ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

**Office de la Formation Professionnelle et de la Promotion du Travail**

# Système DNS
# www.ofppt.info

**D**IRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

**SECTEUR NTIC**

# Sommaire

# 1. Système DNS

## 1.1. Définition

*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.

## 1.2. Fonction de DNS

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.
Comme la base de données DNS est distribuée, sa taille est illimitée et l'ajout de serveurs ne dégrade guère ses performances.

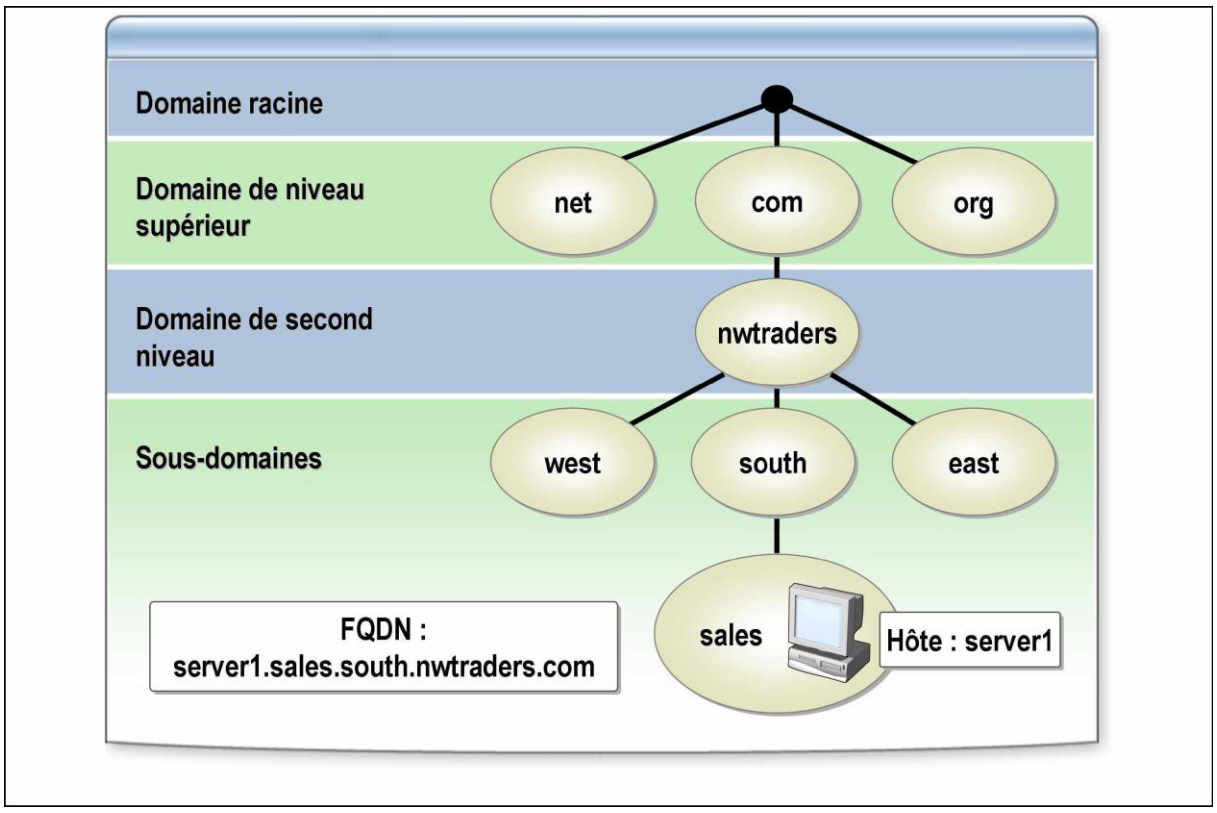
## 1.3. Historique de DNS

L'histoire du système DNS commence au tout début d'Internet qui n'était alors qu'un petit réseau créé par le Département de la Défense des États-Unis à des fins de recherche. Les noms d'hôtes des ordinateurs de ce réseau étaient gérés à l'aide d'un unique fichier Hosts qui se trouvait sur un serveur central. Les sites qui avaient besoin de résoudre des noms d'hôtes sur le réseau téléchargeaient ce fichier.
Avec la multiplication des hôtes sur Internet, le trafic généré par le

processus de mise à jour a augmenté, ainsi que la taille du fichier Hosts. Il était de plus en plus nécessaire d'instaurer un nouveau système qui se caractériserait par son évolutivité, une administration décentralisée et la prise en charge de divers types de données.
Instauré en 1984, DNS est devenu ce nouveau système.

# 2. 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).




## 2.1. Fonction d'un espace de noms de domaines

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.

## 2.2. Espace de noms de domaine

L'espace de noms de domaine est une arborescence hiérarchisée de noms utilisée par DNS pour identifier et trouver un hôte donné dans un domaine donné, par rapport à la racine de l'arborescence.
Les noms inscrits dans la base de données DNS constituent une arborescence logique appelée espace de noms de domaine. Le nom de domaine identifie la position d'un domaine par rapport à son domaine parent dans l'arborescence.
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.

## 2.3. Domaine

Dans le système DNS, on appelle domaine toute arborescence ou sousarborescence 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.

## 2.4. Domaine 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.

## 2.5. Domaine de niveau supérieur

Il s'agit de la portion finale (à l'extrême droite) d'un nom de domaine. En général, un domaine 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.

### 2.6. Domaine 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.

### 2.7. Sous-domaine

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 sousdomaines:

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

### 2.8. Nom de domaine pleinement qualifié

Un nom de domaine pleinement qualifié (FQDN, fully qualified domain name) est un nom de domaine DNS qui a été défini de façon non ambiguë pour indiquer avec certitude son emplacement dans l'arborescence de l'espace de noms de domaine.

# 3. Conventions d'appellation standard DNS

Les conventions d'appellation standard DNS sont conçues pour assurer la cohérence entre toutes les implémentations de DNS. La manière dont les clients DNS inscrivent et mettent à jour leurs propres conventions constituent des règles globales dont l'implémentation peut entrer en interaction avec d'autres implémentations DNS, quel que soit leur auteur. Grâce aux conventions d'appellation standard DNS, les organisations qui

implémentent un espace de noms DNS peuvent aussi utiliser ce dernier sur Internet.
Les conventions d'appellation standard DNS autorisent un sous-ensemble limité du jeu de caractères ASCII. La RFC (Request for Comments) 1123 spécifie les caractères valides dans les noms DNS :
A-Z
a-z
0-9
Trait d'union (-)
Tous les caractères non valides sont remplacés par des traits d'union. Par exemple, si vous utilisez le trait de soulignement dans un nom d'ordinateur, il est remplacé par un trait d'union.

# 4. Installation du service Serveur DNS

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**.

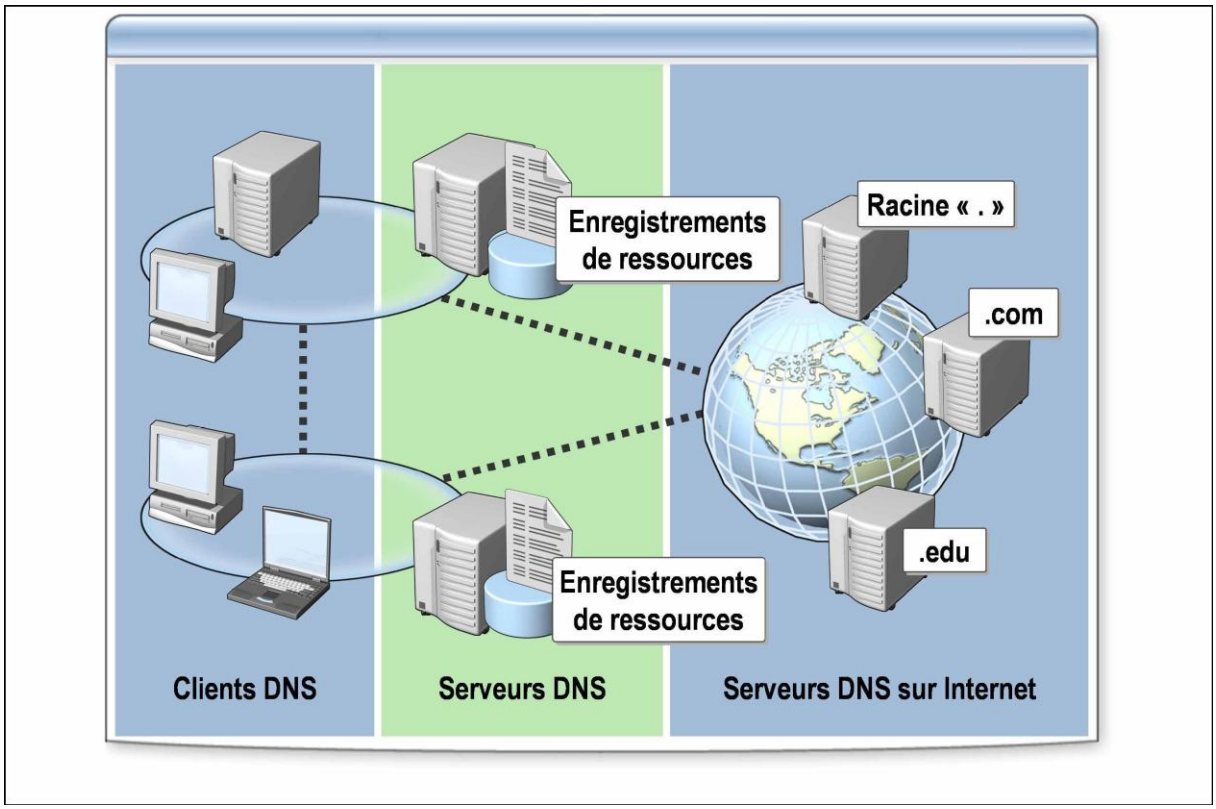
Vous aurez l'occasion de configurer le service DNS dans une application pratique ultérieure.

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

# 5. Configuration des propriétés du service Serveur DNS

## *5.1. Composants d'une solution DNS*

Les composants d'une solution DNS sont les clients DNS, les serveurs DNS et les enregistrements de ressources DNS. Les enregistrements de ressources se trouvent dans la base de données du serveur DNS. Si votre solution DNS est connectée à Internet, les serveurs DNS situés sur Internet peuvent être utilisés




## *5.2. Qu'est-ce qu'une requête DNS*

Une *requête* est une demande de résolution de noms envoyée à un serveur DNS. Il existe deux types de requêtes : requêtes récursives et requêtes itératives.

### 5.2.1. Requête récursive

Une requête récursive est une requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur de fournir une réponse complète. 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.

### 5.2.2. Fonctionnement d'une requête récursive

Le fonctionnement d'une requête récursive envoyée par un client à son serveur DNS configuré comprend les étapes suivantes :

1. Le client envoie une requête récursive au serveur DNS local.
2. Le serveur DNS local essaie de trouver une réponse dans la zone de recherche directe et dans le cache.
3. S'il trouve la réponse à la requête, le serveur DNS la renvoie au client.
4. S'il *ne* trouve *pas* de réponse, le serveur DNS utilise l'adresse d'un redirecteur ou des indications de racine pour chercher plus haut dans l'arborescence.

### 5.2.3. Requêtes itératives

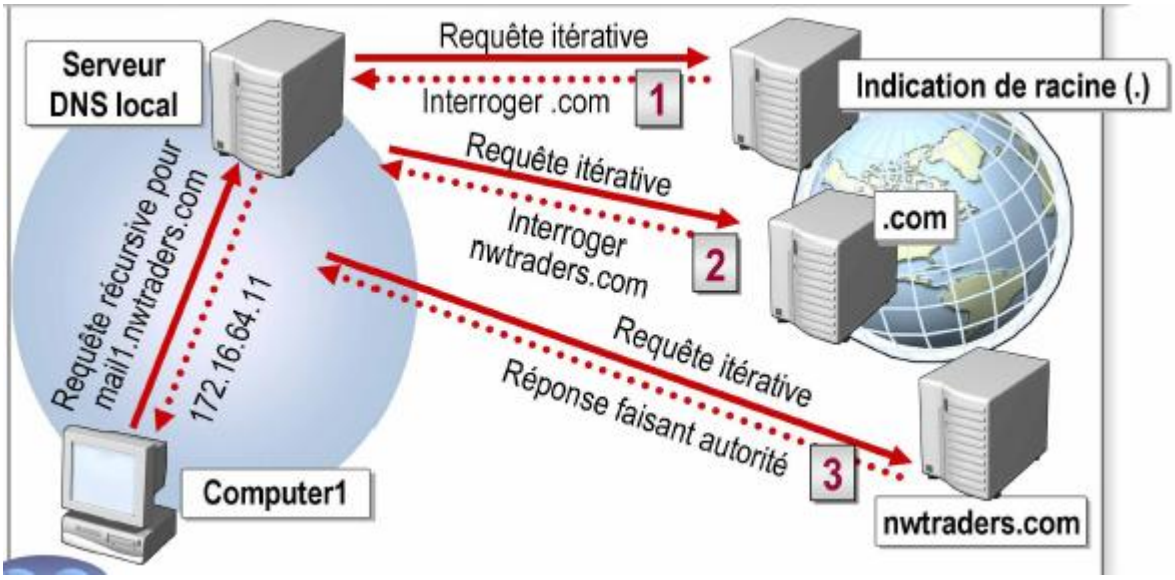
Une requête *itérative* est une requête envoyée à un serveur DNS dans laquelle le client DNS demande la meilleure réponse que peut fournir le serveur DNS sans faire appel à d'autres serveurs DNS. Les requêtes itératives sont parfois appelées requêtes non récursives. Le résultat d'une requête itérative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

Une requête itérative vise à ce que le serveur DNS, désormais en mesure d'utiliser la requête récursive du client, soit chargé de trouver une réponse à la question de ce dernier. Le serveur DNS interroge alors sa propre base de données ou s'adresse à d'autres serveurs DNS, situés à différents niveaux de l'espace de noms de domaines, afin de trouver le serveur DNS qui fait autorité pour la requête d'origine.
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.

### 5.2.4. 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 pour obtenir un nom faisant autorité du serveur de noms faisant autorité. 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 faisant autorité à Computer1 qui peut alors se connecter à mail1.nwtraders.com en utilisant l'adresse IP correcte.

## 5.3. Les indications de racine

Les *indications de racine* sont des enregistrements de ressources DNS stockés sur un serveur DNS qui répertorient les adresses IP des serveurs racines du système DNS.

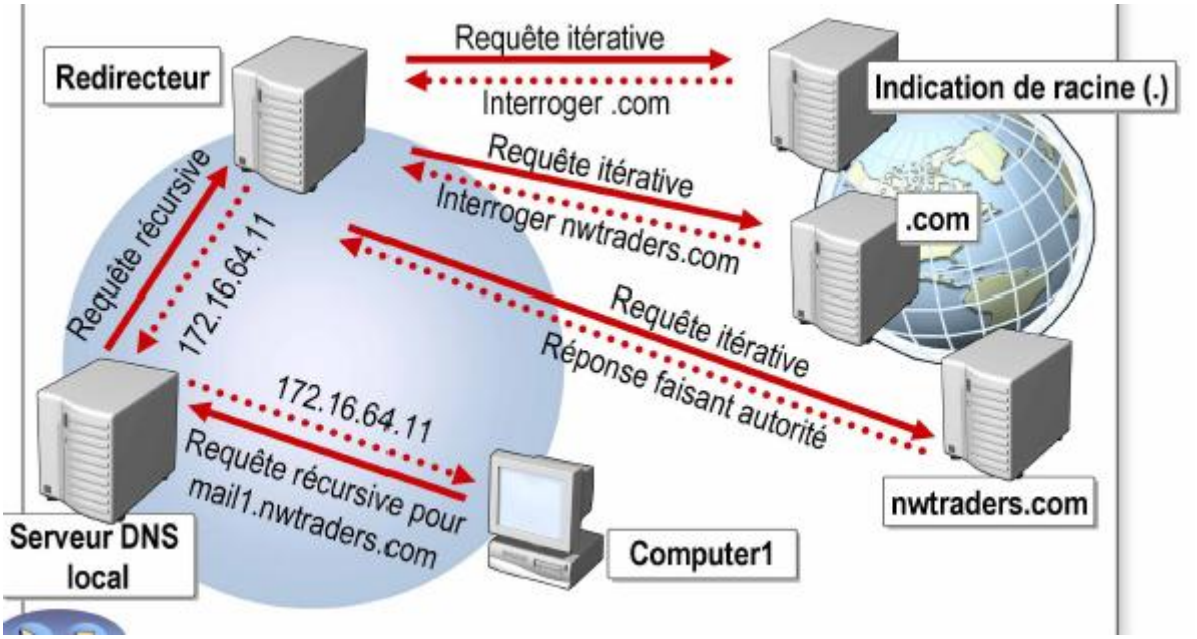
## 5.4. Fonction d'une indication de racine

Lorsque le serveur DNS reçoit une requête DNS, il consulte sa mémoire cache. Il essaie ensuite de trouver le serveur DNS qui fait autorité pour le domaine demandé. S'il n'a pas l'adresse IP du serveur DNS faisant autorité pour ce domaine et qu'il est configuré avec les adresses IP des indications de racine, le serveur DNS interroge un serveur racine sur le domaine situé à gauche du domaine racine de la requête.
Le serveur racine DNS renvoie alors l'adresse IP du domaine à gauche du domaine racine et le serveur DNS continue de parcourir le nom de domaine pleinement qualifié jusqu'à ce qu'il trouve le domaine qui fait autorité.
Les indications de racine sont stockées dans le fichier Cache.dns qui se trouve dans le dossier %Systemroot%\System32\Dns.

## 5.5. Les redirecteurs

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.
Lorsqu'un serveur de noms DNS reçoit une requête, il tente de trouver l'information demandée dans ses propres fichiers de zone. Si cette méthode échoue (parce que le serveur ne fait pas autorité pour le domaine demandé ou parce qu'il n'a pas mis l'enregistrement en mémoire cache lors d'une recherche précédente), le serveur doit communiquer avec d'autres serveurs de noms pour résoudre la requête. Dans un réseau mondial comme Internet, les requêtes
DNS hors d'une zone locale exigent parfois une interaction avec des serveurs de noms DNS via des liaisons de réseau étendu (WAN), à l'extérieur de l'organisation. La création de redirecteurs DNS permet de désigner des serveurs de noms particuliers pour le trafic DNS qui

emprunte des liaisons WAN.
Vous pouvez sélectionner comme redirecteurs des serveurs de noms DNS spécifiques qui résoudront des requêtes DNS pour le compte d'autres serveurs DNS.




Dans l'illustration, le serveur DNS local n'a pas réussi à résoudre le nom demandé en utilisant sa mémoire cache et ses fichiers de zone. Il transmet donc la demande au redirecteur. Le redirecteur commence alors à interroger d'autres serveurs de noms à l'aide de requêtes itératives. Les redirecteurs DNS procèdent 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.

2. Le serveur DNS local transmet la demande au redirecteur.
3. Le redirecteur envoie une requête itérative au serveur racine pour obtenir une réponse d'un serveur de noms faisant autorité.

4. 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.

5. Le redirecteur envoie ensuite une requête itérative au serveur DNS plus proche du nom de domaine demandé.

Par exemple : Le redirecteur envoie une requête itérative au serveur DNS de .com.

6. Le processus continue jusqu'à ce que le redirecteur reçoive une réponse faisant autorité.

Par exemple : Le serveur DNS de .com répond par une référence au serveur DNS de nwtraders.com. Ensuite, le redirecteur envoie une requête itérative au serveur DNS de nwtraders.com pour obtenir un serveur de noms faisant autorité. Le redirecteur reçoit alors une réponse faisant autorité du serveur DNS de nwtraders.com.

7. Le redirecteur envoie la réponse au serveur DNS local qui la transmet au client DNS.

Par exemple : Le redirecteur envoie la réponse au serveur DNS local qui la transmet à Computer1.

## *5.6. La mise en cache du serveur DNS*

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.

### *5.7. Fonctionnement du cache des serveurs DNS*

Pendant qu'il traite une requête récursive, un serveur peut être amené à envoyer plusieurs requêtes pour obtenir la réponse définitive. Dans un scénario du pire cas, le serveur de noms local commence en haut de l'arborescence DNS par l'un des serveurs de noms racines, puis descend progressivement dans l'arborescence jusqu'à ce qu'il obtienne les données demandées.
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. 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. À partir du moment où les données sont placées en mémoire cache, les modifications affectant les enregistrements de ressources risquent de ne pas être disponibles immédiatement sur Internet tout entier.
Une fois que les données sont placées en mémoire cache, leur durée de vie commence à décrémenter, de sorte que le serveur DNS sait quand il doit les supprimer du cache. Quand le serveur DNS répond à une requête grâce à sa mémoire cache, il fournit également la durée de vie restante des données. Le programme de résolution met ensuite les données dans son propre cache et utilise la durée de vie communiquée par le serveur

# 6. Configuration des zones DNS

### *6.1. Enregistrements de ressources*

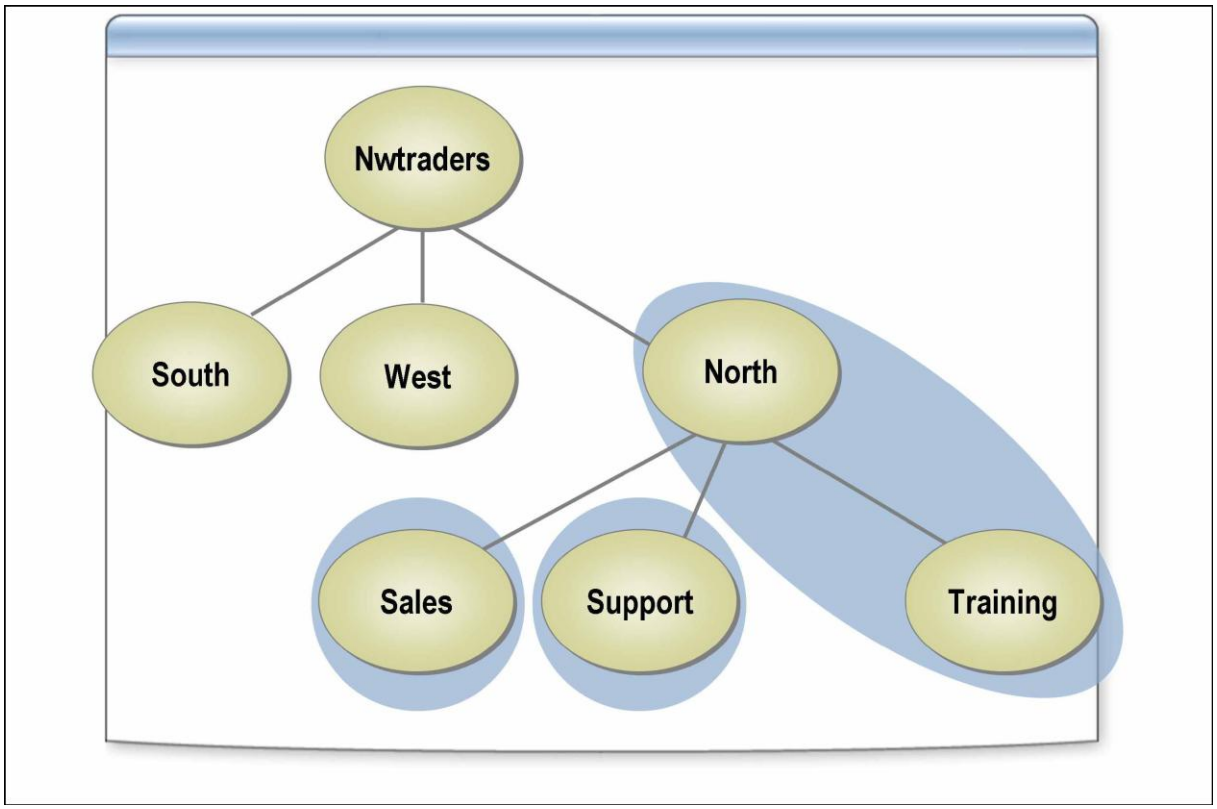
Un *enregistrement de ressource* est une structure de base de données

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.

| Type d'enregistrement | Description |
|---|---|
| A | Résout un nom d'hôte en adresse IP |
| PTR | Résout une adresse IP en nom d'hôte |
| SOA | Premier enregistrement dans tout fichier de zone |
| SRV | Résout les noms des serveurs qui fournissent des services |
| NS | Identifie le serveur DNS associé à chaque zone |
| MX | Serveur de messagerie |
| CNAME | Résout un nom d'hôte en nom d'hôte |

## 6.2. Zones DNS

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***. Lorsque vous créez une zone, vous créez un fichier de zone pour stocker les propriétés et les enregistrements de ressources de la zone. 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 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.




Une zone est également la représentation physique d'un ou plusieurs domaines DNS. Par exemple, si vous avez un espace de noms de domaines DNS south.nwtraders.com, vous pouvez créer sur un serveur DNS une zone south.nwtraders.com qui contient tous les enregistrements de ressources situés dans le domaine Training.
Le système DNS permet de diviser un espace de noms DNS en zones. Pour chaque nom de domaine DNS inclus dans une zone, la zone devient la source qui fait autorité pour les informations concernant ce domaine.
Les fichiers de zone sont gérés sur des serveurs DNS. Vous pouvez configurer un serveur DNS unique pour héberger zéro, une ou plusieurs zones. 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.
Les caractéristiques d'une zone sont les suivantes :

- 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.

Une zone DNS est :

- soit une zone principale, secondaire ou de stub.
- soit une zone de recherche directe ou inversée.

## 6.3. Sécurisation d'une zone DNS

Pour plus de sécurité, vous pouvez contrôler les personnes autorisées à administrer les zones DNS en modifiant la liste de contrôle d'accès discrétionnaire (DACL, *discretionary access control list*) sur les zones DNS qui sont stockées dans Active Directory. La liste DACL permet de contrôler les autorisations accordées aux utilisateurs et aux groupes Active Directory qui peuvent contrôler les zones DNS

## 6.4. 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.

Il existe de nombreuses options pour obtenir une configuration optimale du serveur DNS en fonction des décisions que vous prenez concernant notamment la topologie du réseau et la taille de l'espace de noms. Le fonctionnement normal des serveurs DNS fait intervenir trois zones :

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

### 6.4.1. Zone principale

Une zone principale est l'exemplaire faisant autorité de la zone DNS. Les enregistrements de ressources y sont créés et gérés.

Lorsque vous configurez des serveurs DNS pour héberger les zones d'un domaine, le serveur principal est normalement situé à un emplacement où il est accessible pour administrer le fichier de zone.

### 6.4.2. Zone secondaire

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.

### 6.4.3. Zone de stub

Les zones de stub sont des copies d'une zone qui contiennent uniquement les enregistrements de ressources nécessaires à l'identification du serveur DNS faisant autorité pour la zone en question. Une zone de stub contient un sousensemble des données de la zone qui se compose d'un enregistrement SOA, NS et A, également appelé enregistrement de résolution par requêtes successives.
Une zone de stub est en quelque sorte un signet qui pointe simplement vers le serveur DNS qui fait autorité pour la zone DNS concernée.
Vous pouvez utiliser des zones de stub lorsque les indications de racine pointent vers un serveur DNS interne et non vers les serveurs racines situés sur Internet.
À des fins de sécurité, le serveur DNS est conçu pour résoudre certaines zones seulement.

*Les serveurs dédiés à la mise en cache n'ont pas de zone.*

Pour modifier un type de zone DNS :

1. Ouvrez la console DNS.
2. Dans la console **DNS**, sélectionnez la zone à modifier.
3. Dans le menu **Action**, cliquez sur **Propriétés**.
4. Sous l'onglet **Général**, cliquez sur **Modifier**.
5. Dans la boîte de dialogue **Modification du type de zone**, sélectionnez l'une des options suivantes, puis cliquez sur **OK**.

• **Zone principale** si cette zone doit contenir une copie de la zone

acceptant les mises à jour directes.
• **Zone secondaire** si cette zone doit contenir une copie d'une zone existante.
• **Zone de stub** si cette zone doit contenir une copie d'une zone contenant uniquement des enregistrements NS (serveur de noms), des enregistrements SOA (source de noms) et éventuellement des enregistrements de résolution par requêtes successives.
6. Dans la boîte de dialogue **Propriétés** de la zone, cliquez sur **OK**.

### 6.4.4. Zones de recherche directe et inversée

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.

**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).

**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).

Pour configurer une zone de recherche directe sur une zone principale :

1. Ouvrez la console DNS.
2. Dans la console DNS, cliquez avec le bouton droit sur le serveur DNS, puis cliquez sur **Nouvelle zone**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la page **Type de zone**, vérifiez que l'option **Zone principale** est

sélectionnée, puis cliquez sur **Suivant**.
5. Dans la page **Zone de recherche directe ou inversée**, vérifiez que l'option
**Zone de recherche directe** est sélectionnée, puis cliquez sur **Suivant**.
6. Dans la page **Nom de la zone**, entrez le nom DNS de la zone pour laquelle le serveur DNS considéré fera autorité, puis cliquez sur **Suivant**.
7. Dans la page **Fichier zone**, cliquez sur **Suivant** pour accepter les valeurs par défaut.
8. Dans la page **Mise à niveau dynamique**, sélectionnez l'une des options suivantes, puis cliquez sur **Suivant**.
a. **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.
b. **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées**. Cette option n'est pas recommandée car elle accepte les mises à jour provenant de sources non approuvées.
c. **Ne pas autoriser les mises à jour dynamiques**. Cette option vous oblige à mettre à jour les enregistrements manuellement.
9. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
10. Fermez la console DNS.

Pour configurer une zone de recherche inversée sur une zone principale :

1. Ouvrez la console DNS.
2. Dans la console DNS, cliquez avec le bouton droit sur le serveur DNS, puis cliquez sur **Nouvelle zone**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la page **Type de zone**, vérifiez que l'option **Zone principale** est sélectionnée, puis cliquez sur **Suivant**.
5. Dans la page **Zone de recherche directe ou inversée**, sélectionnez l'option
**Zone de recherche inversée**, puis cliquez sur **Suivant**.
6. Dans la page **Nom de la zone de recherche inversée**, dans le champ **ID réseau**, tapez la partie de l'adresse IP de la zone qui représente l'ID réseau, puis cliquez sur **Suivant**.
7. Dans la page **Fichier zone**, cliquez sur **Suivant** pour accepter les valeurs par défaut.

8. Dans la page **Mise à niveau dynamique**, sélectionnez l'une des options suivantes, puis cliquez sur **Suivant**.

a. **N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)**

b. **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées**

c. **Ne pas autoriser les mises à jour dynamiques**

9. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.

10. Fermez la console DNS.

## *6.5. 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 :

***Transfert de zone complet*** est 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.

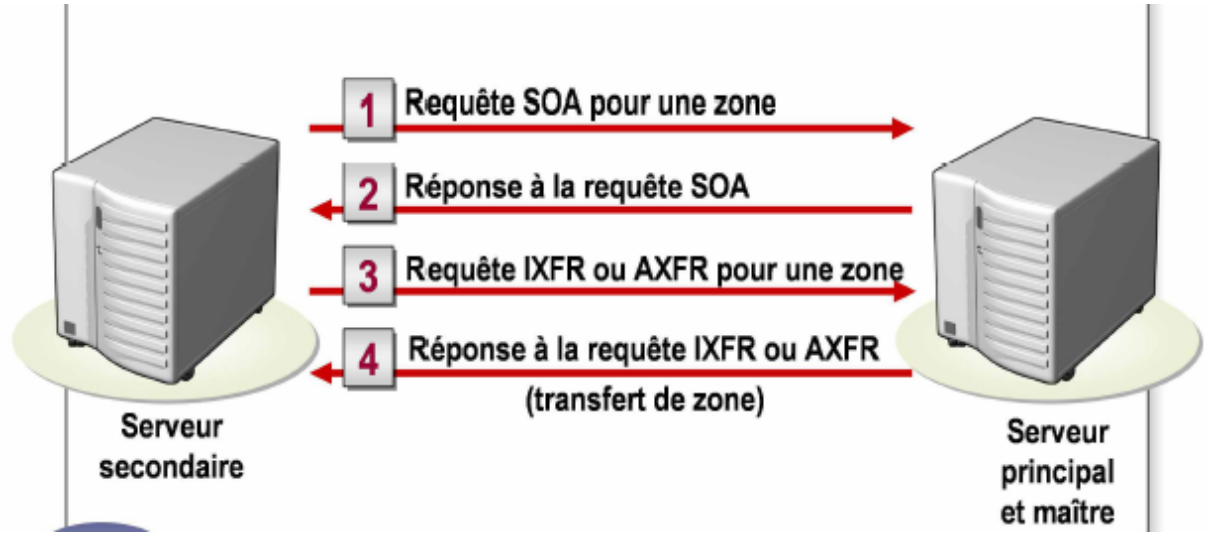
**Transfert de zone incrémentiel** est un autre type de requête utilisé par certains serveurs DNS pour mettre à jour et synchroniser les données d'une zone lorsque celle-ci a subi des modifications depuis la dernière mise à jour. Lorsque deux serveurs DNS prennent en charge le transfert de zone incrémentiel, 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.

### 6.5.1. 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 maître 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.




## 6.6. 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.

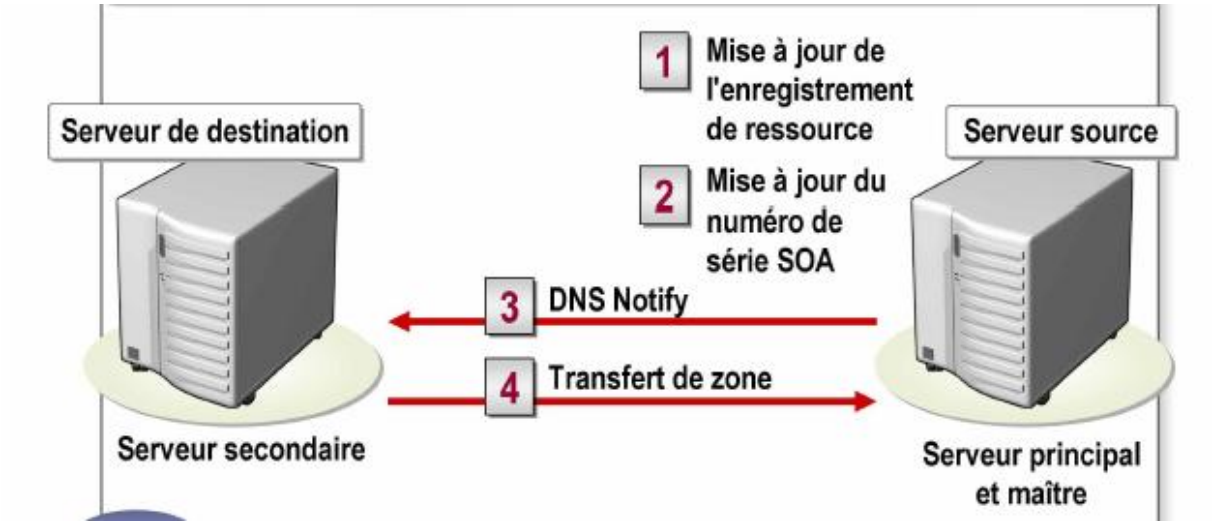
Une *liste de notification* répertorie les autres serveurs DNS d'une zone qui doivent être informés des modifications de cette zone. La liste de notification que le serveur maître tient à jour est constituée des adresses IP des serveurs DNS configurés comme serveurs secondaires pour la zone considérée. 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.

### 6.6.1. 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.



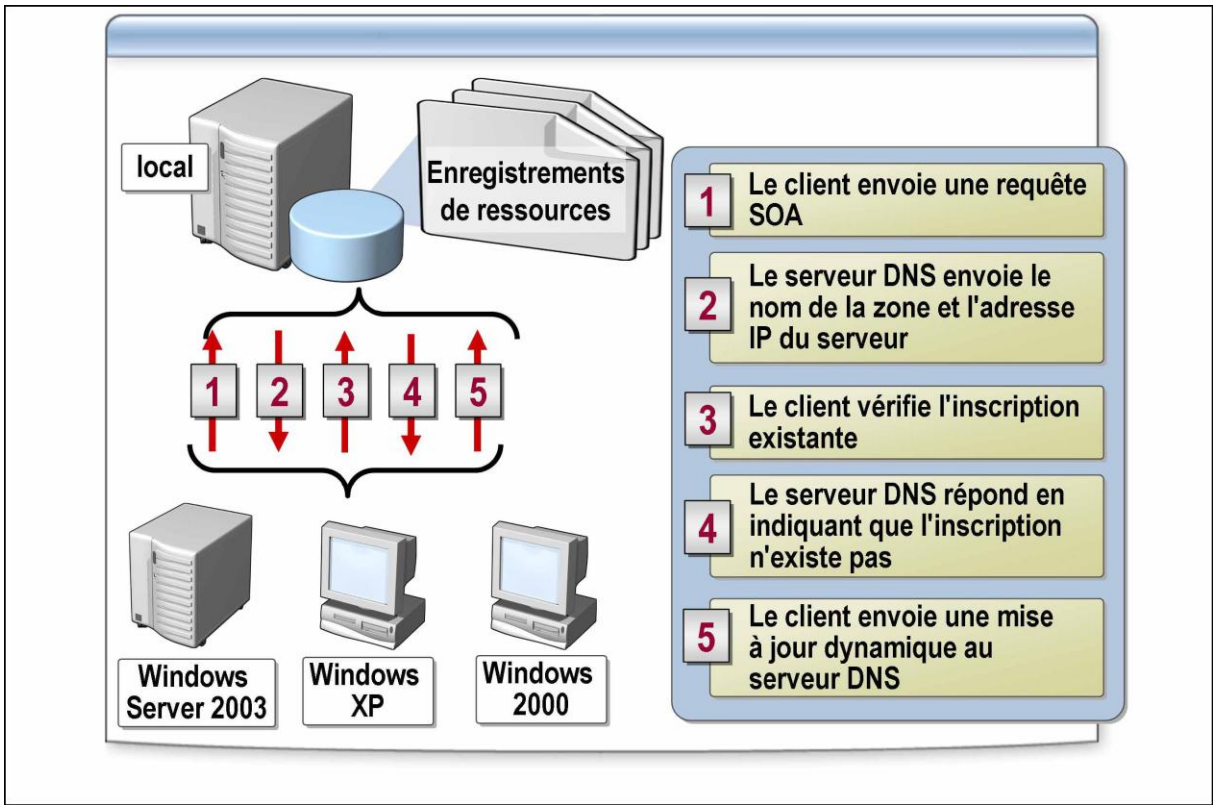

Pour configurer un transfert de zone DNS et DNS Notify :
1. Ouvrez la console DNS.
2. Développez le serveur approprié, puis développez soit **Zones de recherche directe**, soit **Zones de recherche inversée**.
3. Sélectionnez la zone DNS appropriée.
4. Dans le menu **Action**, cliquez sur **Propriétés**.
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.

## *6.7. 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 ettre à jour leurs propres enregistrements de ressources. Dans une implémentation de DNS qui utilise un serveur DNS exécutant Microsoft Windows NT® 4.0 et les versions antérieures de BIND (Berkeley Internet Name Domain), l'administrateur doit modifier manuellement le fichier de zone approprié si les informations de référence d'un enregistrement de ressource doivent être modifiées. À mesure que le nombre d'enregistrements DNS augmente dans une zone, au point qu'il devient impossible de les gérer manuellement, le passage à la mise à jour dynamique devient indispensable.

### 6.7.1. Comment les clients DNS inscrivent et mettent à jour de manière dynamique leurs enregistrements de ressources

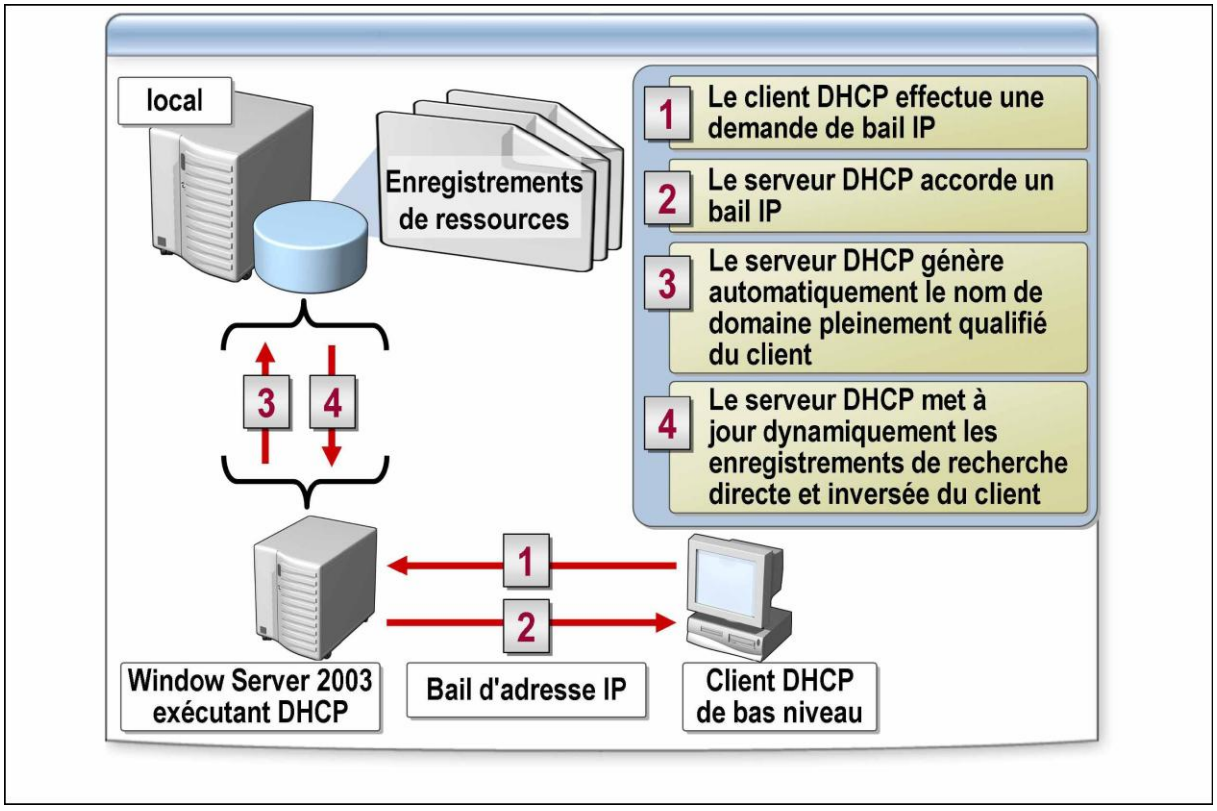



Les clients DNS exécutant Windows Server 2003, Windows 2000 et Windows XP sont configurés par défaut pour inscrire et mettre à jour dynamiquement leurs noms d'hôtes et leurs adresses IP dans DNS.
Qu'un client DNS se voit affecter son adresse IP par DHCP ou de façon statique, il peut inscrire et mettre à jour dynamiquement son nom d'hôte et son adresse IP dans DNS.
Le composant qui inscrit l'enregistrement de ressource DNS pour un client DNS est le service Client DHCP. Même sur les clients qui sont configurés avec des données pour une adresse IP statique, le service Client DHCP doit être exécuté pour que le client statique inscrive ses enregistrements de ressources dans DNS.
La procédure ci-dessous résume les étapes à suivre pour mettre à jour dynamiquement des clients DNS :
1. Le client DNS envoie une requête SOA au serveur DNS qui fait autorité pour l'enregistrement de ressource avec lequel le client DNS souhaite s'inscrire.
2. Le serveur DNS renvoie le nom de zone et l'adresse IP du serveur DNS faisant autorité pour la zone que le client DNS souhaite inscrire sur le serveur DNS.
3. Le client DNS envoie ensuite au serveur DNS faisant autorité pour la zone une mise à jour d'assertion qui vérifie l'absence d'inscription

antérieure dans la zone.
4. Le serveur DNS répond au client DNS.
5. Si aucune inscription n'existe dans la zone DNS, le client DNS envoie un package de mise à jour dynamique pour inscrire l'enregistrement de ressource.

Si le client DNS ne met pas à jour son enregistrement de ressource dans la base de données DNS comme indiqué dans la procédure précédente, il continue d'essayer de mettre à jour son enregistrement de ressource dans DNS.
1. Le client DNS essaie d'inscrire l'enregistrement auprès d'autres serveurs principaux de la zone. Seule une zone intégrée à Active Directory peut avoir plusieurs serveurs principaux.
2. Si toutes les tentatives échouent, le client essaie à nouveau d'inscrire l'enregistrement au bout de cinq minutes, puis au bout de dix minutes.
3. Ces échecs aboutissent à un modèle répétitif de tentatives 50 minutes après la dernière tentative.

### 6.7.2. Comment un serveur DHCP inscrit et met à jour de manière dynamique les enregistrements de ressources



### Fonction de la mise à jour dynamique DNS à l'aide d'un serveur DHCP

Dans la mesure où les clients de bas niveau ne peuvent pas inscrire ni mettre à jour leurs propres enregistrements de ressources, Microsoft a conçu leur implémentation du serveur DHCP de manière à ce qu'il puisse inscrire les enregistrements de ressources de clients DNS dans le système DNS pour le compte des clients DHCP.

Sur un serveur DHCP exécutant Windows Server 2003 ou Windows 2000, vous pouvez configurer le serveur DHCP pour qu'il mette à jour dynamiquement les enregistrements de ressources dans DNS pour le compte des clients DHCP du réseau. Les enregistrements de ressources des clients qui exécutent Windows NT 4.0 ou une version antérieure peuvent être entrés dans la base de données DNS si DHCP est configuré pour les mettre à jour dynamiquement pour le compte de ces clients.

Les administrateurs peuvent configurer les serveurs DHCP qui exécutent Windows Server 2003 ou Windows 2000 pour qu'ils mettent à jour les enregistrements de ressources des clients DNS des types suivants :

- Tout client DHCP de bas niveau qui ne demande pas de mises à jour dynamiques.
- Tout client DHCP, y compris ceux qui exécutent Windows XP et Windows 2000, qu'il demande ou non une mise à jour dynamique.

### Processus de mise à jour dynamique pour un client de bas niveau

Dans l'illustration, le serveur DHCP qui exécute Windows Server 2003 effectue des mises à jour dynamiques pour un client de bas niveau :

1. Le client DHCP effectue une demande de bail IP.
2. Le serveur DHCP accorde un bail IP.
3. Le serveur DHCP génère automatiquement le nom de domaine pleinement qualifié (FQDN) du client en ajoutant au nom du client le nom de domaine défini pour l'étendue DHCP. Le nom du client est fourni dans le message DHCPREQUEST envoyé par le client.
4. En utilisant le protocole de mise à jour dynamique, le serveur DHCP met à jour:

a. le nom DNS du client pour la recherche directe (A) ;
b. le nom DNS du client pour la recherche inversée (PTR).

La possibilité d'inscrire les deux types d'enregistrements A et PTR permet à un serveur DHCP exécutant Windows Server 2003 de jouer le rôle de proxy pour les clients de bas niveau dans le cadre de l'inscription DNS.

### Processus de mise à jour dynamique pour un client Windows XP

Les étapes ci-dessous décrivent le processus de mise à jour dynamique

DNS effectué par un serveur DHCP exécutant Windows Server 2003 en configuration par défaut pour le compte d'un client Windows XP :
1. Le client DHCP effectue une demande de bail IP qui contient son nom de domaine pleinement qualifié (FQDN) dans l'option 81 de la demande DHCP.
2. Le serveur DHCP accorde un bail IP.
3. Le client se connecte au serveur DNS pour mettre à jour son enregistrementA.
4. Le serveur DHCP met à jour le nom DNS inversé (PTR) du client en utilisant le protocole de mise à jour dynamique.

### 6.7.3. 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**.

### 6.7.4. 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 l'interface 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**.

### 6.7.5. 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.

### 6.7.6. 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.

## *6.8. Zone DNS intégrée à Active Directory*

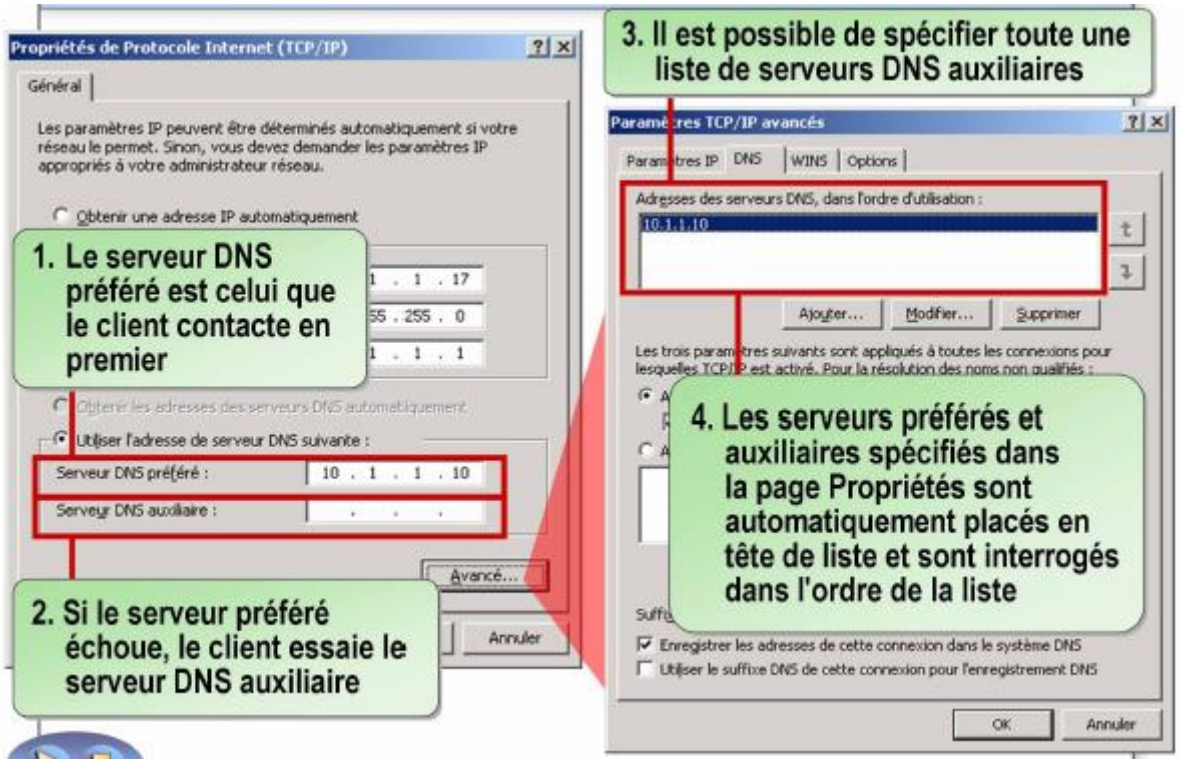
Une *zone DNS intégrée à Active Directory* est une zone DNS stockée dans Active Directory.
Lorsque vous configurez un contrôleur de domaine, Active Directory exige l'installation de DNS. Les zones qui sont créées sur un serveur DNS configuré comme contrôleur de domaine Active Directory peuvent être des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

# 7. 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.

## *7.1. Serveurs DNS préférés et auxiliaires*




Un *serveur DNS préféré* est un serveur qui reçoit les requêtes DNS envoyées par le client DNS. C'est également le serveur sur lequel le client DNS met à jour ses enregistrements de ressources.

Un *serveur DNS auxiliaire* est un serveur qui est utilisé lorsque le serveur DNS préféré est inaccessible ou ne peut pas résoudre les requêtes DNS en provenance d'un client DNS particulier parce que le service DNS est en panne.

Le serveur auxiliaire n'est pas interrogé dans le cas d'une réponse négative à la requête de résolution de noms.

S'il n'a pas de serveur DNS préféré, le client DNS ne peut pas interroger un serveur DNS.

Sans serveur DNS auxiliaire, aucune requête DNS n'est résolue si le serveur

DNS préféré est hors service. Vous pouvez avoir plusieurs serveurs DNS auxiliaires.
La procédure ci-dessous décrit les étapes à suivre pour contacter les serveurs
DNS préférés et auxiliaires.
1. Le serveur DNS préféré répond à une requête ou une mise à jour DNS.
2. Si le serveur DNS préféré ne répond pas à une requête ou une mise à jour
DNS, celle-ci est redirigée vers le serveur DNS auxiliaire.
3. Si le serveur DNS auxiliaire ne répond pas et que le client DNS est configuré avec les adresses IP d'autres serveurs DNS, le client DNS envoie la requête ou la mise à jour au serveur DNS suivant de la liste.
4. Si l'un quelconque des serveurs DNS (serveur préféré, serveur auxiliaire ou tout autre serveur de la liste) ne répond pas, il est supprimé temporairement de la liste.
5. Si aucun des serveurs DNS ne répond, la requête (ou mise à jour) du client DNS échoue.

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.
L'option de sélection de suffixe indique que la résolution de noms non qualifiés sur l'ordinateur considéré est limitée aux suffixes du domaine principal et du domaine de second niveau.

Par exemple : Si votre suffixe DNS principal est nwtraders.msft et que vous essayez de contacter Server1, l'ordinateur recherche Server1.nwtraders.msft et tous les suffixes qui sont configurés comme suffixes spécifiques à la connexion.

L'option Ajouter des suffixes parents indique que la résolution de noms non qualifiés sur l'ordinateur considéré est limitée aux suffixes du domaine principal et au suffixe spécifique à la connexion.
Par exemple : Si votre suffixe DNS principal est sales.south.nwtraders.msft et que vous essayez de contacter Server1, l'ordinateur interroge server1.south.nwtraders.msft. Si la requête n'est pas résolue, l'ordinateur interroge ensuite server1.nwtraders.msft.

Le suffixe spécifique à la connexion fournit un espace pour configurer un suffixe DNS propre à une connexion spécifique. Si un serveur DHCP configure cette connexion et que vous ne spécifiez pas de suffixe DNS, le serveur DHCP affecte un suffixe DNS s'il est configuré pour le faire.

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.

# 8. 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 déléguer un sous-domaine à une zone DNS :
1. Ouvrez la console DNS.
2. Développez le serveur DNS approprié, développez **Zones de recherche directe** ou **Zones de recherche inversée**, puis sélectionnez la zone à déléguer.
3. Dans le menu **Action**, cliquez sur **Nouvelle délégation**.
4. Dans la page **Bienvenue**, cliquez sur **Suivant**.
5. Dans la page **Nom du domaine délégué**, dans le champ **Domaine délégué**, entrez le nom du domaine délégué et cliquez sur **Suivant**.
6. Dans la page **Serveurs de noms**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans le champ **Nom de domaine pleinement qualifié du serveur (FQDN)**, entrez le nom de domaine pleinement qualifié du serveur DNS auquel déléguer le domaine, puis cliquez sur **Résoudre**.
8. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans le champ **Adresse IP**, vérifiez que l'adresse IP du serveur résolu est correcte, puis cliquez sur **OK**.
9. Dans la page **Serveurs de noms**, cliquez sur **Suivant**.
10. Dans la page **L'Assistant Nouvelle délégation est terminé**, cliquez sur **Terminer**.
11. Fermez la console DNS.

# 9. Gestion DNS

## *9.1. Durée de vie*

Dans le cadre de la gestion du système DNS, vous pouvez configurer la

valeur de durée de vie (TTL, Time-to-Live), utilisée dans les enregistrements de ressources d'une zone pour déterminer la durée de mise en cache des enregistrements par les clients ayant effectué une demande.
La valeur de *durée de vie* est un délai exprimé en secondes qui figure dans les enregistrements DNS retournés par une requête DNS. Ce délai indique aux destinataires combien de temps ils peuvent conserver ou utiliser l'enregistrement de ressource ou les données qu'il contient avant que ces données n'arrivent à expiration et ne soient supprimées.
La valeur de durée de vie d'une zone est appliquée à tous les enregistrements créés dans cette zone. La valeur de durée de vie d'un enregistrement est appliquée à l'enregistrement en question.
Le processus de durée de vie opère comme suit :
1. Les enregistrements de la zone sont envoyés à d'autres serveurs et clients
DNS sous la forme de réponses aux requêtes.
2. Les serveurs et clients DNS qui stockent un enregistrement dans leur cache conservent cet enregistrement pendant la période de durée de vie indiquée dans celui-ci.
3. À l'expiration de la durée de vie, l'enregistrement est supprimé du cache à la fois sur le serveur DNS et sur le client DNS.
Si la valeur de durée de vie prescrite est trop faible, le trafic lié aux requêtes
DNS augmente dans la mesure où les clients DNS demandent ces informations chaque fois qu'elles sont supprimées de leur cache.
En revanche, si la valeur de durée de vie d'un enregistrement est trop élevée, des enregistrements obsolètes peuvent perdurer dans le cache des clients DNS.

## 9.2. Configuration des paramètres de vieillissement et de nettoyage

Le *vieillissement* est un processus qui détermine si un enregistrement de ressource DNS obsolète doit être supprimé de la base de données DNS.
Le *nettoyage* est un processus qui consiste à supprimer les noms obsolètes ou caducs de la base de données DNS.

Avec la mise à jour dynamique, des enregistrements de ressources sont automatiquement ajoutés aux zones dès qu'un ordinateur est démarré sur

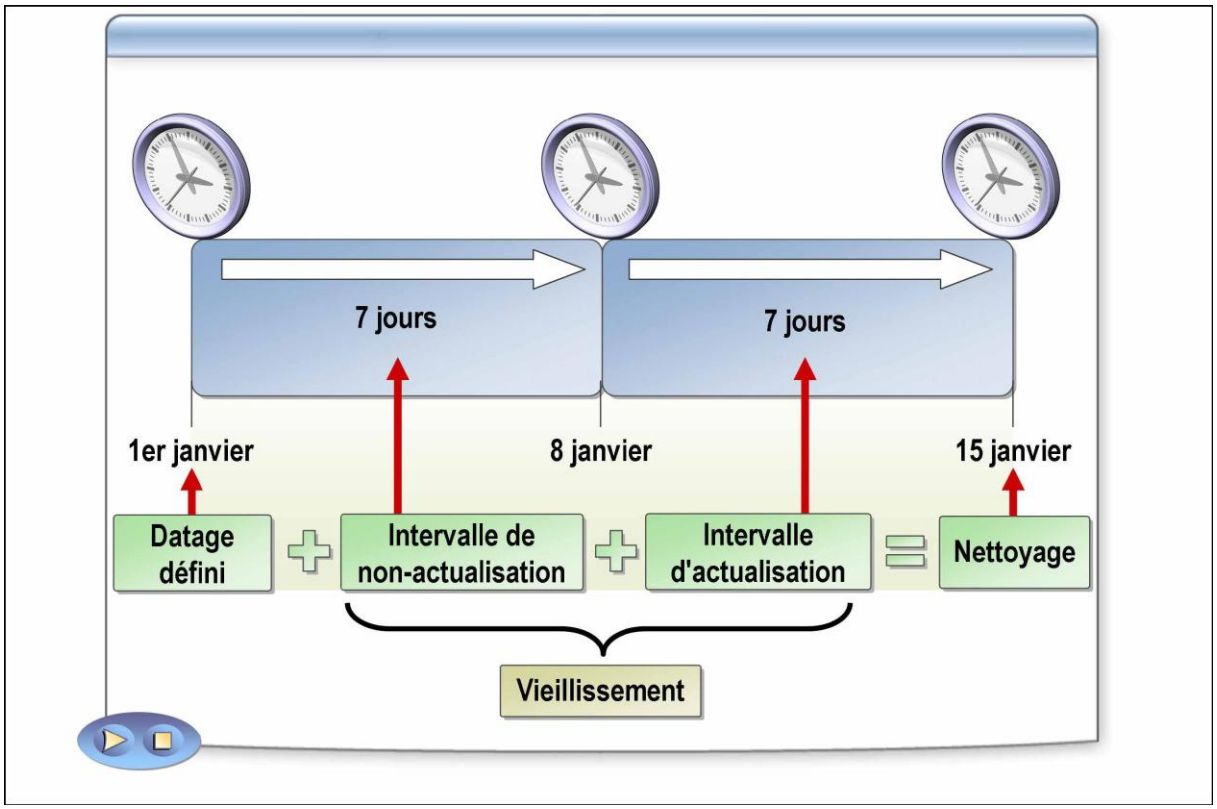
le réseau. Dans certains cas, toutefois, ces enregistrements ne sont pas supprimés automatiquement si l'ordinateur est supprimé du réseau. Ainsi, si un ordinateur inscrit son propre enregistrement de ressource hôte (A) au démarrage et qu'ensuite, sa connexion au réseau est rompue de manière incorrecte, cet enregistrement hôte A risque ne pas être supprimé. Cette situation peut être fréquente sur les réseaux comportant des ordinateurs et des utilisateurs mobiles.
De plus, les enregistrements de ressources obsolètes occupent de l'espace dans la base de données DNS et peuvent allonger inutilement les délais des transferts de zone. Ils peuvent en outre être envoyés en guise de réponse aux requêtes, ce qui peut entraîner des problèmes de résolution de noms pour les clients DNS.
Pour supprimer les enregistrements de ressources obsolètes de la base de données DNS, Microsoft® Windows Server. 2003 avec DNS est capable de les nettoyer en recherchant dans la base de données les enregistrements de ressources dont la durée de vie est supérieure à une période spécifiée et de les en supprimer.

### 9.2.1. Paramètres de vieillissement et de nettoyage d'une zone

Pour déterminer à quel moment les enregistrements doivent être nettoyés, DNS utilise le datage attribué à chaque enregistrement, associé aux paramètres que vous définissez.
Le vieillissement et le nettoyage doivent être activés sur le serveur DNS et sur la zone DNS. Ils comportent deux options configurables :
! L'*intervalle de non-actualisation* correspond à la période durant laquelle le serveur DNS n'accepte pas les tentatives d'actualisation. Pendant cet intervalle, les enregistrements de ressources ne peuvent pas actualiser leur datage.
! L'*intervalle d'actualisation* correspond à la période au cours de laquelle le serveur DNS accepte les tentatives d'actualisation. Pendant cet intervalle, les enregistrements de ressources peuvent actualiser leur datage.
Une *tentative d'actualisation* est le processus par lequel un ordinateur demande une actualisation de son enregistrement DNS. Elle a lieu lorsque le client, qui possède l'enregistrement DNS, essaie de réinscrire son enregistrement de ressource. Elle ne survient *pas* lorsqu'un client possédant l'enregistrement DNS met à jour l'enregistrement de ressource (par exemple, quand il modifie son adresse IP mais conserve le même nom d'hôte).

Il est important de paramétrer les intervalles d'actualisation et de nonactualisation de sorte à trouver le juste compromis qui permet au système DNS de ne pas garder trop longtemps les enregistrements de ressources, sans toutefois les supprimer trop tôt.

### 9.2.2. Fonctionnement du vieillissement et du nettoyage




Le processus de vieillissement et de nettoyage opère comme suit :

1. Un hôte DNS exemple, host-a.example.nwtraders.msft, inscrit son enregistrement de ressource hôte (A) sur le serveur DNS pour une zone dans laquelle le vieillissement et le nettoyage sont activés.
2. Lors de l'inscription de l'enregistrement de ressource, le serveur DNS se réfère à l'heure en cours pour affecter un datage à cet enregistrement.
3. Une fois que le datage de l'enregistrement de ressource a été effectué, le serveur DNS n'accepte pas d'actualisations de cet enregistrement de ressource pendant toute la durée de l'intervalle de non-actualisation de la zone. Avant cela, il peut toutefois accepter les mises à jour.

• Par exemple, si l'adresse IP de server1.it.nwtraders.msft est modifiée, le serveur DNS peut accepter la mise à jour. Dans ce cas, le serveur met également à jour (réinitialise) le datage de l'enregistrement de ressource.

4. À l'expiration de l'intervalle de non-actualisation, le serveur

recommence à accepter les tentatives d'actualisation de l'enregistrement de ressource.

• À l'issue de l'intervalle de non-actualisation initial, un intervalle d'actualisation débute immédiatement pour l'enregistrement de ressource. Alors, le serveur ne supprime pas les tentatives d'actualisation de l'enregistrement de ressource pendant le reste de sa durée de vie.

5. Au cours de l'intervalle d'actualisation, si le serveur reçoit une demande d'actualisation de l'enregistrement de ressource, il la traite.

• Toute mise à jour de l'enregistrement de ressource entraîne une réinitialisation de son datage, suivant la méthode décrite à l'étape 2.

6. Lorsque, par la suite, le serveur procède au nettoyage de la zone it.microsoft.com, il examine cet enregistrement de ressource ainsi que tous les autres enregistrements de la zone.

• Chaque enregistrement de ressource est comparé à l'heure en cours sur le serveur sur la base de l'addition ci-dessous, afin de déterminer si l'enregistrement doit être supprimé :

Datage de l'enregistrement de ressource + Intervalle de non-actualisation de la zone + Intervalle d'actualisation de la zone

7. Si cette addition donne un résultat supérieur à l'heure en cours sur le serveur, aucune opération n'est effectuée, et le vieillissement de l'enregistrement de ressource se poursuit.

8. Si elle donne un résultat inférieur à l'heure en cours sur le serveur, l'enregistrement de ressource est supprimé des données de la zone actuellement chargées en mémoire sur le serveur ainsi que de l'objet DnsZone applicable stocké dans Active Directory pour la zone **Exemple.microsoft.com** intégrée à Active Directory.

# 10. Surveillance du service DNS

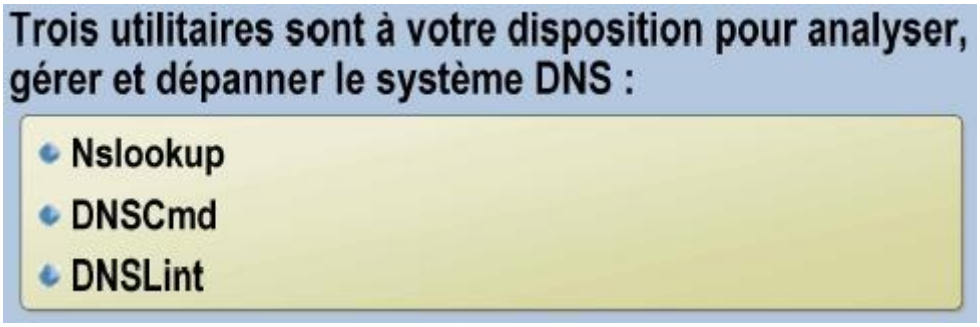
## *10.1. Test de la configuration du serveur DNS*

Dès que des modifications sont apportées à la configuration du serveur DNS, il est important de tester ce dernier pour s'assurer que la nouvelle configuration fonctionne correctement.

En utilisant des fonctions de requête de test sur le serveur DNS, vous pouvez vous assurer du bon fonctionnement des requêtes DNS. Cette mesure est utile si vous devez résoudre des problèmes liés aux requêtes DNS. Tester la configuration du serveur DNS vous permet d'isoler plus facilement la cause des problèmes.

Une *requête simple* est une requête qui exécute un test local en utilisant le client DNS pour interroger le serveur DNS.
Ce type de test spécifie que le serveur DNS exécute une requête simple ou itérative. Il s'agit d'une requête localisée qui se sert de la résolution de client DNS sur le serveur DNS pour interroger le service DNS local, qui se trouve sur le même serveur DNS.
Une *requête récursive* est une requête qui teste un serveur DNS en transmettant une requête récursive à un autre serveur DNS.
Ce type de test spécifie que le serveur DNS exécute une requête récursive. Il est similaire au test par requête simple en termes de traitement initial de la requête dans la mesure où il utilise la résolution de client DNS local pour interroger le serveur DNS local, hébergé sur le même ordinateur.
Cependant, ce test implique que le client demande au serveur d'utiliser la récursivité pour résoudre une requête de type serveur de noms (NS) pour la racine de l'espace de noms de domaine DNS, formulée sous la forme d'un point unique (« . »). Ce type de requête nécessite généralement un traitement récursif supplémentaire et peut se révéler utile pour vérifier que des indications de racine du serveur ou des délégations de zone ont été configurés correctement.

## 10.2. Vérification de la présence d'un enregistrement de ressource à l'aide de Nslookup, de DNSCmd et de DNSLint




La vérification de la présence d'un enregistrement de ressource est une

fonction de base de l'analyse et du dépannage du système DNS.
Si le serveur DNS comporte des mappages nom d'hôte-adresse IP qui sont périmés, obsolètes ou incorrects, les clients ne sont pas en mesure de se connecter aux services réseau. Étant donné le volume considérable de modifications dynamiques effectuées au niveau du service DNS, il est important de pouvoir vérifier que les enregistrements de ressources DNS sont à la fois corrects et parfaitement à jour.
Pour identifier les problèmes potentiels d'une solution DNS, il est possible de contrôler les points suivants :

- Enregistrements manquants
- Enregistrements incomplets
- Enregistrements mal configurés

Les trois utilitaires suivants sont à votre disposition pour analyser, gérer et dépanner le système DNS :

- Nslookup
- DNSCmd
- DNSLint

Dans le cadre de cette leçon, nous allons nous concentrer sur la vérification de l'existence d'un enregistrement de ressource, qui constitue seulement l'une des nombreuses tâches pouvant être accomplies à l'aide de ces trois outils.

**Nslookup**

Nslookup est un utilitaire de ligne de commande employé pour diagnostiquer les éventuels problèmes liés à l'infrastructure DNS.
Nslookup offre la possibilité d'exécuter le test de requête sur des serveurs DNS et d'obtenir, en guise de sortie de la commande, des réponses détaillées. Ces informations sont utiles pour procéder au dépannage de la résolution de noms, pour vérifier que des enregistrements de ressources ont été correctement ajoutés ou mis à jour dans une zone et pour effectuer le débogage en cas d'autres problèmes liés au serveur.

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.

- Ce mode est utile si vous devez configurer une alerte de performance en vue de l'exécution d'un fichier de commandes.

# 11. Analyse des performances du serveur DNS

## *11.1. Analyse des performances du serveur DNS à l'aide de la console de performances*

Les serveurs DNS revêtent une importance capitale dans la plupart des environnements, c'est pourquoi l'analyse de leurs performances procure des avantages tels que ceux-ci :

- Elle fournit des lignes de base utiles pour prévoir, estimer et optimiser les performances du serveur DNS.
- Elle facilite le dépannage des serveurs DNS victimes d'une baisse de performances que ce soit dans le temps ou pendant les périodes d'activité intense.
- Pour commencer l'analyse du serveur DNS, vous pouvez passer en revue l'échantillon de résultats des tests des serveurs DNS exécutant Windows Server 2003 collectés durant le développement et les tests du produit. Ces informations peuvent vous servir de référence initiale pour débuter l'analyse des serveurs DNS en vue de l'évaluation des performances.

Windows Server 2003 propose en outre un ensemble de compteurs de performance pour le serveur DNS qui peuvent être utilisés avec le Moniteur système pour mesurer et analyser divers aspects de l'activité du serveur.

| Compteurs de performance | Données collectées | Signification des données | Tendance à évaluer une fois la ligne de base établie |
|---|---|---|---|
| **Mises à jour dynamiques refusées** | Nombre total de mises à jour dynamiques refusées par le serveur DNS | Un nombre élevé de demandes refusées par un serveur DNS configuré pour autoriser les mises à jour sécurisées peut signifier que des ordinateurs non autorisés effectuent des tentatives des mises à jour. | Si ce nombre passe au-dessus de la ligne de base, il convient de réaliser des recherches supplémentaires. |
| **Requêtes récursives/seconde** | Nombre moyen de requêtes récursives reçues par un serveur DNS chaque seconde. | Ce compteur fournit une indication de la charge liées au requêtes imposée au serveur DNS. | Si la valeur de ce compteur chute ou augmente considérablement, il convient de réaliser des recherches supplémentaires. |
| **Demandes AXFR envoyées** | Nombre total de transferts de zone complets envoyés par le service Serveur DNS lorsqu'il joue le rôle d'un serveur secondaire pour une zone. | Le serveur DNS qui héberge la zone secondaire demande des transferts de zone incrémentiels. Si ce nombre est élevé, les modifications effectuées sur la zone principale sont fort nombreuses. | Si la valeur de ce compteur dépasse largement la ligne de base, il est possible que vous deviez revoir le nombre de modifications apportées à la zone et à la configuration des transferts de zone. |

## *11.2. Journal des événements DNS*

Un journal des événements DNS est un journal système configuré pour n'enregistrer que les événements DNS.
Vous pouvez avoir recours à l'Observateur d'événements pour consulter et analyser les événements DNS liés aux clients. Ceux-ci s'affichent dans le journal système et sont écrits par le service Client DNS sur tous les ordinateurs Windows (toutes les versions).
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.

## *11.3. 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.
L'enregistrement de débogage DNS permet de collecter des informations en consignant dans le journal tout le trafic DNS qui correspond aux critères définis pour l'enregistrement de débogage.
L'enregistrement se poursuit jusqu'à ce que la taille de journal spécifiée soit atteinte ou que le lecteur sur lequel se trouve le fichier journal vient à manquer d'espace disponible. Une fois la limite en termes de taille de fichier atteinte, le processus d'enregistrement commence à écraser les entrées les plus anciennes.
Les fichiers journaux peuvent devenir très volumineux, c'est pourquoi il est recommandé de les stocker sur un lecteur distinct.

Le tableau ci-dessous répertorie et décrit les options disponibles lors de la configuration de l'enregistrement de débogage DNS.

| **Options** | **Valeurs** | **Description** |
|---|---|---|
| Direction du paquet | Sortant | Des informations sur les paquets envoyés par le serveur DNS sont consignées dans le fichier journal du serveur DNS. |
| | Entrant | Des informations sur les paquets reçus par le serveur DNS sont |

| | | |
|---|---|---|
| | | consignées dans le fichier journal. |
| Contenu du paquet | Demandes/transferts | Enregistre des informations sur les paquets contenant des requêtes standard dans le fichier journal du serveur DNS. |
| | Mises à jour | Enregistre des informations sur les paquets contenant des requêtes standard dans le fichier journal du serveur DNS. |
| | Notifications | Enregistre des informations sur les paquets contenant des notifications dans le fichier journal du serveur DNS. |
| Protocole de transport | UDP | Enregistre des informations sur les paquets envoyés et reçus via UDP dans le fichier journal du serveur DNS. |
| | TCP | Enregistre des informations sur les paquets envoyés et reçus via TCP dans le fichier journal du serveur DNS. |
| Type de paquet | Demande | Enregistre des informations sur les paquets de demande dans le fichier journal du serveur DNS. |
| | Réponse | Enregistre des informations sur les paquets de réponse dans le fichier journal du serveur DNS. |
| Autres options | Filtrer les paquets par adresse IP | Fournit d'autres options de filtrage des paquets au sujet desquels des informations sont consignées dans le fichier journal du serveur DNS. Cette |

| | | |
|---|---|---|
| | | option permet d'enregistrer dans le journal des informations sur les paquets envoyés à partir d'adresses IP spécifiques vers un serveur DNS ou inversement. |
| | Chemin et nom de fichier | Indique le nom et l'emplacement du fichier journal du serveur DNS. |
| | Taille maximale (octets) | Définit la taille de fichier maximale du fichier journal du serveur DNS. |

## *11.4. Procédure d'activation et de configuration des options de l'enregistrement de débogage sur le serveur DNS*

Pour activer et configurer les options de l'enregistrement de débogage sur le serveur DNS :

1. Ouvrez la console DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur le serveur DNS voulu, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de serveur_DNS**, cliquez sur **Enregistrement de débogage**.
4. Sous cet onglet, activez la case à cocher **Enregistrer les paquets dans le journal pour le débogage.**
5. Ensuite, sélectionnez les options de critère de débogage voulues pour définir les informations que vous voulez consigner dans le fichier journal.
6. Dans le champ **Chemin et nom de fichier**, tapez le chemin d'accès au répertoire de stockage du journal de débogage et le nom du fichier journal.

Si vous ne spécifiez pas le chemin d'accès et le nom, le chemin par défaut est %systemroot%\System32\Dns et le nom par défaut est Dns.log.
7. Toujours sous l'onglet **Enregistrement de débogage**, tapez la taille maximale du fichier Dns.log dans le champ Taille maximale (octets). Il est recommandé de spécifier une taille de journal maximale et de stocker ce fichier sur un lecteur différent du lecteur système.
8. Cliquez sur **OK**.
9. Fermez la console DNS.

Mettre l’accent sur un point particulier

*Note d’attention particulière.*

## Pour approfondir le sujet….

Proposition de références utiles permettant d'approfondir le thème abordé

## Sources de référence

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support