

1. Présentation du système DNS

1.1 Introduction à la résolution de noms

Pour pouvoir communiquer, chaque machine présente sur un réseau doit avoir un identifiant unique. Avec le protocole IP (Internet protocole), cet identifiant se présente sous la forme d'un nombre d'une longueur de 32 bits. On parle d'adresses IP. Cependant pour un utilisateur, il est impensable de retenir les adresses IP de chaque ordinateur. C'est pourquoi des mécanisme de résolution de noms ont été mis en place. Un mécanisme de résolution de noms permet de traduire des noms en adresses IP et inversement.

Au départ, chaque machine stockait localement les mappages noms / adresse IP (un mappage est une correspondance entre un nom et une adresse IP). Cependant ce système a l'inconvénient de demander une trop lourde charge administrative. En effet, à chaque ajout de machine dans le réseau ou bien à chaque modification de la configuration d'une machine, il faut éditer manuellement le fichier contenant les mappages noms / adresse IP.

Le premier mécanisme de résolution de noms mis en place sous Windows est NetBIOS (NetBIOS Extended User Interface), un protocole crée par IBM dans les années 80. Cette méthode de résolution de noms a de nombreux inconvénients :

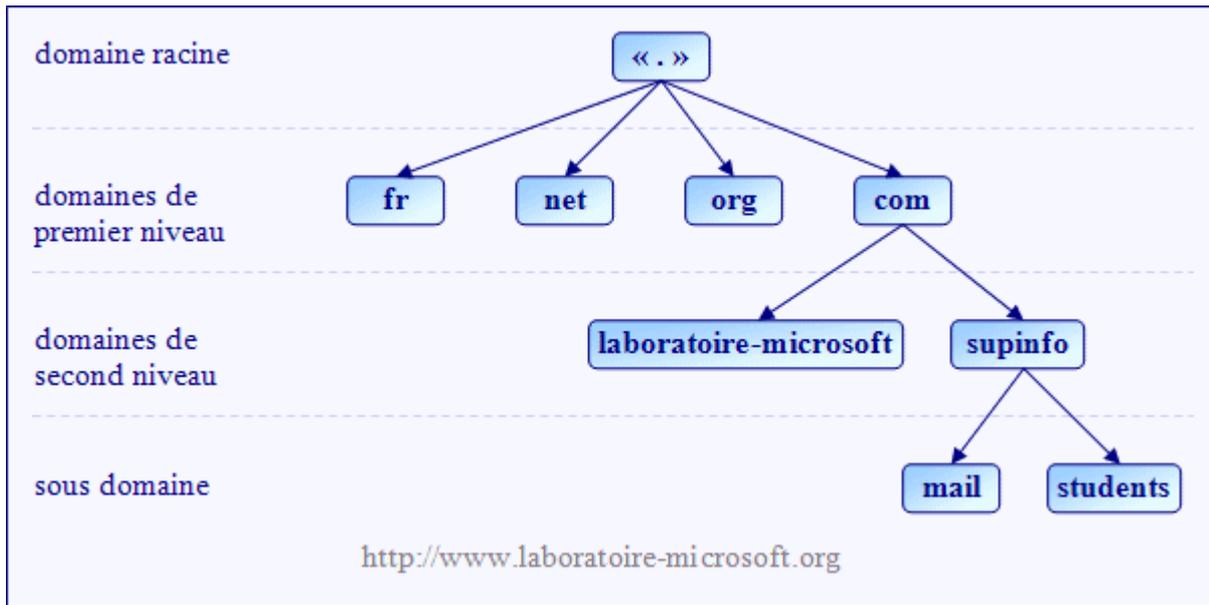
- Les noms NetBIOS sont limités à 16 caractères (15 caractères pour le noms de la machine et un 16è caractère indiquant le type de services hébergés par la machine).
- Le protocole NetBIOS utilise la diffusion (ou broadcast) pour résoudre les noms en adresses IP ce qui surcharge la bande passante du réseau.
- Les noms NetBIOS ne possèdent pas de hiérarchie ce qui les rends inutilisables sur Internet.
- Le protocole NetBIOS n'est pas utilisé sur les plateformes non Microsoft ce qui pose un problème d'interopérabilité.

C'est pourquoi sous Windows 2000/2003/XP un nouveau système de résolution de noms appelé DNS (Domain Name System) a été adopté. Il corrige les inconvénients du protocole NetBIOS.

1.2 Le système DNS

Le système DNS introduit **une convention de nommage hiérarchique** des domaines qui commence par un domaine racine appelé ".". Les domaines situés directement sous le domaine racine sont appelés domaines de premier niveau. Ils sont gérés par l'ICANN et représentent souvent la localisation géographique (fr, be, eu, ru, de ...) ou le type de service (museum, info, org, gov, mail, ...). Les domaines de second niveau sont disponibles pour les entreprises et les particuliers. Ils sont distribués et gérés par d'autres sociétés comme l'InterNIC (une filiale le l'ICANN) ou bien l'AFNIC (Association Française pour le Nommage Internet en Coopération) qui

gère le domaine *fr*. Enfin une multitude de sous domaines peuvent être créés à l'intérieur d'un domaine de second niveau.



la hiérarchie du système DNS

Les noms de machine utilisant le système DNS sont appelés **noms d'hôtes**. Un nom d'hôte peut contenir jusqu'à 255 caractères alphanumériques (chiffres et lettres) et le caractère trait d'union "-". L'utilisation du caractère "." est interdite car il est réservé afin de séparer un domaine supérieur d'un domaine inférieur.

En effet, on distingue deux types de noms avec le système DNS :

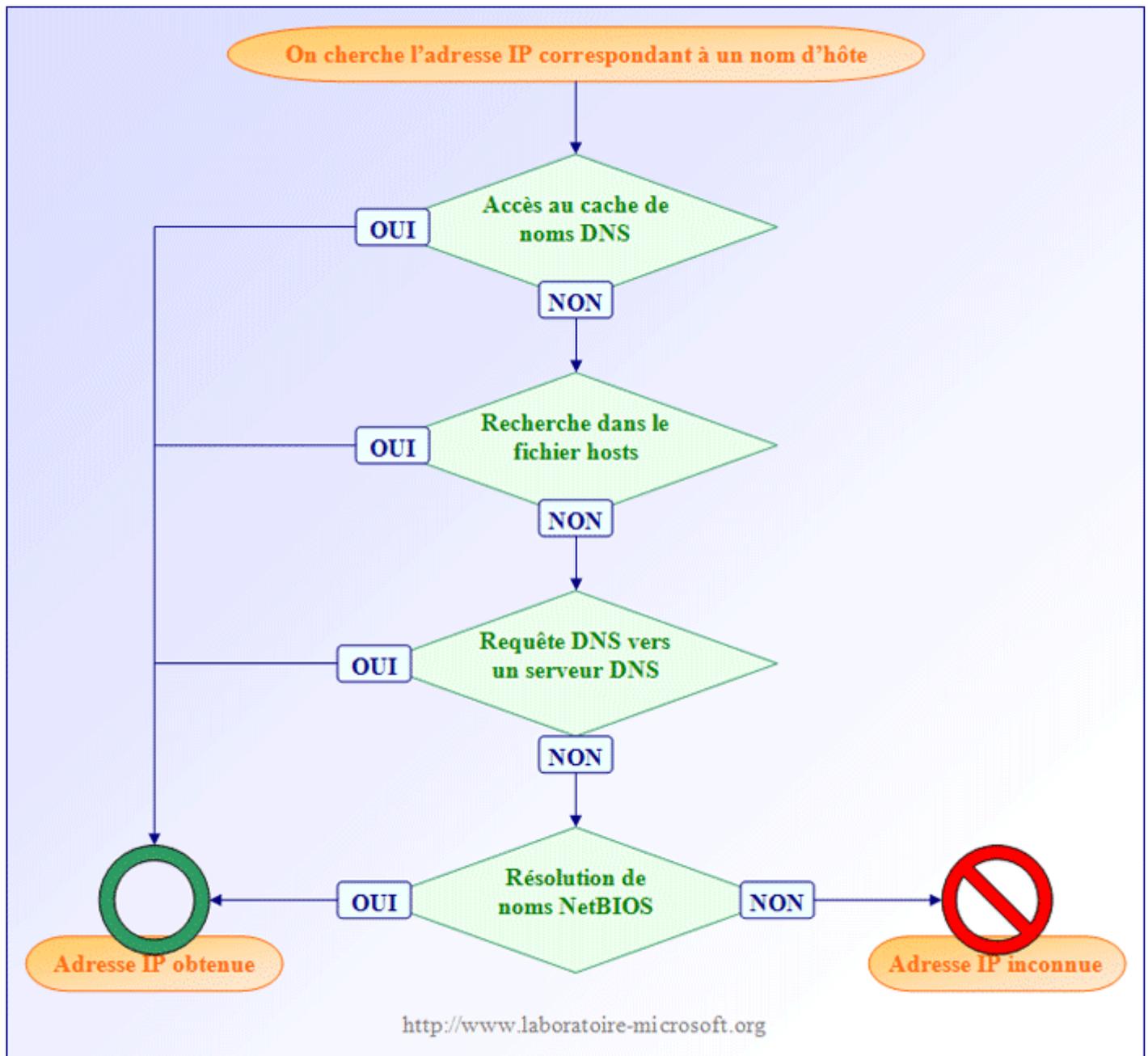
- le **nom d'hôte** qui représente le nom d'une machine (un ordinateur, une imprimante ou bien encore un routeur).
- le **nom de domaine pleinement qualifié ou FQDN** (Fully Qualified Domain Name).

Le FQDN est en fait composé de deux parties : le nom d'hôte et le suffixe DNS. Le suffixe DNS définit la relation entre le domaine auquel appartient la machine et le domaine racine. Par exemple, si l'on considère une machine avec le nom d'hôte *CLIENT-11* située dans le domaine *students*, son suffixe DNS est : *students.supinfo.com*. Le nom de domaine pleinement qualifié (FQDN) de la machine *CLIENT-11* est donc **CLIENT-11.students.supinfo.com**.

2. Configuration des clients DNS

2.1 Fonctionnement de la résolution de nom d'hôte côté client

Lorsqu'un client DNS exécutant Windows souhaite résoudre un nom de domaine en adresse IP (par exemple lors de l'accès à une page web ayant l'URL www.laboratoire-microsoft.org ou bien lors de l'accès à un dossier partagé \\ServeurFichiers\Documents), un processus décomposable en plusieurs étapes est exécuté :



fonctionnement de la résolution de nom d'hôte

La première chose que doit faire le client avant de pouvoir se connecter au serveur web ou bien au serveur de fichier est de trouver son adresse IP à partir de son nom d'hôte. Le client commence par vérifier si une adresse IP correspondant au nom

d'hôte est présente dans **le cache de noms DNS**. Le cache de noms DNS contient tous les mappages noms d'hôte / adresses IP qui ont été précédemment résolus. Le cache de noms DNS est stocké en mémoire vive ce qui permet d'accélérer le processus de résolution de noms d'hôte lorsque l'utilisateur accède souvent au même serveur. On peut afficher le cache de noms DNS en utilisant la commande **ipconfig /displaydns**. Il est aussi possible de vider cette mémoire cache grâce à la commande **ipconfig /flushdns**.

Si l'adresse IP recherchée n'est pas présente dans le cache de noms DNS, alors le client consulte **le fichier hosts**. Ce fichier est situé dans le répertoire `%SYSTEMROOT%\system32\drivers\etc`. Toutes les entrées sont faites de manière statiques. Par défaut, il contient uniquement le mappage entre le nom d'hôte `localhost` et l'adresse IP `127.0.0.1`.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP
# pour Windows.
#
# Ce fichier contient les correspondances des adresses IP aux noms d'hôtes.
# Chaque entrée doit être sur une ligne propre. L'adresse IP doit être placée
# dans la première colonne, suivie par le nom d'hôte correspondant. L'adresse
# IP et le nom d'hôte doivent être séparés par au moins un espace.
#
# De plus, des commentaires (tels que celui-ci) peuvent être insérés sur des
# lignes propres ou après le nom d'ordinateur. Ils sont indiqués par le
# symbole '#'.
#
# Par exemple :
#
#      102.54.94.97      rhino.acme.com      # serveur source
#      38.25.63.10      x.acme.com        # hôte client x
#
127.0.0.1      localhost
```

le fichier *hosts*

Si le mappage n'a pas été trouvé dans le fichier *hosts*, alors le client va envoyer une requête DNS au premier **serveur DNS** dont l'adresse IP a été définie dans ses paramètres TCP/IP. Si le premier serveur DNS est injoignable alors le client envoie une requête au second et ainsi de suite... Si aucun serveur DNS n'a été paramétré dans les paramètres TCP/IP du client ou bien si aucun serveur DNS n'est capable de résoudre le nom en adresse IP alors le client passe à la quatrième et dernière étape.<

Si le client n'a pas trouvé le mappage recherché alors il considère que l'adresse IP recherchée ne correspond pas à un nom d'hôte mais à un nom NetBIOS et lance **une résolution de nom NetBIOS**. La résolution de noms NetBIOS se passe en plusieurs étapes :

1. vérification de la présence de l'adresse IP dans le cache de noms NetBIOS.
2. envoi d'une requête au premier serveur WINS dont l'adresse IP a été définie dans ses paramètres TCP/IP du client. (*)
3. le client cherche l'adresse IP de la machine sur son sous-réseau en réalisant une diffusion (broadcast). (*)

4. recherche d'une éventuelle entrée dans le fichier
%SYSTEMROOT%\system32\drivers\etc\lmhosts.

(*) Les étapes 2 et 3 peuvent être inversées ou non présentes selon le type de noeud NetBT défini sur le client. Par défaut, le noeud NetBT H (Hybride) est utilisé et il réalise les étapes dans l'ordre ci-dessus. Le type de noeud NetBT peut se paramétrer au niveau du serveur DHCP (le type de noeud NetBT correspond à l'option DHCP numéro 46).

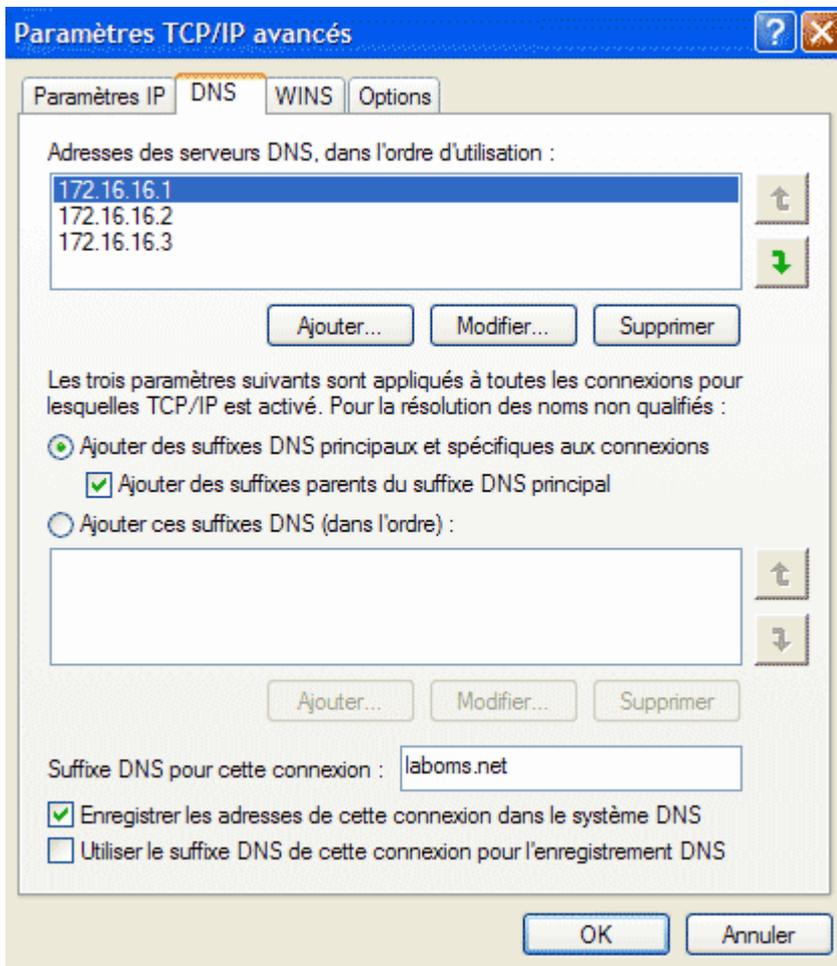
Si à la fin de ce processus aucune adresse IP n'a été trouvée alors le client ne peut pas obtenir l'adresse IP correspondante et ne peut pas joindre la ressource (par exemple un serveur web ou un serveur de fichier). Dans tous les cas le résultat de la requête DNS sera mis dans le cache de noms DNS.

2.2 Paramétrage des ordinateurs clients

Lorsque l'on veut accéder à une ressource située sur un réseau (un partage réseau par exemple), il peut être fastidieux de taper son nom de domaine pleinement qualifié (FQDN). C'est pourquoi Windows offre la possibilité de définir un **suffixe DNS** spécifique à un compte d'ordinateur ou bien à une connexion particulière. Ainsi un utilisateur peut taper le nom d'hôte de la ressource au lieu de son FQDN. Par exemple, si l'on dispose d'un serveur de fichier nommé *srv-file-1* situé dans le domaine *labomicrosoft.lan* et si le suffixe DNS des comptes d'ordinateur a été correctement paramétré, alors l'utilisateur peut taper [\\srv-file-1](#) au lieu de [\\srv-file-1.labomicrosoft.lan](#) pour accéder au partage réseau.

Si l'on définit un suffixe DNS au niveau d'une connexion particulière, celui-ci s'applique à la place du suffixe DNS du compte d'ordinateur (ou **suffixe DNS principal**). Pour définir un suffixe DNS principal, il faut aller dans *panneau de configuration / système*, sélectionner l'onglet *nom de l'ordinateur*, cliquer sur le bouton *modifier*, puis sur le bouton *autres*. Vous pouvez ensuite entrer le suffixe DNS principal dans le champ réservé à cet effet.





Pour définir **un suffixe DNS spécifique à une connexion donnée**, il faut aller dans les propriétés du protocole TCP/IP de cette connexion, puis cliquer sur l'onglet *DNS*. Il suffit ensuite d'entrer le suffixe DNS dans la zone de texte *Suffixe DNS pour cette connexion*. Cette fenêtre vous permet également de **définir les serveurs DNS que le client essaiera de contacter pour résoudre les noms d'hôtes**.

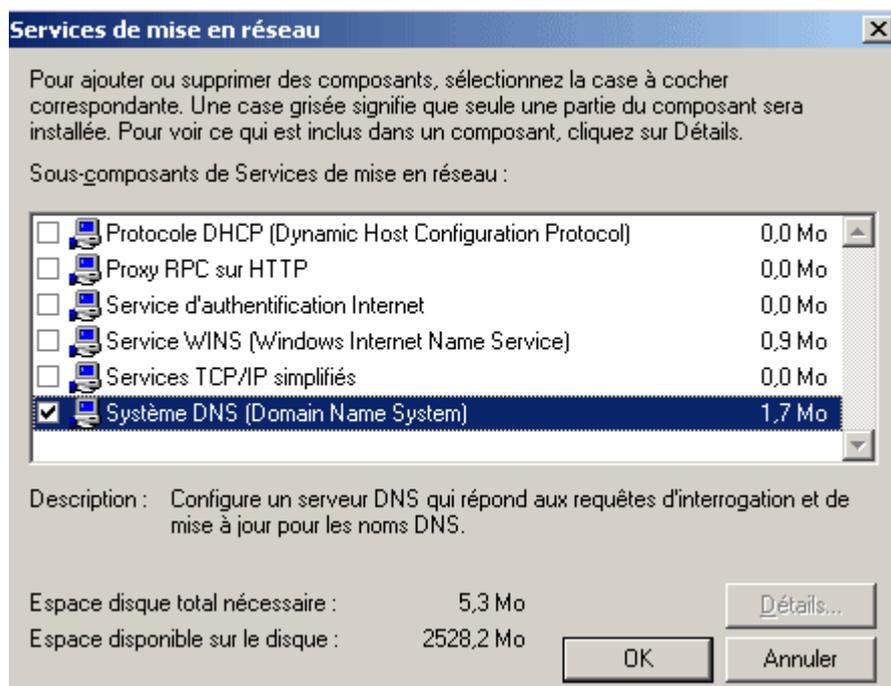
Vous pouvez aussi **activer ou désactiver les mises à jour automatiques des enregistrements de ressources par les clients** grâce à la case *Enregistrer les adresses de cette connexion dans le système DNS*.

3. Configuration du serveur DNS

3.1 Installation du service DNS

Lors de la planification de l'installation du serveur DNS vous devez vérifier si les ressources matérielles de votre machine sont suffisantes. En effet, le service DNS utilise environ 4Mo de mémoire vive pour s'exécuter et chaque enregistrement de ressource ajoutée au serveur utilise 100 octets (source : [documentation Windows 2000 Server](#)). Ainsi si votre serveur doit héberger 10 000 ressources, cela occupera 10Mo supplémentaires dans la mémoire vive.

Vous pouvez installer le service DNS en passant par l'assistant *Configurer votre serveur* ou bien en utilisant la fenêtre *Ajout/Suppression de programmes* du *panneau de configuration*. Dans le second cas, il faut cliquer sur le bouton *Ajouter ou Supprimer des Composants Windows*, sélectionner *Services de mise en réseau*, puis *Système DNS (Domain Name System)*. Avant de lancer la procédure d'installation, assurez-vous de disposer d'une carte réseau paramétrée avec une adresse IP fixe ainsi que du CD-ROM de Windows 2003 Server.



Une fois le service DNS installé, vous pouvez le configurer grâce à une console dédiée accessible dans *panneau de configuration / outils d'administration* ou bien en tapant *dnsmgmt.msc* dans la boîte de dialogue *exécuter*.

3.2 Les différents types de requêtes

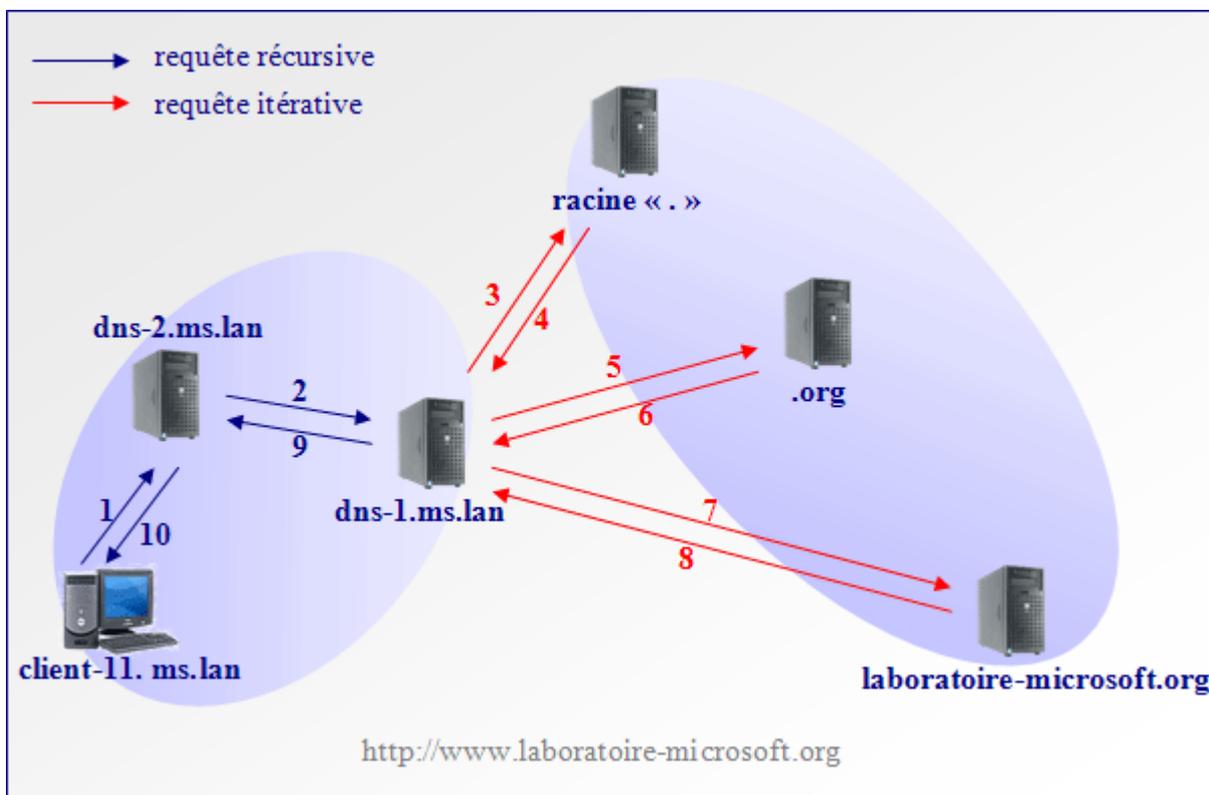
Un serveur DNS peut recevoir deux types de requêtes DNS :

- **une requête récursive** : Lorsqu'un serveur DNS reçoit une requête récursive, il doit donner **la réponse la plus complète possible**. C'est pourquoi le serveur DNS est souvent amené à joindre d'autres serveurs de noms dans le but de trouver la réponse exacte.
- **une requête itérative** : Lorsqu'un serveur reçoit une requête itérative, il renvoie **la meilleure réponse qu'il peut donner sans contacter d'autres serveurs DNS** (c'est-à-dire en consultant uniquement sa propre base de données).

Lorsqu'une machine cliente envoie une requête à un serveur DNS (étape 3 de la résolution de nom d'hôte), elle est **toujours de type récursif**. Dans l'exemple ci-dessous, l'ordinateur client nommé *client23.laboms.lan* cherche l'adresse IP correspondant au nom d'hôte *websrever.laboms.lan*. C'est pourquoi il envoie une requête récursive au serveur DNS nommé *dns1.laboms.lan*. A partir de cet instant *dns1.laboms.lan* a pour obligation renvoyer une réponse au client. Pour cela il va chercher dans sa mémoire cache, puis la base de données qu'il héberge et va éventuellement contacter d'autres serveurs DNS. Une fois qu'il a obtenu la réponse (la réponse peut être négative), il la renvoie au client. Dans notre exemple, le serveur DNS a trouvé l'adresse IP recherchée qui est : *172.16.104.30*. L'ordinateur client peut ensuite contacter le serveur web nommé *webserver.laboms.lan*.



Lorsqu'un serveur DNS ne peut pas répondre à la requête récursive d'un client, **il va d'abord essayer de contacter ses redirecteurs**. Si le serveur DNS est paramétré pour utilisé des redirecteurs alors il envoie une requête récursive au premier serveur DNS défini dans sa liste de redirecteurs. Par contre, si le serveur DNS n'a pas de redirecteurs, il va envoyer une requête itérative au premier serveur DNS situé dans sa liste de serveur DNS racine. **Le serveurs DNS n'envoie donc des requêtes itératives que si il n'a pas de redirecteurs.**

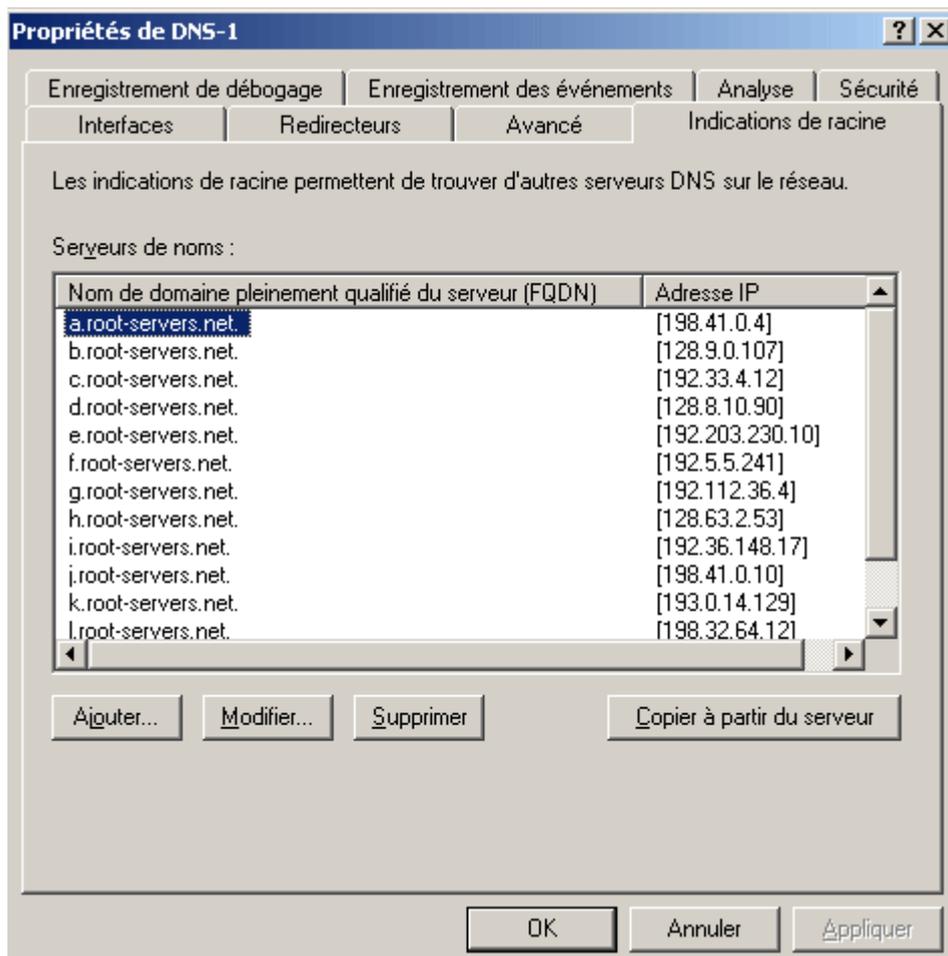


Dans l'exemple ci-dessus, un client nommé **client-11.ms.lan** souhaite accéder au site web du laboratoire Microsoft. La procédure de résolution de nom se passe en plusieurs étapes :

1. L'ordinateur client **client-11.ms.lan** commence par chercher l'adresse IP du serveur Web. Pour cela il envoie une requête récursive au premier serveur DNS de sa liste de serveurs DNS soit **dns-2.ms.lan**.
2. Le serveur **dns-2.ms.lan** ne connaît pas la réponse, il envoie donc une requête récursive à **dns-1.ms.lan** qui est le premier serveur DNS de sa liste de redirecteurs.

3. Dans le cas présent **dns-1.ms.lan** ne connaît pas l'adresse IP recherchée et n'est pas configuré pour utiliser des redirecteurs. Il envoie donc une requête itérative au premier **serveur DNS racine** parmi sa liste d'indications de racine.
4. Le **serveur DNS racine** ne connaît pas la réponse mais il sait quel serveur DNS fait autorité pour le domaine *org*. Il renvoie donc l'adresse IP du serveur DNS faisant autorité pour le domaine *org* à **dns-1.ms.lan**.
5. Le serveur **dns-1.ms.lan** envoie alors une requête itérative au serveur DNS du domaine *org*.
6. Le serveur DNS du domaine *org* ne connaît pas la réponse et renvoie l'adresse IP du serveur DNS faisant autorité pour le domaine *laboratoire-microsoft* au serveur **dns-1.ms.lan**.
7. Le serveur **dns-1.ms.lan** contacte alors le serveur DNS faisant autorité pour la zone *laboratoire-microsoft* au moyen d'une requête itérative.
8. Le serveur DNS faisant autorité pour la zone *laboratoire-microsoft* possède le mappage dans sa zone de recherche directe locale. Il envoie donc l'adresse IP recherché à **dns-1.ms.lan**.
9. **dns-1.ms.lan** transmet la réponse au serveur **dns-2.ms.lan**.
10. Le serveur **dns-2.ms.lan** fait suivre la réponse au client qui peut ensuite joindre le serveur HTTP et afficher le site du laboratoire Microsoft.

3.3 Configuration des indications de racine



Lorsque le serveur DNS n'est pas configuré pour utiliser des redirecteurs, **il se sert des indications de racine pour résoudre les noms d'hôtes ou les adresses IP appartenant à des zones qu'il n'héberge pas**. Les indications de racine sont un ensemble de serveurs hébergeant la zone contenant les enregistrements du domaine racine ou domaine ".".

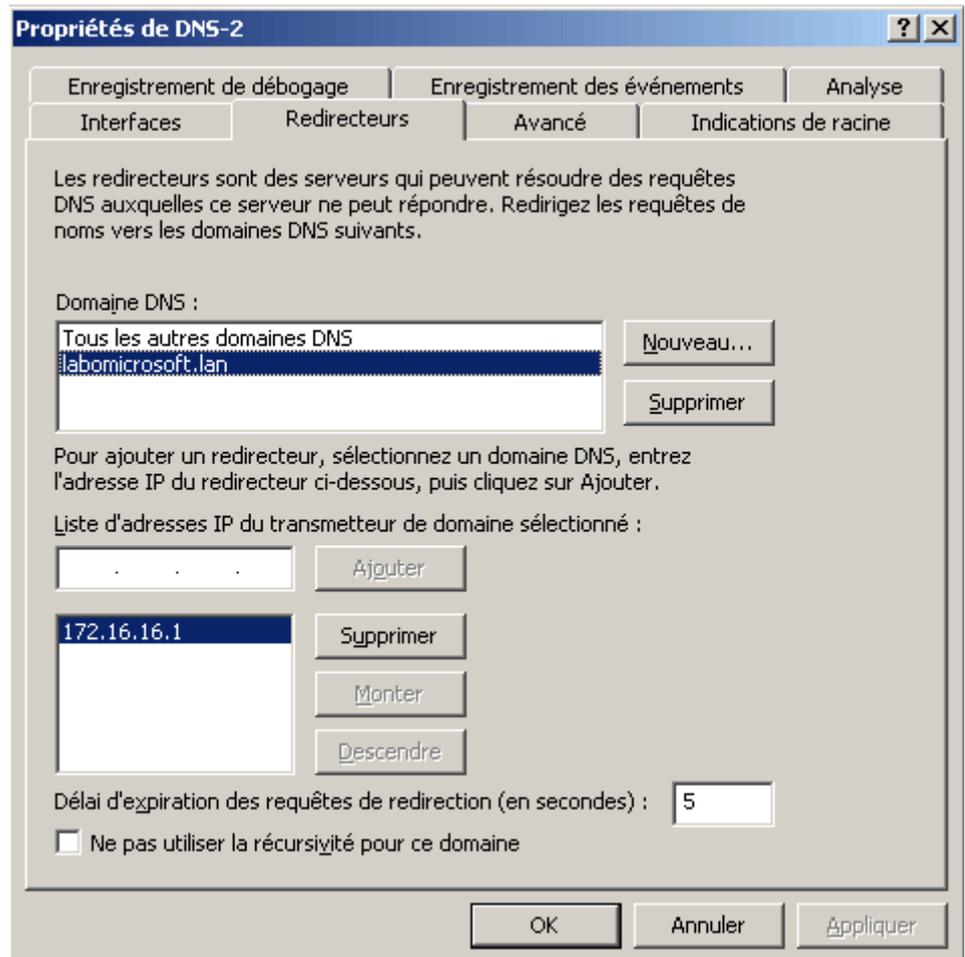
Les "serveurs DNS racines" sont au nombre de 13 à travers le monde. Ils appartiennent tous à un même domaine nommé *root-servers.net*.

Par défaut, le serveur DNS de Windows 2003 Server est configuré pour utiliser ces treize serveurs DNS. Cela signifie que si le serveur DNS reçoit une requête DNS dont il ignore la réponse, il va contacter un de ces serveurs racine pour l'obtenir.

Si l'on ne souhaite pas que les clients puissent résoudre les noms de domaines utilisés sur Internet, il suffit de ne mettre aucun serveur DNS dans la liste des serveurs racine ou bien de spécifier le nom d'hôte d'un serveur DNS local. On peut configurer les "serveurs DNS racine" dans l'onglet *Indication de racine* (*clic droit / propriétés* sur le nom du serveur DNS dans la console MMC).

3.4 Configuration des redirections

Lorsque le serveur DNS n'est pas capable de résoudre un nom en adresse IP, il va essayer de contacter un autre serveur DNS. On appelle ce serveur DNS **redirectionneur**. Sous Windows 2003 Server **il est possible de configurer un ou plusieurs redirectionneurs pour un domaine précis** (attention, sous Windows 2000 server cette fonctionnalité n'est pas disponible !).



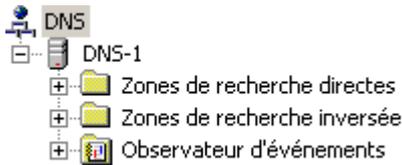
Par exemple, on peut spécifier que tous les enregistrements appartenant au domaine *labomicrosoft.lan* seront résolus par les serveurs DNS ayant les adresses IP *172.16.16.1* et *172.16.16.2*. Ainsi à chaque fois que le serveur DNS reçoit une requête de résolution de noms concernant le domaine *labomicrosoft.lan*, il regarde dans sa mémoire cache, puis si l'entrée n'y est pas, **il contacte immédiatement le premier redirectionneur spécifié** (ici le serveur DNS ayant l'adresse IP *172.16.16.1*).

Il est possible de définir un redirectionneur s'appliquant à tous les domaines sauf ceux qui ont déjà des redirectionneurs. Dans ce cas, le serveur DNS n'utilisera plus du tout les indications de racine et n'enverra donc jamais de requête récursive. De manière générale, les redirectionneurs indiqués pour le domaine *Tous les autres domaines DNS* correspondent aux **serveurs DNS des fournisseurs d'accès Internet (FAI)** de l'entreprise.

L'utilisation des redirecteurs permet d'utiliser des serveurs DNS locaux pour résoudre les enregistrements de ressources des domaines locaux et des serveurs DNS extérieurs (ceux des FAI ou bien les serveur DNS racines via les indications de racine) pour résoudre les enregistrements de ressources des domaines Internet, ce qui provoque **une amélioration des performances du processus de résolution de noms** tout en conservant la possibilité de résoudre la totalité des noms de domaines mondiaux.

4. Configuration des zones DNS primaires et secondaires

4.1 Introduction aux zones de recherche



La console de gestion du service DNS présente une arborescence simple. Les deux premiers conteneurs listent les zones de recherches alors que le troisième liste les évènements relatifs au service DNS (ex. : Le serveur DNS a démarré). Une **zone de recherche directe** contient des mappages *nom d'hôte / adresse IP* alors qu'une **zone de recherche inversée** contient des mappages *adresse IP / nom d'hôte*. Ainsi, une zone de recherche directe permet de trouver l'adresse IP correspondant à un nom d'hôte alors qu'une zone de recherche inversée permet de trouver un nom d'hôte à partir d'une adresse IP.

Dans le cas d'une recherche directe, le serveur DNS commence par analyser le suffixe DNS pour trouver la zone dans laquelle est située le noms d'hôte, puis recherche ensuite le mappage à l'intérieur de cette zone.

Dans le cas d'une recherche indirecte, le serveur DNS ne connaît que l'adresse IP de l'hôte. Il ne peut donc pas utiliser la hiérarchie de l'espace de noms pour retrouver le nom d'hôte. En effet si le serveur devait interroger toutes les zones DNS pour trouver le nom d'hôte, la recherche indirecte prendrait trop de temps et de ressources pour être réellement efficace.

C'est pourquoi un domaine spécifique, nommé *in-addr.arpa* a été réservé dans l'espace de noms DNS. Ce domaine est subdivisé en sous-domaines correspondant chacun à un réseau donné. Ainsi le domaine contenant tous les mappages *adresse IP / nom d'hôte* du réseau privé de classe C (la page des adresses IP privées de classe C va de 192.168.0.1 à 192.168.255.254) se nomme *168.192.in-addr.arpa*. Par exemple, lorsqu'un serveur DNS recherche le nom d'hôte correspondant à l'adresse IP 172.16.16.1, il s'adresse à la zone nommée *16.172.in-addr.arpa*.

Selon le plan d'adressage du réseau, il arrive que plusieurs zones de recherches inversées doivent être créés afin de contenir tous les mappages *adresse IP / nom d'hôte* d'un domaine donné. Par exemple si une entreprise utilise le domaine *laboms.lan* et que son plan d'adressage fait intervenir des adresses IP privés de classes B et des adresses IP privées de classe C alors elle devra créer une zone de

recherche directe nommée *laboms.lan* et deux zones de recherches inversées nommées *16.172.in-addr.arpa* et *168.192.in-addr.arpa*.

4.2 Les enregistrements de ressources

Dans un environnement Microsoft, les mappages nom d'hôte / adresse IP et adresse IP / nom d'hôte sont appelés **enregistrements de ressources**. On distingue plusieurs types d'enregistrements de ressources. Voici la liste des principaux types :

- **A** : Les enregistrements de ressources A (pour Adresse d'hôte) sont des mappage entre un nom d'hôte et une adresse IPv4 (adresse IP d'une longueur de 32 bits). Ils représentent généralement la majorité des enregistrements de ressources des zones de recherches directes.
- **AAAA** : Les enregistrements de ressources de ce type sont des mappages entre un nom d'hôte et une adresse IPv6 (adresse IP d'une longueur de 128 bits).
- **CNAME** : les enregistrement de ressources de type CNAME (Canonical NAME ou nom canonique) sont des mappages entre un nom d'hôte et un autre nom d'hôte. Ils permettent de créer des alias pour un nom d'hôte donné (c'est-à-dire d'associer plusieurs noms d'hôte à une même machine).
- **HINFO** : Les enregistrements de ressources de type HINFO (Host INFO ou informations sur l'hôte) spécifient le type de processeur (ex. : INTEL-386) et le système d'exploitation (ex. : WIN32) correspondant à un nom d'hôte.
- **MX** : les enregistrements de ressources de type MX (Mail eXchanger) identifient les serveurs de messageries. Chaque serveur de messagerie doit aussi disposer d'un enregistrement de ressource A. Il est possible de donner une priorité différente à chaque enregistrement MX.
- **NS** : les enregistrements de ressources de type NS (Name Server ou serveur de nom) identifient les serveurs DNS de la zone DNS. Ils sont utilisés dans le cadre de la délégation DNS.
- **PTR** : les enregistrements de ressources de type PTR (PoinTeR ou pointeur) sont des mappages entre une adresse IP et un nom d'hôte. Il représentent la majorité des enregistrements des zones de recherches inversées.
- **SOA** : les enregistrement de ressources de type SOA (Start Of Authority) contiennent le nom d'hôte et l'adresse IP du serveur DNS qui héberge actuellement la zone DNS principale. Il y a un seul enregistrement SOA par zone DNS. C'est le premier enregistrement crée dans une zone DNS.
- **SRV** : les enregistrements de type SRV (service) permettent de mapper un nom d'hôte à un type de service donné. Ainsi les enregistrements SRV peuvent permettre de retrouver la liste des serveurs HTTP ou bien encore des contrôleurs de domaines. Il est possible de donner une priorité différente à chaque enregistrement SRV.
- **WINS** : les enregistrements de ressources de type WINS indiquent au serveur DNS l'adresse IP d'un serveur WINS a contacter en cas d'échec lors de la résolution de nom d'hôte. Les enregistrements WINS ne peuvent être crée que dans une zone de recherche directe.
- **WINS-R** : les enregistrements de ressources de type WINS-R ne peuvent être crée que dans une zone de recherche inversée.

4.3 Les différents types de zones DNS

Une zone de noms ou zone DNS est un ensemble d'enregistrements de ressources appartenant à la même portion de l'espace de noms DNS. Par exemple une zone DNS peut contenir l'ensemble des enregistrements de ressource de type A (c'est-à-dire des mappages noms d'hôte / adresses IP) du domaine *laboms.lan*. Il existe trois types de zones DNS :

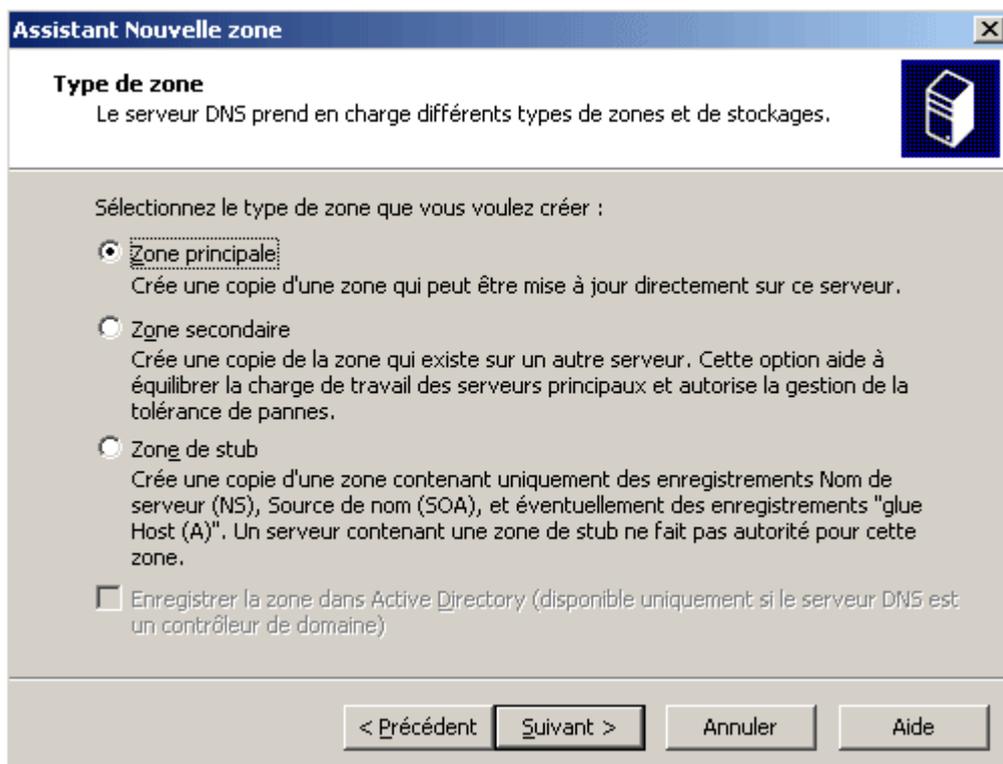
- **les zones principales** peuvent ajouter, modifier et supprimer des enregistrements de ressource.
- **les zones secondaires** sont des *copies en lecture seule* d'une zone principale donnée. Un serveur DNS qui héberge une zone secondaire ne peut pas ajouter ni modifier d'enregistrements de ressource. Les zones secondaires ont donc pour seul intérêt de garantir une tolérance aux pannes.
- **les zones de stub** sont des copies partielle d'une autre zone. Elle contiennent uniquement les enregistrements de ressource de types SOA, NS et A.

Les enregistrements d'une zone DNS donnée sont stockés localement par le serveur DNS sous la forme d'un fichier. Cependant si le serveur DNS joue aussi le rôle de contrôleur de domaine, il est possible de stocker les zones principales et les zones de stub dans le service d'annuaire Active Directory. On parlera alors de **zones intégrées à Active Directory**. Cette seconde solution apporte des avantages en termes de performance et de sécurité.

4.4 Configuration d'une zone principale

a/ configurer une zone de recherche directe

Si votre réseau ne contient aucun serveur DNS, vous devez commencer par créer une zone de recherche principale. Pour cela il faut faire un clic droit sur le conteneur *zones de recherches directes*, puis sélectionner *Nouvelle zone*. Dans l'assistant cliquez sur *Suivant*, puis sélectionnez *Zone principale* dans la fenêtre *Type de zone*. On remarque que la case Enregistrer la zone dans Active Directory est grisée ce qui est normal étant donné que dans notre exemple la machine n'est pas un contrôleur de domaine.



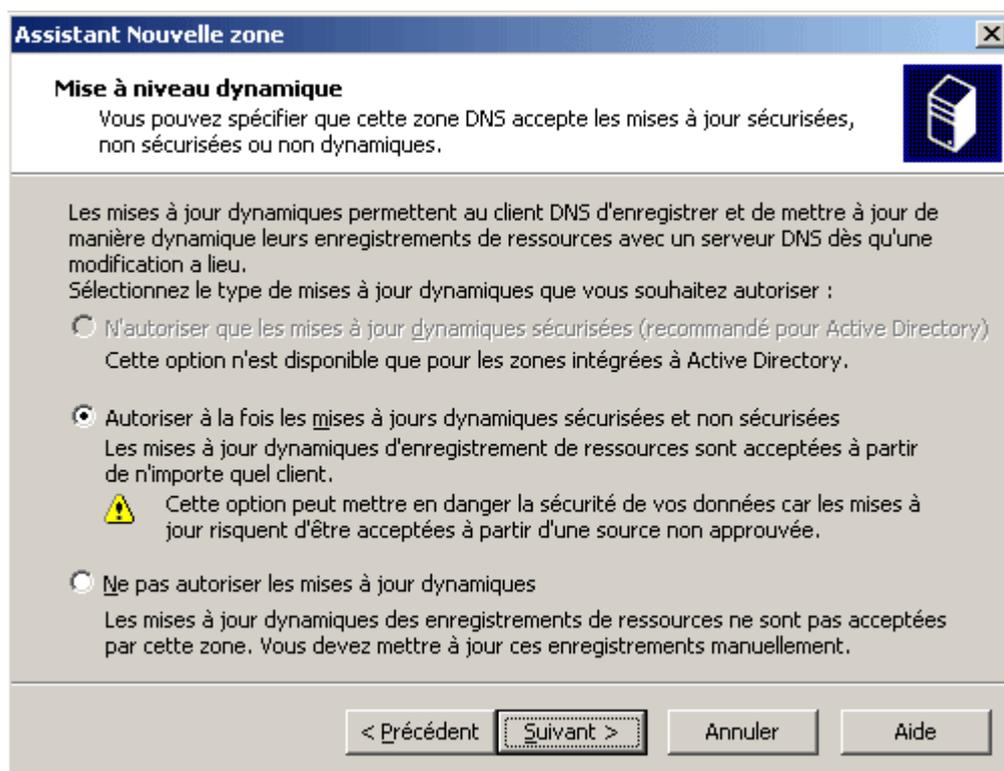
Dans la fenêtre *Nom de la zone*, entrez la partie de l'espace de nom que devra contenir la zone de recherche directe principale, puis cliquez sur *Suivant*. Dans notre exemple, le nom de la zone est : *labomicrosoft.lan*. Vous êtes ensuite amené à créer un nouveau fichier de zone et à le nommer. Le nom proposé par défaut est *labomicrosoft.lan.dns*.



Dans la fenêtre *Mise à niveau dynamique*, vous devez donner ou non la permission aux machines cliente de mettre à jour automatiquement leurs enregistrements de ressources. En effet, si vous utilisez un plan d'adressage dynamique (avec le

protocole DHCP par exemple) les machines clientes peuvent changer d'adresse IP ce qui invalide les enregistrements de ressources A et PTR correspondant. Cependant, les machines exécutant Windows 2000/XP/2003 peuvent mettre à jour automatiquement les enregistrements A et PTR les concernant à chaque modification de leur configuration. Trois choix sont disponibles :

- *N'autoriser que les mises à jour dynamiques sécurisées* : seuls les ordinateurs possédant un compte d'ordinateur dans Active Directory peuvent créer et mettre à jour automatiquement leurs enregistrements de ressources. Cette option n'est disponible que dans le cas d'une **zone intégrée à Active Directory**.
- *Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées* : tous les ordinateurs exécutant Windows 2000/XP/2003 peuvent créer et mettre à jour automatiquement leurs enregistrements de ressources. Même une machine qui n'est pas membre du domaine peut créer des enregistrements, ce qui peut poser des problèmes de sécurité.
- *Ne pas autoriser les mises à jour dynamiques* : Dans ce cas, la seule façon de mettre à jour les enregistrements de ressources est d'utiliser la commande **ipconfig /registerdns** sur chaque machine cliente. Si cette solution est utilisable avec un petit nombre de machine, elle s'avère trop contraignante dans un réseau d'envergure.



Une fois votre choix effectué, cliquez sur *Suivant*, puis sur *Terminer* pour quitter l'assistant.

b/ configurer une zone de recherche inversée

Vous pouvez ensuite créer une zone de recherche inversée principale. Pour cela, faites un clic droit sur le conteneur *zones de recherche inversée*, puis sélectionner *Nouvelle zone*. Dans l'assistant cliquez sur *Suivant*, sélectionnez *Zone principale* dans

la fenêtre *Type de zone* puis faites *Suivant*. Vous devez ensuite choisir le nom de la zone de recherche inversée. Pour cela vous pouvez entrer l'adresse IP du réseau auquel appartiennent les machines considérées (dans ce cas l'assistant générera automatiquement le nom de la zone) ou bien choisir le nom de la zone manuellement. Une fois le nom de zone correctement entré, cliquez sur *Suivant*.

Assistant Nouvelle zone

Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

172 .16 . .

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :

16.172.in-addr.arpa

Cliquez sur Aide pour obtenir davantage d'informations concernant la création d'une zone de recherche inversée.

< Précédent **Suivant >** Annuler Aide

Dans la fenêtre *Fichier zone*, donnez un nom au fichier qui contiendra la zone DNS puis cliquez sur *Suivant*. Vous devez ensuite autoriser ou non les mises à jour dynamique des enregistrements de ressources.

Assistant Nouvelle zone

Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent **Suivant >** Annuler Aide

Une fois ce choix effectué, cliquez sur *Suivant* puis sur *Terminer* pour quitter l'assistant.

4.5 Configuration d'une zone secondaire

a/ introduction

Pour alléger la charge du serveur DNS hébergeant une principale, vous pouvez créer une copie de cette zone en lecture seule sur un second serveur DNS. Ce type de zone est appelé zone secondaire. Pour créer une zone secondaire il faut donc que le réseau contienne déjà un serveur DNS hébergeant une zone principale.

b/ configurer une zone de recherche directe

Pour créer une zone secondaire, il faut faire un clic droit sur le conteneur *Zones de recherche directes*, puis cliquer sur *Nouvelle zone*. Cliquez sur *Suivant*, sélectionnez *Zone secondaire* puis faites *Suivant*. Vous devez ensuite donner le nom de la zone à dupliquer. Dans notre exemple, il s'agit de *labomicrosoft.lan*.

Assistant Nouvelle zone

Nom de la zone
Quel est le nom de la nouvelle zone ?

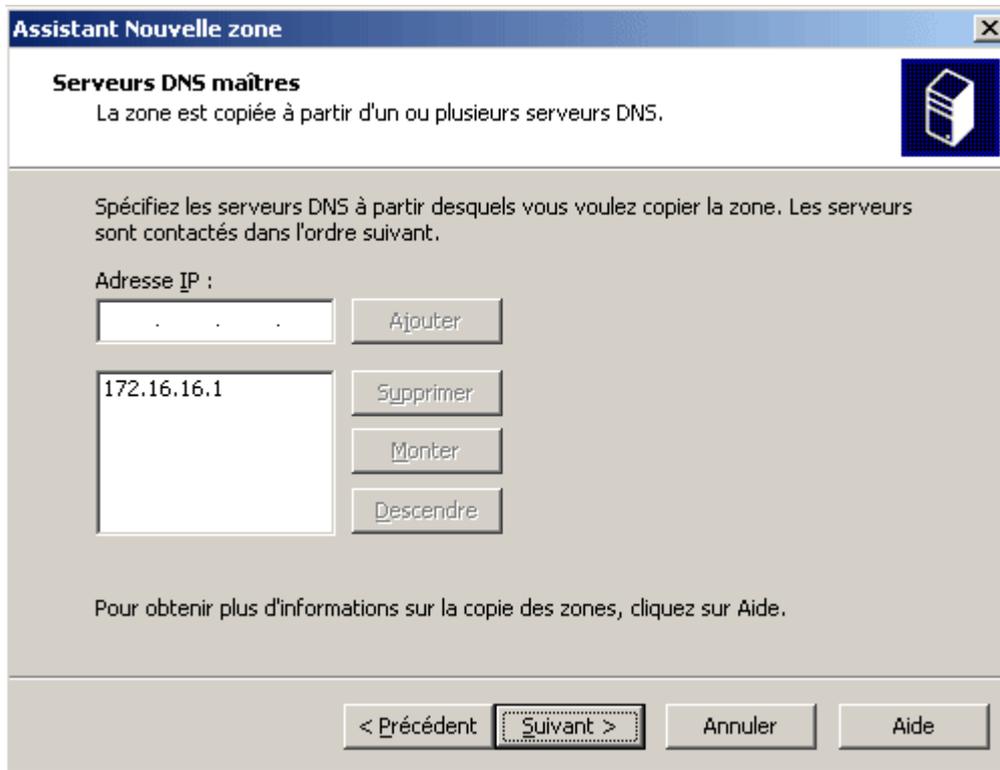
Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

Pour obtenir plus d'informations sur les noms de zones, cliquez sur Aide.

< Précédent Suivant > Annuler Aide

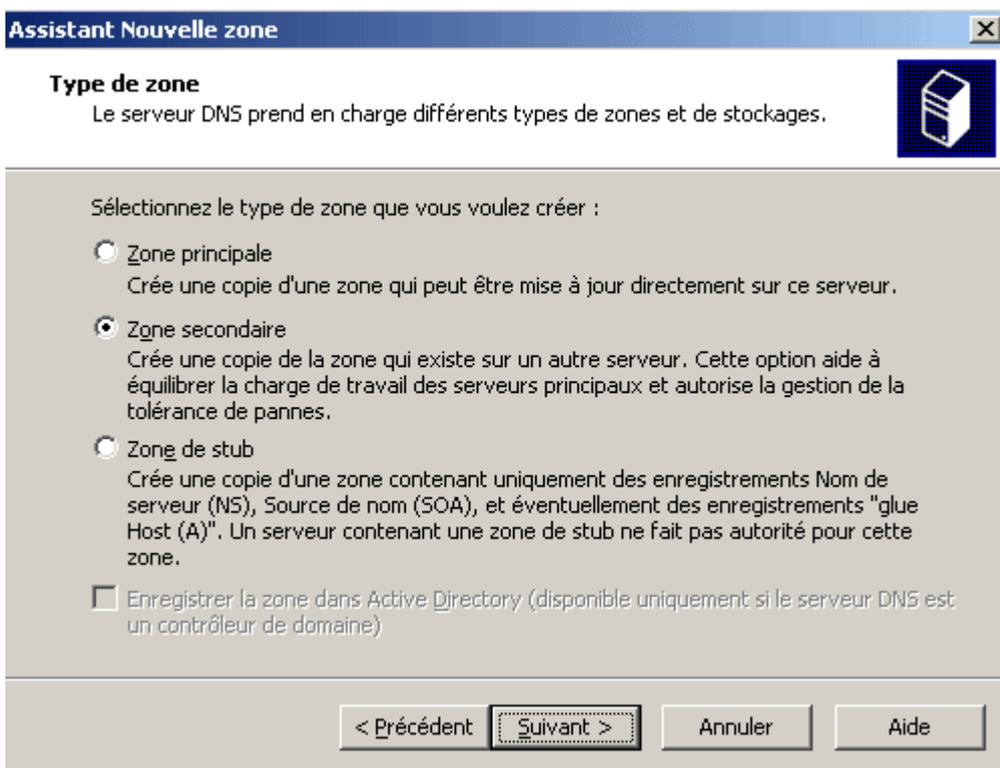
Vous devez ensuite, entrer l'adresse IP du serveur hébergeant la zone principale.



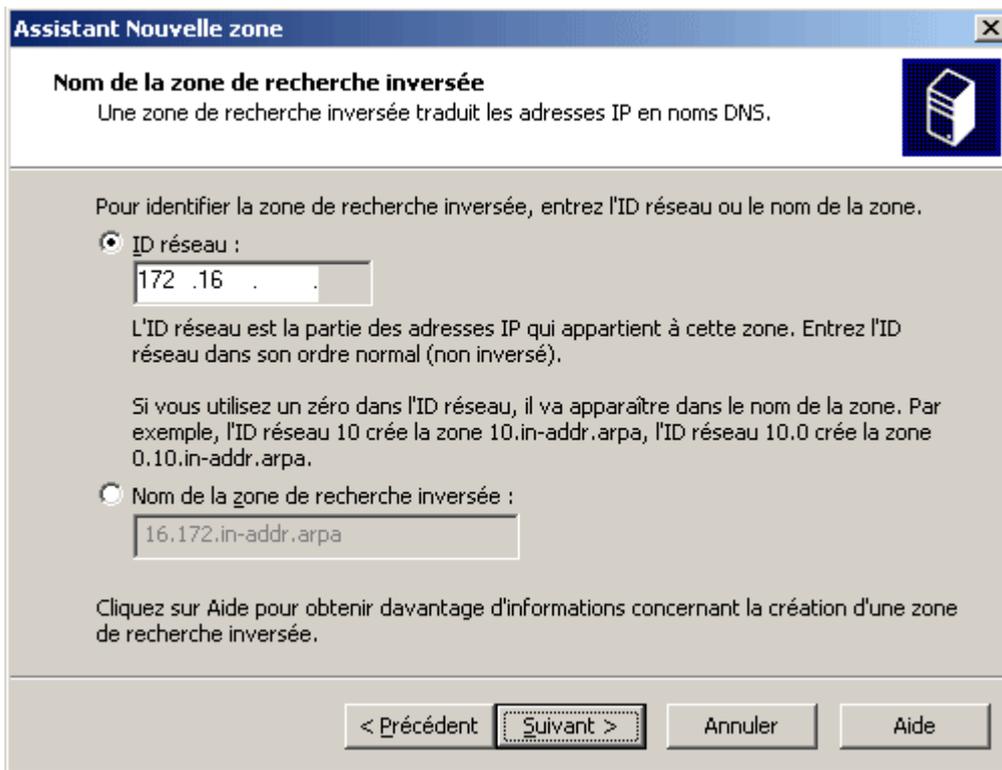
Cliquez ensuite sur *Suivant* puis sur *Terminer* pour quitter l'assistant.

c/ configurer une zone de recherche inversée

Pour créer une zone de recherche inversée secondaire, faites un clic droit sur le conteneur *Zones de recherche inversée*, puis cliquez sur *Nouvelle zone*. Cliquez sur *Suivant* pour passer la fenêtre de présentation de l'assistant. Dans la fenêtre *Type de zone*, sélectionnez *Zone secondaire* puis *Suivant*.



Saisissez l'adresse IP du réseau dans la zone de texte *ID réseau* . Cliquez sur *Suivant*.



Assistant Nouvelle zone

Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

172 .16 . .

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

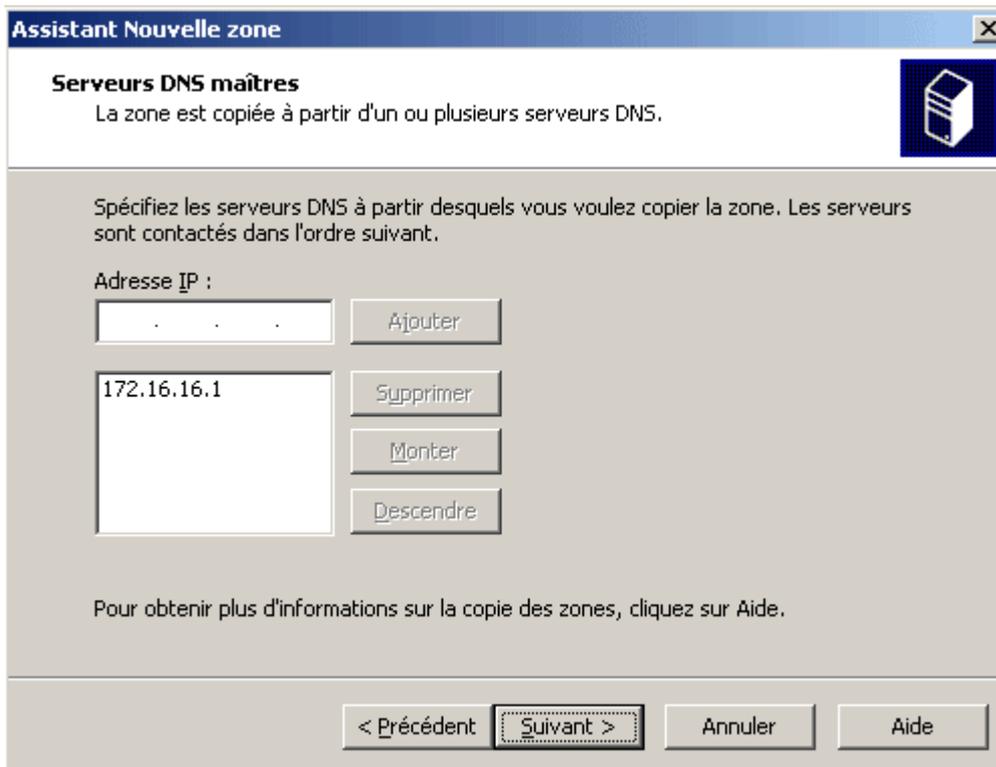
Nom de la zone de recherche inversée :

16.172.in-addr.arpa

Cliquez sur Aide pour obtenir davantage d'informations concernant la création d'une zone de recherche inversée.

< Précédent **Suivant >** Annuler Aide

Vous devez ensuite, entrer l'adresse IP du serveur hébergeant la zone principale.



Assistant Nouvelle zone

Serveurs DNS maîtres
La zone est copiée à partir d'un ou plusieurs serveurs DNS.

Spécifiez les serveurs DNS à partir desquels vous voulez copier la zone. Les serveurs sont contactés dans l'ordre suivant.

Adresse IP :

. . . Ajouter

172.16.16.1 Supprimer

Monter

Descendre

Pour obtenir plus d'informations sur la copie des zones, cliquez sur Aide.

< Précédent **Suivant >** Annuler Aide

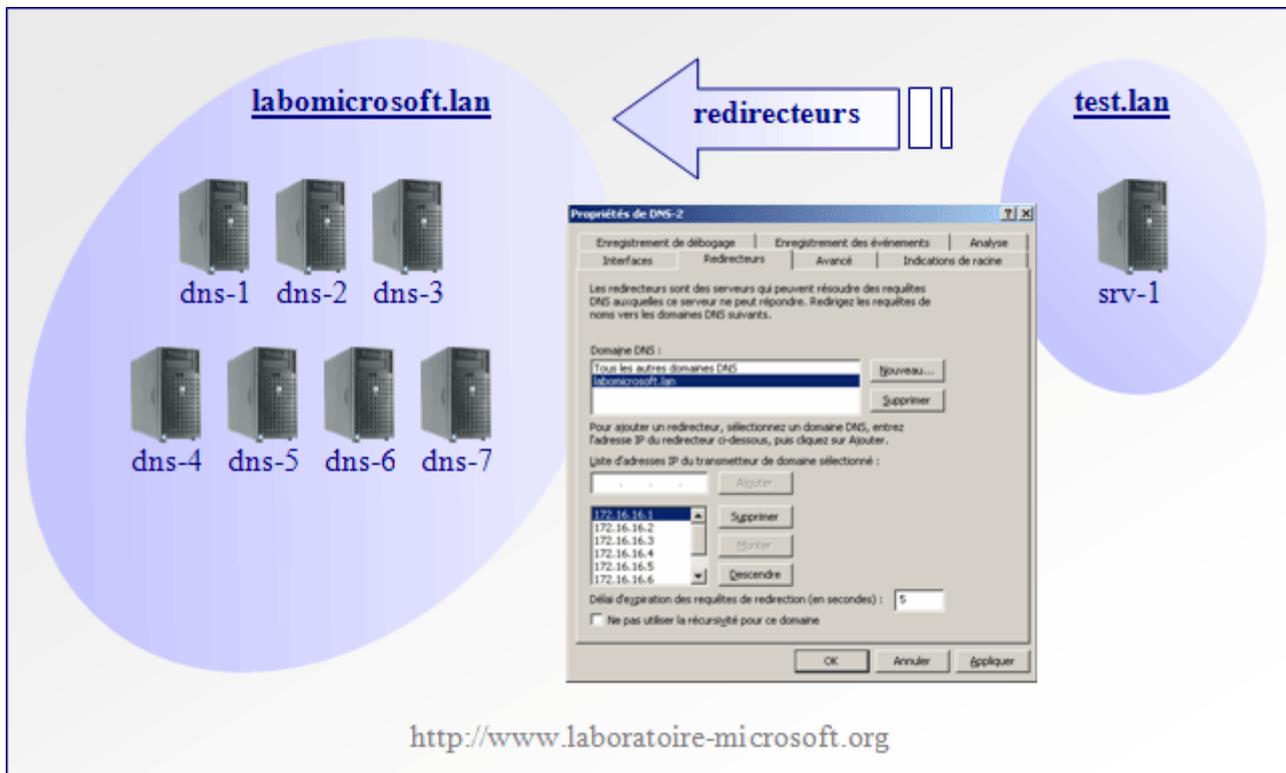
Cliquez ensuite sur *Suivant* puis sur *Terminer* pour quitter l'assistant.

5. Les autres types de zones DNS

5.1 Intérêt des zones de stub

Sous Windows 2003 Server on peut paramétrer des redirecteurs pour un domaine donné. Cependant **les adresses IP des serveurs DNS qui jouent le rôle de redirecteurs doivent être entrées manuellement** ce qui peut s'avérer contraignant si les serveurs DNS sont nombreux. De plus **la liste de redirecteurs est statique**. Ainsi, si l'un des serveurs DNS est supprimé ou bien si son adresse IP change, l'entrée ne sera plus valide.

Dans l'exemple ci-dessous, on observe 2 domaines au sein d'une même forêt. Le domaine *labomicrosoft.lan* contient 7 serveurs DNS et le domaine *test.lan* contient un seul serveur DNS. Si l'on souhaite que le serveur DNS *srv-1.test.lan* puisse résoudre les noms d'hôtes du domaine *labomicrosoft.lan*, il faudra configurer les sept serveurs DNS en tant que redirecteurs.



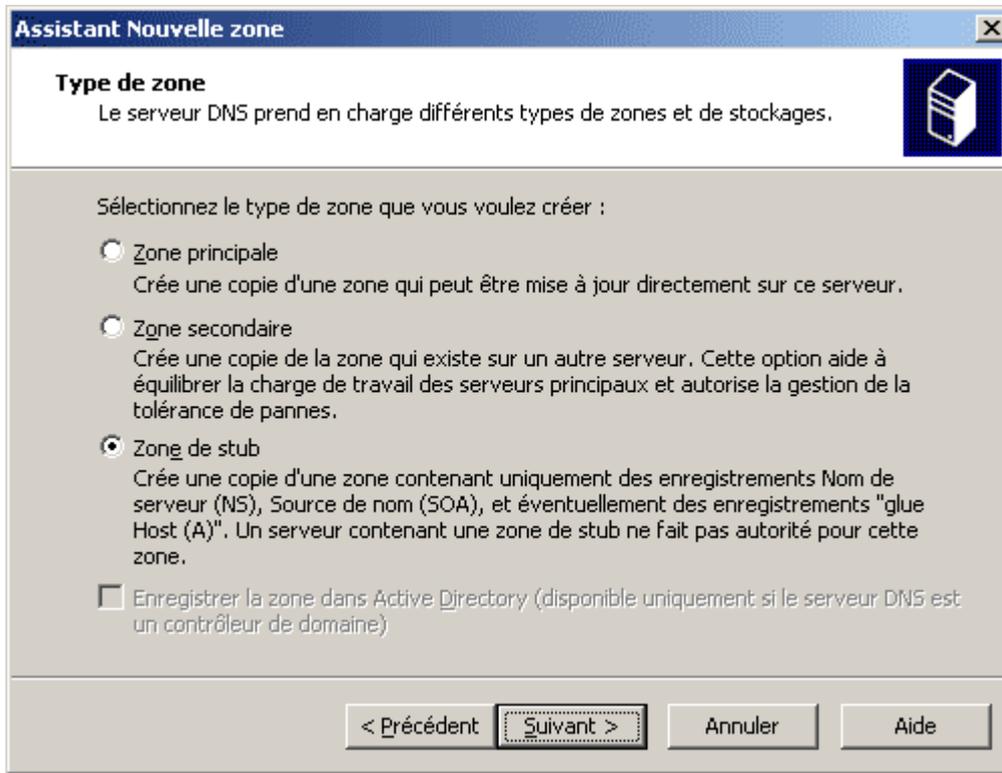
Il existe une alternative à l'utilisation des redirecteurs. En effet, Windows 2003 Server offre la possibilité de créer un type de zone spécifique nommé **zone de stub**, ne contenant que les enregistrements de ressources de types NS et SOA d'une zone DNS. **La zone de stub est automatiquement mise à jour** lorsque les paramètres d'un enregistrement NS ou SOA sont modifiés. Dans notre exemple, il est recommandé d'utiliser une zone de stub plutôt que des redirecteurs. En effet, la création de la zone de stub s'avère moins contraignante que celle des redirecteurs et offre l'avantage de mettre à jour les enregistrements de ressources à chaque modification.



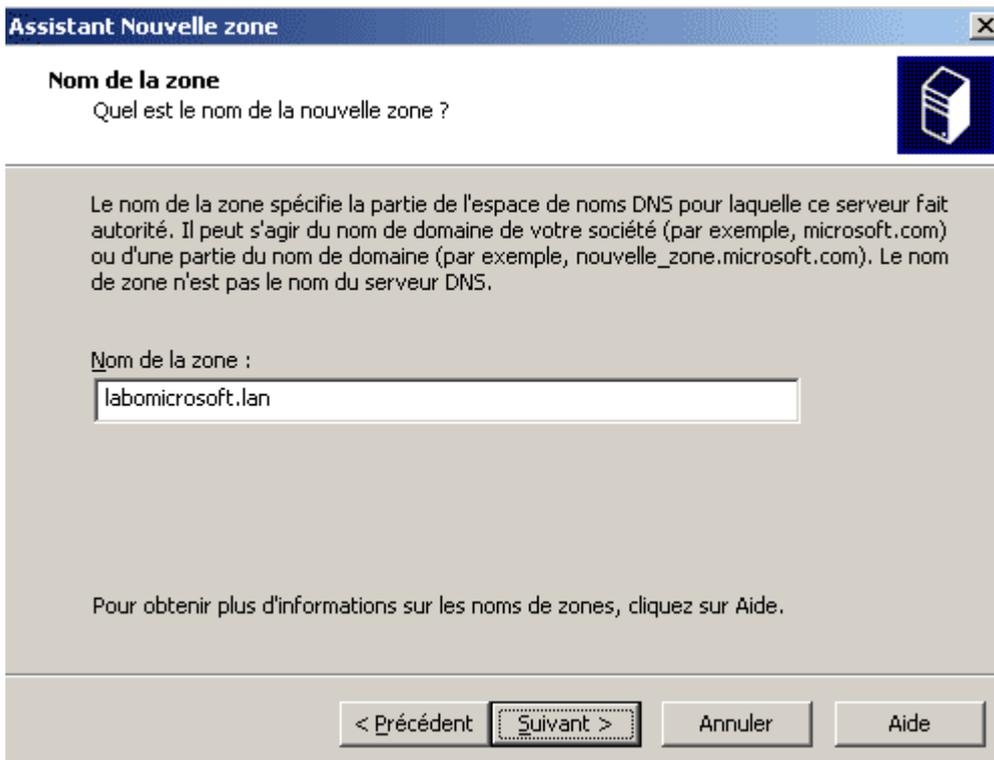
5.2 Configurer une zone de stub

a/ configurer une zone de recherche directe

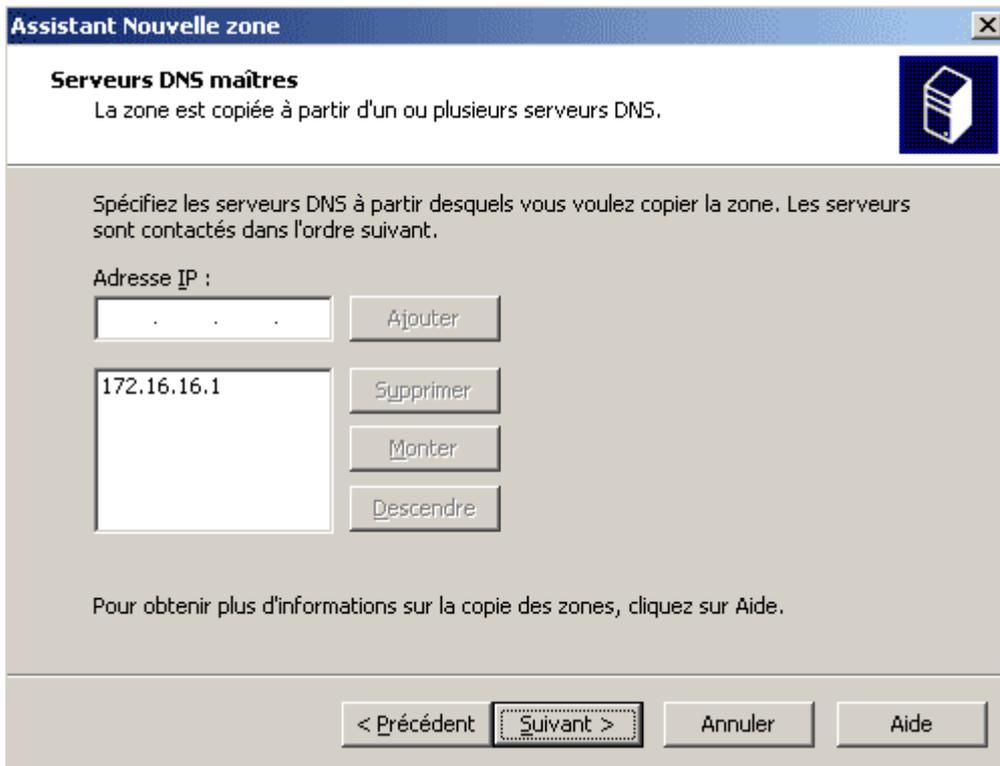
Pour créer une zone de recherche directe de stub, faites un clic droit sur le conteneur *Zones de recherche inversée*, puis cliquez sur *Nouvelle zone*. Cliquez sur *Suivant* pour passer la fenêtre de présentation de l'assistant. Dans la fenêtre *Type de zone*, sélectionnez *Zone de stub* puis *Suivant*.



Vous devez ensuite entrer le nom de la zone DNS à partir de laquelle vous voulez copier les enregistrements SOA et NS. Cliquez sur *Suivant* pour valider votre choix.



Dans la fenêtre *Fichier de zone*, donnez un nom au fichier qui contiendra les enregistrements de la zone de stub, puis faites *Suivant*. Vous devez ensuite indiquer l'adresse IP du serveur DNS à partir duquel vous voulez copier la zone. Cliquez sur *Suivant*, puis sur *Terminer* pour lancer le processus de création de la zone.



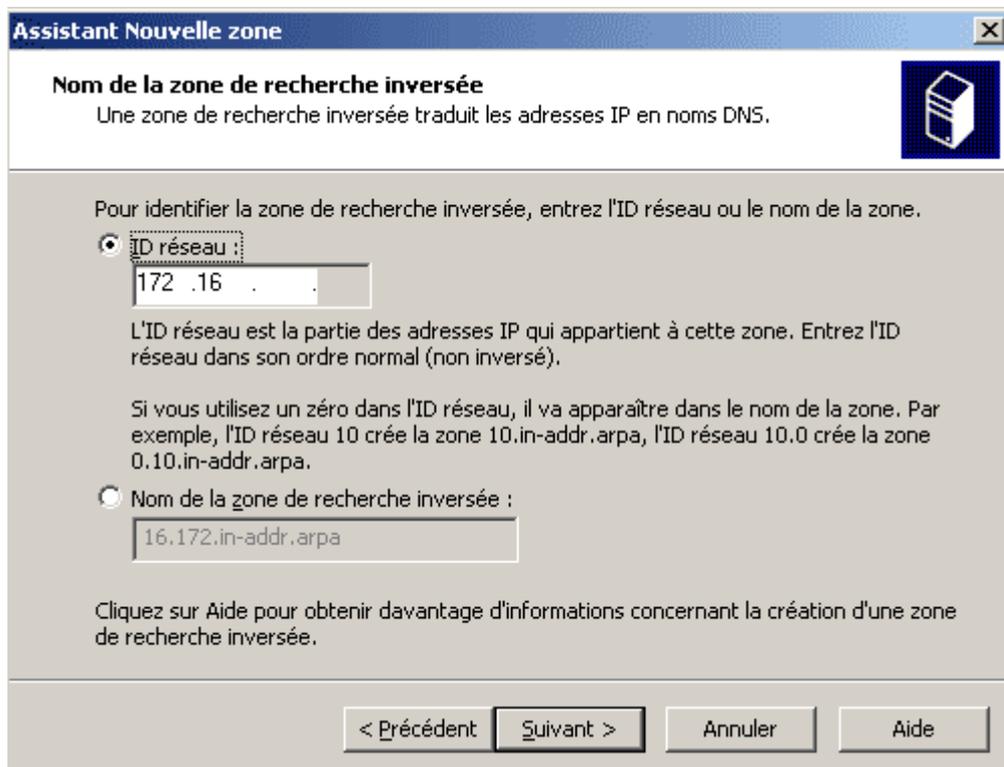
Vous pouvez ensuite visualiser les enregistrements contenus dans la zone de stub. On remarque qu'elle contient effectivement les enregistrements de ressources SOA, NS et A des serveurs DNS de la zone d'origine.

labomicrosoft.lan 15 enregistrements			
Nom	Type	Données	
(identique au dossier parent)	Source de nom (SOA)	[72], dns-1.labomicrosoft.lan.,	
(identique au dossier parent)	Serveur de noms (NS)	dns-3.labomicrosoft.lan.	
(identique au dossier parent)	Serveur de noms (NS)	dns-4.labomicrosoft.lan.	
(identique au dossier parent)	Serveur de noms (NS)	dns-5.labomicrosoft.lan.	
(identique au dossier parent)	Serveur de noms (NS)	dns-6.labomicrosoft.lan.	
(identique au dossier parent)	Serveur de noms (NS)	dns-7.labomicrosoft.lan.	
(identique au dossier parent)	Serveur de noms (NS)	dns-2.labomicrosoft.lan.	
(identique au dossier parent)	Serveur de noms (NS)	dns-1.labomicrosoft.lan.	
dns-1	Hôte (A)	172.16.16.1	
dns-2	Hôte (A)	172.16.16.2	
dns-3	Hôte (A)	172.16.16.3	
dns-4	Hôte (A)	172.16.16.4	
dns-5	Hôte (A)	172.16.16.5	
dns-6	Hôte (A)	172.16.16.5	
dns-7	Hôte (A)	172.16.16.7	

une zone de stub ne contient que des enregistrements de ressources de type SOA, NS et A.

b/ configurer une zone de recherche inversée

La configuration d'une zone de recherche inversée de stub est identique à celle d'une zone de recherche directe de stub hormis le choix du nom de la zone à dupliquer :



5.3 Les avantages des zones DNS intégrées à Active Directory

Contrairement aux zones DNS classiques qui stockent les enregistrements de ressources dans des fichiers, **les zones DNS intégrées à Active Directory stockent les enregistrements de ressources directement dans le service d'annuaire Active Directory.** Seules **les zones primaires et les zones de stub peuvent être intégrées à Active Directory.** De plus, **seuls les contrôleurs de domaine** jouant aussi le rôle de serveur DNS peuvent héberger des zones intégrées à Active Directory.

Les zones DNS intégrées à Active Directory sont intéressantes puisqu'elles permettent de **renforcer la sécurité du processus de résolution de noms** de diverses manières :

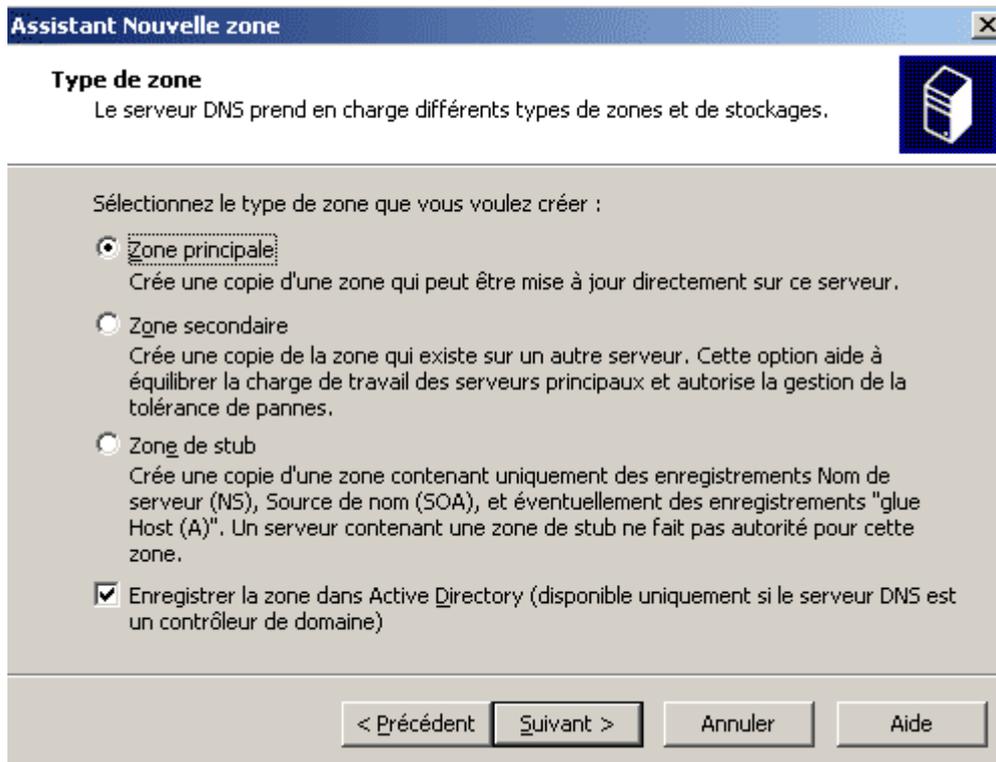
- Les zones intégrées à Active Directory peuvent être dupliquées sur tous les contrôleurs de domaine. Cela permet d'assurer **la tolérance de panne**, puisque si un contrôleur de domaine connaît une défaillance, alors la résolution de noms sera toujours assurée.
- De plus l'intégration à Active Directory **sécurise les transactions entre les serveurs DNS.** En effet, les zones DNS intégrées au service d'annuaire utilisent le mécanisme de réplication Active Directory qui s'avère plus sécurisé que les échanges AXFR et IXFR réalisés entre des serveurs DNS utilisant des zones standard.
- Enfin les zones intégrées à Active Directory permettent de **sécuriser les mises à jours automatiques des ordinateurs clients** (seuls les ordinateurs clients équipés de Windows 2000/XP/2003 peuvent faire des mises à jour automatiques). En effet, si les mises à jours automatiques sont activées, seuls

les ordinateurs clients membres du domaine peuvent mettre à jour automatiquement leurs enregistrements A et PTR.

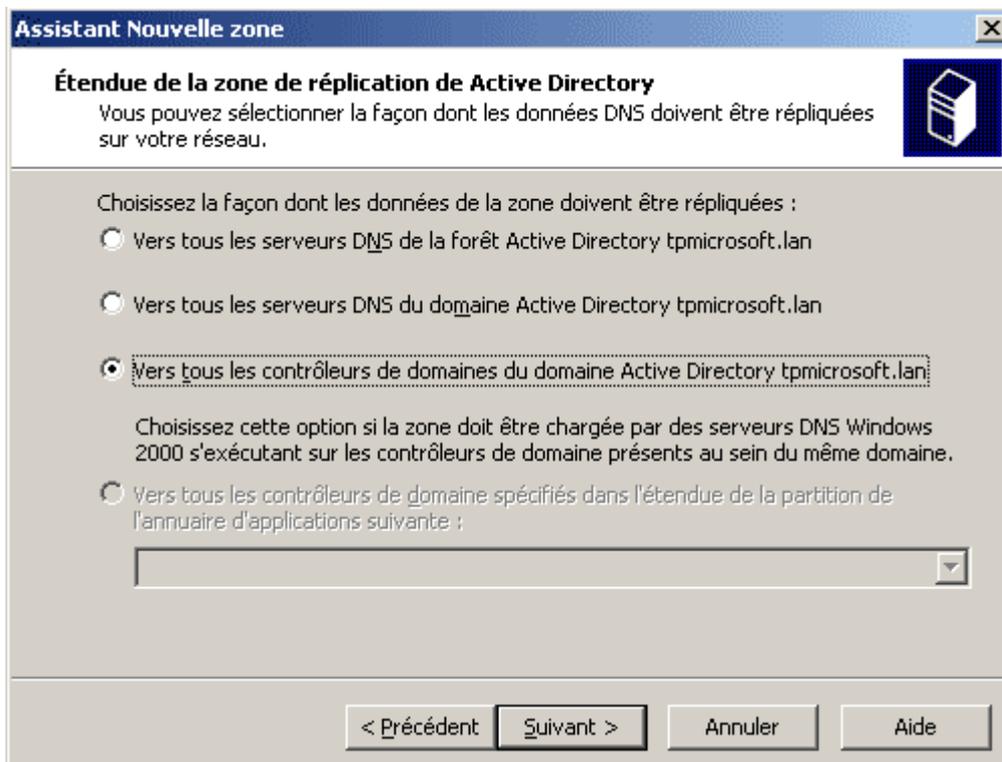
5.4 Configurer une zone DNS intégrée à Active Directory

a/ créer une zone DN intégrée à Active Directory

Pour créer une zone intégrée à Active Directory, il suffit de cocher la case nommé *Enregistrer la zone dans Active Directory* lors de la création d'une zone.

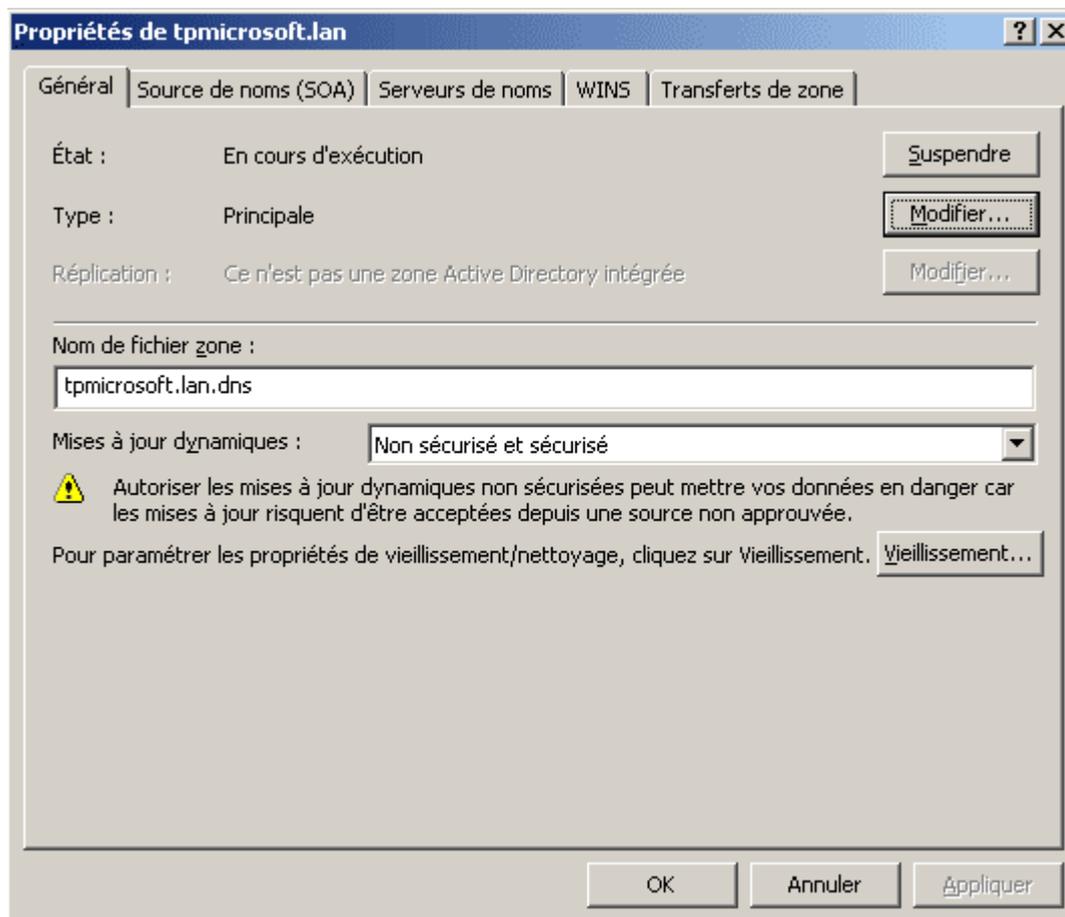


Il faut ensuite **choisir comment sera répliquée la zone DNS**. Il est possible de répliquer la zone DNS vers tous les serveurs DNS de la forêt, vers tous les serveurs DNS du domaine ou bien vers tous les contrôleurs de domaines du domaine.

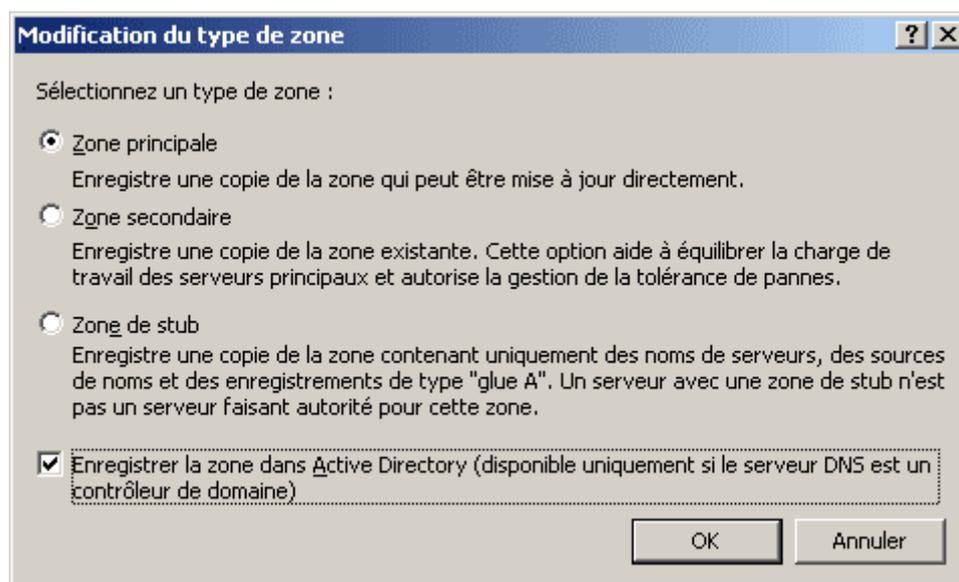


b/ Modifier une zone DNS standard en zone DNS intégrée à Active Directory

Il est également possible de **convertir une zone DNS standard en zone DNS intégrée à Active Directory**. Pour cela, il suffit de faire *clic droit / propriétés* sur la zone DNS à convertir dans la console MMC *DNS*. Cliquez ensuite sur le bouton *Modifier* pour changer le type de la zone.



Côchez ensuite la case *Enregistrer la zone dans Active Directory*, puis cliquez sur *OK* pour convertir la zone. Vous devrez ensuite sélectionner le type de réplication à mettre en oeuvre pour cette zone DNS.



6. La délégation de zone DNS

6.1 Intérêt de la délégation de zones DNS

Considérons une **arborescence de domaine**, doté d'un domaine parent et de deux sous-domaines. La solution la plus simple est de mettre en place un serveur DNS dans le domaine parent avec une zone DNS primaire. Cependant, il peut être

intéressant du point de vu des performances de mettre en place 3 serveur DNS (un dans le domaine parents et un dans chaque sous-domaine). Dans ce cas de figure (un serveur DNS dans chaque sous-domaine), **il faut créer des délégations de zones au niveau du serveur DNS appartenant au domaine parent**. Une délégation permet d'autoriser un autre serveur DNS à contrôler une partie des enregistrements de la zone.

Dans l'exemple ci-dessous, le domaine *supinfo.com* est subdivisé en deux sous-domaines nommés *administration.supinfo.com* et *students.supinfo.com*. Chaque domaine possède son propre serveur DNS. Le serveur DNS du domaine parent héberge la zone DNS primaire *supinfo.com*. On souhaite déléguer l'administration des enregistrements de ressources du domaine *administration.supinfo.com* et du domaine *students.supinfo.com* aux serveurs DNS respectivement nommés *dns.administration.supinfo.com* et *dns.students.supinfo.com*. Il va donc falloir créer **deux nouvelles délégations** sur le serveur DNS du domaine parent.

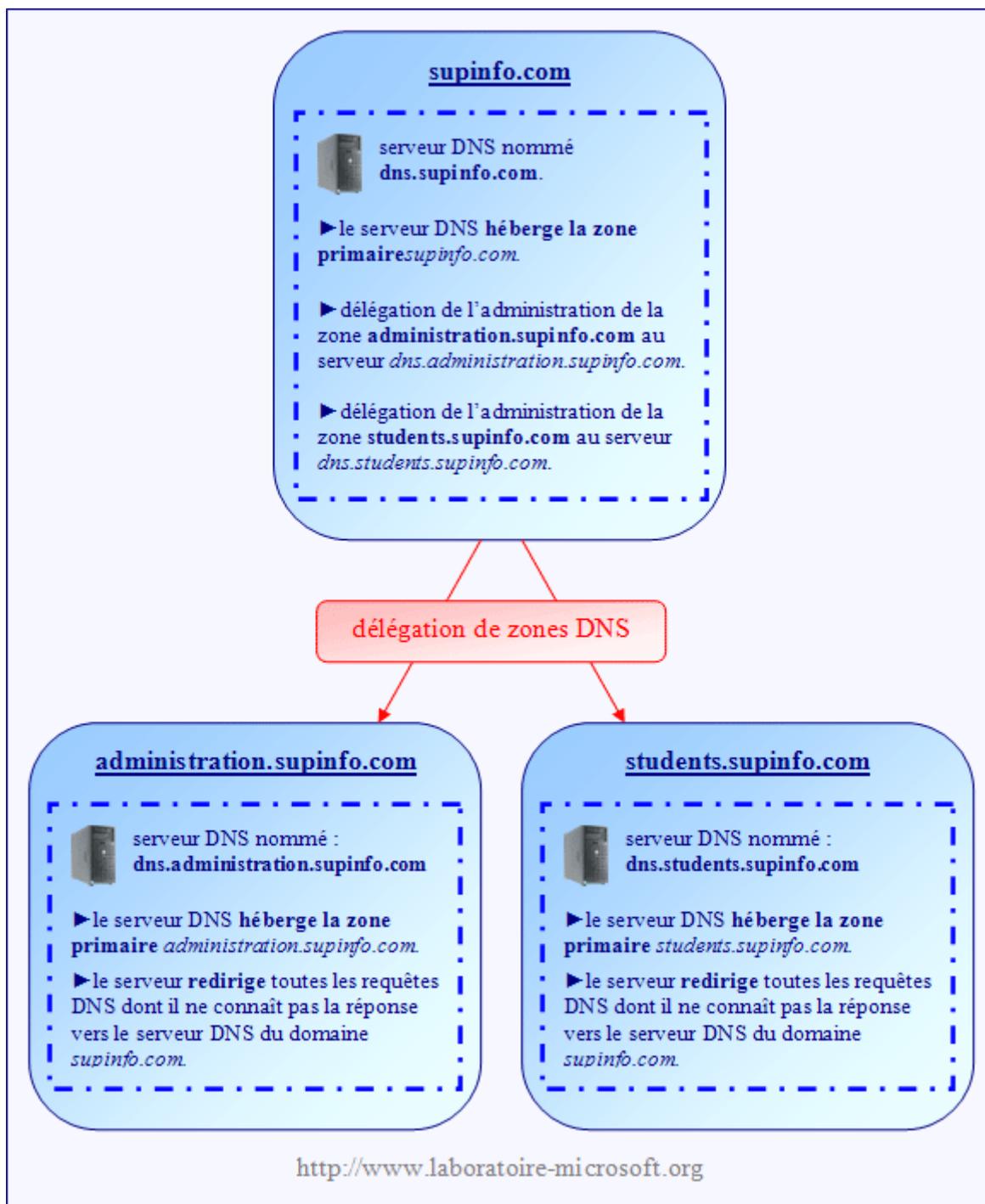
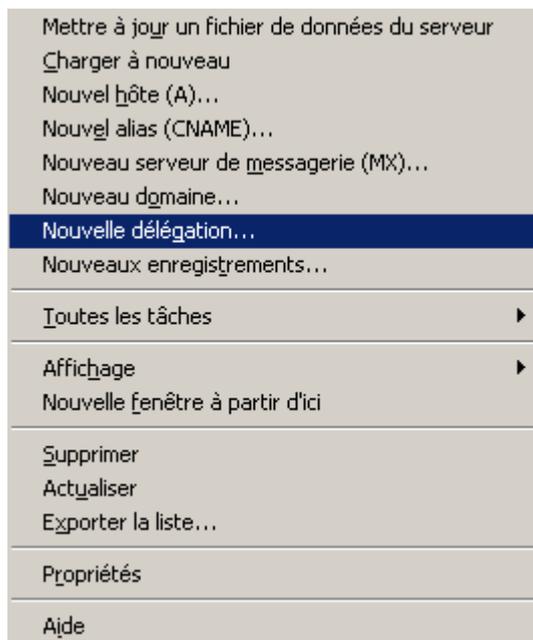


schéma illustrant la délégation de zone DNS

Une fois que les délégations sont créées, les machines clientes situées dans le domaine *supinfo.com* utilisent le serveur DNS situé dans le domaine parent pour résoudre les noms d'hôtes du domaine *supinfo.com* et utilisent les serveurs DNS situés dans les sous-domaines pour résoudre les noms d'hôtes des domaines *administration.supinfo.com* et *students.supinfo.com*. En revanche les machines clientes situées dans les sous-domaines peuvent uniquement résoudre les noms d'hôtes appartenant à leur sous-domaine. C'est pourquoi **il faut créer un redirecteur pointant vers le serveur DNS du domaine parent sur les serveurs DNS des sous-domaines**.

6.2 Créer et configurer une délégation de zone DNS

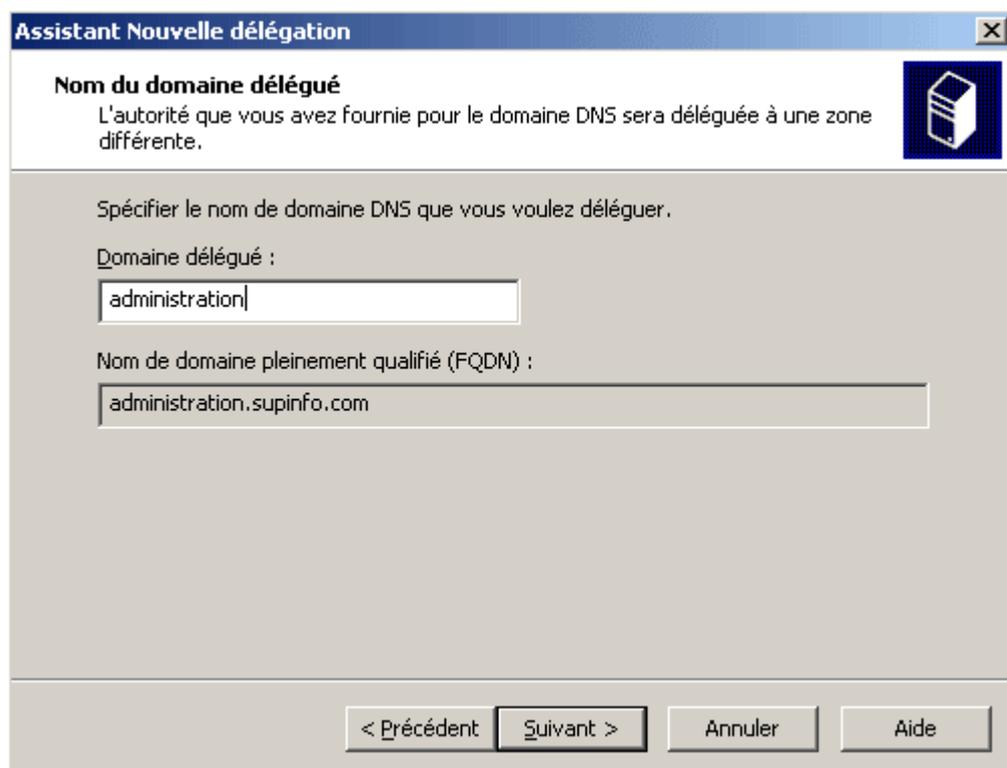


Le fonctionnement et la configuration des redirections a déjà été abordé précédemment et nous ne montrerons pas comment créer les redirections vers le serveur parent. Nous allons maintenant montrer comment créer les deux délégations de zones sur le serveur DNS du domaine *supinfo.com*.

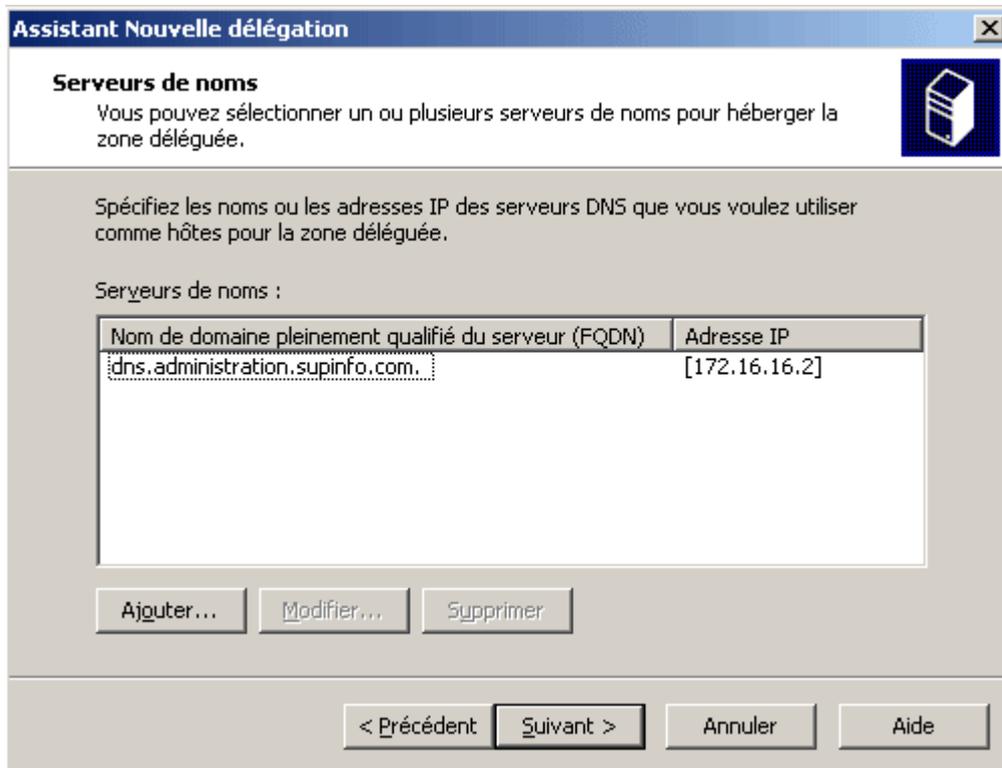
Pour commencer, il faut développer le conteneur *Zones de recherche directes* puis faire un clic droit sur la zone DNS primaire nommée *supinfo.com* et sélectionner *Nouvelle délégation*.

Dans l'assistant *Nouvelle délégation* cliquez sur *Suivant*.

Dans la fenêtre *Nom du domaine délégué*, vous devez entrer le nom d'hôte du sous-domaine sur lequel vous souhaitez faire la délégation. Dans notre exemple, il faut taper *administration* pour déléguer l'administration du domaine *administration.supinfo.com*.

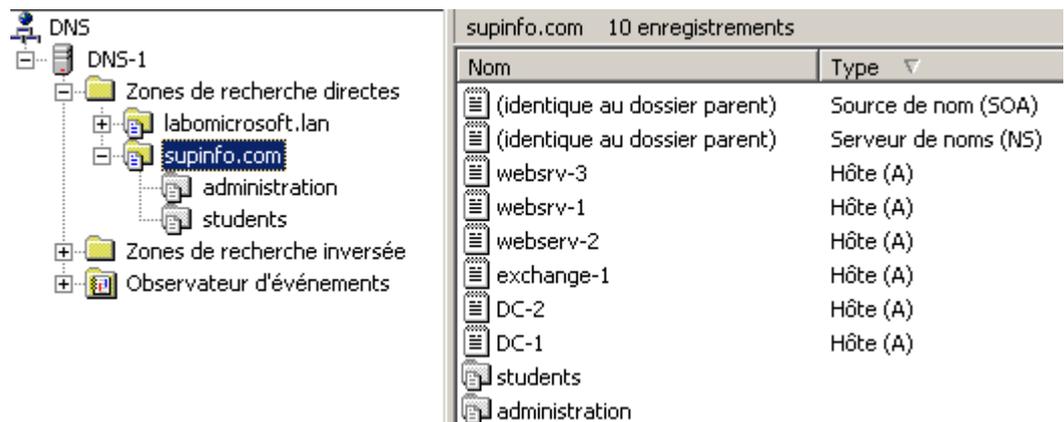


Dans l'onglet *Serveurs de noms*, utilisez le bouton *Ajouter* pour choisir les serveurs DNS auxquels vous allez déléguer l'administration du domaine *administration.supinfo.com*.



Cliquez ensuite sur *Suivant* puis sur *Terminer* pour quitter l'assistant. Procédez de la même manière pour déléguer l'administration des enregistrements de ressources du sous-domaine *students.supinfo.com* vers le serveur *dns.students.supinfo.com*.

Les domaines délégués apparaissent ensuite sous la forme de dossier grisés dans la zone DNS primaire *supinfo.com*.



7. Les outils d'administration en ligne de commande

7.1 Introduction

Il existe divers outils en ligne de commande permettant de vérifier le bon fonctionnement de la résolution de noms. On peut citer nslookup, DNScmd ou bien encore DNSLint. Seul nslookup est intégré au système d'exploitation. Les deux autres outils devront être installés avec les outils de support Windows 2003 server.

7.2 Utiliser nslookup

```
C:\>nslookup
Serveur par défaut : dns-2.labomicrosoft.lan
Address: 172.16.16.2
>
```

nslookup permet de **tester la résolution des noms d'hôtes en adresses IP** et inversement. Lorsque l'on tape nslookup en mode texte, une invite de commande apparaît. En outre le nom d'hôte et l'adresse IP du serveur DNS par défaut sont affichés.

Lorsque l'on tape un nom d'hôte ou un FQDN, nslookup renvoie l'adresse IP correspondante et indique éventuellement si la réponse fait ou non autorité sur le domaine. Dans l'exemple ci-contre, lorsque l'on tape le nom d'hôte *client-7*, le serveur DNS nommé *dns-2.labomicrosoft.lan* renvoie l'adresse IP *172.16.16.16* et rappelle le nom de domaine pleinement qualifié : *client-7.labomicrosoft.lan*.

```
> client-7
Serveur : dns-2.labomicrosoft.lan
Address: 172.16.16.2

Nom : client-7.labomicrosoft.lan
Address: 172.16.16.16
>
```

Lorsque l'on tape une adresse IP, nslookup renvoie le nom de domaine pleinement qualifié correspondant et indique éventuellement si la réponse fait ou non autorité sur le domaine. Dans l'exemple ci-à-droite, lorsque l'on l'adresse IP *172.16.16.15*, le serveur DNS nommé *dns-2.labomicrosoft.lan* renvoie le nom de domaine pleinement qualifié *client-6.labomicrosoft.lan*.

```
> 172.16.16.15
Serveur : dns-2.labomicrosoft.lan
Address: 172.16.16.2

Nom : client-6.labomicrosoft.lan
Address: 172.16.16.15
>
```

7.3 utiliser dnscmd

dnscmd est un utilitaire permettant d'**administrer votre serveur DNS** sans passer par la console MMC. Vous pouvez ainsi réaliser diverses tâches allant de la création d'un enregistrement à la suppression d'une zone. Cela peut s'avérer utile pour créer des scripts automatisant certaines tâches (par exemple la création d'enregistrements A et PTR).

Il n'est pas disponible en standard sous Windows 2003 Server mais on peut **l'installer avec les outils de support**. Pour cela, il faut développer *SUPPORT/TOOLS* dans le CD-ROM de Windows 2003 Server, puis faire *clic-droit / Explorer* sur le fichier *SUPPORT.CAB*. Il suffit ensuite d'extraire le fichier dnscmd.exe dans le répertoire %SYSTEMROOT%\system32 afin que la commande soit directement utilisable depuis l'invite de commande. Bien entendu, vous pouvez extraire ce fichier dans tout autre répertoire contenu dans la variable d'environnement Path. Si vous ne disposez pas du CD-ROM d'installation de Windows 2003 Server, vous pouvez télécharger [les outils de support pour Windows XP Service Pack 2](#) qui contiennent cet utilitaire.

Vous pouvez par exemple utiliser `dnscmd` pour ajouter ou supprimer une zone DNS. Voici la syntaxe à respecter pour l'ajout d'une zone DNS principale : `dnscmd <serveur_DNS> /ZoneAdd <nom_de_zone> /Primary /File <nom_du_fichier_de_zone>`.

```
C:\>dnscmd dns-2 /ZoneAdd enfant.labomicrosoft.lan /Primary /File enfant.labomicro
rosoft.lan.dns
DNS Server dns-2 created zone enfant.labomicrosoft.lan:
Command completed successfully.

C:\>dnscmd dns-2 /ZoneDelete enfant.labomicrosoft.lan
Are you sure you want to DeleteZone? (y/n) y

DNS Server dns-2 deleted zone enfant.labomicrosoft.lan:
Status = 0 (0x00000000)
Command completed successfully.

C:\>
```

Ajout/Suppression d'une zone DNS avec l'outil en ligne de commande `dnscmd.exe`

L'utilitaire `dnscmd.exe` peut aussi être utilisé afin de rajouter des enregistrements de ressources dans une zone DNS. Pour ajouter un enregistrement de ressource, il faut utiliser la syntaxe suivante : `dnscmd <serveur_dns> /RecordAdd <nom_zone_DNS> <nom_hôte> <type_enregistrement> <adresse_IP>`. L'exemple ci-dessous montre comment ajouter un enregistrement de ressource A et un enregistrement de ressources PTR.

```
C:\>dnscmd dns-1 /RecordAdd labomicrosoft.lan client-7 A 172.16.16.16
Add A Record for client-7.labomicrosoft.lan at labomicrosoft.lan
Command completed successfully.

C:\>dnscmd dns-1 /RecordAdd labomicrosoft.lan client-7 PTR 172.16.16.16
Add PTR Record for client-7.labomicrosoft.lan at labomicrosoft.lan
Command completed successfully.

C:\>
```

Ajout d'enregistrements de ressources à l'aide de l'outil en ligne de commande `dnscmd.exe`

`Dnscmd.exe` peut aussi être utilisé pour forcer la réplication d'une zone DNS.

```
C:\>dnscmd dns-2 /ZoneRefresh labomicrosoft.lan
DNS Server dns-2 forced refresh of zone labomicrosoft.lan:
Status = 0 (0x00000000)
Command completed successfully.

C:\>
```

7.4 utiliser `dnslint`

`Dnslint` est un outil qui permet de **diagnostiquer les problèmes liés à la résolution de noms d'hôtes**. Il permet par exemple de vérifier les enregistrements de ressources utilisés spécifiquement pour la réplication Active Directory. `Dnslint` est disponible avec les outils de support sur le CD-ROM de Windows 2003 Server. Vous pouvez également le télécharger [ici](#).

L'avantage de `dnslint.exe` est qu'il permet de **générer des rapports au format HTML** sur l'implémentation du système DNS à l'intérieur d'une forêt Active Directory. Le rapport crée liste entre autre, l'ensemble de serveurs DNS de la forêt ainsi qu'un grand nombre d'informations les concernant. La syntaxe à utiliser pour créer un rapport est : `dnslint /ad <adresse_IP_contrôleur_de_domaine> /s <adresse_IP_serveur_DNS>`.

```
C:\>dnslint /ad 172.16.16.1 /s 172.16.16.1

DNSLint will attempt to verify the
DNS entries used in AD replication

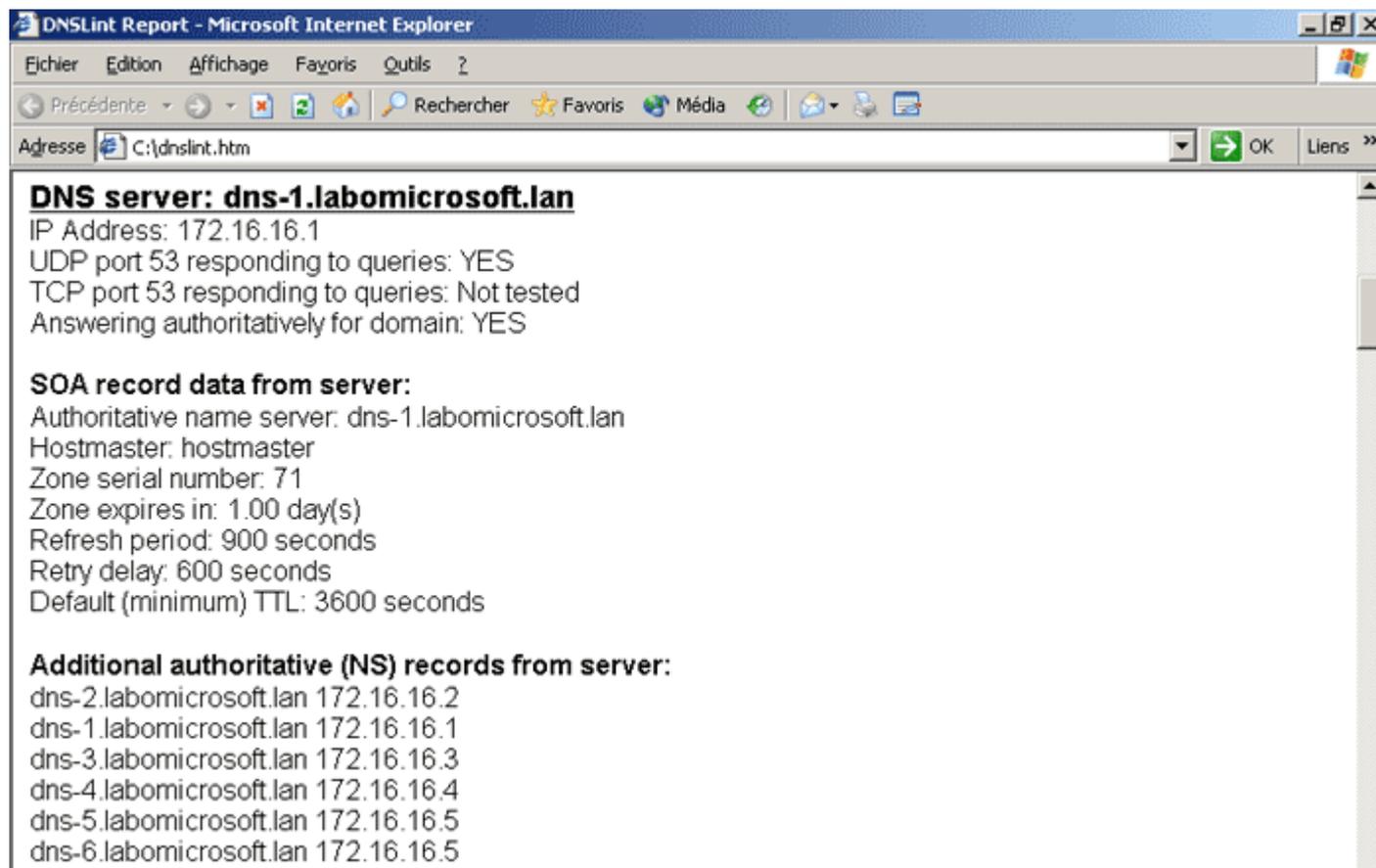
Using 172.16.16.1 for LDAP
Starting with 172.16.16.1 for DNS

This process may take several minutes to complete.....

by-passing www.internic.net lookup...
using 172.16.16.1
-----
Creating report called dnslint.htm in current directory
```

utilisation de l'outil en ligne de commande *dnslint.exe*

Voici un extrait du rapport généré par l'utilitaire *dnslint.exe* :



8. Conclusion

Nous avons montré à travers cet article **le fonctionnement du système DNS** ainsi que son intérêt par rapport au vieillissant protocole NetBIOS. L'implémentation pratique du système DNS a également été traitée du côté client avec Windows XP comme du côté serveur avec Windows 2003 Server.

Le fonctionnement de la résolution de noms d'hôte grâce aux **indications de racine**, aux **redirecteurs** et à **la délégation de zones DNS** a ensuite été explicité. Nous avons aussi vu comment **les zones DNS intégrées à Active Directory** et **les zones de stub** permettent d'augmenter la sécurité et les performances du système DNS.

Enfin divers **outils en ligne de commande** permettant d'administrer le service DNS, de tester le processus de résolution de noms ou bien encore de diagnostiquer les éventuels problèmes liés au service DNS ont été présentés.

Pour conclure, le système DNS est maintenant complètement intégré dans les systèmes d'exploitation de la firme de Redmond ce qui en facilite l'utilisation et la mise en œuvre. De plus nous avons montré comment le service DNS intégré à Windows 2003 Server permet de **déployer rapidement un système de résolution de noms fiable, efficace et sécurisé.**