DNS sous Windows Server 2003

1- Introduction :

Pratiquement tout réseau doit disposer d'un mécanisme de traduction des noms d'ordinateur en adresses IP. Cette exigence vient de ce que les individus et les applications se connectent généralement à des ordinateurs réseau en spécifiant un nom, alors qu'au niveau inférieur on emploie le plus souvent des adresses pour identifier les hôtes.
Pour des raisons historiques, deux systèmes de dénomination d'ordinateur coexistent dans les réseaux Windows Server 2003 : NetBios et DNS. Ces deux systèmes ne sont pas apparentés, ils font recours à des mécanismes distincts pour résoudre les noms en adresses IP.

2- Comparaison de DNS et NetBios :

DNS est le système de dénomination favori de la famille Windows Server 2003.En comparaison avec NetBios, il offre :

- une bien meilleure évolutivité,
- plus de sécurité
- une meilleure compatibilité avec Internet.

- Même si DNS nécessite d'être configuré avant de fonctionner, il reste un élément essentiel des domaines Active Directory et de ce fait employé dans la plupart des réseaux Windows Server 2003.

- NetBios est toutefois toujours fréquemment employé comme méthode de secours de résolution de noms, essentiellement parce qu'il procure sans configuration, une résolution de noms pour les ordinateurs situés sur le même segment réseau.

- NetBios sert en outre de maintien de compatibilité avec d'anciens dispositifs Windows, comme le parcours d'un réseau Microsoft Windows à l'aide de Mes Favoris réseau ou la connexion à des partages à l'aide d'adresses UNC(Universal Naming Convention) comme \\ordinateur1\share1.

- Dans les réseaux Windows Server 2003 ; la résolution de noms DNS est prioritaire par rapport à la résolution de noms NetBios. Cette priorité est géré par le service client DNS (appelé aussi solveur DNS), responsable de la résolution de noms à l'aide de DNS, puis en cas d'échec, soumet le nom à NetBios.

3- Comparaison des noms d'ordinateur :

Lorsque vous installez Windows server 2003 sur un ordinateur, vous devez attribuer un nom à ce dernier. Ce nom, modifiable par la boite de dialogue **Propriétés système**, sert de base tant pour son nom d'hôte DNS que pour son noms NetBios.

Plus spécifiquement, un nom d'hôte DNS, tant qu'il ne dépasse pas 15 caractères, ce même nom est également employé comme nom NetBios.

En dépit de cette similitude, DNS diffère de NetBios en ce que l'espace de noms est hiérarchique. Chaque nom d'hôte DNS n'est qu'une partie d'un nom complet connu sous le nom de domaine pleinement qualifié ou FQDN (Fully Qualified Domain Name), spécifiant tant le nom d'hôte que son domaine.

Un FQDN est formé d'un **nom d'hôte** et d'un **suffixe DNS principal**. Par exemple, dans le FQDN client1.lucernepublishing.com :

- client1 représente la première étiquette et représente le nom d'hôte qui est souvent nommé nom d'ordinateur
- lucernepublishing.com représente le suffixe DNS principal, il est spécifié dans l'onglet Nom de l'ordinateur de la boite de dialogue des propriétés de Poste de travail. Il est également connu comme nom de domaine principal.

Un exemple de FQDN est www.lucernpublishing.com.

NetBios ne possède pas de telle hiérarchie, si bien que chaque nom NetBios doit être unique sur le réseau.

Le tableau suivant illustre une comparaison entre les noms NetBios et DNS :

	Noms d'ordinateur NetBios	Noms d'ordinateur DNS
Type	Plat	Hiérarchique
Restrictions de caractères	Caractères non autorisés : nombres, espaces, symboles / \ [ ] : | < > + = ; , ? et *	Caractères autorisés : toutes les lettres majuscules (A-Z), toutes les lettres minuscules (a-z), tous les nombres (0-9) et le tiret (-).
Taille maximale	15 caractères.	63 octets par étiquette 255 octets par FQDN
Services de noms	WINS, monodiffusion NetBios, fichier Lmhosts	DNS, fichier Hosts

4- Définition et fonctions de DNS:

DNS (Domain Name System) est une base de données distribuée hiérarchisée qui contient les mappages de noms d'hôtes DNS à des adresses IP. Il permet de repérer des ordinateurs et des

services en utilisant des noms alphanumériques faciles à retenir. DNS permet également de découvrir des services réseau comme des serveurs de messagerie et des contrôleurs de domaine dans le service d'annuaire Active Directory :

- DNS est à la base du système de noms Internet, mais aussi du système de noms de domaine Active Directory d'une organisation. Il prend en charge l'accès aux ressources à l'aide de noms alphanumériques.

- Sans DNS, vous devriez trouver les adresses IP des ressources pour accéder à ces ressources. Comme les adresses IP des ressources peuvent changer, il serait difficile d'en tenir à jour une liste exacte. Au lieu de cela, DNS permet aux utilisateurs de faire appel à des noms alphanumériques, lesquels restent assez stables dans une organisation.

- Avec DNS, les noms d'hôtes résident dans une base de données qui peut être distribuée entre plusieurs serveurs, ce qui diminue la charge de chaque serveur et permet d'administrer le système de noms par partitions.

- DNS prend en charge des noms hiérarchiques et permet d'inscrire divers types de données en plus du mappage de noms d'hôtes à adresse IP qui est utilisé dans les fichiers Hosts.

5- Installation du service Serveur DNS sous Windows Server 2003:

Pour installer DNS on suit la procédure suivante :

1. Ouvrez une session avec un compte d'utilisateur sans droits d'administration.
2. Cliquez sur **Démarrer**, puis sur Panneau de configuration.
3. Dans le Panneau de configuration, ouvrez **Outils d'administration**, cliquez avec le bouton droit sur **Gérer votre serveur**, puis sélectionnez **Exécuter en tant que**.
4. Dans la boîte de dialogue **Exécuter en tant que**, sélectionnez **L'utilisateur suivant**, entrez un compte d'utilisateur et un mot de passe bénéficiant des autorisations nécessaires à la réalisation de cette tâche, puis cliquez sur **OK**.
5. Dans la fenêtre **Assistant Gérer votre serveur**, cliquez sur **Ajouter ou supprimer un rôle**.
6. Dans la page **Étapes préliminaires**, cliquez sur **Suivant**.
7. Dans la page **Rôle du serveur**, sélectionnez **Serveur DNS**, puis cliquez sur **Suivant**.
8. Dans la page **Aperçu des sélections**, cliquez sur **Suivant**.
9. Si un message vous y invite, insérez le CD-ROM de Microsoft Windows Server 2003.
10. Dans la page **Bienvenue dans l'Assistant Configurer un serveur DNS**, cliquez sur **Annuler**.

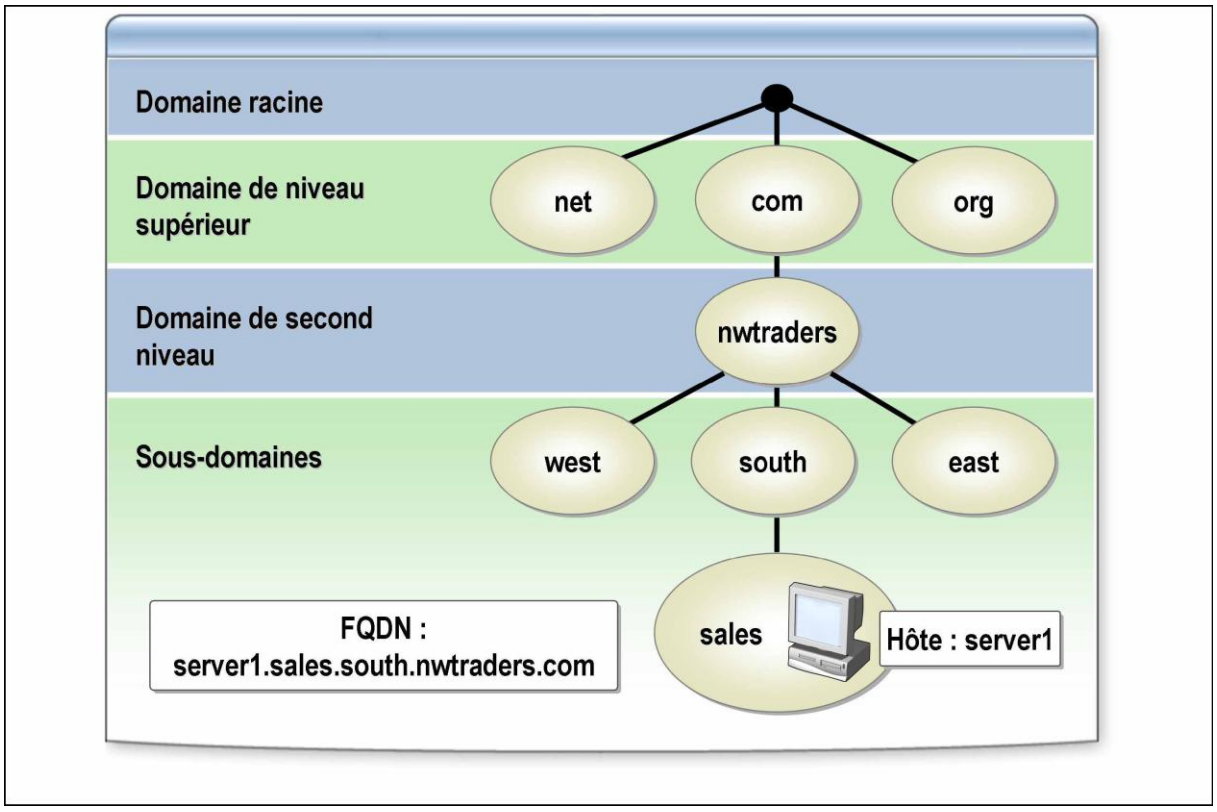
Vous aurez l'occasion de configurer le service DNS dans une application pratique ultérieure.

11. Dans la page **Assistant Configurer votre serveur**, cliquez sur **Terminer**.

6- Espace de noms de domaines :

Un espace de noms DNS comprend le domaine racine, des domaines de niveau supérieur, des domaines de niveau secondaire et (éventuellement) des sous domaines.

La combinaison de l'espace de noms DNS et du nom d'hôte constitue le nom de domaine pleinement qualifié (FQDN, fully qualified domain name).



- L'espace de noms DNS permet d'organiser les noms affichés des ressources en une structure logique, facile à comprendre pour les utilisateurs. La structure hiérarchique de l'espace de noms DNS simplifie considérablement l'organisation et la recherche des ressources.

- Pour utiliser et administrer un service DNS, l'espace de noms de domaine fait référence à l'intégralité de la structure d'un nom de domaine, de la racine au niveau supérieur de l'arborescence jusqu'aux branches de bas niveau.

- L'arborescence doit être conforme aux conventions acceptées pour la représentation des noms DNS. La convention principale est simple : pour chaque domaine, un point (.) est utilisé pour séparer chaque sous-domaine de son domaine parent, de bas en haut dans l'arborescence.

6-1 : Domaine DNS :

Dans le système DNS, on appelle domaine DNS toute arborescence ou sous-arborescence se trouvant dans l'espace de noms de domaine. Bien que les noms de domaine DNS soient utilisés pour nommer les domaines Active Directory, ils ne coïncident pas et ne doivent pas être confondus avec les domaines Active Directory.

a-Domaine DNS racine

Il s'agit du noeud racine de l'arborescence DNS. Le domaine racine n'a pas de nom. Il est parfois représenté dans les noms DNS par un point final (.) indiquant que le nom est à la racine, c'est-à-dire au plus haut niveau, de la hiérarchie des domaines.

b- Domaine DNS de niveau supérieur

Il s'agit de la portion finale (à l'extrême droite) d'un nom de domaine DNS. En général, un domaine DNS de niveau supérieur est représenté par un nom de deux ou trois caractères qui identifie le statut organisationnel ou géographique du nom de domaine. Par exemple, dans www.microsoft.com., la portion « .com » représente le nom du domaine de niveau supérieur et indique que ce nom a été inscrit auprès d'une organisation commerciale pour un usage commercial.

c-Domaine DNS de second niveau :

Un nom de domaine de second niveau est un nom unique de longueur variable, formellement inscrit par InterNIC auprès d'un individu ou d'une organisation qui se connecte à Internet. Dans l'exemple www.microsoft.com, le nom de second niveau est la portion «microsoft » du nom de domaine, inscrite par InterNIC et affectée à Microsoft Corporation.

d-Sous-domaine DNS:

Outre le nom de second niveau inscrit auprès de InterNIC, une organisation de grande envergure peut choisir de subdiviser encore son nom de domaine en ajoutant des départements ou des services représentés chacun par une portion distincte dans le nom de domaine.
Voici quelques exemples de noms de sous-domaines:

- **DRIF.ofppt.ma**
- **DOSI.ofppt.ma**

- **DMG.ofppt.ma**

7- Composants de DNS :

DNS repose sur la configuration adéquate de serveurs DNS, clients DNS, zones, services de résolution et enregistrements de ressources.

a- Serveur DNS :

- C'est un ordinateur exécutant un programme serveur DNS. Un serveur DNS contient une base de données d'informations DNS concernant une portion de la structure de l'arborescence de domaines DNS et répond aux requêtes de résolution de noms émises par les clients DNS.

- Les serveurs DNS peuvent procurer l'information demandée, renvoyer un pointeur vers un autre serveur en mesure de répondre à la requête ou répondre que l'information est inexistante ou indisponible.

- Un serveur DNS fait autorité pour une zone qu'il héberge, comme serveur DNS principal ou secondaire.

- Un serveur peut faire autorité pour un ou plusieurs niveaux de la hiérarchie du domaine. Par exemple, les serveurs DNS racine de l'Internet ne font autorité que pour les noms de domaine de niveau supérieur comme .com toutefois dans l'espace de noms lucernepublishing.com, le ou les serveurs faisant autorité pour exemple.lucerpublishing.com peut (peuvent) également le faire pour widgets.exemple.lucernepublishing.com

b- Zones DNS :

Les zones possèdent les caractéristiques suivantes :

- Avant d'ajouter des enregistrements de ressources, vous devez créer dans le système DNS la structure qui va les accueillir. Dans DNS, ces conteneurs logiques sont appelés des **zones**.

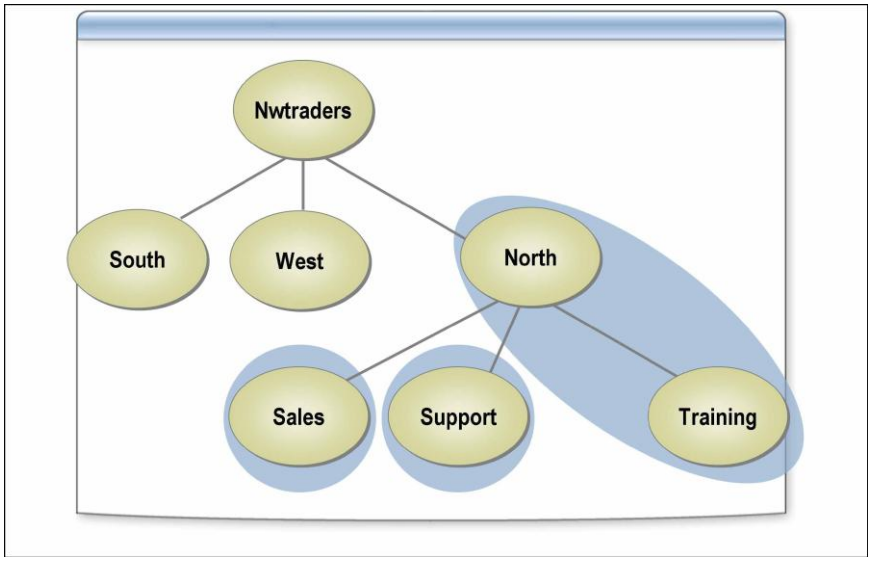
- Il existe plusieurs configurations de zone possibles dans DNS. Les zones que vous allez créer seront déterminées par les besoins en matière de résolution de noms dans votre environnement.

- Une nouvelle zone ne contient que deux enregistrements de ressource : l'enregistrement **SOA** (Start of Autority) correspondant à la zone, et un enregistrement

NS (Name Server) correspondant au serveur DNS local créé pour cette zone.

- Une fois que les zones DNS sont créées et remplies avec des enregistrements de ressources, le service DNS est en mesure de prendre en charge la résolution de noms d'hôtes.

- Un serveur peut faire autorité pour une ou plusieurs zones, une zone pouvant contenir un ou plusieurs domaines contigus. Par exemple, un serveur peut faire autorité à la fois pour les zones microsoft.com et lucerpublishing.com.



- Lorsque vous créez une zone, vous créez un fichier de zone pour stocker les propriétés et les enregistrements de ressources de la zone. Les fichiers de zone contiennent des enregistrements de ressources pour les zones pour lesquelles un serveur fait autorité

- Chaque zone peut faire autorité pour un ou plusieurs domaines DNS, à condition que ces domaines soient contigus dans l'arborescence DNS. Les zones peuvent être stockées dans des fichiers texte plats ou dans la base de données Active Directory.

- Une zone est un ensemble de mappages de nom d'hôte à adresse IP pour des hôtes situés dans une portion contiguë de l'espace de noms DNS.

- Les données d'une zone sont gérées sur un serveur DNS et peuvent être stockées de deux manières :

  - En tant que fichier de zone plat contenant des listes de mappages ;

- Dans une base de données Active Directory.

- Un serveur DNS fait autorité pour une zone s'il héberge les enregistrements de ressources correspondant aux noms et aux adresses que les clients demandent dans le fichier de zone.

8-Types de zones DNS :

Lorsque vous configurez un serveur DNS, vous pouvez définir plusieurs types de zones ou aucun, selon le type de rôle du serveur DNS dans le réseau.
Après avoir créé une zone, vous devez lui ajouter d'autres enregistrements de ressources tels que ceux de type (A), alias (CNAME), MX, SRV et PTR.

Le fonctionnement normal des serveurs DNS fait intervenir trois zones :

- zone principale ;
- zone secondaire ;
- zone de stub.

8-1 Zone principale :

Dans ce type de zone, les données de zone procurent les données sources **originales** pour tous les domaines de la zone. Les enregistrements de ressources y sont créés et gérés.
Ces données de zone peuvent être sauvegardées de cette zone vers une autre zone secondaire.

Il existe deux types de zones principales:

8-1-a Zone standard principale : seul un unique serveur peut héberger et stocker la copie originale de la zone. Aucun autre serveur principal n'est autorisé pour cette zone. Si le serveur principal est inaccessible, aucune modification ne peut être apportée à la zone. Toutefois, les requêtes pour les noms de la zone ne sont pas affectées et peuvent se poursuivre puisqu'il existe des serveurs secondaires.

8-1-b Zone intégrée à Active directory :

Une zone DNS intégrée à Active Directory est une zone DNS stockée dans Active Directory. Lorsque vous configurez un contrôleur de domaine, Active Directory exige l'installation de DNS. Les zones qui sont créées sur un serveur DNS configuré comme contrôleur de domaine Active Directory peuvent être des zones DNS intégrées à Active Directory.

Les zones DNS intégrées à Active Directory présentent plusieurs avantages par rapport aux zones DNS qui ne sont pas intégrées à Active Directory. Elles peuvent utiliser Active Directory pour :

- Stocker les données de configuration de zone dans Active Directory au lieu de les stocker dans un fichier de zone.
- Utiliser la réplication Active Directory à la place des transferts de zone.
- Autoriser uniquement les mises à jour dynamiques sécurisées (à la place des mises à jour sécurisées et non sécurisées sur une zone DNS non intégrée à Active Directory.

8-2 Zone secondaire :

Ce type de zone est une **zone de sauvegarde** de la zone principale ou d'autres zones secondaires.

Une zone secondaire est une copie en lecture seule de la zone DNS. Les enregistrements contenus dans la zone secondaire **ne peuvent pas être modifiés,** les administrateurs peuvent modifier uniquement les enregistrements de la zone DNS principale.

Normalement, un serveur secondaire au moins est configuré pour la tolérance de panne. Toutefois, il est possible de configurer plusieurs serveurs secondaires à d'autres emplacements, de telle sorte que les enregistrements de la zone puissent être résolus sans que la requête ne franchisse des liaisons WAN.

Après avoir décidé si une zone est une zone principale, une zone secondaire ou une zone de stub, vous devez déterminer dans quel type de zone de recherche les enregistrements de ressources seront stockés, à savoir une zone de recherche directe ou une zone de recherche inversée.

8-3 Zone de recherche directe :

Dans le système DNS, une recherche directe est un processus d'interrogation qui recherche le nom affiché du domaine DNS d'un ordinateur hôte pour trouver son adresse IP.
Dans le Gestionnaire DNS, les zones de recherche directe s'appuient sur des noms de domaines DNS et contiennent généralement des enregistrements de ressources de type A (hôte).

8-4 Zone de recherche inversée :

Dans le système DNS, une recherche inversée est un processus d'interrogation qui recherche l'adresse IP d'un ordinateur hôte pour trouver son nom affiché dans le domaine DNS.

Dans le Gestionnaire DNS, les zones de recherche inversée s'appuient sur le nom de domaine in-addr.arpa et contiennent généralement des enregistrements de ressources de type PTR (pointeur).

8-5 Zone stub :

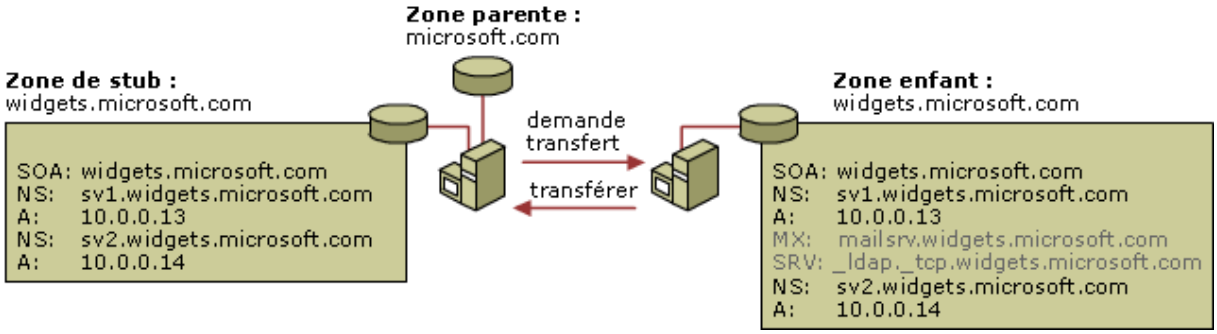
Cette zone contient une copie d'une zone ne contenant que les enregistrements de ressource nécessaire à l'identification des serveurs DNS faisant autorité pour la zone maîtresse.

Une zone de stub est utilisée pour veiller à ce qu'un serveur DNS hébergeant une zone parent sache quels serveurs DNS font autorité sur sa zone enfant et maintenir ainsi l'efficacité de la résolution des noms DNS.

Une zone de stub est composée des éléments suivants :

- Un enregistrement de ressource de noms (SOA), enregistrements de nom de serveur (NS) et enregistrements de type « glue A » associés à la zone déléguée.
- adresse IP d'un ou plusieurs serveurs maîtres pouvant être utilisés pour mettre à jour la zone de stub.

L'illustration suivante montre comment une zone de stub hébergée sur le même serveur DNS que la zone parent met à jour les informations relatives aux serveurs faisant autorité pour la zone enfant.



8-6 Types de serveurs :

De même, le type de serveur fait référence au type de zone hébergée par le serveur.

Un serveur DNS hébergeant une zone principale est dit agir comme **serveur principal** et stocke des données sources originales des zones :

Un serveur DNS hébergeant une zone secondaire est dit agir comme **serveur secondaire**. Un serveur DNS secondaire est un serveur faisant autorité de secours d'un serveur principal. Les

serveurs à partir desquels les serveurs secondaires récupèrent les informations de zone sont appelés maîtres. Un maître peut être un serveur principal ou un autre serveur secondaire.

Un **serveur en cache seul** fait suivre les requêtes vers d'autres serveurs DNS sans héberger de zone. Un tel serveur met toutefois en cache les réponses reçues des autres serveurs DNS et peut ainsi améliorer la résolution de noms pour un réseau n'hébergeant pas de zone.

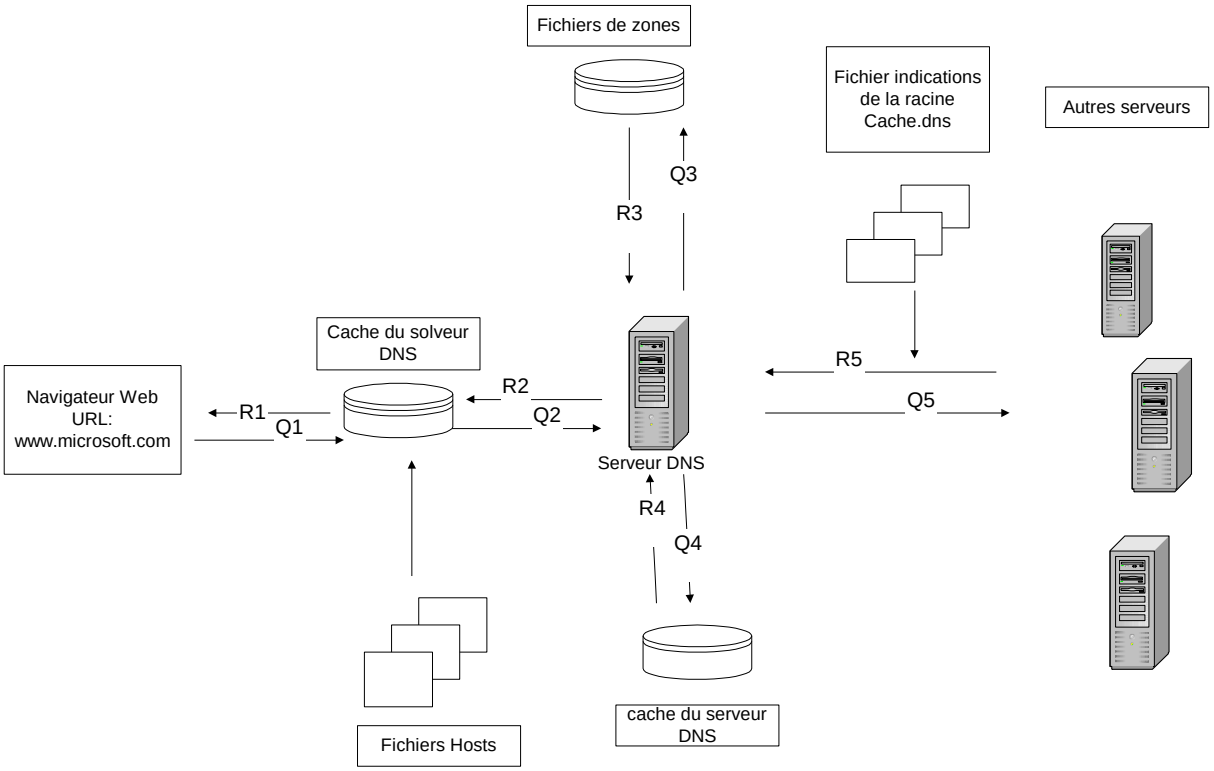
La mise en cache est le processus qui consiste à stocker temporairement dans un sous-système de mémoire spécial des informations ayant fait l'objet d'un accès récent pour y accéder plus rapidement ensuite.
La mise en cache permet de répondre plus rapidement aux requêtes et réduit le trafic DNS sur le réseau. En plaçant en mémoire cache les réponses fournies par le système DNS, le serveur DNS peut ensuite résoudre certaines requêtes déjà traitées à partir de sa seule mémoire cache. Cela réduit considérablement le temps de réponse et élimine le trafic réseau associé à l'envoi de la requête à un autre serveur DNS

Le serveur place en mémoire cache toutes les informations reçues au cours de ce processus, pendant une durée spécifiée dans les données qu'il reçoit. Cette durée de conservation, appelée durée de vie (TTL, time to live), est exprimée en secondes. Elle est déterminée par l'administrateur de serveur associé à la zone principale qui contient les données.

Dans la plupart des configurations de zone, la valeur **Durée de vie minimale (par défaut)** est attribuée pour la mise en cache des enregistrements de ressources. Cette valeur est définie dans l'enregistrement de ressource d'autorité principale (SOA) de la zone. Par défaut, la durée de vie minimale est de 3 600 secondes (1 heure). Cette valeur peut être modifiée ou des durées de vie de mise en cache peuvent être définies individuellement pour chaque enregistrement de ressource.

Une durée de vie courte permet de garantir une meilleure cohérence des informations concernant le domaine à travers le réseau dans l'éventualité où ces données changent souvent. D'un autre côté, cela alourdit la charge des serveurs qui contiennent ces données et augmente le trafic Internet.

9- Processus d'une requête DNS :



Le processus de requête débute lorsqu'un nom de domaine DNS est employé dans un programme de l'ordinateur local.

Partie 1 :

Dans l'exemple ci-dessus, un navigateur web appelle le FQDN www.microsoft.com. La requête est alors transmise au service client DNS (le cache du solveur) pour résoudre le nom à l'aide des informations localement mises en cache.

Le cache du solveur local peut comprendre des informations de noms obtenues depuis deux sources possibles :

a- Un fichier Hosts configuré localement

b- Les enregistrements de ressource obtenus à partir des réponses reçues suite à des requêtes DNS antérieures.

Si le nom recherché peut être résolu, la requête reçoit une réponse et le processus prend fin.
Si la requête ne correspond à aucune entrée du cache, le processus de résolution se poursuit par l'envoi du client d'une requête vers un serveur DNS pour résoudre le nom.

Partie 2 :

Le service client DNS fait recours à une liste de recherche de serveurs classée par préférence. Cette liste comprend tous les serveurs DNS préférés ou auxiliaires configurés pour chaque connexion réseau active du système.

Le client envoie d'abord une requête vers le serveur DNS spécifié comme serveur DNS préféré dans la boite de dialogue Propriétés TCP/IP de la connexion. Si aucun serveur DNS préféré n'est disponible, il fait appel aux serveurs DNS auxiliaires.

Lorsqu'un serveur DNS reçoit une requête, il vérifie d'abord s'il peut répondre à celle-ci par autorité (c'est-à-dire d'après les informations contenues dans une zone configurée localement sur le serveur).

S'il n'existe aucune information de zone pour le nom recherché, le serveur cherche alors s'il peut résoudre le nom à l'aide d'informations mises en cache localement suite à des requêtes antérieures.

Parite 3 :

Si la requête de noms ne trouve pas de réponse adéquate sur le serveur préféré depuis son cache ou ses informations de zone, le processus se poursuit d'une façon dépendante de la configuration du serveur DNS.

Dans la configuration par défaut, le serveur DNS a recours à la récursivité pour résoudre le nom. La récursivité DNS fait référence au processus selon lequel un serveur DNS envoie une requête vers d'autres serveurs DNS pour le compte du client de la requête originale.

Pour pouvoir correctement utiliser le processus de récursivité, le serveur DNS a besoin de connaître les coordonnées des autres serveurs DNS de l'espace de noms de domaines DNS. Ces informations sont fournies sous la forme d'indications racine, une liste utilisée par le service DNS pour localiser d'autre serveurs DNS qui font autorité pour la racine de l'arborescence des espaces de noms de domaines DNS.

Les serveurs racine font autorité pour la racine et les domaines de premier niveau du domaine dans l'arborescence des espaces de noms de domaines DNS

Les indications de racine sont stockées dans le fichier Cache.dns qui se trouve dans le dossier %Systemroot%\System32\Dns.

9-1 Définition d'une 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. En retour, le serveur peut uniquement

renvoyer une réponse complète ou indiquer qu'il ne sait pas résoudre le nom. Une requête récursive ne peut pas être redirigée vers un autre serveur DNS.

Les requêtes récursives sont lancées par un client DNS ou par un serveur DNS configuré pour utiliser des redirecteurs. Une requête récursive place toute la responsabilité de la réponse finale sur le serveur interrogé.

La réponse à une requête récursive peut être positive ou négative. Dans une requête récursive, le serveur DNS interrogé est sommé de renvoyer l'une des trois réponses suivantes :

- Les données demandées.
- Un message d'erreur indiquant que les données du type demandé n'existent pas.
- Un message indiquant que le nom de domaine spécifié n'existe pas.

9-2 Définition d'une requête itérative :

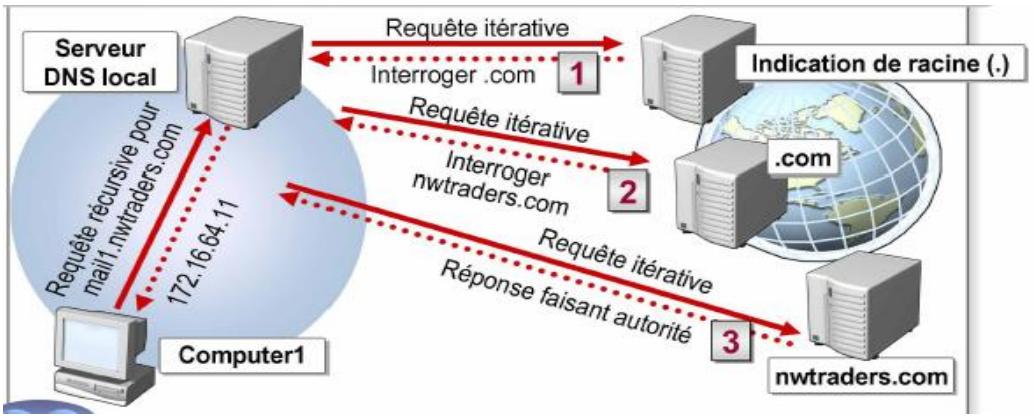
Une requête itérative est une requête envoyée à un serveur DNS dans laquelle le client DNS demande la meilleure réponse possible que peut fournir le serveur DNS sans faire appel à d'autres serveurs DNS. Les requêtes itératives sont parfois appelées requêtes non récursives. Le résultat d'une requête itérative est souvent **une référence** à un autre serveur DNS situé plus bas dans l'arborescence DNS.

Dans le cas d'une requête récursive, une référence n'est pas une réponse acceptable.

En règle générale, un serveur DNS envoie une requête itérative à d'autres serveurs DNS après avoir reçu d'un client une requête récursive. Dans une requête itérative, le serveur de noms interrogé renvoie au demandeur la meilleure réponse qu'il possède. La réponse à une requête itérative peut être :

- une réponse positive ;
- une réponse négative ;
- une référence à un autre serveur.

9-3 Fonctionnement d'une requête itérative :



Dans l'illustration, le serveur DNS local n'a pas réussi à résoudre le nom demandé en utilisant sa mémoire cache et il ne fait pas autorité pour le domaine.
Il commence donc à rechercher le serveur DNS qui fait autorité en interrogeant d'autres serveurs DNS. Pour trouver le serveur DNS qui fait autorité pour le domaine, le serveur DNS résout le nom de domaine pleinement qualifié, de la racine jusqu'à l'hôte, en utilisant des requêtes itératives. Le traitement de cet exemple se déroule comme suit :

1. Le serveur DNS local reçoit une requête récursive d'un client DNS. Par exemple : Le serveur DNS local reçoit une requête récursive de Computer1 concernant mail1.nwtraders.com.
2. Le serveur DNS local envoie une requête itérative au serveur racine pour obtenir un serveur de noms faisant autorité.
3. Le serveur racine répond par une référence à un serveur DNS plus proche du nom de domaine demandé. Par exemple : Le serveur racine répond par une référence au serveur DNS associé au domaine .com.

4. Le serveur DNS local envoie ensuite une requête itérative au serveur DNS plus proche du nom de domaine demandé. Par exemple : Le serveur DNS local envoie une requête itérative au serveur DNS de .com.

5. Le processus continue jusqu'à ce que le serveur DNS local reçoive une réponse faisant autorité. Par exemple : Le serveur DNS de .com répond par une référence au serveur DNS de nwtraders.com. Ensuite, le serveur DNS local envoie une requête itérative au serveur DNS de nwtraders.com. Par la suite, le serveur DNS local reçoit une réponse faisant autorité du serveur DNS de nwtraders.com.

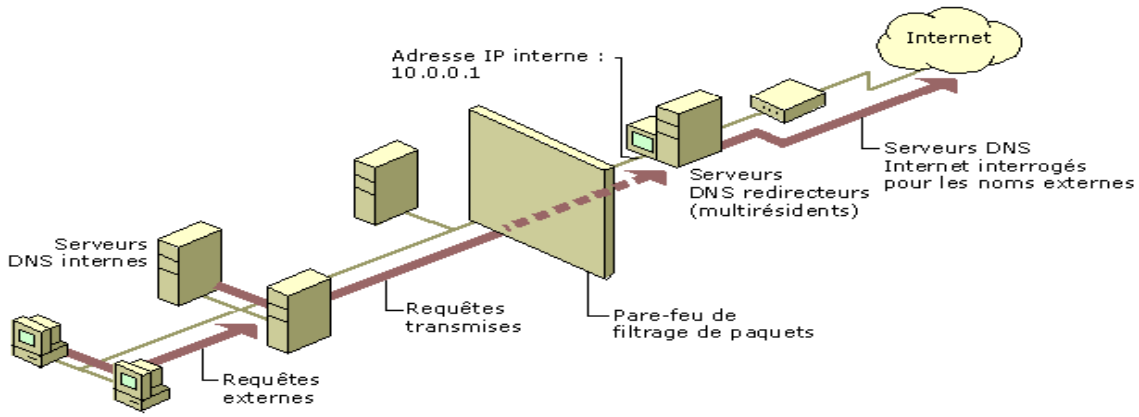
6. Cette réponse est alors envoyée au client DNS. Par exemple : Le serveur DNS local envoie la réponse relative au serveur faisant autorité à Computer1 qui peut alors se connecter à mail1.nwtraders.com en utilisant l'adresse IP correcte.

9-4 Définition d'un redirecteur :

Un redirecteur est un serveur DNS que d'autres serveurs DNS internes désignent comme responsable du transfert des requêtes pour la résolution de noms de domaines externes ou hors site.

Pour utiliser des redirecteurs afin de gérer le trafic DNS entre votre réseau et Internet, configurez le pare-feu de votre réseau de manière à ce qu'un seul serveur DNS puisse communiquer avec Internet. Lorsque vous avez configuré les autres serveurs DNS de votre réseau pour qu'ils redirigent vers ce serveur DNS les requêtes qu'ils ne peuvent pas résoudre localement, ce serveur fait office de redirecteur.

En configurant un serveur DNS derrière un pare-feu pour rediriger des requêtes externes vers un unique redirecteur DNS extérieur au pare-feu, puis en n'ouvrant des ports sur le pare-feu que vers ce redirecteur, vous pouvez résoudre des noms DNS sans exposer votre réseau à des serveurs extérieurs.



En l'absence d'un serveur DNS spécialement désigné comme redirecteur, tous les serveurs DNS peuvent envoyer des requêtes hors d'un réseau à l'aide de leurs indications de racine. Cela peut aboutir à l'exposition sur Internet d'un grand nombre d'informations DNS internes parfois essentielles.

10- Enregistrement de ressources dans une zone :

Un enregistrement de ressource est une structure de base de données DNS standard qui contient des informations utilisées pour traiter les requêtes DNS.

Après avoir installé le service Serveur DNS et configuré les propriétés du service DNS, il ne vous reste plus qu'à achever le service en ajoutant des mappages de nom d'hôte à adresse IP.

Ces mappages sont appelés enregistrements de ressources dans le système DNS. Il existe différents types d'enregistrements de ressources. Les types d'enregistrements de ressources que vous créez dans le système DNS dépendent de vos besoins en matière de résolution de noms :

Dans les fichiers de zone, les possèdes la syntaxe suivante :
Proriétaire TTL Classe Type RDATA

Lors de la création d'une nouvelle zone, deux enregistrements de ressource se créent automatiquement: Il s'agit de l'enregistrement **SOA** (Start of Autority) correspondant à la zone, et l'enregistrement **NS** (Name Server) correspondant au serveur DNS local créé pour cette zone.

10-1 Enregistrements de ressources hôtes (A)

Les enregistrements de ressources hôtes (A) sont utilisés dans une zone pour associer des noms de domaine DNS d'ordinateurs (ou hôtes) à leurs adresses IP et peuvent être ajoutés à une zone de plusieurs façons :

- Vous pouvez créer manuellement un enregistrement de ressource A pour un ordinateur client TCP/IP statique à l'aide de la console DNS.
- Les clients et serveurs Windows utilisent le service Client DHCP pour enregistrer et mettre à jour dynamiquement leurs propres enregistrements de ressources A dans DNS lorsque la configuration IP est modifiée.

Tout ordinateur qui partage des ressources et qui doit être identifié par son nom de domaine DNS doit utiliser des enregistrements de ressources A pour fournir la résolution de nom DNS sur l'adresse IP.

10-2 Enregistrements de ressources Nom canonique (CNAME)

Les enregistrements de ressources CNAME sont également appelés noms canoniques. Grâce à ces enregistrements vous pouvez utiliser plusieurs noms pour pointer vers un seul hôte, ce qui vous permet d'exécuter des tâches telles que l'hébergement simultané d'un serveur FTP et d'un serveur Web sur le même ordinateur. Par exemple, les noms de serveur courants (ftp, www) sont enregistrés en utilisant les RR CNAME qui mappent vers le nom d'hôte DNS, tel que « serveur-1 », pour l'ordinateur serveur qui héberge ces services.

Il est recommandé d'utiliser les RR CNAME dans les cas suivants :

- lorsqu'un hôte est spécifié dans un RR A de la même zone doit être renommé ;
- lorsque le nom générique d'un serveur connu, tel que www, doit être résolu sur un groupe d'ordinateurs individuels (chacun avec des RR A individuels) qui fournissent le même service ; par exemple, un groupe de serveurs Web redondants.

Dans l'exemple suivant, un ordinateur appelé hote-a.exemple.microsoft.com doit fonctionner à la fois en tant que serveur Web nommé « www.exemple.microsoft.com » et en tant que serveur FTP nommé « ftp.exemple.microsoft.com ». Pour nommer cet ordinateur comme il devrait l'être, vous pouvez ajouter les entrées CNAME suivantes dans la zone exemple.microsoft.com et les utiliser par la suite :

```
host-a     IN  A      10.0.0.20
ftp        IN  CNAME  host-a
www        IN  CNAME  host-a
```

10-3 Enregistrements de ressources de serveur de messagerie (MX)

Les enregistrements de ressources de serveur de messagerie (MX) sont utilisés par les applications de messagerie pour retrouver un serveur de messagerie basé sur un nom de domaine DNS utilisé dans l'adresse de destination du destinataire d'un message électronique. Par exemple, une requête DNS qui demande le nom « exemple.microsoft.com » pourrait être utilisée pour rechercher un RR MX, permettant ainsi à une application de messagerie de transmettre ou d'échanger du courrier avec un utilisateur qui a comme adresse électronique « utilisateur@microsoft.com ».

Le RR MX affiche le nom de domaine DNS de l'ordinateur ou de l'ensemble d'ordinateurs qui traitent le courrier dans un domaine. S'il existe plusieurs RR MX, le service Client DNS essaie de contacter des serveurs de messagerie selon l'ordre de préférence ; de la valeur la moins élevée (la plus haute priorité) à la valeur la plus élevée (la priorité la plus basse). L'exemple suivant illustre la syntaxe de base d'un RR MX.

nom_domaine_messagerie **IN MX** hôte_serveurmessagerie_prioritaire

En utilisant les RR MX ci-dessous dans la zone exemple.microsoft.com, le courrier adressé à utilisateur@exemple.microsoft.com est remis d'abord à utilisateur@serveurmessagerie0.exemple.microsoft.com, si possible. Si le serveur n'est pas disponible, le programme de résolution client peut utiliser à la place utilisateur@serveurmessagerie1.exemple.microsoft.com.

```
@          IN  MX   1    mailserver0
@          IN  MX   2    mailserver1
```

Remarquez que l'utilisation du signe A commercial (@) dans les enregistrements indique que le nom de domaine DNS du distributeur est le même que le nom d'origine (exemple.microsoft.com) pour la zone.

10-4 Enregistrements de ressources Pointeur (PTR)

Les enregistrements de ressources Pointeur (PTR) sont utilisés pour gérer le processus de recherche indirecte, basé sur des zones ayant pour racine le domaine in-addr.arpa, où elles ont été créées. Ces enregistrements sont utilisés pour rechercher un ordinateur à partir de son adresse IP et résoudre ces informations à son nom de domaine DNS.

Les RR PTR peuvent être ajoutés à une zone de plusieurs façons :

- Vous pouvez créer manuellement un RR PTR pour un ordinateur client TCP/IP statique à l'aide de DNS, soit en tant que procédure indépendante, soit en tant que partie intégrante de la procédure de création d'un RR A.
- Les ordinateurs utilisent le service Client DHCP pour enregistrer et mettre à jour dynamiquement leur RR PTR dans DNS lorsque la configuration IP est modifiée.
- Le serveur DHCP peut enregistrer et mettre à jour les RR PTR de tous les autres ordinateurs clients qui ont le service DHCP activé, à condition qu'ils obtiennent leur bail IP auprès d'un serveur qualifié. Le service Serveur DHCP fourni avec Windows 2000 et Windows Server 2003 offre cette fonctionnalité.

L'enregistrement de ressource Pointeur (PTR) est utilisé uniquement dans les zones de recherche indirecte pour prendre en charge ce type de recherche

10-5 Enregistrements de ressources Emplacement du service (SRV)

Les enregistrements de ressource Emplacement du service (SRV) sont obligatoires pour rechercher des contrôleurs de domaine Active Directory. En règle générale, vous pouvez éviter l'administration manuelle des RR SRV lorsque vous installez Active Directory

9-1 Création manuelle d'enregistrements de ressources DNS :

Pour créer manuellement un enregistrement de ressource DNS :
1. Ouvrez la console DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone de recherche directe principale appropriée, puis cliquez sur
Nouvel hôte (A).

3. Dans la boîte de dialogue **Nouvel hôte**, entrez dans le champ **Nom** le nom d'ordinateur DNS du nouvel hôte.
4. Dans la boîte de dialogue **Nouvel hôte**, entrez dans le champ **Adresse IP** l'adresse IP du nouvel hôte.
5. Si vous le souhaitez, sélectionnez **Créer un pointeur d'enregistrement PTR associé** pour créer un enregistrement PTR dans une zone de recherche inversée à partir des informations que vous avez entrées dans les zones **Nom** et **Adresse IP**.
6. Dans la boîte de dialogue **Nouvel hôte**, cliquez sur **Ajouter un hôte** pour ajouter le nouvel enregistrement d'hôte à la zone.
7. Dans la boîte de message **DNS**, cliquez sur **OK**.
8. Dans la boîte de dialogue **Nouvel hôte**, cliquez sur **Terminé**.
9. Fermez la console DNS.

11- Transferts de zone DNS :

Un transfert de zone est le transfert total ou partiel des données d'une zone à partir du serveur DNS principal qui héberge la zone vers un serveur DNS secondaire qui héberge une copie de cette zone.

Lorsque des modifications sont apportées à la zone sur un serveur DNS principal, ce dernier informe les serveurs DNS secondaires que ces modifications ont eu lieu et qu'elles sont répliquées vers tous les serveurs DNS secondaires de la zone concernée par le biais de transferts de zone.

Il existe deux types de transferts de zone DNS :

9-1 Transfert de zone complet :

Il représente le type de requête standard pris en charge par tous les serveurs DNS pour mettre à jour et synchroniser les données d'une zone lorsque celle-ci a subi des modifications. Lorsqu'une requête DNS est effectuée avec le type de requête AXFR, la réponse est un transfert de l'intégralité de la zone. Une requête AXFR est une demande de transfert de zone complet.

9-2 Transfert de zone incrémentiel :

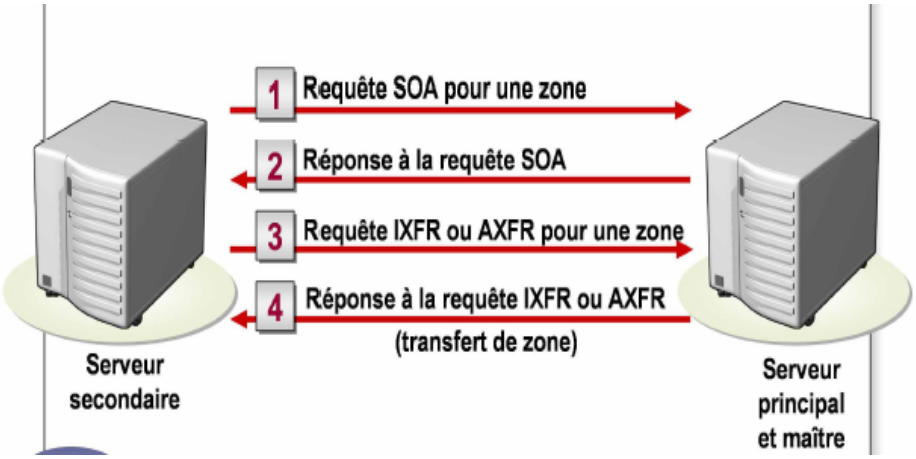
C'est un autre type de requête utilisé par certains serveurs DNS pour mettre à jour et synchroniser les données d'une zone lorsque celle-ci a subi des modifications depuis la dernière mise à jour. Lorsque deux serveurs DNS prennent en charge le transfert de zone incrémentiel, ils peuvent effectuer un suivi et transférer uniquement les modifications incrémentielles des enregistrements de ressources entre deux versions de la zone. Une requête IXFR est une demande de transfert de zone incrémentiel.

Le but d'un transfert de zone est de garantir que les deux serveurs DNS, hébergeant la même zone, détiennent les mêmes informations concernant cette zone. Sans transfert de zone, les données seraient à jour sur le serveur principal, mais pas sur le serveur secondaire. Par conséquent, le serveur DNS secondaire ne pourrait pas prendre en charge la résolution de noms pour la zone considérée.

9-3 Processus de transfert de zone :

La procédure suivante résume les étapes d'un transfert de zone, qu'il soit complet ou incrémentiel.

1. Le serveur secondaire de la zone attend un certain temps (spécifié par l'intervalle d'actualisation dans l'enregistrement de ressource SOA obtenu du serveur maître). Le serveur secondaire demande alors son SOA au serveur maître.
2. Le serveur maître de la zone répond en renvoyant l'enregistrement de ressource SOA.
3. Le serveur secondaire de la zone compare le numéro de série renvoyé à son propre numéro de série. Si le numéro de série envoyé par le serveur maître pour la zone est supérieur au numéro de série stocké sur le serveur secondaire, cela signifie que la base de données du serveur secondaire n'est pas à jour. Le serveur secondaire envoie alors une requête AXFR pour demander un transfert de zone complet. Si le serveur DNS prend en charge les transferts de zone incrémentiels (comme dans Windows Server 2003 et Windows 2000), il envoie une requête IXFR pour demander un transfert de zone incrémentiel afin de récupérer les enregistrements de ressources qui ont été modifiés depuis le transfert précédent.
4. Dans le cas d'un transfert de zone complet, le serveur maître envoie la base de données de la zone au serveur secondaire ; dans le cas d'un transfert de zone incrémentiel, le serveur maître envoie uniquement les données de la zone qui ont changé.



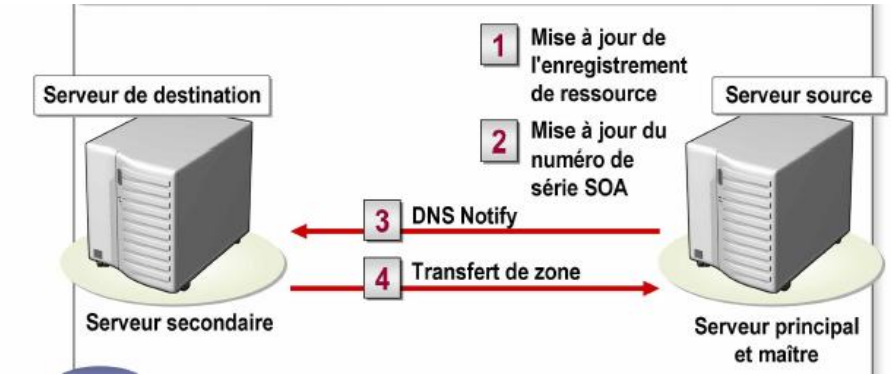
12- Notification DNS (DNS Notify) :

DNS Notify est une mise à jour de la spécification d'origine du protocole DNS qui permet d'informer les serveurs secondaires lorsqu'une zone est modifiée.

Une liste de notification répertorie les autres serveurs DNS d'une zone qui doivent être informés des modifications de cette zone. La liste de notification que le serveur maître tient à jour est constituée des adresses IP des serveurs DNS configurés comme serveurs secondaires pour la zone considérée. Lorsque les serveurs figurant dans cette liste reçoivent une notification de modification, ils initialisent un transfert de zone avec un autre serveur DNS et mettent à jour la zone.

12-1 Fonctionnement de DNS Notify :

Conformément à l'illustration, le processus DNS Notify se déroule de la manière suivante :
1. La zone locale hébergée sur un serveur DNS principal est mise à jour.
2. Dans l'enregistrement de ressource SOA, le champ **Numéro de série** est mis à jour pour indiquer qu'une nouvelle version de la zone a été écrite sur un disque.
3. Le serveur principal envoie un message de notification à tous les serveurs qui figurent dans sa liste de notification.
4. Tous les serveurs secondaires de la zone qui reçoivent le message de notification réagissent en renvoyant une requête de type SOA au serveur principal expéditeur de la notification. Cette requête lance le processus de transfert de zone DNS.



Pour configurer un transfert de zone DNS et DNS Notify :
1. Ouvrez la console DNS.
2. Développez le serveur approprié, puis développez soit **Zones de recherche directe**, soit **Zones de recherche inversée**.
3. Sélectionnez la zone DNS appropriée.
4. Dans le menu **Action**, cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés** de la zone DNS, sélectionnez l'onglet **Transferts de zone** et vérifiez que l'option **Autoriser les transferts de zone** est activée.
6. Sélectionnez la case d'option **Uniquement vers les serveurs suivants**.
7. Dans le champ **Adresse IP**, tapez l'adresse IP du serveur DNS vers lequel les données de la zone seront transférées, puis cliquez sur **Ajouter**.
8. Sous l'onglet **Transferts de zone** de la boîte de dialogue **Propriétés** de la zone DNS, cliquez sur **Notifier**.
9. Dans la boîte de dialogue **Notifier**, cliquez sur l'option **Les serveurs suivants**.

10. Dans le champ **Adresse IP**, tapez l'adresse IP du serveur DNS qui recevra la notification automatique, puis cliquez sur **OK**.
11. Dans la boîte de dialogue **Propriétés** de la zone, cliquez sur **OK**.
12. Fermez la console DNS.

13- Mise à jour dynamique :

Une mise à jour dynamique est le processus par lequel un client DNS crée, inscrit ou met à jour de façon dynamique ses enregistrements dans des zones maintenues par des serveurs DNS qui peuvent accepter et traiter des messages pour des mises à jour dynamiques.

Le processus de mise à jour manuelle des enregistrements de ressources clients est mal adapté dans le cas d'une grande organisation qui modifie en permanence les enregistrements de ressources DNS. Une organisation de grande taille avec des modifications dynamiques doit avoir recours à la méthode dynamique de mise à jour des enregistrements de ressources DNS.

L'inscription et la mise à jour dynamiques permettent à des ordinateurs clients DNS de communiquer automatiquement avec le serveur DNS pour inscrire et mettre à jour leurs propres enregistrements de ressources.

Par défaut, les clients DNS exécutant Windows 2000, Windows XP ou Windows Server 2003 tentent d'enregistrer et de mettre à jour dynamiquement leurs enregistrements de ressource dans DNS. Les clients possédant une adresse IP statique tentent de mettre à jour les enregistrements de ressource A et PTR. Les clients dont l'adresse IP a été affectée par DHCP ne tentent de mettre à jour que les enregistrements de ressource A, la mise à jour des enregistrements de ressource PTR étant effectuée par le serveur DHCP.

Pour forcer un client DNS à tenter un enregistrement dynamique, servez-vous de la commande **ipconfig/registerdns** ou redémarrez l'ordinateur.

Pour examiner le cache du client DNS, tapez la commande **ipconfig/displaydns.** Pour vider le cache client DNS tapez **ipconfig/flushdns.**

13-1 Procédure de configuration d'un serveur DNS pour les mises à jour dynamiques :

Pour configurer un serveur DNS exécutant Windows Server 2003 afin qu'il accepte les mises à jour dynamiques des enregistrements de ressources DNS :
1. Ouvrez la console DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone concernée, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Général** puis, dans la liste déroulante **Mises à jour dynamiques**, cliquez sur **Non sécurisé et sécurisé**.

4. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés** de la zone DNS, puis fermez la console **DNS**.

13-2 Configuration des clients DNS exécutant Windows XP Professionnel pour les mises à jour dynamiques

Pour configurer un client Windows XP Professionnel afin qu'il mette à jour dynamiquement ses enregistrements de ressources DNS dans le système DNS :
1. Dans le Panneau de configuration, ouvrez la boîte de dialogue **Propriétés** de la connexion réseau appropriée.
2. Dans la boîte de dialogue **Propriétés**, cliquez sur **Protocole Internet (TCP/IP)**, puis sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, cliquez sur **Avancé**.
4. Sous l'onglet **DNS** de la boîte de dialogue **Paramètres TCP/IP avancés**, activez la case à cocher **Enregistrer les adresses de cette connexion dans le système DNS**.
5. Sous l'onglet **DNS** de la boîte de dialogue **Paramètres TCP/IP avancés**, activez la case à cocher **Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS**.
6. Dans la boîte de dialogue **Paramètres TCP/IP avancés**, cliquez sur **OK**.
7. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, cliquez sur **OK**.
8. Dans la boîte de dialogue **Propriétés** de la connexion réseau, cliquez sur **OK**.

13-3 Configuration d'un serveur DHCP pour la mise à jour dynamique des enregistrements de ressources de clients DHCP

Pour configurer un serveur DHCP exécutant Windows Server 2003 afin qu'il mette à jour dynamiquement des enregistrements de ressources DNS dans le système DNS pour le compte de clients DHCP :
1. Ouvrez la console DHCP.
2. Dans la console **DHCP**, sélectionnez le serveur DHCP approprié.
3. Dans le menu **Action**, cliquez sur **Propriétés**.
4. Sous l'onglet **DNS**, vérifiez que l'option **Activer les mises à jour dynamiques DNS en utilisant les paramètres ci-dessous** est activée, puis sélectionnez l'une des deux options proposées :
• **Mettre à jour les enregistrements PTR et A DNS uniquement si des clients DHCP le demandent**
• **Toujours mettre à jour dynamiquement les enregistrements PTR et A DNS**
5. Sous l'onglet **DNS**, vérifiez que l'option **Ignorer les enregistrements PTR et A lorsque le bail est supprimé** est activée.
6. Sous l'onglet **DNS**, activez si nécessaire l'option **Mettre à jour dynamiquement les enregistrements PTR et A DNS pour des clients DHCP qui ne nécessitent aucune mise à jour**, puis cliquez sur **OK**.
7. Fermez la console DHCP.

14- Configuration d'un client DNS:

Vous avez installé le serveur DNS et configuré ses propriétés ; vous avez également créé sur le serveur les zones DNS appropriées. Vous devez à présent faire en sorte que les clients puissent s'inscrire ou créer leurs enregistrements de ressources dans DNS et utiliser le système DNS pour résoudre des requêtes.

Si vous n'avez pas de suffixe DNS configuré sur le client, la résolution et la mise à jour des noms risquent de ne pas fonctionner correctement. En configurant correctement des suffixes DNS sur le client, vous garantissez la réussite de la résolution de noms.

Pour configurer manuellement un client DNS afin qu'il utilise des serveurs DNS préférés et auxiliaires :

1. À partir de Connexions réseau, ouvrez la boîte de dialogue **Propriétés** associée à l'interface réseau sur laquelle vous souhaitez configurer DNS.
2. Sous l'onglet **Général**, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, sélectionnez la case d'option **Utiliser l'adresse de serveur DNS suivante**.
4. Dans le champ **Serveur DNS préféré**, tapez l'adresse IP du serveur DNS préféré.
5. Dans le champ **Serveur DNS auxiliaire**, tapez l'adresse IP du serveur DNS auxiliaire, puis cliquez sur **Avancé**.

6. Dans la boîte de dialogue **Paramètres TCP/IP avancés**, sélectionnez l'onglet **DNS** ; dans le champ **Suffixe DNS pour cette connexion**, tapez le suffixe DNS à attacher au nom d'hôte de l'ordinateur, puis cliquez sur **OK**.
7. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, cliquez sur **OK**.
8. Fermez toutes les fenêtres.

15- Délégation d'une zone DNS :

En termes techniques, la délégation est le processus qui affecte l'autorité sur les domaines enfants de votre espace de noms DNS à une autre entité en ajoutant des enregistrements dans la base de données DNS.

En tant que gestionnaire d'un domaine DNS, vous avez la possibilité de créer des domaines enfants et leurs zones respectives qui pourront ensuite être stockés, distribués et répliqués vers d'autres serveurs DNS. La gestion de ces zones supplémentaires peut être déléguée à d'autres

administrateurs. Pour déterminer si vous devez ou non diviser votre espace de noms DNS pour déléguer des zones, prenez en compte les facteurs suivants :

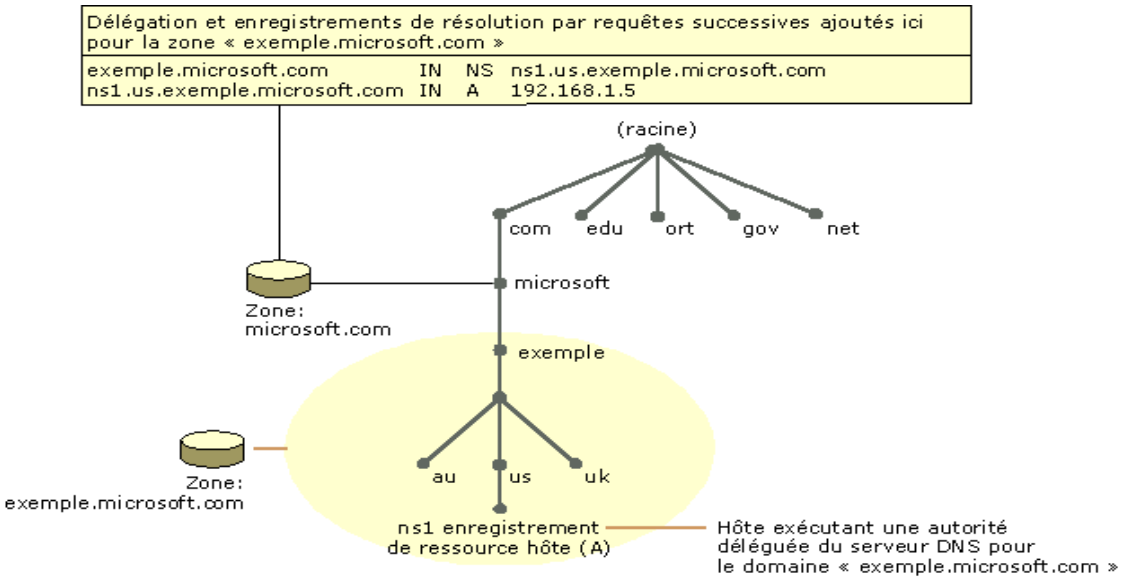
- Nécessité de déléguer la gestion d'une partie de votre espace de noms DNS à un autre emplacement ou un autre secteur de votre organisation.
- Nécessité de diviser une zone de grande taille en zones plus petites afin de répartir le trafic entre plusieurs serveurs, d'améliorer les performances de la résolution de noms DNS ou de créer un environnement DNS qui tolère mieux les pannes.
- Nécessité d'étendre l'espace de noms en ajoutant des sous-domaines (par exemple, pour prendre en charge l'ouverture d'une nouvelle filiale ou d'un nouveau site).

Pour qu'une délégation soit mise en oeuvre, la zone parente doit contenir à la fois un enregistrement de ressource A et un enregistrement de ressource NS pointant vers le serveur faisant autorité pour le domaine nouvellement délégué. Ces enregistrements sont nécessaires à la fois pour transférer l'autorité vers les nouveaux serveurs de noms et pour procurer des références aux clients effectuant des requêtes itératives. Ces enregistrements sont automatiquement créés par la console DNS lorsque vous créez une nouvelle délégation.

Pour créer une délégation de zone, créez d'abord le domaine à déléguer sur le serveur devant héberger la zone déléguée. Exécutez ensuite **l'Assistant Nouvelle délégation** sur les serveur hébergeant la zone parente en effectuant un clic droit sur le nœud de la zone parente de la console DNS et en sélectionnant **Nouvelle délégation**.

Exemple : délégation d'un sous-domaine à une nouvelle zone

Comme le montre l'illustration suivante, lorsque la nouvelle zone d'un sous-domaine (exemple.microsoft.com) est créée, une délégation de la zone parente (microsoft.com) est nécessaire.



Dans cet exemple, un ordinateur serveur DNS faisant autorité pour le nouveau sous-domaine délégué exemple.microsoft.com reçoit un nom fondé sur un sous-domaine dérivé inclus dans la nouvelle zone(ns1.us.exemple.microsoft.com).

Pour faire connaître ce serveur aux autres serveurs situés à l'extérieur de la zone récemment déléguée, deux enregistrements de ressources sont nécessaires dans la zone microsoft.com pour achever la délégation vers la nouvelle zone :

- Un enregistrement de ressource NS pour rendre la délégation effective. Cet enregistrement de ressource sert à annoncer que le serveur nommé ns1.us.exemple.microsoft.com est un serveur de référence pour le sous-domaine délégué.

- Un enregistrement de ressource A (également appelé enregistrement de résolution par requêtes successives) est nécessaire pour convertir le nom du serveur spécifié dans l'enregistrement de ressource NS en adresse IP. Le processus de résolution du nom d'hôte dans cet enregistrement de ressource vers le serveur DNS délégué dans l'enregistrement de ressource NS est parfois appelé recherche de résolution par requêtes successives.

Dans l'exemple précédent, supposons qu'un serveur DNS externe(agissant comme un client) souhaite résoudre le FQDN box.exemple.microsoft.com. Lorsque cet ordinateur envoie une requête vers un serveur de noms faisant autorité sur le domaine microsoft.com, ce serveur de noms répond par l'enregistrement « glue » (enregistrement A) informant le client que le serveur de noms faisant autorité pour le domaine exemple.micrsoft.com est ns1.us.exemple.microsoft.com et a pour adresse 192.168.1.5. L'ordinateur demandeur effectue une autre requête itérative vers le serveur de noms ns1.us.exemple.microsoft.com. Ce

dernier répond finalement à l'ordinateur demandeur avec l'adresse IP de l'hôte box.exemple.microsoft.com.

Remarque: Les délégations sont prioritaires par rapport à la redirection.

16- Gestion du vieillissement et du nettoyage :

Les serveurs DNS exécutant Windows Server 2003 prennent en charge les fonctionnalités de vieillissement et de nettoyage. Ces fonctionnalités constituent un mécanisme de nettoyage et de suppression des enregistrements de ressources périmés qui peuvent s'accumuler dans les données de zone au fil du temps.

Avec la mise à jour dynamique, les enregistrements de ressources sont automatiquement ajoutés aux zones lors du démarrage des ordinateurs sur le réseau. Cependant, ils ne sont pas toujours supprimés automatiquement lorsque les ordinateurs quittent le réseau. En effet, si un ordinateur ayant inscrit son propre enregistrement de ressource hôte (A) au démarrage est par la suite déconnecté du réseau de manière incorrecte, l'enregistrement de ressource hôte (A) n'est pas toujours supprimé. Si votre réseau est constitué d'utilisateurs et d'ordinateurs mobiles, cette situation peut se produire fréquemment.

Si vous ne prenez aucune mesure, la présence d'enregistrements de ressources périmés dans les données de zone peut entraîner des problèmes. En voici quelques exemples :

- Si de nombreux enregistrements de ressources périmés sont conservés dans les zones d'un serveur, ils peuvent occuper l'espace disque du serveur et ralentir les transferts de zones.
- Les serveurs DNS qui chargent des zones contenant des enregistrements de ressources périmés risquent d'utiliser des informations obsolètes pour répondre aux requêtes des clients, ce qui peut entraîner des problèmes de résolution de noms sur le réseau.
- L'accumulation d'enregistrements de ressources périmés sur le serveur DNS peut avoir un impact négatif sur ses performances et sa réactivité.
- Dans certains cas, la présence d'un enregistrement de ressource périmé peut empêcher l'utilisation d'un nom de domaine DNS par un autre ordinateur ou périphérique hôte.

Pour résoudre ces problèmes, le service Serveur DNS propose les fonctionnalités suivantes :

- Le datage, reposant sur la date et l'heure actuelles définies au niveau de l'ordinateur serveur, pour tout enregistrement de ressource ajouté de façon dynamique aux zones principales. D'autre part, les datages sont enregistrés dans les zones principales standard où le vieillissement et le nettoyage sont activés.

- Pour les enregistrements de ressources ajoutés manuellement, la valeur de datage zéro est utilisée pour indiquer qu'ils ne sont pas concernés par le processus de vieillissement et qu'ils peuvent être conservés dans les données de zone sans limite de durée, sauf si vous modifiez leur datage ou que vous les supprimez.

- Vieillissement des enregistrements de ressources dans les données locales, reposant sur un intervalle d'actualisation spécifié, pour toute zone choisie.

- Seules les zones principales qui sont chargées par le service Serveur DNS peuvent participer à ce processus.

- Nettoyage de tout enregistrement de ressource conservé au-delà de l'intervalle d'actualisation spécifié.

- Lorsqu'un serveur DNS effectue une opération de nettoyage, il peut déterminer que les enregistrements de ressources ont vieilli et sont désormais périmés et il les supprime des données de zone. Les serveurs peuvent être configurés de manière à effectuer automatiquement des opérations récurrentes de nettoyage. Vous avez également la possibilité de lancer une opération de nettoyage immédiate au niveau du serveur.

17- Surveillance du service DNS :

Les trois outils sont utilisés pour faire le diagnostic et la surveillance du service DNS dans Windows Server 2003 :

- Nslookup
- Journal des événements DNS
- Enregistrement de débogage DNS

17-1 Nslookup :

Nslookup permet d'effectuer des requêtes de test vers des serveurs DNS et d'obtenir des réponses détaillées depuis l'invite de commande.

Nslookup peut être exécuté dans deux modes :

- Interactif. Ce mode permet de taper des commandes dans Nslookup et d'afficher les résultats à une invite de commandes. Utilisez-le si vous avez besoin de plusieurs éléments de données.

- Non interactif. Ce mode permet d'exécuter une commande Nslookup en une seule étape, c'est-à-dire soit en l'exécutant seul à partir de la ligne de commande, soit en l'insérant dans un fichier de commandes. Il fournit comme sortie un élément de

données unique. Cette sortie peut être enregistrée dans un fichier texte afin d'être consultée ultérieurement.

17-2 Journal des événements DNS

Le journal des événements DNS est un journal système configuré pour n'enregistrer que les événements DNS.
Dans Windows Server 2003, les messages d'événements de serveur DNS sont conservés séparément dans un journal qui leur est propre (le journal du serveur DNS). Ce journal peut être consulté à l'aide de la console DNS ou de l'Observateur d'événements.
Son fichier journal contient des événements consignés par le service Serveur DNS. Par exemple, lors de l'arrêt ou du démarrage du serveur DNS, un message d'événement correspondant est inscrit dans ce journal. Les événements d'erreur du service DNS y sont également enregistrés, par exemple lorsque le serveur démarre mais que les transferts de zone échouent ou quand les informations de zone nécessaires au démarrage ne sont pas disponibles.

17-3 Enregistrement de débogage DNS

L'enregistrement de débogage DNS est un outil journal facultatif pour DNS, qui stocke les informations DNS que vous sélectionnez.
Dans la mesure où, d'une manière générale, l'enregistrement dans un journal consomme des ressources du serveur, l'enregistrement de débogage n'est pas activé par défaut. Il est configuré au niveau du serveur DNS et ses paramètres ont donc une incidence sur toutes les zones hébergées sur le serveur DNS.
L'enregistrement de débogage DNS peut utiliser les ressources de manière intense, ce qui risque de nuire aux performances générales du serveur et consomme de l'espace disque. Par conséquent, son utilisation doit constituer une mesure provisoire uniquement, appliquée uniquement lorsque des informations plus détaillées au sujet des performances du serveur sont requises.
Ce journal de débogage DNS est un fichier nommé Dns.log stocké dans le dossier WINDOWS\System32\Dns\.

18- Configuration des propriétés et transferts de zone :

Le moyen principal pour configurer les paramètres d'une zone est d'utiliser la boite de dialogue des propriétés de la zone, accessible via la console DNS. La boite de dialogue des propriétés d'une zone standard possède cinq onglets : Général, Source de noms (SOA), Serveurs de noms, WINS et Transferts de zone. Les boites de dialogue Propriétés des zones intégrées à Active Directory possèdent un sixième onglet, Sécurité, permettant de configurer les permissions d'accès de cette zone.

Pour ouvrir la boite de dialogue des propriétés d'une zone particulière, effectuez un **clic droit** sur le **nœud de la zone** à configurer dans la console DNS, puis sélectionnez **Propriétés**.

L'onglet **Interfaces** de la boite de dialogue des propriétés du serveur DNS permet de spécifier laquelle des adresses IP de l'ordinateur local doit être écoutée par le serveur DNS pour des requêtes DNS.

L'onglet **Redirecteurs** de la boite de dialogue des propriétés du serveur DNS permet de rediriger des requêtes DNS reçues par le serveur DNS local vers les serveurs DNS d'amont, nommés redirecteurs. Cet onglet permet également de désactiver la récursivité pour des requêtes sélectionnées.

L'onglet **Indications de racine** fournit un moyen simple de modifier le contenu du fichier cache.dns. Si votre serveur DNS doit résoudre des noms Internet, vous ne modifiez en principe pas ces entrées. En revanche, si les serveur DNS ne sert qu'à répondre aux requêtes d'hôtes d'un espace de noms DNS séparé et privé, vous devriez modifiez ces entrées pour qu'elles pointent vers les serveurs racine de votre réseau. Enfin, si votre serveur DNS est lui-même le serveur racine (nommé «.») de votre espace de noms privé, vous devriez supprimer le fichier cache.dns

L'onglet **Analyse** de la boite de dialogue des propriétés du serveur DNS permet de contrôler la fonctionnalité DNS fondamentale à l'aide de deux tests simples : une requête simple vers le serveur DNS local et une requête récursive vers les serveurs DNS racine.

19- Configuration des propriétés avancées du serveur DNS :

Les propriétés avancées du serveur DNS font référence aux neufs réglages pouvant être configurés sur l'onglet Avancées de la boite de dialogue des propriétés du serveur DNS.

L'option serveur **Désactiver la récursivité** pour activer ou désactiver la récursivité sur e serveur DNS.

L'option **Lier les zones secondaires** est activée par défaut. Ainsi les serveurs DNS de Windows Server 2003 n'ont pas recours au format de transfert rapide lors de transfert de zone vers des serveurs fondés sur BIND. Ce dispositif permet une compatibilité de transfert de zone avec les versions anciennes de BIND.

L'option **Activer le tri de masques** réseau est sélectionnée par défaut. En conséquence, en réponse à une réponse de requête de résolution de noms d'un ordinateur à hôtes multiples (un ordinateur qui possède plus d'une adresse IP), les serveurs DNS de Windows Server 2003 renvoient par défaut au client toute adresse IP située sur le sous-réseau du client.

L'option **Activer la fonction (répétition alternée) Round Robin** est sélectionnée par défaut. Ainsi, en réponse à une requête de résolution d'un nom hébergée sur plusieurs adresses, et lorsque la priorité de sous-réseau ne s'applique pas, les serveurs DNS de Windows server 2003 permutent de façon circulaire par défaut les enregistrements de ressource A correspondants dans la liste de réponse renvoyées aux différents clients.

Par défaut, le service Serveur DNS dans Windows Server 2003 utilise la répétition alternée (Round Robin)

DNS utilise la répétition alternée pour faire tourner l'ordre des données RR renvoyées dans une réponse de requête lorsqu'il existe plusieurs enregistrements de ressources de même type pour un nom de domaine DNS ayant fait l'objet d'une requête. Cette fonctionnalité fournit une méthode simple pour équilibrer la charge de l'utilisation des serveurs Web et d'autres ordinateurs à hôtes multiples demandés fréquemment par les clients