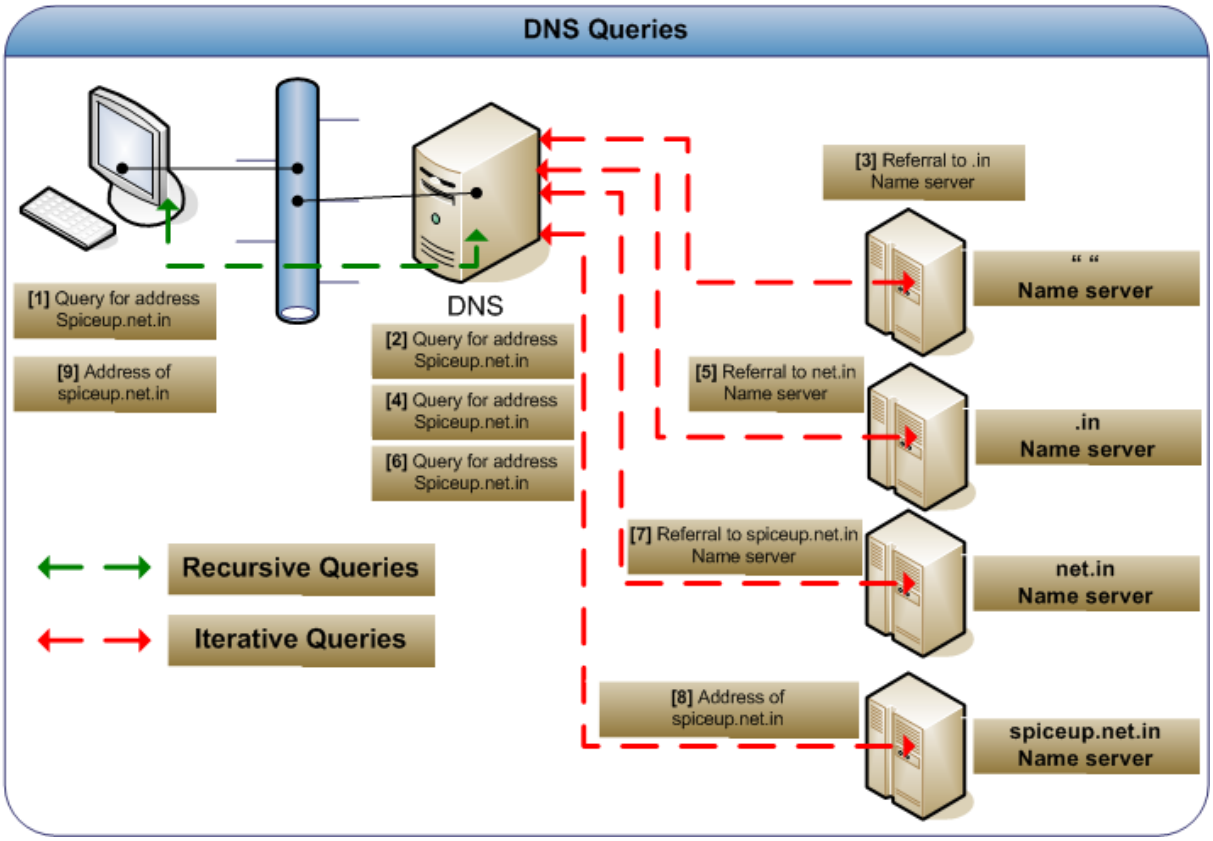
Une requête itérative est une requête envoyée à un serveur DNS dans laquelle le client DNS demande la meilleure réponse que peut fournir le serveur DNS. Le résultat d'une requête itérative est souvent une référence à un autre serveur DNS situé plus bas dans l'arborescence DNS.

6.3 Exemple

Un ordinateur fait une requête pour spiceup.net.in à un serveur DNS. Il soumet une requête au serveur DNS et attend de ce dernier une réponse : l'IP ou une erreur. Il s'agit d'une requête récursive.

Le serveur DNS qui a reçu la requête du client ne gère pas la zone demandée. Il va donc émettre une série de requêtes itératives en remontant si besoin jusqu'à la racine « . » afin d'interroger le bon name server. Le cheminement se fait par un processus récursif via la communication de l'adresse IP du serveur en charge des zones. Le serveur racine « . » donne l'IP du DNS en charge de la zone *in*, le serveur DNS en charge de *in* donne l'adresse IP du serveur DNS en charge de *net.in.*

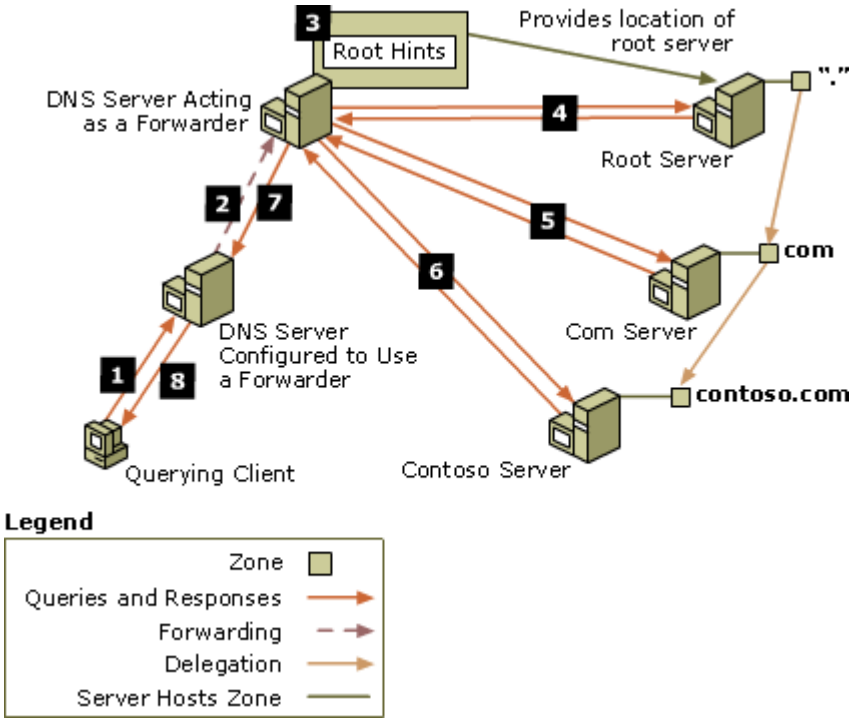
Le serveur en charge de la zone *net.in* fournit une réponse de type autoritaire (« authoritative »). C'est lui qui au final donnera l'IP correspondante à spiceup.net.in (ou signalera que la machine n'existe pas).


DNS Queries
[1] Query for address Spiceup.net.in
[9] Address of spiceup.net.in
DNS
[2] Query for address Spiceup.net.in
[4] Query for address Spiceup.net.in
[6] Query for address Spiceup.net.in
[3] Referral to .in Name server
" " Name server
[5] Referral to net.in Name server
.in Name server
[7] Referral to spiceup.net.in Name server
net.in Name server
[8] Address of spiceup.net.in
spiceup.net.in Name server
Recursive Queries
Iterative Queries

7 Forwarder et délégation

Un « forwarder » est un serveur DNS qui envoie à un serveur externe toutes les requêtes « hors zone ». L'exemple le plus simple est le DNS du FAI vers qui sont redirigées les requêtes que le serveur DNS local ne peut résoudre.

Sur l'illustration de droite, le client interroge un premier serveur DNS configuré comme forwarder. Si ce serveur ne peut répondre directement au client, il transmet la requête au serveur DNS renseigné dans sa liste de forwarders.



Un « conditionnal forwarder » est un serveur DNS qui envoie à un serveur externe les requêtes externes sur base du nom présent dans la requête. Par exemple toute requête sur une zone se terminant par test.abc.de est envoyée à un serveur DNS spécifique.

Le « forwarder » refile toutes les « patates chaudes » : tout ce que je ne connais pas, je le refile à qqu qui sait peut-être... Le « conditionnal forwarder » fait pareil, à un détail près : si la demande concerne un nom spécifique, il la forward au serveur spécifique.

La délégation consiste à transférer l'autorité d'une sous zone à un autre serveur. Exemple : Le domaine abc.de va être divisé en deux sous-zones : test.abc.de et news.abc.de. Grâce au système de délégation, l'autorité sur les sous zones va être transférée.

La délégation transfère la gestion : ce n'est pas moi qui m'occupe de ça, c'est mon « sous fifre » !

8 Cache DNS

Si toutes les requêtes devaient être systématiquement résolues, le système serait horriblement lent et la bande passante serait cannibalisée par ces requêtes. Un système de cache existe à plusieurs niveaux.

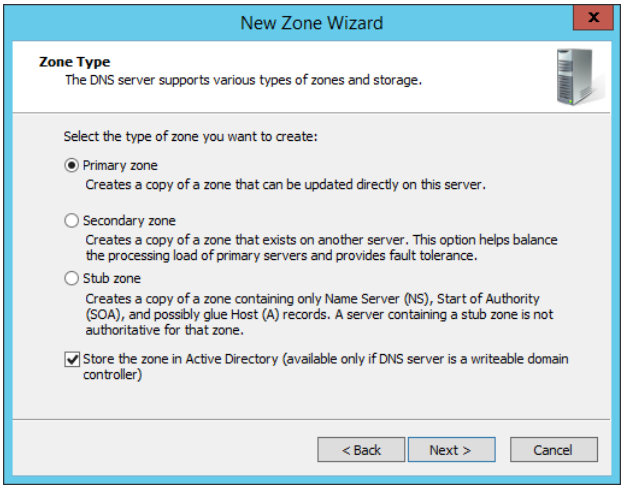
- Les clients DNS conservent en cache pendant 1 heure les réponses à leurs requêtes.
- Les serveurs stockent de manière plus conséquente les résolutions effectuées.

9 Le service DNS de Windows

Le DNS n'est pas spécifique à Microsoft, c'est d'ailleurs une de ses forces : il permet une interopérabilité entre les systèmes. Dans Windows Server, le DNS est intimement lié à l'AD, ce qui présente de nombreux avantages au niveau de la gestion et de la sécurité.

9.1 Installation et intégration

Lors de la promotion d'un serveur en domaine contrôleur, le rôle DNS peut être installé et configuré dans la foulée par Windows Server. La zone principale ainsi crée est directement intégrée à l'Active Directory.



Lors de la création d'une nouvelle zone principale ou d'une zone stub, une case à cocher permet l'intégration à l'AD

9.2 Zone primaire

Une zone primaire bénéficie de nombreux avantages :

- Accessible en lecture et en écriture : ajout, suppression et édition d'enregistrements
- Peut s'intégrer dans l'Active Directory et bénéficier de la réplication
- Les ordinateurs du domaine sont directement intégrés
- Les mises à jour sont automatiques

9.3 Zone secondaire

Une zone secondaire est une copie d'une zone primaire. Elle présente des caractéristiques différentes :

- Accessible uniquement en lecture seule : les enregistrements sont juste lisibles.
- Ne s'intègre pas dans l'AD et ne se réplique donc pas automatiquement.

9.4 Zone stub

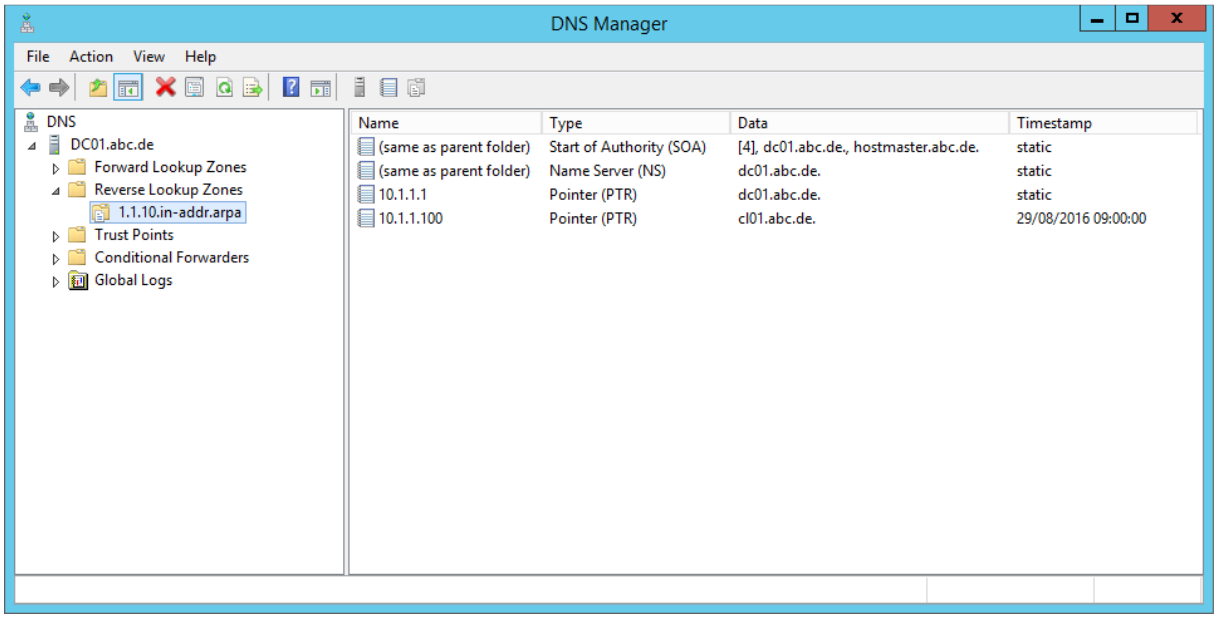
Une zone stub est une copie partielle d'une zone :

- Accessible en lecture seule
- Peut s'intégrer dans l'Active Directory et bénéficier de la réplication
- Contient uniquement les enregistrements SOA et NS ainsi que des Host A

9.5 Zone reverse

Les documents de Microsoft signalent que la création de zones reverse n'est pas obligatoire pour les « petites zones ». La configuration d'une zone reverse ne demandant guère de temps, il peut être judicieux de créer la zone reverse directement après avoir créé le zone principale, secondaire ou stub…

L'assistant de création d'une zone reverse est assez court… La capture montre une zone reverse avec l'enregistrement PTR statique du contrôleur de domaine DC01.ABC.DE (créé et à créer manuellement) et l'enregistrement PTR crée automatiquement de l'ordinateur CL01 du domaine.



9.6 Enregistrements

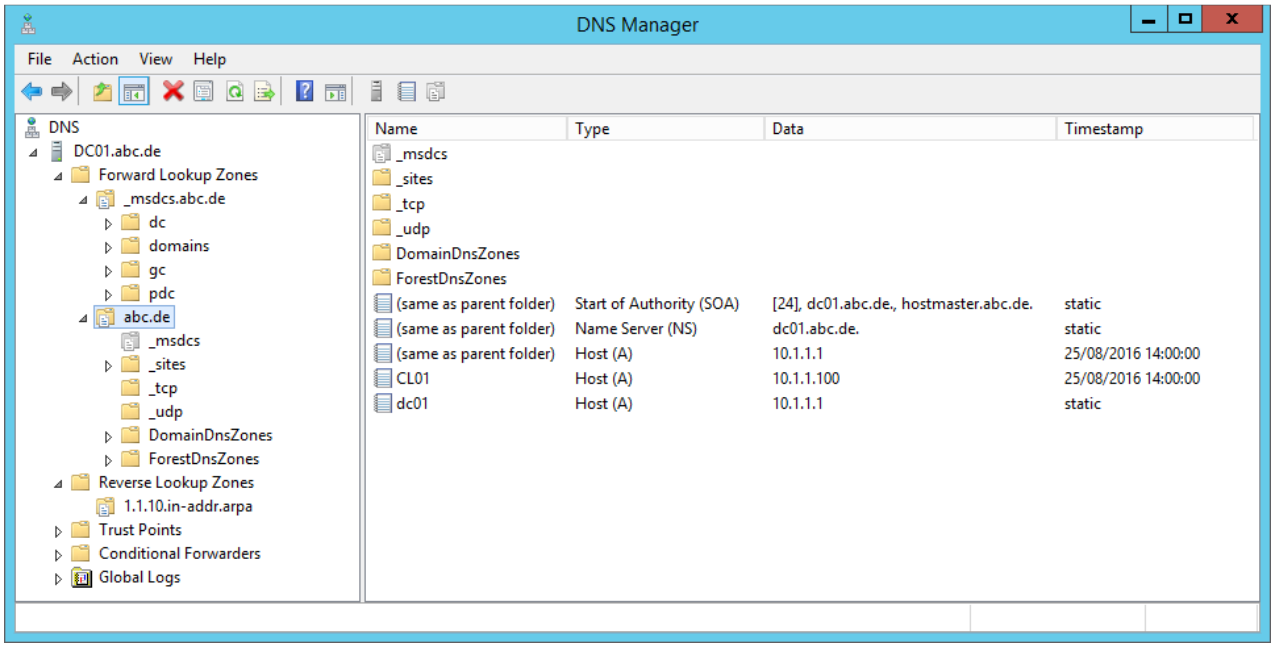
Différents types d'enregistrement existent dans le DNS. Ils permettent de localiser un client, un serveur mail, un serveur de nom, un contrôleur de domaine, etc.

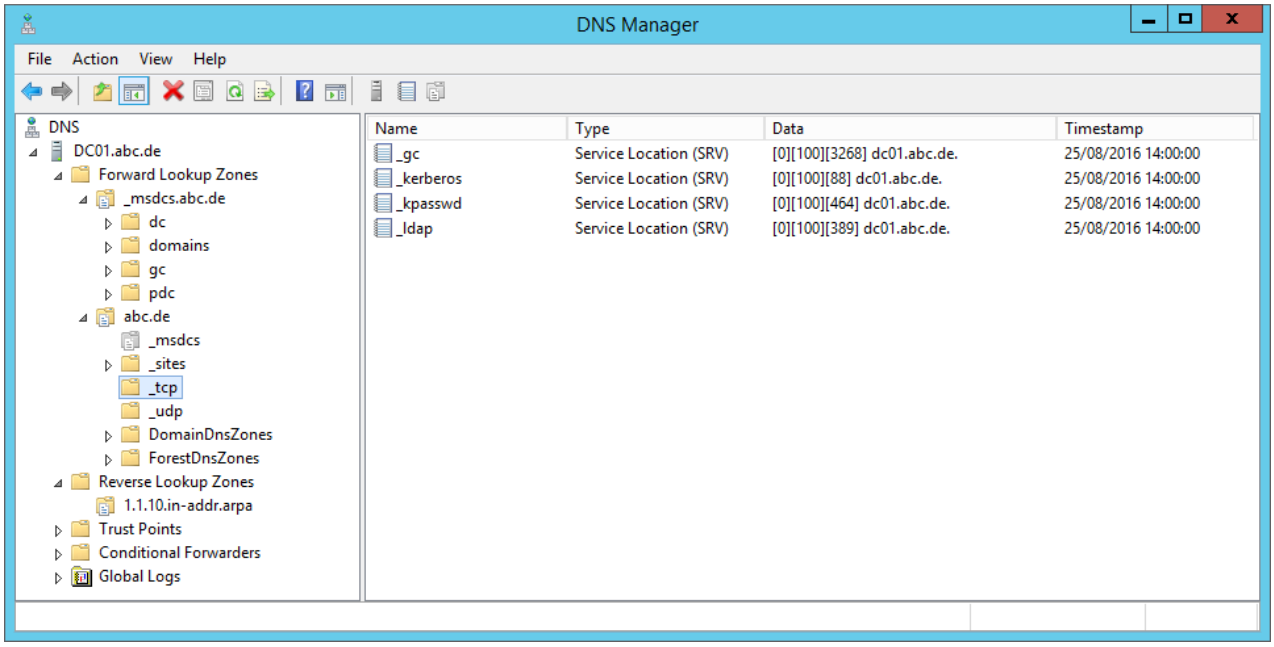
9.6.1 MX, NS, CNAME, SRV Host A et AAAA

- Host A ou AAAA : correspondance entre un nom de machine (FQDN) et une adresse IP v4 (A) ou IP v6 (AAAA).
- CNAME (Canonical Name) : alias qui permet de créer un second nom pour une même machine.
- MX (Mail eXchange) : définit un serveur de mail.
- NS (Name Server) : définit un serveur de noms de domaine (DNS).
- SRV (Server) : définit un serveur destiné à une application spécifique : Kerberos, Global Catalog, LDAP, etc.
- PTR (Pointer) : Présent dans en zone reverse, il assure la correspondance entre une adresse IP et un nom FQDN.

Les zones « reverse » ne sont pas créées automatiquement et pas obligatoires. Leur création est cependant recommandée car le PRT est parfois utiliser pour vérifier qu'une IP est bien associée au nom de domaine. La zone reverse compte des enregistrements : SOA, NS et PTR.

Les captures suivantes montrent différents types d'enregistrements dans le DNS Manager : les enregistrements classiques (Host A, SOA et NS) sur la première et SRV sur la seconde (Global Catalog, Kerberos [_kerberos et _kpasswwd] et LDAP).





9.6.2 SOA

Le SOA (Start Of Authority) est le premier enregistrement crée lors de la création d'une zone. Cet enregistrement particulier contient les paramètres de zone notamment :

- Serial Number : valeur incrémentée à chaque charment effectué dans la zone.
- Primary server : adresse du serveur qui héberge le SOA.
- Refresh interval : intervalle d'attente avant d'interroger le serveur d'une zone primaire pour rafraichir une zone secondaire.
- Retry interval : intervalle d'attente avant de recontacter le serveur d'une zone primaire pour rafraichir une zone secondaire.

- Expire after : délai au-delà duquel le serveur d'une zone secondaire ne répondra plus aux demandes pour cette zone (il considère que ses informations sont dépassées).
- TTL : Time To Live, durée pendant laquelle une information est considérée comme valable et conservée comme cache. Par défaut : 3600 secondes soit 1 heure.