http://www.laboratoire-microsoft.org

Essentiel Windows 2003

IMPLEMENTATION, ADMINISTRATION ET MAINTENANCE D'UNE INFRASTRUCTURE RESEAU

Auteurs : **LHOMEL Guillaume, POPOTTE Sammy, RICHET Antoine, RIVALLAN Jean-Yves**

Version 1.0 – Août 2004

Paris Academy of Computer Science SUPINFO Paris Ecole Supérieure d'Informatique

Ecole Supérieure d'Informatique de Paris
23. rue Château Landon 75010 – PARIS
www.supinfo.com

Table des matières

1. Configuration du routage à l'aide du service Routage et accès distant

1.1. Activation et configuration du service Routage et accès distant

La partie suivante vous présente les différentes entités du routage et accès distant dans un environnement Microsoft Windows.

1.1.1. Que sont les routeurs ?

Les routeurs sont des dispositifs réseau de couche 3 (couche réseau) du modèle OSI (Open Systems Interconnection) permettant d'une part l'interconnexion de réseaux **LAN** et **WAN,** d'autre part un routeur peut également permettre de faire de la segmentation de réseau entre plusieurs domaines de diffusion (broadcast), ce qui permet de préserver la bande passante.

Il existe d'autres dispositifs réseaux :

- Le concentrateur (hub), couche 1 (couche physique)
- Le commutateur (switch), couche 2 (couche liaison de données)
- Le routeur, couche 3 (couche réseau)

En règle générale, les routeurs sont divisés en deux catégories :

- **Le routeur matériel** : Dispositif physique exclusivement dédié au routage au sein d'un réseau.
- **Le routeur logiciel** : Logiciel permettant le routage dans un réseau, installé sur un ordinateur et pouvant exercé d'autres tâches. Exemple, Windows 2003 Server qui en plus du service de routage peut aussi bien effectuer un partage de fichiers et/ou d'imprimantes.

Une solution de routage consiste en trois composants principaux :

- **Interface de routage** : interface logique ou physique permettant l'acheminement des paquets (Exemple : la carte réseau).
- **Tables de routage** : Table indiquant le chemin à prendre pour atteindre le réseau souhaité.
- **Protocole de routage** : Règle de communication entre les routeurs pour échanger les informations contenues dans leur table de routage afin de déterminer le meilleur chemin.

1.1.2. Que sont les interfaces de routage ?

Comme dit précédemment, l'interface de routage permet d'acheminer les paquets. Par exemple, Windows Server 2003 achemine des paquets IP.

Il existe deux types d'interfaces de routage :

- **Interface de réseau local** (LAN, Local Aera Network) : Généralement les dispositifs de ce type sont des cartes réseau LAN même si une carte réseau étendue (WAN, Wide Aera Network) peut servir d'interface.

- **Interface de numérotation à la demande** : Il s'agit de connexions point à point qui nécessitent une authentification pour être établies. Dans la plupart des cas, il s'agit de connexions à l'aide de modem ou de réseau VPN entre routeur. Pour rappel, un réseau VPN est l'extension d'un réseau privé par le biais d'un réseau public ou partagé.

1.1.3. Que sont les protocoles de routage ?

Un protocole de routage supporte des protocoles routés pour fournir des mécanismes de partages d'informations de routage afin de permettre aux routeurs de communiquer entre eux pour mettre à jour et gérer leur table de routage.

Dans le cas où aucun protocole de routage n'est configuré, le service de routage et d'accès distant procédera au routage uniquement sur les réseaux auxquels il est physiquement connecté et ceux renseignés statiquement dans la table de routage par l'administrateur.

Le service de routage et d'accès distant de Windows Server 2003 supporte 2 protocoles de routages :

- **RIP (*Routing Information Protocol*)** : Utilisé dans les petites et moyennes infrastructures, il s'agit d'un protocole à vecteur de distance qui créer dynamiquement sa table de routage puis échange ces informations avec les autres routeurs connectés à ces interfaces. Cette opération se déroule périodiquement afin d'atteindre la convergence du réseau. Ce protocole reste le plus simple à configurer.

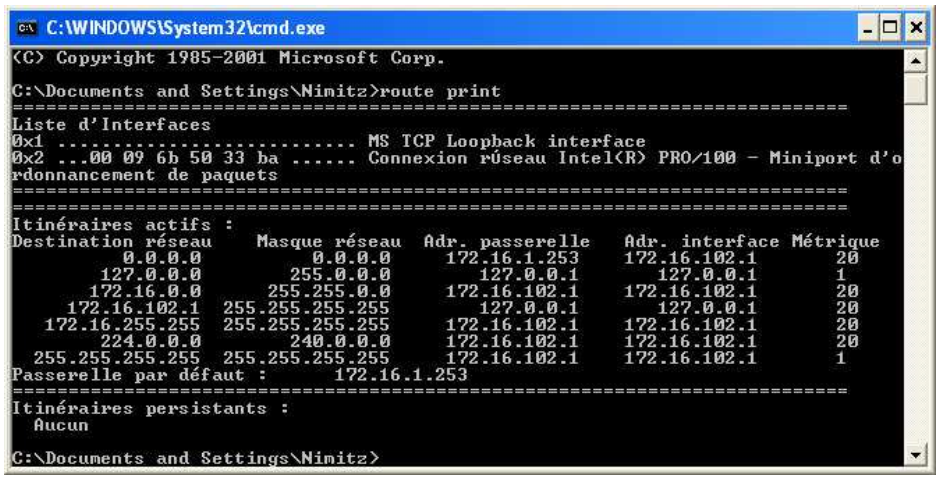
- **OSPF (*Open Shortest Path First*)** : Utilisé pour de plus grandes infrastructures que RIP, l'OSPF est un protocole à état de liens. Il forme une carte à partir de la configuration du réseau. Cette carte permet au routeur de calculer le plus court chemin à parcourir.

1.1.4. Que sont les tables de routage

Une table de routage recense les informations sur l'emplacement des ID réseaux au sein du réseau. Le but de la table de routage est de déterminer le chemin le plus court suivant l'algorithme utilisé par le routeur.

Dans une table de routage, il existe trois types d'entrées :

- **Itinéraire réseau** : C'est le chemin indiquant l'interface réseau à utiliser pour parvenir à un autre réseau.
- **Itinéraire hôte** : Chemin personnalisé vers un hôte (poste, serveur ou autre dispositif administrable à distance) permettant de contrôler et optimiser le trafic réseau.
- **Itinéraire par défaut** : Cet itinéraire est emprunté à chaque fois qu'aucune information vers la destination n'est disponible. Tout paquet ne trouvant pas son chemin empruntera cette route.



Les entrées d'une table de routage comportent plusieurs informations :

- **Destination réseau** : Adresse IP du réseau (bit des hôtes à 0) ou d'un client qui représente la destination réseau de l'itinéraire enregistré. La destination 0.0.0.0 représente l'itinéraire par défaut.
- **Masque réseau** : Représente le masque de sous-réseau utilisé sur le réseau de destination. Le masque 255.255.255.255 est réservé pour les enregistrements d'un hôte.
- **Adresse Passerelle :** Indique l'adresse de l'élément intermédiaire le plus proche permettant d'atteindre la destination et de changer de sous-réseau par exemple.
- **Adresse Interface** : Adresse de l'interface par laquelle les paquets vont être envoyés.
- **Métrique** : Eléments de mesure permettant de déterminer l'itinéraire préféré.

1.1.5. Pourquoi utiliser le service Routage et accès distant de Windows Server 2003 ?

Le service routage et d'accès distant permet d'effectuer plusieurs tâches :

- Segmentation de réseaux LAN et WAN
- Accès distant par l'intermédiaire de la numérotation à la demande.
- Accès au réseau LAN privé par l'intermédiaire de tunnels cryptés (VPN) en passant par un réseau public ou partagé

La console de ce service sur Windows Server 2003 permet d'afficher tous les serveurs routeurs Windows Server 2003 et les serveurs d'accès distant sur votre réseau. De plus, le service est extensible grâce à des API (*Application Programming Interface*) afin de personnaliser votre gestion de réseau.

1.2. Configuration des filtres de paquets

1.2.1. Qu'est-ce que le filtrage des paquets ?

Le *filtrage des paquets* spécifie le type de trafic circulant en entrée et en sortie en empêchant certains types de paquets d'être envoyés ou reçus par l'intermédiaire du routeur. C'est justement par l'intermédiaire d'*un filtre de paquets* (Paramètre de configuration TCP/IP) que le routeur autorise ou non des paquets entrants ou sortants.

Avec l'utilisation du service routage et accès distant, il est possible d'affecter des filtres de paquets par interface et les configurer comme suit :

- faire passer tout le trafic à l'exception des paquets interdits par les filtres
- ignorer tout le trafic à l'exception des paquets autorisés par les filtres.

Il existe plusieurs utilités à l'utilisation de filtres de paquets :

- Interdire l'accès aux utilisateurs non autorisés
- Interdire l'accès à une ressource
- Filtrer le trafic d'une liaison lente pour le rediriger sur une plus rapide.

1.2.2. Comment les filtres de paquets sont-ils appliqués ?

Un même filtre peut englober plusieurs paramètres comme le réseau d'origine, le réseau de destination et le protocole utilisé. Ensuite ce filtre peut autoriser ou non le trafic en entrée ou en sortie sur une interface.

Dans le cas d'un filtre à plusieurs paramètres, ils seront tous examinés les uns après les autres pour déterminer le devenir d'un paquet.

Étant donné que vous pouvez définir des filtres d'entrée et de sortie pour chaque interface, il est possible de créer des filtres contradictoires. Lorsque plusieurs filtres sont configurés, les filtres distincts appliqués aux paquets entrants ou sortants sont comparés en utilisant un OU logique.

L'application des filtres de paquets s'effectue dans cet ordre :

- Comparaison des paquets (entrants ou sortants) avec les filtres
- Si les paramètres correspondent, le filtrage (accepter ou refuser) est effectué.
- Si les paramètres ne correspondent pas en totalité, le paquet est comparé au prochain filtre
- Si aucun filtre de paquets n'est configuré mais que le routeur est configuré avec un filtre d'exclusion, le paquet pourra alors traverser le routeur, au contraire si le routeur est configuré avec filtre d'inclusion, le paquet est alors rejeté.

2. Attribution automatique d'adresses IP à l'aide du protocole DHCP

2.1. Pourquoi utiliser le protocole DHCP ?

Le serveur DHCP permet d'alléger la charge administrative. Les ordinateurs du réseau ont toujours une adresse IP correcte et des informations de configuration correctes. Cette technologie permet de limiter les tâches administratives à réaliser sur les clients au niveau de la configuration réseau.

2.2. Comment le protocole DHCP alloue des adresses IP

Un serveur DHCP permet de gérer l'allocation d'adresses IP automatiques à partir d'un point centralisé. Un serveur DHCP affecte un *bail DHCP* aux clients, ce bail contient tous les paramètres réseau à appliquer.
Un *bail* est la durée pendant laquelle le client pourra utiliser la configuration attribuée.

Le serveur DHCP gère l'attribution et le renouvellement du bail. Ces fonctions se nomment, *processus de création d'un bail DHCP* et *processus de renouvellement d'un bail DHCP.*

2.2.1. Comment fonctionne le processus de création d'un bail DHCP

Lorsque vous allumez votre ordinateur pour la première fois, il fait une demande de bail IP en diffusant le message **DHCPDISCOVER** à l'aide d'une version limitée du protocole TCP/IP.

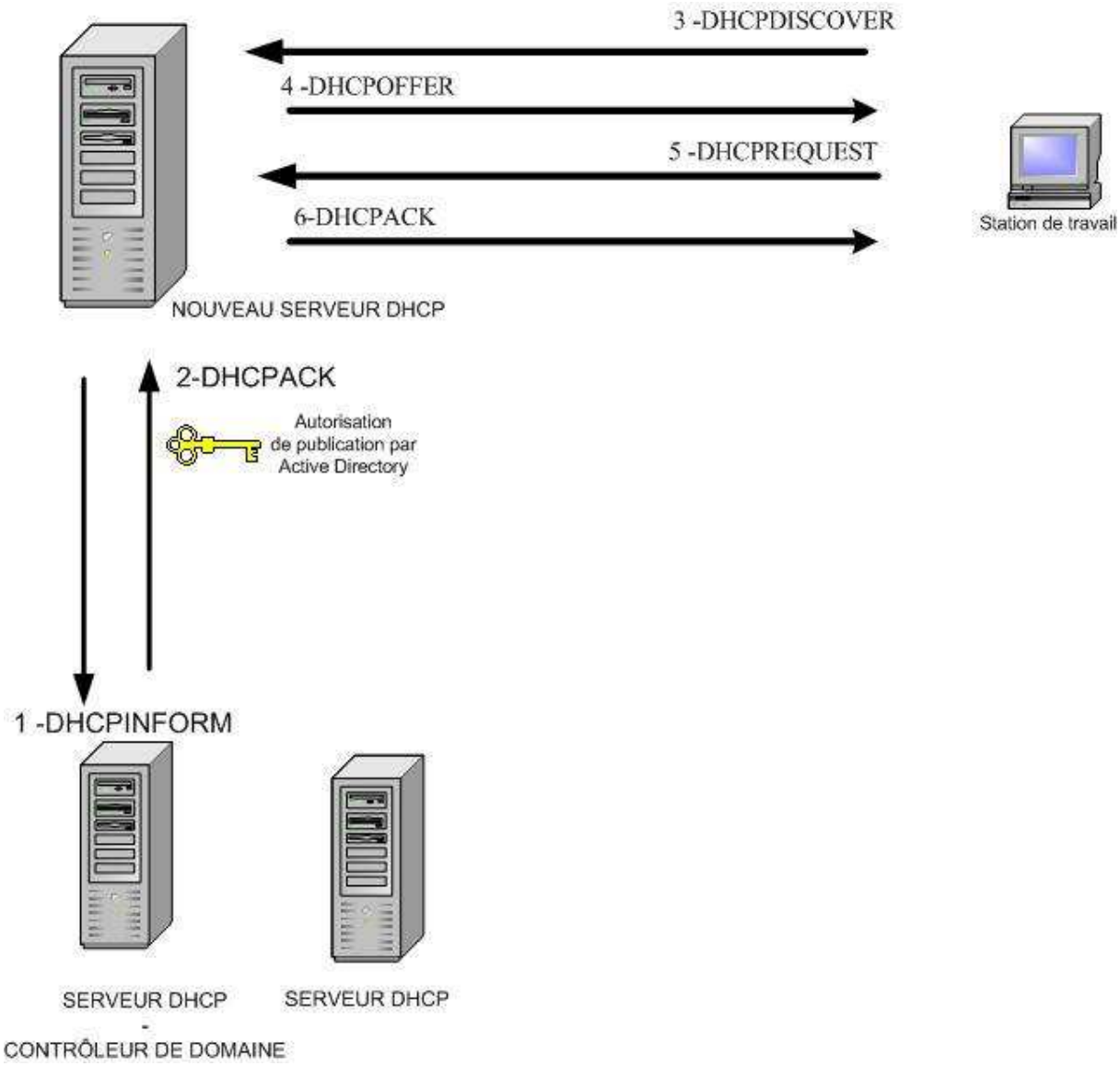
Tous les serveurs DHCP qui disposent d'une adresse IP valide pour le segment répondent avec un message **DHCPOFFER** contenant l'adresse matérielle du client, l'adresse IP proposée, un masque de sous réseau, la durée du bail et l'adresse IP du serveur DHCP.

L'adresse IP proposée est réservée par le serveur, pour éviter de la proposer à un autre client durant le laps de temps qui sépare la proposition de la réservation par le client.

Si le client ne reçoit pas de réponse d'un serveur DHCP, il renvoie un **DHCPDISCOVER** au bout de 2 puis 4, 8, 16 secondes à laquelle on ajoute une durée aléatoire ente 0 et 1000 ms.
Si le client n'a pas obtenu de réponse, il utilise une adresse IP comprise dans la plage d'adresses 169.254.0.1 et 169.254.255.254 (APIPA). Le client continue de rechercher un serveur DHCP toutes les 5 minutes.

Lorsque le client reçoit une offre d'adresse IP, il répond à la première qu'il reçoit en diffusant un message **DHCPREQUEST** pour l'accepter. Toutes les adresses IP proposées par les autres serveurs DHCP sont alors libérées.

Le serveur DHCP qui a émis l'offre acceptée envoie un accusé de réception **DHCPACK**. Ce message contient le bail ainsi que les informations de configuration.
Lorsque le client DHCP reçoit l'accusé de réception, il initialise le protocole TCP/IP.



2.2.2. Comment fonctionne le processus de renouvellement d'un bail DHCP

Un client DHCP tente automatiquement de renouveler son bail à 50% de sa durée. Pour cela, il envoie un message **DHCPREQUEST** au serveur DHCP qui lui a fourni son bail. Le serveur DHCP lui retourne un **DHCPACK** contenant la durée du nouveau bail ainsi que les paramètres de configuration mis à jour.

Si le serveur DHCP n'est pas présent, il réessaiera à **75% de la durée du bail puis à 87,5%** ; s'il n'a pas reçu de réponse à 87,5% alors il enverra un message DHCPDISCOVER auprès de tous les serveurs DHCP. S'il reçoit un DHCPOFFER pour mettre à jour son bail en cours, alors il effectuera le renouvellement auprès de ce serveur DHCP à compter de ce moment.

Si le bail expire, alors le client cesse immédiatement d'utiliser l'adresse IP et recommencera toute la procédure d'attribution

Lorsque vous démarrez un ordinateur qui dispose d'un bail toujours valide, il commence par tenter le renouvellement de bail.
Si un client demande le renouvellement d'un bail non valide (machine déplacée) ou en double, le serveur DHCP répond par un **DHCPNAK**, le client est alors contraint d'obtenir une nouvelle adresse IP.

Il est possible de demander le renouvellement du bail manuellement à l'aide de la commande **ipconfig /renew**.

Il est aussi possible de forcer l'abandon d'un bail avec la commande **ipconfig /release.**

Le message **DHCPRELEASE** sera envoyé au serveur DHCP et le protocole TCP/IP sera stoppé.

2.3. Comment un service Serveur DHCP est autorisé

Sur un réseau avec un domaine Windows 2000/2003, vous devez autoriser le serveur DHCP, sinon, celui-ci ne répondra pas aux clients.

☞ Seuls les serveurs DHCP Windows 2000/2003 vérifient l'autorisation.

Un serveur DHCP, pendant son initialisation, diffuse le message **DHCPINFORM.** Les serveurs DHCP en fonctionnement lui retournent un **DHCPACK** contenant les informations du domaine racine Active Directory. Avec ces informations, il contacte le contrôleur de domaine pour vérifier qu'il fait partie de la liste des serveurs DHCP autorisés puis démarre. S'il n'est pas autorisé, le service DHCP ajoute un message d'erreur au journal des événements et ne répond pas aux clients.

Pour autoriser un serveur DCHP, il faut être membre du groupe Administrateurs d'Entreprise ou de Domaine.

2.4. Configuration d'une étendue DHCP

2.4.1. Que sont les étendues DHCP ?

Pour utiliser l'adressage IP dynamique, vous devez créer une étendue sur le serveur. Chaque étendue se caractérise par un nom, une description, une plage d'adresses IP avec le masque de sous réseau correspondant, une durée de bail, les plages d'IP exclues (facultatif) et l'adresse de la passerelle (routeur). Chaque sous réseau possède une étendue DHCP unique contenant une plage d'adresses IP unique et permanente.
Il faut activer une étendue pour qu'elle soit disponible.

Configuration de la durée de bail :

Une durée de bail courte est conseillée lorsque vous avez moins d'adresses IP que de machines. Dans ce cas, lorsque l'on éteint des machines, leur adresse IP est plus rapidement libérée. C'est aussi utile lorsque les paramètres du réseau changent souvent.
Une durée de bail plus longue permet de diminuer le trafic réseau engendré par le renouvellement des IP.
Une durée de bail illimitée supprime le trafic engendré par le protocole DHCP. En effet, les clients ne l'utilisent qu'au démarrage de la machine.

✍ La durée du bail par défaut est de 8 jours.

Options d'étendues :

Les options d'étendues permettent de fournir diverses informations en même temps que la distribution de l'adresse IP.
Les options d'étendues courantes sont l'adresse de la passerelle par défaut, le nom de domaine DNS, l'adresse des serveurs DNS et WINS, le type de Nœud WINS à utiliser.

Les options d'étendues peuvent être définies à plusieurs niveaux, cela simplifie l'administration.
Au niveau du serveur, les options s'appliquent à tous les clients DHCP.
Au niveau de l'étendue, les options s'appliquent uniquement aux clients DHCP qui reçoivent un bail de cette étendue, elles sont prioritaires sur les options de serveur.
Au niveau de la classe, les options sont appliquées sur les clients qui appartiennent à une même classe. **Les classes doivent être définies sur les clients**. Les options de classe sont prioritaires sur les options d'étendues et les options de serveur.
Au niveau du client réservé, les options que vous définissez au niveau du client sont prioritaires sur toutes les autres options.

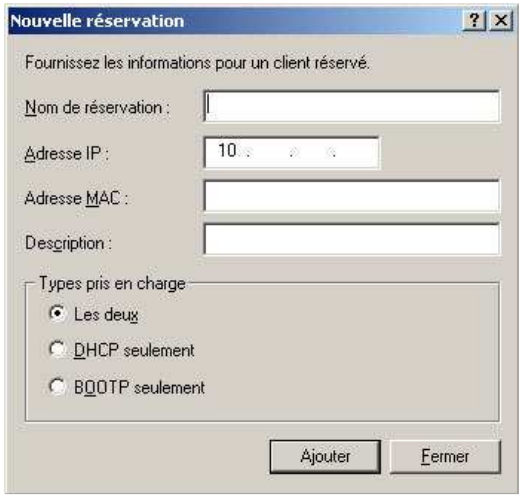
2.5. Configuration d'une réservation DHCP

2.5.1. Qu'est-ce qu'une réservation DHCP ?

Vous pouvez réserver une adresse IP spécifique pour un client en faisant une réservation **(basée sur l'adresse MAC du client).**

Il est avantageux d'utiliser une réservation d'adresse IP pour des postes qui doivent toujours utiliser la même IP comme pour les serveurs de fichiers, d'impression ou autres serveurs d'applications par exemple.

Une réservation est basée sur plusieurs informations comme, un nom de réservation, l'adresse IP réservée, l'adresse MAC du poste, une description et un type pris en charge (DHCP, BOOTP ou les 2).



2.6. Configuration des options DHCP

2.6.1. Que sont les options DHCP ?

Les options DHCP sont les paramètres supplémentaires que le serveur DHCP peut configurer sur les clients lors de l'attribution d'un bail.

Voici les options les plus courantes :

- **Routeur** : adresse d'une passerelle par défaut ou d'un routeur.
- **Nom de domaine** : Celui-ci permet de préciser le domaine de la machine. Ce qui permet au client de pouvoir s'enregistrer auprès du domaine correspondant.
- **Serveur DNS et WINS** : Adresse de ces serveurs pour la communication cliente.

2.6.2. Comment sont appliquées les options au niveau du serveur DHCP, de l'étendue et du client réservé

Le service DHCP applique des options aux ordinateurs clients dans un ordre précis :

1. Au niveau du serveur
2. Au niveau de l'étendue
3. Au niveau de la classe
4. Au niveau du client réservé

Par conséquent, vous pouvez définir des options attribuées par le service DHCP en utilisant différents niveaux d'autorité afin que certaines options soient prioritaires sur d'autres.

Le tableau suivant décrit les ordres de priorité et les niveaux des options DHCP :

Option DHCP	Ordre de priorité
Option au niveau du serveur	Est attribué à tous les clients du serveur DHCP
Option au niveau de l'étendue	Est attribué à tous les clients de l'étendue
Option au niveau de la classe	Est attribué à tous les clients appartenant à la classe
Option au niveau du client réservé	Est attribué à un seul client DHCP

Exemple de configuration :

- Le niveau serveur permet aux clients d'utiliser tous les mêmes serveurs WINS et/ou DNS
- Le niveau étendue permet à chaque étendue d'utiliser le même routeur
- Le niveau client réservé permet par contre l'utilisation d'un autre routeur.

2.6.3. Comment sont appliquées les options au niveau de la classe DHCP

Les options au niveau de classe sont utilisées pour modifier les valeurs des autres niveaux. Les options de la classe s'appliquent au client s'identifiant dans une classe. Vous pouvez utiliser deux types d'option de classe :

- La ***Classe de Fournisseur*** est une fonction qui permet de regrouper les clients DHCP en fonction de leur type de configuration, de fournisseur et de matériel.
- La ***Classe d'utilisateur*** est une fonction qui permet de regrouper les utilisateurs DHCP en fonction d'un identifiant partagé ou commun.

2.7. Configuration d'un agent de relais DHCP

Dans la plupart des cas, les routeurs prennent en charge le relais **DHCP/BOOTP**. Si un routeur ne peut pas fonctionner en tant qu'agent de relais DHCP/BOOTP, vous pouvez utiliser un agent de relais DHCP.

2.7.1. Qu'est-ce qu'un agent de relais DHCP ?

Un *agent de relais DHCP* est un ordinateur ou un routeur pouvant écouter les messages DHCP/BOOTP des clients pour les transmettre au serveur DHCP sur différents sous réseaux. Ces agents font partie des normes DHCP et BOOTP et fonctionnent en conformité avec les RFC.

☞ Un routeur conforme à la RFC 1542 prend en charge les messages DHCP.

Certaines entreprises pensent qu'il est plus facile de gérer un serveur DHCP global pour tous leurs réseaux. A cause de l'utilisation de diffusion lors du processus de demande de bail, les serveurs DHCP ne fournissent des baux que sur leur sous réseau. Il est alors nécessaire d'utiliser des routeurs compatibles ou des agents de relais logiciels. Par exemple, le service routage et accès distant de Windows Server 2003 est configuré pour fonctionner en agent de relais DHCP.

2.7.2. Comment fonctionne un agent de relais DHCP

Les procédures suivantes décrivent le fonctionnement d'un agent de relais DHCP :

1. Le client DHCP diffuse un paquet DHCPDISCOVER.
2. L'agent de relais DHCP sur le sous-réseau du client envoie le message DHCPDISCOVER au serveur DHCP à l'aide de la monodiffusion.
3. Le serveur DHCP utilise la monodiffusion pour envoyer un message DHCPOFFER à l'agent de relais DHCP.
4. L'agent de relais DHCP diffuse le paquet DHCPOFFER au sous-réseau du client DHCP.
5. Le client DHCP diffuse un paquet DHCPREQUEST.
6. L'agent de relais DHCP sur le sous-réseau du client envoie le message DHCPREQUEST au serveur DHCP à l'aide de la monodiffusion.
7. Le serveur DHCP utilise la monodiffusion pour envoyer un message DHCPACK à l'agent de relais DHCP.
8. L'agent de relais DHCP diffuse le paquet DHCPACK au sous-réseau du client DHCP.

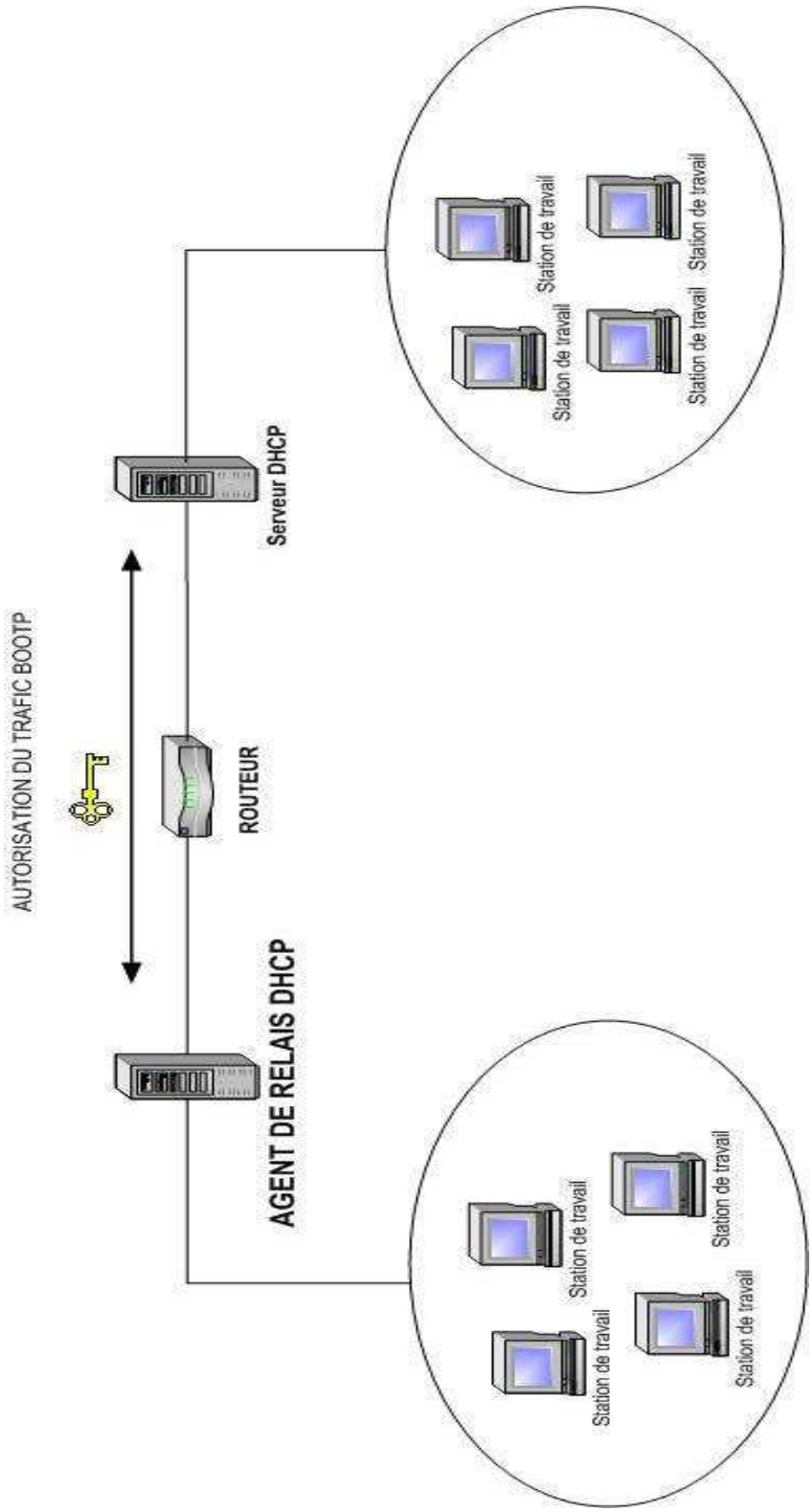
2.7.3. Comment un agent de relais DHCP utilise le nombre de tronçons

Le seuil du nombre de tronçons correspond au nombre de routeurs que le paquet peut traverser avant d'être rejeté. Le nombre de tronçons permet de déterminer la distance en routeurs entre l'agent de relais DHCP et le serveur DHCP le plus éloigné. Si le nombre de tronçons est inférieur à la distance avec le serveur DHCP, l'agent ne pourra pas fournir de baux. **Le nombre maximum de tronçons est de 16**.

2.7.4. Comment un agent de relais DHCP utilise le seuil de démarrage

Le *seuil de démarrage* est une temporisation pendant laquelle l'agent de relais va attendre pour laisser le serveur DHCP local au sous-réseau de répondre au client. Ce délai permet au serveur local de répondre le premier et quand le client va recevoir le DHCPOFFER du serveur DHCP distant (par

l'intermédiaire de l'agent de relais), il le refusera. Par contre dans le cas d'un disfonctionnement du serveur DHCP local, l'offre distante arrivant la première sera acceptée.



3. Gestion et analyse du service DHCP

3.1. Gestion d'une base de données DHCP

3.1.1. Vue d'ensemble de la gestion du service DHCP

Une fois un service quelconque installé, vous devez le surveiller pour le faire évoluer au sein de votre environnement. Pour le serveur DHCP, c'est la même chose du fait que l'environnement réseau est susceptible d'évoluer.

Il est nécessaire de gérer le service DHCP pour qu'il réponde aux besoins d'adressage IP des clients lorsque que le réseau est modifié (Ajout de clients, de serveurs par exemple). Il est aussi nécessaire de veiller aux conditions de fonctionnement du serveur sur lequel s'exécute le service DHCP et protéger la base de données contre toutes défaillances.

3.1.2. Qu'est-ce qu'une base de données DHCP ?

La base de données du serveur DHCP contient les données de configuration DHCP. C'est une base de données mise à jour dynamiquement lorsqu'un client acquiert ou libère un bail.

✍ Le service DHCP ne peut pas démarrer sans base de données.

Cette base est stockée dans le répertoire ***%Systemroot%\System32\Dhcp*** et par défaut, elle est sauvegardée dans le répertoire ***Systemroot%\System32\Dhcp\Backup\New*.**

La base de données est composée de plusieurs fichiers :

- **DHCP.mdb :** Fichier de base de données du service.
- **Tmp.edb** : Fichier temporaire de la base de données DHCP utilisé comme fichier d'échange pendant la maintenance.
- **J50.log et J50*.log** : Journaux utilisés pour enregistrer les transactions.
- **Res*.log** : Fichiers journaux réservés qui enregistrent les transactions existantes si l'on manque de l'espace disque système.
- **J50.chk** : Fichier de point de contrôle.

3.1.3. Modalités de sauvegarde et de restauration d'une base de données DHCP

La sauvegarde de la base de données DHCP permet de faire une restauration en cas de défaillance. Par défaut, le service DHCP sauvegarde toutes les heures la base et les entrées du registre dans le répertoire **Backup\New**. L'administrateur peut ensuite copier ces fichiers sur un support magnétique ou sur un autre disque.

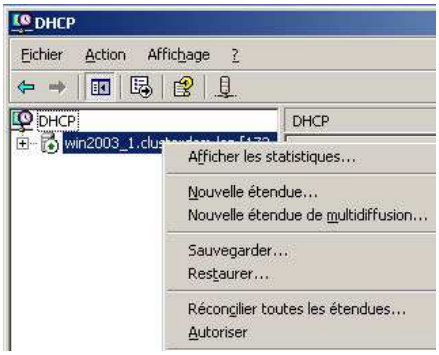
Si le serveur n'arrive pas à démarrer à partir de sa base de données, il effectue automatiquement une restauration à partir du répertoire de sauvegarde par défaut (qui peut être modifié).

3.1.4. Comment sauvegarder et restaurer une base de données DHCP

Il est possible de sauvegarder ou de restaurer la base de données aussi bien automatiquement que manuellement, mais s'il s'agit d'utiliser un support externe, l'opération sera obligatoirement manuelle.

Lors d'une sauvegarde manuelle, il faut choisir un autre répertoire que celui par défaut, car en cas de modification des fichiers de sauvegarde automatique manuellement, le service DHCP ne fonctionnera pas correctement.

La sauvegarde et la restauration manuelle s'effectuent à partir de la console DHCP.



3.1.5. Modalités de réconciliation d'une base de données DHCP

La ***réconciliation*** est le processus qui vérifie la base de données en fonction des valeurs de registre DHCP.

Il existe deux circonstances nécessitant la réconciliation de la base :

- Lorsque les données de la base sont correctes mais ne s'affichent pas correctement dans la console.
- Lors d'une restauration de la base qui ne contient pas les valeurs les plus récentes.

Lorsqu'on réconcilie un serveur ou une étendue, le service reconstruit sa configuration grâce aux informations résumées contenues dans le registre de Windows et des informations détaillées de la base de données DHCP.

3.1.6. Comment réconcilier une base de données DHCP

Avant de réconcilier une ou toutes les étendues, vous devez vous assurer que le serveur respecte les conditions suivantes :

- Toutes les clés du registre doivent être restées intactes suite à l'activité antérieure du serveur DHCP ou alors restaurer ces clés de registres.

- Une nouvelle version du fichier de base de données du serveur DHCP doit se trouver dans le dossier ***%Systemroot%\System32\Dhcp***.

Une fois la réconciliation effectuée, il est possible que les propriétés des clients individuels figurant dans les baux actifs soient affichées de manière incorrecte. Ces informations seront mises à jour lors du renouvellement du bail par les clients.

La réconciliation s'effectue à partir de la console DHCP en dessous de la restauration (voir image ci-dessus).
En cas de croissance de la base de données, il faut utiliser l'outil ***Jetpack.exe*** pour compacter la base de données DHCP.

3.2. Analyse du service DHCP

3.2.1. Vue d'ensemble de l'analyse du service DHCP

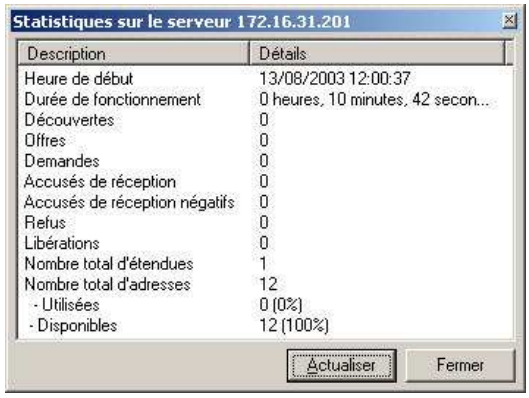
Etant donné que l'environnement DHCP est dynamique, les besoins des clients et de l'organisation changent constamment par de nouvelles options, d'ajouts d'étendues pour d'éventuels clients supplémentaires. Comme le serveur DHCP est un point très important du réseau, il faut établir une base de performances pour permettre d'évaluer les serveurs.

Dans la plupart des cas, les serveurs qui officient en tant que serveurs DHCP ne sont pas exclusivement dédiés à cette activité. Il faut donc tenir compte des possibles interactions entre les services DHCP et leur utilisation respective des ressources systèmes.

Des informations concernant le service DHCP sont disponibles dans les statistiques DHCP, les événements DHCP et les données de performances DHCP.

3.2.2. Présentation des statistiques DHCP

Les statistiques DHCP représentent les informations collectées depuis le dernier démarrage du serveur DHCP. Le but des statistiques DHCP est d'offrir une vue en temps réel afin de vérifier l'état du serveur.



3.2.3. Qu'est-ce qu'un fichier journal d'audit DHCP ?

Un fichier journal d'audit DHCP recense les événements relatifs liés au service, par exemple quand le service démarre ou s'arrête, quand des autorisations ont été vérifiées ou quand des adresses IP sont louées, renouvelées, libérées ou refusées.

Le journal d'audit DHCP permet à l'administrateur d'analyser les événements quotidiens, voir plus longs, de l'activité du serveur DHCP.

Les fichiers journaux sont des fichiers texte contenant des enregistrements qui représentent des lignes de texte avec des virgules comme séparateurs de colonnes.

Les champs disponibles pour ces fichiers sont :

- ID : Code de l'événement
- Date
- Heure
- Description
- Adresse IP
- Nom d'hôte
- Adresse MAC

3.2.4. Fonctionnement de l'enregistrement d'audit DHCP

Voici le fonctionnement quotidien de l'enregistrement de l'audit DHCP :

1. Lorsque le serveur DHCP démarre ou que c'est un nouveau jour (heure 00 :00), le serveur écrit une nouvelle entête dans le fichier journal.

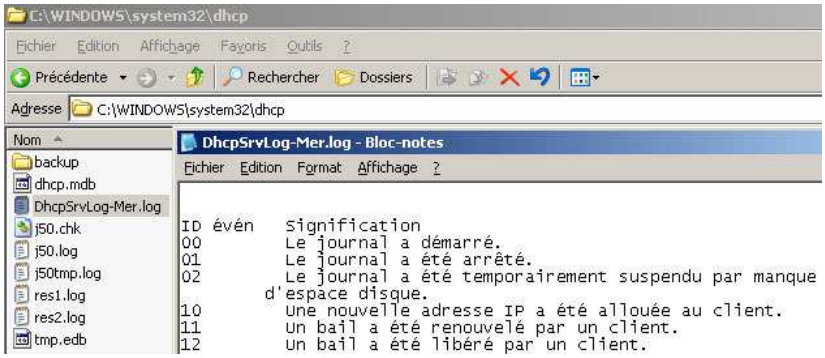
    a. Si le fichier existe mais n'a pas subi de modifications au cours des dernières 24 heures, il est remplacé.
    b. Si le fichier existe mais a été modifié depuis moins de 24 heures, il n'est pas remplacé, c'est le cas lorsque le serveur démarre par exemple.

2. Dès que l'enregistrement d'audit a débuté, le serveur DHCP fait des vérifications d'espace au niveau du disque mais aussi de la taille du fichier d'audit pour que celui-ci ne soit pas trop volumineux.
   A chaque fois que l'horloge du serveur atteint 00:00 ou qu'un certain nombre d'événements a été enregistré, par défaut 50, le serveur effectue une vérification totale du disque. A chaque contrôle du disque, le serveur vérifie si l'espace disque est rempli. Le disque est considéré plein lorsque l'une des conditions suivantes est vraie :

    a. L'espace disque restant est inférieur au minimum requis par le serveur DHCP pour l'enregistrement d'audit (par défaut : 20Mo).
    b. La taille du fichier journal d'audit actuel est supérieure à un septième (1/7) de l'espace maximal alloué pour l'ensemble des journaux d'audit actuellement stockés sur le serveur. La limite par défaut est configurée dans le registre à 70 Mo.

   Dans tous les cas, si le disque est considéré comme plein, aucun enregistrement d'événement ne sera accepté tant qu'il n'y aura pas d'autre place ou tant que le serveur n'arrive pas à 00:00.

3. A 00:00 heure locale sur l'ordinateur serveur, le journal courant est fermé pour passer au suivant. Par exemple, si on passe du mercredi au jeudi, le fichier de log passera du DhcpSrvLog-Mer à DhcpSrvLog-Jeu.



3.2.5. Instructions pour analyser les performances de serveur DHCP

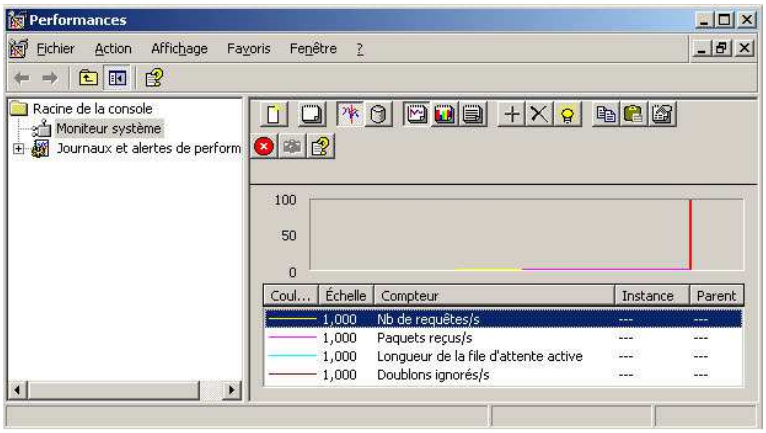
Il faut dans un premier temps créer une ligne de base (minimum requis au niveau performance) pour avoir un seuil précis des performances sous lesquelles on estime que le serveur qui héberge le DHCP est surchargé.

Ensuite il faut, si le serveur héberge d'autres services ou applications pouvant utiliser les ressources de la machine, évaluer la charge totale du serveur et les circonstances dans lesquelles ces différentes applications pourraient influencer sur le fonctionnement du service Serveur DHCP.

Puis, il est judicieux d'examiner les propres compteurs du serveur DHCP pour voir par exemple le nombre de baux traités. Une augmentation pourrait être due à une diminution du temps accordé aux baux mais une augmentation pourrait refléter d'un disfonctionnement d'une partie du réseau.

3.2.6. Compteurs de performance communément utilisés pour analyser les performances de serveur DHCP

La console de performances de Windows Server 2003 permet de vérifier les performances précises de l'activité du serveur DHCP.
Le **Moniteur système** permet d'ajouter des objets et des compteurs de performance dans l'un des trois modes d'affichage graphique : courbe, histogramme et rapport. Vous pouvez également afficher les données enregistrées dans les journaux. Si vous ajoutez un compteur comportant plusieurs instances, vous avez la possibilité de sélectionner l'instance souhaitée.



Compteurs de performance	Données collectées	Interprétation	Événements à rechercher après l'établissement d'une ligne de base
Paquets reçus/seconde	Nombre de paquets de messages que le serveur DHCP reçoit par seconde.	Un nombre élevé indique un volume important de messages DHCP transmis au serveur.	Surveillez les augmentations ou les diminutions soudaines qui pourraient dénoter des problèmes sur le réseau.
Nombre de	Nombre de messages	Une augmentation soudaine	Surveillez les

requêtes/seconde	de demande DHCP que le serveur DHCP reçoit par seconde de clients.	ou inhabituelle de ce nombre indique qu'un grand nombre de clients essaient de renouveler leurs baux auprès du serveur DHCP. Ceci peut dénoter que les durées de bail de l'étendue sont trop courtes.	augmentations ou les diminutions soudaines qui pourraient dénoter des problèmes sur le réseau.
Longueur de la file d'attente active	Longueur actuelle de la file d'attente de messages interne du serveur DHCP. Cette valeur est égale au nombre de messages non traités que reçoit le serveur.	Une valeur élevée peut indiquer que le serveur DHCP est débordé par le nombre de demandes qu'il reçoit.	Surveillez les augmentations soudaines ou graduelles, qui pourraient dénoter un accroissement de la charge ou une baisse de la capacité de traitement du serveur.
Doublons ignorés/seconde	Nombre de paquets en double que le serveur DHCP supprime par seconde.	Ce nombre peut augmenter lorsque plusieurs agents de relais DHCP ou interfaces réseau transmettent le même paquet au serveur. Une valeur élevée indique que le serveur ne répond pas assez vite ou que le nombre de secondes spécifié comme seuil de redémarrage pour l'agent de relais n'est pas assez élevé.	Surveillez avec ce compteur toute activité pouvant indiquer que plusieurs demandes sont transmises au serveur au nom des clients.

3.2.7. Instructions pour créer des alertes pour un serveur DHCP

Une *alerte* est un processus qui se déclenche lorsque la valeur surveillée est soit inférieure, soit supérieure au seuil indiqué nommé *seuil d'alerte*.

Affecter des alertes auprès de certains compteurs de performances du serveur DHCP qui ont une activité anormale avant l'apparition de problèmes connus, peut permettre à l'administrateur d'y configurer le lancement d'un script.

Pour définir ces compteurs, il faut auditer les compteurs DHCP durant une certaine période afin de surveiller l'évolution des compteurs pour créer une zone de fonctionnement normal. Il faudra ensuite créer des alertes pour prévenir lorsque que le compteur est en dehors de sa zone.

Afin de répondre aux alertes DHCP par un script, il existe les commandes Netshell pour DHCP. Les commandes Netshell pour DHCP offrent pour l'administration des serveurs DHCP un outil d'aide de ligne de commande totalement équivalent, Dhcpmon.dll, qui constitue une alternative à la gestion sur console.

3.3. Application des instructions de sécurité pour le service DHCP

3.3.1. Instructions pour empêcher un utilisateur non autorisé d'obtenir un bail

Lorsqu'un utilisateur possède un accès physique (câble ou wireless) à un réseau possédant un serveur DHCP, il peut récupérer un bail auprès de ce serveur sans fournir son nom d'utilisateur ou mot de passe. Un utilisateur mal intentionné peut donc bloquer de nombreux baux et donc diminuer les baux disponibles aux utilisateurs du réseau.

Il existe des précautions simples pour empêcher un utilisateur non autorisé d'obtenir un bail :

- S'assurer que seules les personnes autorisées ont un accès au réseau
- Activer l'audit sur tous les serveurs DHCP du réseau pour les analyser lorsque ceux-ci reçoivent un nombre élevé de demandes de baux DHCP.
- Utiliser des commutateurs ou des points d'accès basés sur les technologies 802.1x pour l'accès au réseau. Il permet l'authentification (Certificat ou Clé WEP) avant l'accès au DHCP.

3.3.2. Instructions pour empêcher les serveurs DHCP non autorisés, non-Microsoft, de louer des adresses IP

Seuls les serveurs DHCP Windows 2000 et Windows 2003 peuvent être autorisés dans l'annuaire Active Directory. Dans le cas où un serveur découvre qu'il n'est pas autorisé dans Active Directory, ce serveur ne fournira pas de baux. Cette option permet d'empêcher les serveurs installés par un utilisateur malveillant ou incompétent sur Windows 2000 et 2003 de fournir des baux et de ne pas corrompre la configuration réseau des postes.

Par contre dans le cas de l'utilisation de serveur DHCP non-Microsoft, il est impossible d'utiliser cette option, il faudra donc bien veiller à interdire l'accès physique d'autres personnes à votre réseau.

3.3.3. Instructions pour limiter le cercle des personnes autorisées à administrer le service DHCP

Lors de l'installation du service DHCP sur un serveur membre ou autonome, deux groupes locaux sont créés :

- Utilisateurs DHCP
- Administrateurs DHCP

Par contre lors de l'installation de ce service sur un contrôleur de domaine, ces deux groupes sont créés en tant que groupes locaux du domaine.

Pour administrer le serveur DHCP (avec **NETSH** ou console DHCP), il faut soit faire parti du groupe Administrateurs, soit du groupe Administrateurs DHCP. De plus, il est à l'origine nécessaire d'être **membre du groupe Administrateurs de l'entreprise pour autoriser ou interdire le serveur DHCP dans l'annuaire Active Directory**. Mais il est possible de déléguer ce droit à d'autres entités de sécurité.

Administrateurs DHCP

Les membres de ce groupe peuvent afficher et modifier toutes les données liées au service serveur DHCP. Les droits de ce compte sont limités au service serveur DHCP, ils n'ont aucun autre droit sur les autres services du serveur.

Utilisateur DHCP

Les membres de ce groupe ne possèdent qu'un accès en lecture seule aux données du serveur.

Pour administrer des serveurs DHCP dans un domaine, il faut ajouter un utilisateur ou un groupe à tous les groupes Administrateurs DHCP de chaque serveur DHCP du domaine.

3.3.4. Instructions pour sécuriser la base de données DHCP

Les autorisations par défaut pour le dossier DHCP ont pour but d'empêcher quiconque, à l'exception des utilisateurs autorisés, d'accéder aux fichiers de base de données et aux fichiers d'audit. Modifiez ces autorisations par défaut s'il y a lieu pour accorder un accès à ces fichiers aux personnes qui doivent effectuer des tâches administratives (par exemple analyser et sauvegarder les fichiers journaux de serveur DHCP).

Ne modifiez pas les autorisations des groupes Système ou Administrateurs. Si vous le faites, vous risquez de provoquer des dysfonctionnements du serveur DHCP et d'empêcher les administrateurs d'assurer sa maintenance, par exemple en sauvegardant la base de données.

4. Résolution de noms

4.1. Affichage de noms sur un client

Un nom pour un poste permet l'identification de celui-ci sur un réseau par toute autre entité.
Chaque ordinateur possède deux identificateurs : un nom alphanumérique et une adresse IP.

4.1.1. Comment les noms sont mappés à des adresses IP

La résolution de noms	Un service de résolution de noms
Il est difficile pour un utilisateur de travailler avec des adresses IP. La résolution est le processus qui permet d'effectuer automatiquement une traduction entre des noms alphanumériques et des adresses IP.	C'est ce service qui effectue la résolution de noms complets (ou alphanumériques). Ce service est fourni par WINS (Windows Internet Name Service) et DNS (Domain Name System).

Lorsqu'un utilisateur veut atteindre une ressource disponible sur un serveur, il y fait appel par le nom du serveur (ex : ServSupinfo1). L'ordinateur va déterminer l'adresse IP associé au serveur (ex : 192.168.1.1) et ensuite effectuer la connexion à partir de celle-ci.

Il existe deux types de noms dans les réseaux : nom d'hôtes et noms NetBIOS.

4.1.2. Que sont les noms d'hôtes ?

Dans *noms d'hôtes*, il y a :
Nom : Identificateur du poste dans le réseau.
Nom d'hôtes : Nom DNS d'un périphérique réseau.

Un *nom de domaine pleinement qualifié* (*FQDN*) est un nom de domaine DNS. C'est la forme lisible et hiérarchique du nom complet d'un ordinateur. Le ***FQDN*** **(Fully Qualified Domain Name)** définit un nom d'hôte complet (ex: www.labo-microsoft.com). Il inclut la partie domaine ou *suffixe* (ex: labo-microsoft.com) et la partie hôte (ex: www), ce qui permet la résolution des noms d'hôtes sur Internet.

Les noms d'hôtes sont utilisés pour trouver un périphérique réseau sur un réseau. Afin de trouver un dispositif réseau à partir de son nom d'hôte, il faut qu'il soit connu du fichier Hosts ou d'un serveur DNS.

Caractéristiques du nom d'hôte
Alias attribué à un poste pour l'identifier
Identique au nom NetBIOS par défaut sur Windows 2003 et XP
Chaîne comportant au maximum 255 caractères
Nom unique avec comme méthodes de résolution, le fichier Hosts et le serveur DNS

✍ A une adresse IP peut correspondre plusieurs noms d'hôtes ou l'inverse.

4.1.3. Que sont les noms NetBIOS ?

Un nom NetBIOS est un nom qui permet d'identifier les services NetBIOS sur un ordinateur. Ce nom est composé d'un nom de 15 caractères plus 1 qui indique le service (Station de travail, Serveur, Messenger, Groupe,…).

Par contre les noms NetBIOS n'ont aucune utilité sur Internet car ils ne possèdent aucune hiérarchie. Un exemple simple : aucun nom NetBIOS ne peut être en double sur le même sous réseau.

Caractéristiques du nom NetBIOS
Pas forcement égal au nom d'hôte
Longueur max de 15 caractères
Unique sur le réseau
L'utilitaire Nbtstat affiche les noms NetBIOS de la machine locale ou distante

4.1.4. Comment afficher les noms sur un client

Nom d'hôte

Localité	Affichage
Commande **Ipconfig /all**	Nom de l'hôte Suffixe DNS principal
Commande hostname	Nom d'hôte
Système dans le Panneau de configuration, onglet nom de l'ordinateur.	Nom d'hôte Nom de domaine

Nom NetBIOS

Localité	Affichage
Commande **Nbtstat -n**	Noms NetBIOS locaux
Commande Nbtstat -A @IP	Noms NetBIOS distants
Système dans Panneau de configuration, onglet nom de l'ordinateur.	Nom NetBIOS Nom du groupe de travail

Pour modifier, le nom du poste, il faut aller dans Système dans le Panneau de configuration (clic droit → propriétés sur poste de travail), onglet nom de l'ordinateur puis faire modifier.

Si l'ordinateur est membre d'un domaine, vous devrez posséder un compte sur le domaine ayant les droits de renommer le poste.

4.2. Configuration de la résolution de noms d'hôtes

4.2.1. Processus de résolution de noms d'hôtes

1. Utilisation d'un nom d'hôte par une application ou un service
2. Recherche dans le cache de résolution client (créé à partir du fichier Hosts et des dernières recherches).
3. Si l'entrée n'existe pas dans le cache, le poste client envoie une requête à un serveur DNS.
4. Si ces méthodes de résolutions ont échoué et que le nom ne dépasse pas 15 caractères, le poste client passe à la méthode de résolution de noms NetBIOS.
5. Lorsque le nom d'hôte est trouvé, L'adresse IP est retournée au service ou à l'application qui est à l'origine de cette procédure

4.2.2. Cache de résolution client

Le cache de résolution client stocke le contenu du fichier Hosts (enregistrement PTR) et les noms d'hôtes récemment résolus pendant un temps défini (durée de vie) pour ne pas avoir un cache trop important..

Ce cache est le premier endroit utilisé lors de la résolution de nom d'hôte car il ne génère aucune requête réseau et reste plus rapide.

Les résolutions échouées (entrées de cache négatives) sont enregistrées 5 minutes dans le cache afin de ne pas réinterroger le serveur DNS pour rien. (ex : www.existepas.fr).

Pour afficher le cache de résolution, il faut utiliser la commande ***Ipconfig /displaydns***, de plus, il est possible depuis la version Windows 2000 de vider ce cache avec la commande ***Ipconfig /flushdns***.

4.2.3. Fichier Hosts

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP pour
Windows.
#
# Ce fichier contient les correspondances des adresses IP aux noms d'hôtes.
# Chaque entrée doit être sur une ligne propre. L'adresse IP doit être
placée dans la # première colonne, suivie par le nom d'hôte correspondant.
L'adresse IP et le nom
```

```
# d'hôte doivent être séparés par au moins un espace.
#
# De plus, des commentaires (tels que celui-ci) peuvent être insérés sur
des lignes
# propres ou après le nom d'ordinateur. Ils sont indiqué par le symbole
'#'.
#
# Par exemple :
#
#      102.54.94.97     rhino.acme.com          # serveur source
#       38.25.63.10     x.acme.com              # hôte client x

127.0.0.1       Localhost
```

Le fichier Hosts (exemple ci-dessus) est stocké sur l'ordinateur client à l'emplacement ***%Systemroot%\System32\Drivers\Etc*** et se nomme *Hosts*.

Il sert à stocker dans le cache de résolution client des entrées statiques comme par exemple 127.0.0.1 qui correspond à *localhost*. De plus une entrée de ce fichier ne contient aucune durée de vie dans le cache.

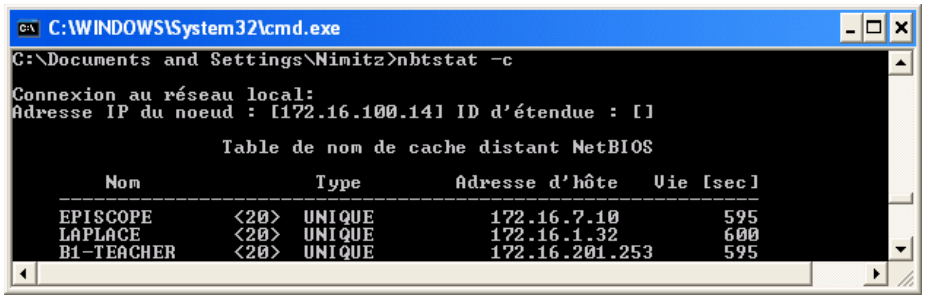
Chaque poste client peut posséder le même fichier Hosts car ce fichier est compatible avec les fichiers Hosts d'UNIX.

4.3. Configuration de la résolution de noms NetBIOS

4.3.1. Processus de résolution de noms NetBIOS

1. Lorsqu'une application a besoin de résoudre un nom NetBIOS, elle recherche dans le cache NetBIOS.
2. Si le cache NetBIOS ne résout pas la requête, le serveur WINS est alors interrogé.
3. Si le serveur WINS ne résout pas le nom NetBIOS en adresse IP, le client tente de la diffusion au sein de son réseau local.
4. Si la diffusion n'aboutit à rien, le poste regarde dans son fichier **Lmhosts**.
5. Lorsque le nom NetBIOS est trouvé, l'adresse IP correspondante est renvoyée à l'application.

4.3.2. Cache de noms NetBIOS



Le cache de nom NetBIOS est l'emplacement mémoire où se trouvent les noms correspondants aux adresses IP récemment résolues par une diffusion, fichier Lmhosts, un serveur WINS ou les noms préchargés à partir du fichier Lmhosts.

Le cache de nom NetBIOS est utilisé avant le serveur WINS, car l'utilisation du fichier Lmhosts ne produit aucun trafic réseau et reste très rapide.

La durée de vie d'une entrée dans le cache de nom NetBIOS est de 10 minutes. Cette durée est réinitialisée à chaque résolution du nom.

Il existe deux types de noms NetBIOS :

- ***Uniques* :** Fait référence à un service NetBIOS existant sur un ordinateur individuel.
- ***Collectifs*** : Fait référence à un service NetBIOS regroupant plusieurs ordinateurs.

4.3.3. Comment afficher et libérer le cache de noms NetBIOS

L'outil utilisé pour interagir avec le cache de noms NetBIOS est **nbtstat**. Utilisé sans argument, il permet d'afficher l'aide.
Commandes courantes :

- **Nbtstat –c** : Afficher le cache
- **Nbtstat –R** : Vide le cache et recharge les entrées préchargées à partir du fichier Lmhosts
- **Nbtstat –n** : Affiche la table de noms NetBIOS locale.

4.3.4. Diffusions

Les diffusions dites **broadcast** sont des messages produits par un poste à destination de tous les hôtes de son segment réseau.

La diffusion se produit si la résolution du nom NetBIOS n'a pas fonctionné avec le cache et le serveur WINS. Il n'y pas de configuration requise pour la diffusion.

Le principe de la diffusion est de lancer un message à destination de tous les nœuds sur le segment réseau afin que l'ordinateur possédant le nom NetBIOS recherché renvoie son adresse au destinataire de la diffusion.

4.3.5. Fichier Lmhosts

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Ce fichier est un modèle de fichier LMHOSTS utilisé par Microsoft TCP/IP
pour
# Windows.
#
# Ce fichier contient les mappages des noms d'ordinateur NT (NetBIOS) sur
des adresses
# IP. Vous devez vous en tenir … une seule entrée par ligne.
# L'adresse IP doit être placée dans la première colonne, suivie du nom
d'ordinateur
# correspondant. L'adresse et le nom d'ordinateur doivent être séparés par
au moins un
```

```
# Espace ou une tabulation. Le caractère # est généralement utilisé pour
marquer le
# Début d'un commentaire (voir les exceptions ci-dessous).
#
# Toutes ces extensions sont présentées dans les exemples suivants :
#
# 102.54.94.97     rhino         #PRE #DOM:networking  #DC du groupe réseau
# 102.54.94.102     "appname   \0x14"                        #serveur d'app.
spécial
# 102.54.94.123    popular            #PRE             #serveur source
# 102.54.94.117    localsrv           #PRE              #nécessaire pour le
include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
```

Le fichier **LMHOSTS** est un fichier statique situé sur l'ordinateur et configuré par l'administrateur pour mapper les adresses IP à des noms NetBIOS pour des ordinateurs situés en dehors du sous réseau local.

Ce fichier est utilisé dans le cas où aucune autre méthode de résolution n'a fonctionné. C'est un fichier texte ASCII composé du nom NetBIOS de l'ordinateur cible et de l'adresse IP correspondante. Pour utiliser ce fichier situé dans ***%Systemroot%\System32\Drivers\Etc*** qui porte une extension ***.sam*****,** il faut supprimer l'extension pour que le fichier puisse être lu.

Mots clés prédéfinis :

- **#PRE** : Permet de précharger des entrées dans le cache de noms NetBIOS.
- **#DOM:[**nom_domaine**]** : Facilite l'activité de domaine telle que la validation d'une connexion sur un routeur, la synchronisation et la navigation.
- **#BEGIN_ALTERNATE <> #END_ALTERNATE:** Définit une liste d'autres emplacements (chemin UNC définit au préalable dans le fichier Lmhosts) pour des fichiers Lmhosts.
- **#INCLUDE :** Charge et recherche les entrées NetBIOS dans un fichier distinct du fichier Lmhosts par défaut.

5. Résolution de noms d'hôtes à l'aide du systèmes DNS

5.1. Installation du service serveur DNS

5.1.1. Vue d'ensemble du système DNS

Le service de résolution de noms de Windows Server 2003 est nommé DNS (Domain Name System). Il permet de résoudre des adresses URL structurées comme www.laboratoire-microsoft.org en adresse IP: **212.180.91.68**.

Le système de noms DNS est une base de données distribuée, utilisée sur les réseaux IP pour transposer et résoudre les noms d'ordinateurs en adresses IP. C'est la principale méthode de résolution de noms de Windows 2003.

Le système de noms sur lequel est fondé DNS est une structure hiérarchique et logique appelée espace de noms de domaine. L' **InterNIC** (Internet Network Information Center) gère la racine de cette arborescence. L'InterNIC est chargé de déléguer la responsabilité administrative de portions de l'espace de noms de domaine mais aussi d'inscrire les noms de domaine.

5.1.2. Qu'est-ce qu'un espace de noms de domaines ?

La structure hiérarchique de l'espace de noms de domaines est telle que :

- Le domaine racine, qui se trouve en haut de la structure du nom de domaine, est représenté par un point.
- Les domaines de niveau supérieur (premier niveau) suivent directement les domaines racines ; ils peuvent êtres représentés par le type d'organisation ou la localisation géographique (ex : com, org, fr, de, …)
- Les domaines de second niveau (deuxième niveau) sont enregistrés directement auprès des entreprises et peuvent posséder de nombreux sous domaines.
- Les sous-domaines permettent à une organisation de subdiviser encore son nom de domaine par départements ou services (ex : microsoft.supinfo.com).

Le Nom de Domaine Pleinement Qualifié ou FQDN (Fully Qualified Domain Name) décrit la relation exacte entre un hôte et son domaine.

Dans les FQDN suivant : web.labo-microsoft.supinfo.com, le domaine racine est le '.' A partir de la droite du nom de domaine, le '.com' est le nom de domaine de 1er niveau, le '.supinfo' est le nom de domaine du deuxième niveau et le reste sont des sous domaines dans la présente arborescence de noms de domaines.

Le serveur DNS contient des informations sur la portion de l'espace de noms DNS qu'il va fournir au client. Le serveur DNS va stocker des noms / adresses IP de sa zone dans un fichier de zone. Lorsqu'un ordinateur client envoie une requête de résolution de nom à un serveur DNS, ce dernier va consulter sa base de données de noms et va, soit répondre au client s'il possède la correspondance nom / adresse IP, soit interroger les autres serveurs DNS en cas d'échec de la recherche dans sa base de données locale.

5.1.3. Convention d'appellation standard DNS

Les conventions liées à l'appellation standard DNS permettent à l'entreprise qui implémente un espace de noms de l'utiliser sur internet. Ces conventions autorisent un jeu de caractères ASCII limité spécifié par la RFC 1123 qui est :

- A-Z
- a-z
- 0-9
- Trait d'union (-)

☞ Tous les caractères invalides sont remplacés par un trait d'union.

5.1.4. Comment installer le service Serveur DNS

Il est nécessaire de configurer le futur serveur DNS pour qu'il utilise une adresse IP fixe au lieu d'une adresse attribuée dynamiquement par un serveur DHCP. Il faut pour cela configurer le protocole TCP/IP, et entrer une adresse statique dans la boite de dialogue **Propriétés de protocole Internet.** Microsoft recommande également de configurer le nom de domaine sur le serveur DNS, dans **Propriétés de protocole Internet** (TCP/IP).

L'installation se fait via l'assistant « ajout / suppression de programmes ». Le service Serveur DNS fait partie des services de mise en réseau. (Composants intégrés de Windows 2003).

Configuration des propriétés du service Serveur DNS

5.1.5. Quels sont les composants d'une solution DNS ?

Serveur DNS :
Ordinateur exécutant le serveur DNS
Héberge un ou une partie de l'espace de noms
Fait autorité pour un espace de noms de domaine
Traite les demandes de résolution de noms soumises par les clients

Client DNS :
Ordinateur exécutant le Service Client DNS

Enregistrement de ressources DNS :
Entrées de la base de données DNS qui mappent les noms d'hôtes à des ressources

5.1.6. Qu'est-ce qu'une requête DNS ?

Les clients DNS envoient des requêtes au serveur DNS ce qui constitue le processus de résolution du nom. Il existe deux types de requêtes, les récursives et les itératives.

Une requête peut provenir d'un client mais aussi d'un serveur, par exemple, une requête peut être envoyée par un client à un serveur qui peut ensuite l'envoyer à un autre serveur si il ne parvient pas à la résoudre.

Un serveur DNS, qui *fait autorité* sur un espace de nom, possède une copie principale ou secondaire d'une zone DNS.

Lors d'une requête, le serveur faisant autorité renvoie l'adresse IP correspondant au nom, de deux façons possibles :

- Recherche dans le cache local
- Recherche dans la zone DNS

Sinon il renvoie une réponse négative qui fait autorité.
Par contre, s'il ne fait pas autorité, il transmet la requête au redirecteur. Le serveur utilise les adresses connues de plusieurs serveurs racines pour aller chercher la réponse plus haut dans l'arborescence DNS.

5.1.7. Fonctionnement des requêtes récursives

Une requête récursive peut être lancée d'un client mais aussi d'un serveur s'il est configuré avec un redirecteur.

Le serveur DNS doit absolument fournir un résultat au client pour ce type de requête. Dans le cas où il ne possède pas de réponse à la requête, le serveur DNS va effectuer, pour le compte du client des requêtes itératives séparées vers d'autres serveurs qui l'aident à répondre à la requête récursive.

5.1.8. Fonctionnement des indications de racine

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

Pour 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 d'enregistrements de ressources préliminaires peut être utilisée par le service DNS pour localiser d'autres 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.

5.1.9. Fonctionnement des requêtes itératives

Elles sont envoyées par un client à un serveur DNS. Ce dernier renvoie la meilleure réponse qu'il possède à partir de ses données de cache ou de zone. S'il ne possède pas la réponse exacte, il renvoie le client vers un serveur de référence dans un niveau inférieur de l'espace de noms de domaine. Le client va alors interroger le serveur correspondant. Ce processus se poursuit jusqu'à ce que le client localise le serveur qui pourra résoudre le nom en adresse IP ou bien jusqu'à ce qu'une erreur se produise ou encore que le délai soit dépassé.

5.1.10. Fonctionnement des redirecteurs

Il est possible de configurer les serveurs DNS pour qu'ils envoient toutes les requêtes récursives à une liste sélectionnée de serveurs dit redirecteurs. Les serveurs de la liste des redirecteurs assurent les

recherches récursives pour résoudre les requêtes reçues par un serveur DNS qui ne peut pas y répondre en s'appuyant sur ses zones locales. Pendant le processus de redirection, un serveur DNS configuré pour utiliser des redirecteurs (un ou plusieurs serveurs en fonction de la liste de redirecteurs) se comporte essentiellement comme un client DNS vis-à-vis de ses redirecteurs.

Un redirecteur peut être configuré en 2 modes :

- ***Non exclusif*** : Si le redirecteur n'est pas en mesure de résoudre la requête initiale, le serveur de noms va tenter de résoudre la requête lui-même.
- ***Exclusif*** : Si le redirecteur n'est pas en mesure de résoudre la requête, une réponse négative est renvoyée.

5.1.11. Fonctionnement de la mise en cache du serveur DNS

La mise en cache permet de répondre plus rapidement aux requêtes fréquentes en stockant temporairement dans la mémoire les résultats des requêtes récemment résolues.

Lors du traitement d'une requête récursive, le serveur DNS peut être amené à interroger les serveurs de noms racines pour redescendre au fur à mesure des niveaux afin d'obtenir des informations. Ce processus peut prendre plus ou moins de temps et peut utiliser des liaisons coûteuses.

Le serveur place donc toutes les informations collectées lors de ce processus dans son cache DNS pendant une durée spécifiée. Ce temps est appelé TTL (Time To Live) et se mesure en secondes. C'est l'administrateur de serveur associé à la zone principale qui définit le TTL.

Une fois les données en cache, le TTL se décrémente et lorsqu'un client fait une requête pouvant être résolue avec les informations contenues dans le cache, le client obtient l'information à l'aide d'un TTL valide et en cours. Lorsque le TTL d'un enregistrement est expiré celui-ci n'est pas conservé.

Le cache a également pour utilité le stockage des réponses n'ayant pas abouti : ***les réponses négatives.*** Cette mise en cache évite la répétition des requêtes concernant des noms qui n'existent pas. Le TTL associé a ces réponses est inférieur à celui des réponses positives (par défaut : 5 minutes).

Un serveur qui ne possède aucune zone et qui n'a aucune autorité sur un quelconque domaine est un serveur dédié à la mise en cache grâce à la configuration des indicateurs de racine.

5.2. Configuration des zones DNS

5.2.1. Stockage et maintenance des données DNS

Un ***enregistrement de ressource*** stocké dans un fichier de zone définit une zone. Le fichier de zone stocke des informations pour effectuer la résolution de noms. Toutes les tâches administratives liées aux serveurs DNS se font à travers le **SNAP-IN MMC DNS**.

Une *zone* est une portion contiguë de l'espace de noms de domaine pour laquelle un serveur DNS sert de référence pour la résolution des requêtes DNS. Elle permet de stocker des noms concernant un ou plusieurs domaines DNS ou des portions de domaines DNS.

5.2.2. Que sont les enregistrements de ressources et les types d'enregistrements ?

Les utilisateurs peuvent avoir accès aux enregistrements de ressources notamment dans les cas suivants :

- Recherche d'un site Web, le navigateur envoie une requête de recherche directe au serveur.
- Lors de la connexion sur un domaine. A l'ouverture de session, le poste cherche un contrôleur de domaine par l'intermédiaire du DNS.

Les types d'enregistrements représentent les différents types de données pouvant être enregistrées dans le serveur DNS.

Principaux types d'enregistrements :

Type d'enregistrement	Description	Exemple
Hôte (A)	Représente un périphérique réseau. Ils sont les enregistrements les plus courants.	Microsoft.supinfo.com résolu en 192.168.0.43
Pointeur (PTR)	Permet de retrouver le nom à partir de l'adresse IP. Ils se trouvent dans la zone de recherche inversée.	192.168.0.43 résolu en Microsoft.supinfo.com
Source de noms (SOA) (start of authority)	C'est le premier élément dans tout fichier de zone. Il identifie le serveur de noms DNS principal de la zone, l'adresse de messagerie de l'administration chargée de la zone. Recense les informations nécessaires à la réplication.	Résout un nom de domaine en nom d'hôte. Supinfo.com résolu en serv1.supinfo.com.
Service (SRV)	Indique un service réseau offert par un hôte et résout un nom de service et un port d'hôte.	_TCP._LDAP.supinfo.com résolu en serv1.supinfo.com
Serveur de noms (NS) (Nameserver)	Facilite la délégation en identifiant les serveurs DNS de chaque zone. Quand un serveur DNS a besoin d'envoyer une requête à un domaine délégué, il se réfère à l'enregistrement de ressource NS pour trouver les serveurs DNS de la zone cible.	Supinfo.com résolu en NS1.supinfo.com
Serveur de messagerie (MX) (Mail Exchanger)	Indique la présence d'un serveur de messagerie SMTP (Simple Mail Transfert Protocol).	Supinfo.com résolu en mail.supinfo.com
Alias (CNAME)	C'est un nom d'hôte qui fait référence à un autre nom d'hôte.	www.supinfo.com en Webserv.supinfo.com

Exemple d'enregistrement MX :

5.2.3. Qu'est-ce qu'une zone DNS ?

Une zone est une portion contiguë de l'espace de noms de domaine pour laquelle un serveur DNS sert de référence pour la résolution des requêtes DNS. Elle permet de stocker des noms concernant un ou plusieurs domaines DNS (si ces domaines sont contigus : relation parent-enfant) ou des portions de domaines DNS.

Un serveur DNS peut héberger différents types de zones tout comme un ou plusieurs types de zones peuvent être hébergés sur plusieurs serveurs DNS pour fournir une tolérance de panne et répartir la résolution de noms et la charge de travail.

Les caractéristiques d'une zone sont :

- Une zone est un ensemble de mappages de noms d'hôtes à adresses IP.
- Les données d'une zone sont gérées par le serveur et sont stockées dans un fichier de zone ou dans une base de données Active Directory.

Un serveur fait autorité sur une zone s'il possède des enregistrements de ressources correspondants aux noms et aux adresses que les clients demandent dans le fichier de zone.

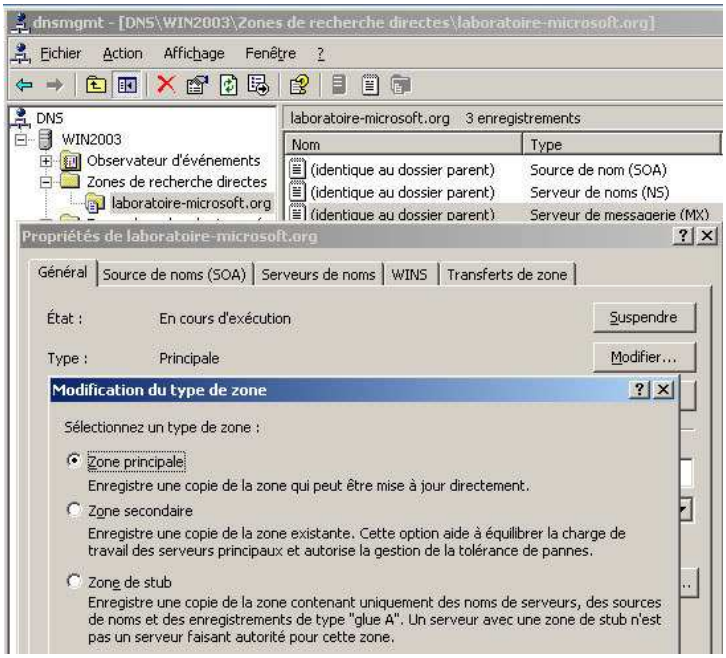
5.2.4. Quels sont les types de zones DNS ?

Il existe différents types de zone :

Principale standard	Contient une version en lecture / écriture dans un fichier. Récupère toutes les modifications de la zone. Doit toujours être créée en premier pour une nouvelle zone.
Secondaire standard	Contient la copie en lecture seule du fichier de la zone principale standard. Toute modification effectuée sur le fichier de zone principale standard est répliquée sur celui-ci. Permet de répartir la charge de résolution de noms des serveurs DNS.
Zone de stub	Contient une copie d'une zone qui possède uniquement les enregistrements de ressources nécessaires à l'identification du serveur DNS faisant autorité pour la zone en question. 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.

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

5.2.5. Comment modifier un type de zone DNS



Pour modifier un type de zone DNS :

Dans la console DNS, sélectionnez la zone à modifier → menu action → propriétés.

Dans la fenêtre propriétés de votre zone, il faut cliquer sur Modifier et modifier la zone.

5.2.6. Que sont les zones de recherche directe et inversée ?

Recherche directe

Lorsque vous créez une zone de recherche directe, l'assistant vous proposera les trois types de zone disponibles, puis il vous invitera à entrer le nom de la zone à gérer et enfin il vous demandera de valider le nom du fichier contenant la zone DNS. Une fois ces étapes passées, l'assistant va créer automatiquement la zone, le fichier et des enregistrements de type "Source de nom" (Serveur ayant l'autorité sur la zone) et "Serveurs de noms" (Serveur pouvant répondre aux requêtes des clients).

Recherche inversée

Lorsque vous créez une zone inversée, l'assistant vous propose d'indiquer l'ID (Partie réseau de votre adresse IP). Pendant que vous entrez l'ID, le nom de la zone de recherche inversée s'affiche sous la forme des nombres de votre ID en ordre inverse suivi de **".in-addr.arpa"** (ex : Pour "172.16.0.0/16" ➔ "16.172.in-addr.arpa"). Le nom in-addr.arpa représente un domaine spécial au niveau DNS, il est réservé à la résolution d'adresses IP en noms d'hôtes.

5.3. Configuration des transferts de zone DNS

5.3.1. Fonctionnement des transferts de zone DNS

Le transfert de zone consiste en la diffusion des entrées contenues dans une zone à l'ensemble des serveurs DNS secondaires de cette zone.

Sous Windows 2003, il est possible de mettre en place des transferts complets et des transferts incrémentiels de zone.

Le ***transfert de zone complet*** est le type de standard pris en compte par tous les serveurs DNS pour mettre à jour et synchroniser les données d'une zone. La requête déclenchant ce type de synchronisation est **AXFR**.

Le ***transfert de zone incrémentiel*** permet de mettre à jour seulement les données de zones modifiées depuis la dernière mise à jour. Ce type de transfert ne s'effectue qu'entre 2 serveurs le prenant en charge à la suite d'une requête de type **IXFR**.

Le processus de transfert de zone intervient dans 2 cas :

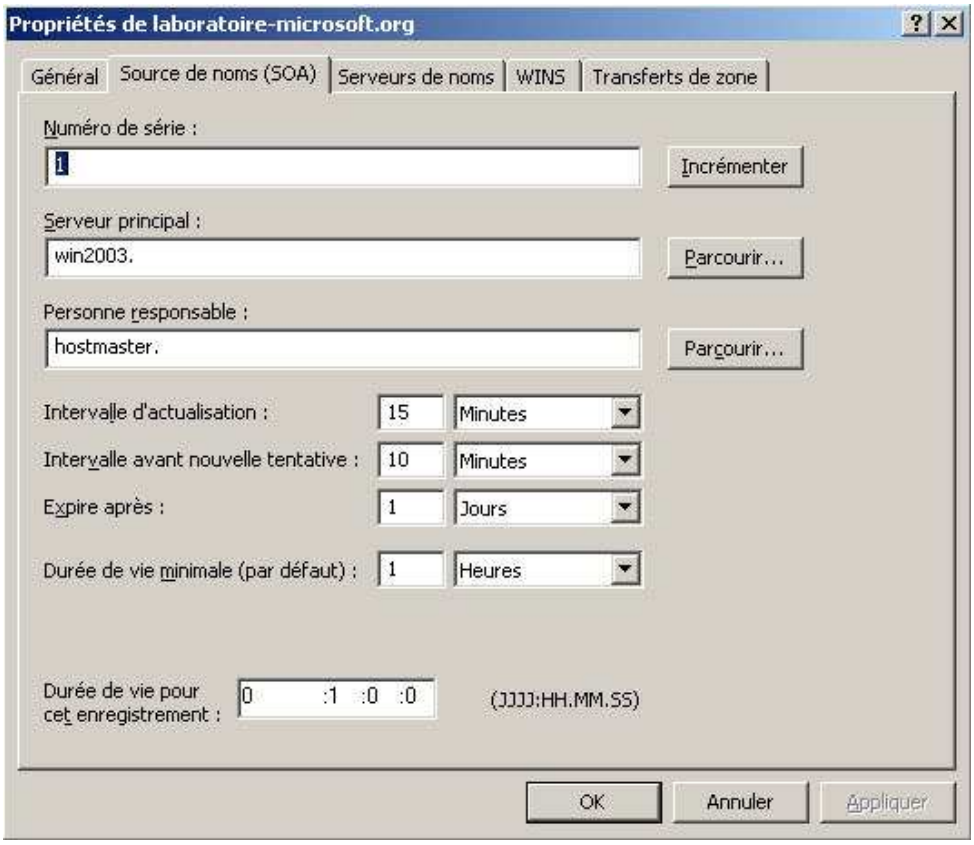
- Un serveur maître envoie une notification de modification de la zone aux serveurs DNS secondaires de la zone. Une fois cette notification reçue, les serveurs secondaires envoient une requête de mise à jour au serveur maître.

- Chaque serveur DNS secondaire interroge à intervalles réguliers ses serveurs maîtres sur les modifications de la zone. Cette requête est lancée aussi à chaque démarrage du service DNS.

Toutes les informations liées à la fréquence d'exécution des transferts de zone sont stockées dans les enregistrements de ressource de noms (**SOA – Start of Authority**).

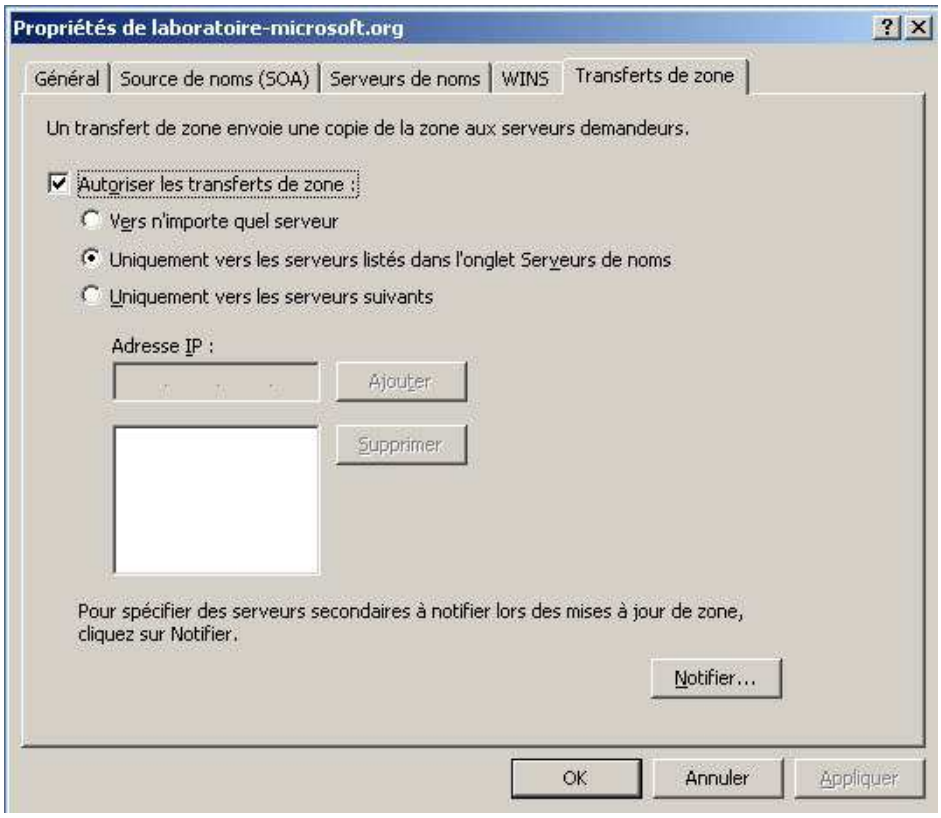
Un certain nombre de paramètres sont modifiables (dans les propriétés de la zone) :

Numéro de série	Le numéro de série fonctionne comme un numéro de version (il est donc incrémenté à chaque version) permettant de savoir si, lors de la synchronisation avec le serveur maître, le fichier de zone doit être mis à jour.
Serveur principal	Le serveur principal précise le nom de domaine complet du serveur principal.
Personne responsable	La personne responsable sera avertie par e-mail à chaque fois qu'une erreur se produit lors d'un transfert de zone.
Intervalle d'actualisation	L'intervalle d'actualisation spécifie la fréquence à laquelle un serveur secondaire va envoyer une requête de mise à jour à son serveur maître.
Intervalle avant nouvelle tentative	L'intervalle avant nouvelle tentative détermine l'intervalle de temps qu'un serveur secondaire va prendre pour re-contacter son serveur maître suite à l'échec de la tentative d'une mise à jour.
Expire après	Définit le délai d'expiration d'un serveur secondaire s'il n'arrive pas à contacter son serveur maître. A la suite de l'expiration il ne répondra plus aux requêtes de la zone.
Durée de vie minimale	La durée de vie (TTL) minimale indique le temps durant lequel un serveur peut mettre en cache des informations pour une zone.
Durée de vie pour cet enregistrement	Spécifie la durée TTL de l'enregistrement SOA.



Il est possible de limiter le nombre de serveurs que vous allez autoriser à recevoir les zones. Ceci est défini soit par une liste d'adresses IP de serveurs DNS soit en limitant les transferts aux serveurs DNS

situés dans le même domaine. De la même manière, il est possible de définir une liste de serveurs DNS secondaires qui recevront une notification des mises à jour d'un fichier de zone.



5.3.2. Fonctionnement de DNS Notify

DNS notify est une mise à jour de la spécification d'origine du protocole DNS qui permet d'informer les serveurs secondaires des modifications de zones.

Les serveurs qui reçoivent une notification peuvent demander un transfert de zone afin de corriger les modifications. Les serveurs qui font autorité dans cette zone préviennent les serveurs secondaires des modifications par l'intermédiaire d'une liste de serveurs secondaires.

Avec **DNS notify**, les mises à jour s'effectuent au rythme des modifications.

5.4. Configuration des mises à jour dynamiques DNS

5.4.1. Que sont les mises à jour dynamiques ?

Il existe 2 méthodes pour inscrire des enregistrements dans la base de données DNS, soit manuellement, soit dynamiquement.

En mode dynamique, le client s'inscrit auprès du serveur DNS.

La méthode manuelle devient vite inadaptée lorsqu'il faut inscrire à la main tous les postes d'un réseau de grande étendue mais peut devenir pratique si on possède un réseau avec des cas isolés, avec des

serveurs UNIX par exemple. Par contre la méthode dynamique permet d'automatiser le processus d'enregistrement mais aussi de le maintenir à jour.

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

Les clients DNS exécutant la famille Server 2003, famille 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.

Un client configuré par un serveur DHCP ou statiquement peut s'inscrire automatiquement sur le serveur DNS. Le composant qui inscrit l'enregistrement de ressource DNS pour un client DNS est le service de client DHCP, il faut donc activer le service de client DHCP.

Le processus ci-dessous résume les étapes pour l'enregistrement dynamique des clients DNS :

a. Le client envoie une requête SOA au serveur DNS faisant autorité pour l'enregistrement de ressource.
b. Le serveur renvoie le nom de zone et l'adresse IP du serveur DNS faisant autorité pour la zone dans laquelle le client DNS veut s'inscrire.
c. Le client DNS envoie ensuite une mise à jour qui vérifie la présence de l'enregistrement.
d. Le serveur répond au client DNS.
e. Si aucune inscription n'existe dans la zone DNS, le client DNS envoie son inscription.

5.4.3. Comment configurer des mises à jour DNS manuelles et dynamiques

Lorsqu'un client DHCP reçoit une adresse IP, les enregistrements DNS le concernant doivent être mis à jour. Ainsi, les machines exécutant Windows 2003, 2000 ou XP (aussi bien les serveurs que les clients) sont capables de mettre à jour les informations du serveur DNS.

Dans le cas d'une machine Windows XP cliente DHCP, lorsque celle-ci va envoyer une requête DHCP pour obtenir une adresse IP elle va joindre à sa requête le nom de domaine complet (FQDN). Le serveur DHCP envoie l'adresse IP au client. Une fois l'adresse IP reçue, le client DHCP envoie une mise à jour de son enregistrement de recherche directe (A) au serveur DNS et le serveur DHCP envoie une mise à jour de l'enregistrement de recherche inversée (PTR) au serveur DNS.

Dans le cas d'une machine exécutant une version antérieure de Windows 2000, celle-ci ne peut mettre à jour elle-même les enregistrements du DNS. Il est alors nécessaire de configurer le serveur DHCP afin qu'il puisse mettre à jour à la fois les enregistrements A et PTR de la machine.

5.4.4. Qu'est-ce qu'une 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 DNS principales ou secondaires configurées dans un domaine Active Directory peuvent devenir des zones DNS intégrées à Active Directory.
Les zones DNS intégrées à Active Directory présentent plusieurs avantages par rapport aux zones DNS principales ou secondaires:

- Elles permettent de stocker les données de configuration de zone dans Active Directory au lieu de les stocker dans un fichier de zone ;
- Elles permettent d'utiliser la réplication Active Directory à la place des transferts de zone ;
- Elles permettent d'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).

Ce modèle est considéré comme multi-maîtres. Tous les contrôleurs de domaine contenant les informations de cette zone DNS peuvent agir comme serveur principal et apporter des modifications à la zone.

L'intégration des zones DNS dans l'Active Directory permet de stocker les zones DNS dans l'Active Directory et ainsi bénéficier d'un certain nombre d'avantages :

Pas de point faible unique	Les mises à jour de la zone ne sont plus limitées à un seul serveur (DNS principal standard) mais peuvent être réalisées sur l'ensemble des serveurs DNS de la zone et toutes les modifications sont répliquées sur l'ensemble des serveurs DNS de la zone.
Topologie de duplication unique	La topologie de duplication est alors liée à celle de l'Active Directory ce qui permet d'éviter une configuration de réplication isolée pour le DNS.
Mises à jour dynamiques sécurisées	Il est possible de limiter les mises à jour dynamiques à un certain nombre d'ordinateurs autorisés.

> Il n'est possible de créer des zones intégrées Active Directory que sur les contrôleurs de domaine sur lesquels le service DNS a été installé.

5.4.5. Utilisation des mises à jour dynamiques sécurisées par les zones DNS intégrées à Active Directory

Pour que les mises à jour dynamiques soient possibles, il est nécessaire de configurer le serveur DNS afin qu'il les accepte. Pour configurer le serveur DNS, on dispose de trois options:

- **Non** : Interdit les mises à jour dynamiques pour la zone.
- **Oui** : Autorise les mises à jour dynamiques pour la zone.
- **Uniquement les mises à jours sécurisées** : Autorise les mises à jour dynamiques pour la zone uniquement aux ordinateurs spécifiés (Uniquement lorsque la zone est intégrée à Active Directory).

> Les mises à jour sécurisées n'autorisent que les nouveaux enregistrements issus des ordinateurs possédant un compte dans l'Active Directory et les mises à jour provenant des ordinateurs qui ont créé l'enregistrement.

Il est nécessaire de configurer le serveur DHCP pour l'enregistrement automatique sur le serveur DNS.
Il faut tout d'abord activer l'option **Mettre à jour automatiquement les informations de client DHCP dans DNS** puis choisir l'une des options suivantes :

- **Mettre à jour uniquement si un client DHCP le demande** : Le client mettra à jour l'enregistrement A et le serveur DHCP l'enregistrement PTR.
- **Toujours mettre à jour DNS** : Indique que le serveur DHCP va mettre à jour à la fois les enregistrements A et PTR.

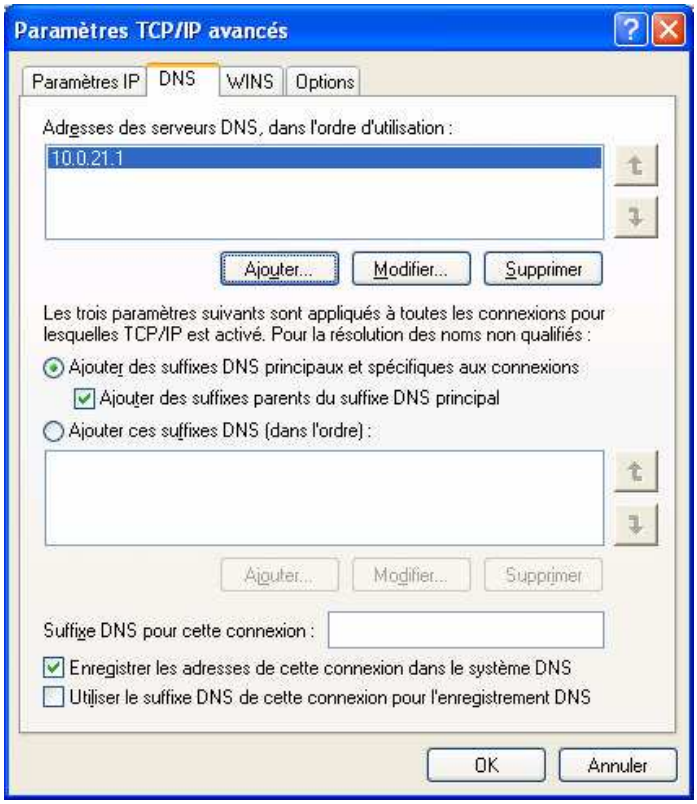
De plus, si vous disposez de clients exécutant des versions antérieures de Windows, assurez vous que l'option **Activer des mises à jour pour les clients DNS qui ne prennent pas en charge la mise à jour dynamique** est activée.

Pour finir, il faudra configurer les clients (uniquement ceux tournant sous Windows 2003) :

Dans la configuration DNS des clients, il faudra activer les options **Enregistrer les adresses de cette connexion dans le système DNS** et **Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS**.

5.5. Configuration d'un client DNS

5.5.1. Fonctionnement des 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 lorsque celui-ci ne peut pas résoudre les requêtes DNS provenant d'un client DNS.

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

Si aucun serveur DNS *préféré* n'est spécifié, alors le client DNS ne pourra 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 (16 au maximum).

5.5.2. Application des suffixes

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.

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.

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.

5.6. Délégation d'autorité pour les zones

5.6.1. Qu'est-ce que la délégation d'une zone DNS ?

Il s'agit du processus distribuant 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 stockées, distribuées et répliquées 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).

6. Gestion et analyse du système DNS

6.1. Configuration de la durée de vie

6.1.1. Fonctionnement de la valeur de durée de vie (TTL)

La valeur de durée de vie (Time to live,TTL) est un délai exprimé en secondes qui figure dans les enregistrements DNS retournés par une requête DNS. Ce délai indique aux destinataires le temps d'enregistrement d'une ressource avant suppression dans les informations DNS.

Il existe deux types de TTL dans le DNS : le TTL d'une zone qui est appliqué à tous les enregistrements créés dans cette zone et le TTL d'un enregistrement qui est appliqué à l'enregistrement en particulier.

Suivant la durée d'un TTL, deux comportements dans votre réseau se produisent :

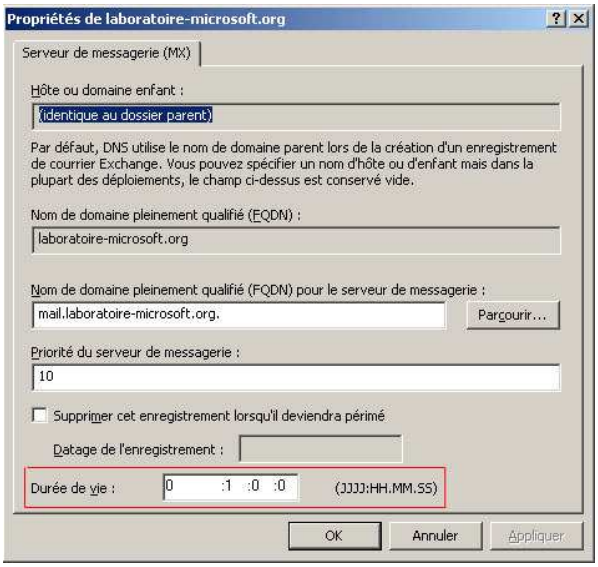
- **Si la valeur du TTL est trop petite,** le trafic des requêtes DNS va augmenter.
- **Si la valeur du TTL est trop grande,** le trafic lié aux requêtes DNS va être faible mais il y a plus de chance pour que des enregistrements obsolètes perdurent dans le cache des clients DNS.

6.1.2. Comment configurer la valeur de durée de vie

TTL d'une zone

Pour configurer le TTL d'une zone, il faut aller dans les propriétés de celle-ci, dans l'onglet **Sources de noms** et la valeur en cours apparaît dans la case : **Durée de vie pour cet enregistrement**.

TTL d'un enregistrement de ressource



Premièrement, il faut activer l'affichage détaillé dans le menu Affichage de la console DNS. Ensuite il suffit d'aller dans les propriétés de l'enregistrement en question et le champ **Durée de vie** apparaît.

6.2. Configuration des paramètres de vieillissement et de nettoyage

6.2.1. Définition 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 DNS, un client DNS s'inscrit dans la base automatiquement. A présent, si celui-ci perd sa connexion au réseau, alors son enregistrement risque de ne pas être supprimé.
Ce cas est de plus en plus fréquent avec l'utilisation de l'informatique mobile. Afin de ne pas polluer la base de données DNS, Microsoft Windows Server 2003 avec DNS est capable de supprimer des enregistrements obsolètes en recherchant dans la base de données les enregistrements de ressources dont la durée de vie est supérieure à une période spécifiée.

DNS utilise un datage qu'il attribue à chaque enregistrement et qui va être associé à 2 intervalles configurables pour déterminer s'il doit nettoyer des enregistrements ou non.

Pour se faire, le vieillissement et le nettoyage doivent être activés sur le serveur DNS et sur la zone DNS. Puis ils comportent deux options configurables :

- ***L'intervalle de non-actualisation*** correspond à la période durant laquelle le serveur DNS n'accepte pas les clients actualisant leur enregistrement. 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 que les clients actualisent leurs enregistrements. Pendant cet intervalle, les enregistrements de ressources peuvent actualiser leur datage.

Il est important de paramétrer les intervalles d'actualisation et de non-actualisation.
Il est nécessaire d'ajuster le temps de conservation des enregistrements de ressources.

Il est aussi pratique de paramétrer ces intervalles afin de réduire la réplication DNS lorsque le système DNS est intégré au service d'annuaire Active Directory.

6.2.2. Fonctionnement du vieillissement et du nettoyage

Processus d'exécution du vieillissement et du nettoyage

1. L'enregistrement est daté

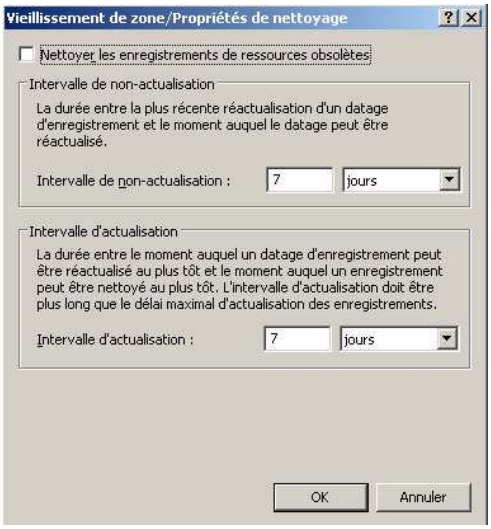
2. Le serveur DNS n'accepte pas d'actualisation pour l'enregistrement de ressource durant la période d'intervalle de non-actualisation de la zone. Mais le serveur DNS accepte la mise à jour de l'enregistrement (IP par exemple).

3. Ensuite, l'enregistrement passe dans l'intervalle d'actualisation. Au cours de l'intervalle d'actualisation, si le serveur reçoit une demande d'actualisation de l'enregistrement de ressource, il la traite et retourne à l'étape 1.

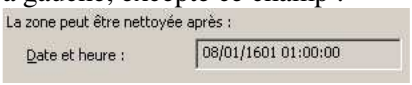
4. Lorsque, par la suite, le serveur procède au nettoyage de la zone, il compare la date en cours au cumul du datage + intervalle de non-actualisation + intervalle d'actualisation. Si la date en cours est supérieure au cumul, le serveur efface l'enregistrement. Dans le cas contraire, celui-ci est conservé.

5. Comment configurer le vieillissement et le nettoyage ?

Pour configurer le vieillissement et le nettoyage du serveur DNS, faites un clic droit dans la console DNS sur le serveur à paramétrer et cliquez sur **Définir le vieillissement/nettoyage pour toutes les zones…**

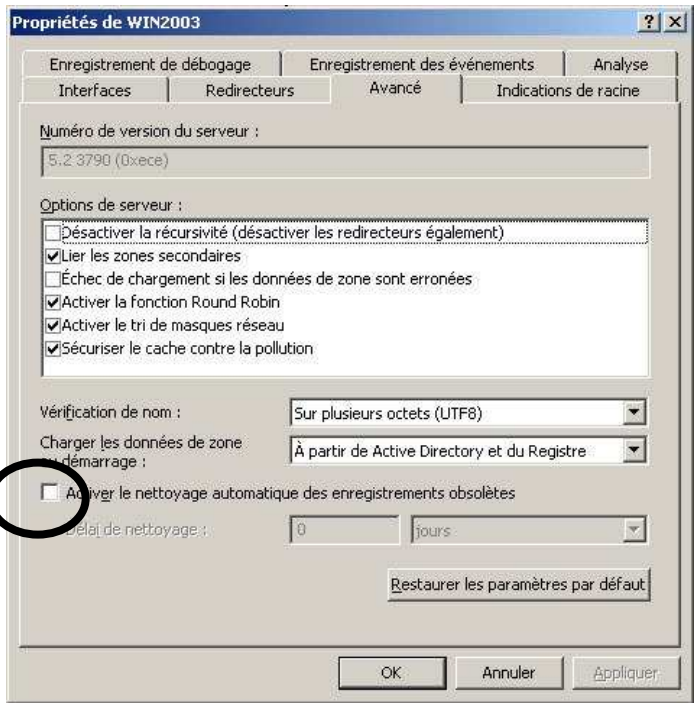


Pour configurer le vieillissement et le nettoyage pour une zone DNS, faites un clic droit sur la zone → **Propriétés**. Puis dans l'onglet général appuyer sur le bouton **Vieillissement**. La fenêtre qui s'affiche est identique à celle à gauche, excepté ce champ :



l'heure du prochain nettoyage de zone y est affichée.

Pour activer le nettoyage automatique des enregistrements obsolètes, vous devez paramétrer les propriétés du serveur DNS depuis la console DNS, dans l'onglet **avancé.** Activez cette option en bas de la fenêtre sans oublier de spécifier le délai de nettoyage.



Il est possible de lancer le nettoyage des enregistrements de ressources obsolètes en faisant un clic droit sur le serveur et en cliquant sur **Nettoyer les enregistrements de ressources obsolètes**.

6.3. Intégration du système DNS et du service WINS

6.3.1. Comment intégrer le système DNS et le service WINS

Le système DNS a pour fonction de résoudre les noms d'hôtes.
Le service WINS a pour fonction de résoudre les noms NetBIOS.
Dans certains cas, il s'avère intéressant d'utiliser la base de données WINS existante pour les recherches de noms d'hôtes, au lieu de configurer à l'identique la base de données DNS.

Grâce à l'intégration du système DNS et du service WINS, les clients DNS peuvent employer les entrées de noms NetBIOS existantes dans le service WINS pour la recherche des noms d'hôtes. Le service DNS offre en effet la possibilité d'utiliser des serveurs WINS pour rechercher des noms absents de l'espace de noms DNS en contrôlant l'espace de noms NetBIOS géré par WINS.

Pour intégrer le service WINS au système DNS, vous devez activer le paramètre dans les propriétés WINS de la zone de recherche directe ou dans l'onglet WINS-R des propriétés de la zone de recherche inversée.

Cochez la case « Utiliser la recherche directe WINS »

IMPORTANT
Activez la case à cocher « Ne pas répliquer cet enregistrement » dans le cas où les données de zone sont répliquées vers des zones secondaires hébergées sur des serveurs DNS tiers ne reconnaissant pas les enregistrements WINS ou WINS-R.
Ainsi, les enregistrements du localisateur WINS ne seront pas répliqués sur d'autres serveurs pendant les transferts de zone. Si une zone participe aux transferts de zone vers des serveurs BIND (Berkeley Internet Name Domain), l'activation de cette option est indispensable car BIND ne reconnaît pas ces types d'enregistrements WINS.

6.4. Test de la configuration du serveur DNS

6.4.1. Fonctionnement des requêtes simples et récursives

Vous pouvez tester un serveur DNS en exécutant des **requêtes simples** ou des **requêtes récursives**.

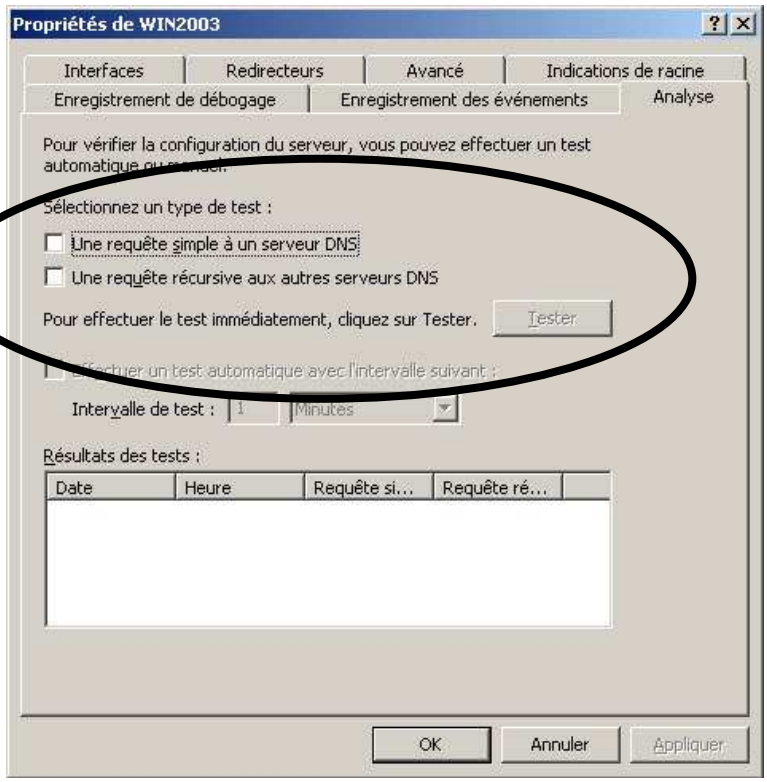
Lors de modifications de configuration du serveur DNS, ce type de requêtes permet de contrôler le fonctionnement de votre serveur. Cette mesure est utile si vous devez résoudre des problèmes liés aux requêtes DNS.

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, 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. La racine est 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 configurées correctement.

6.4.2. Comment tester la configuration du serveur DNS

Ces tests s'effectuent à partir de l'onglet **Analyse** des propriétés du serveur DNS.



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

6.5.1. Pourquoi vérifier s'il existe un enregistrement de ressource ?

La vérification de la présence d'un enregistrement de ressource est une fonction de base de l'analyse et du dépannage d'un système DNS.

Si le serveur DNS comporte des mappages nom d'hôte-adresse IP périmés, obsolètes ou incorrects, les clients ne pourront pas se connecter aux services réseaux. Vu le nombre considérable de mises à jour dynamiques, il est important de s'assurer de la validité des enregistrements.

Pour identifier les problèmes potentiels d'une solution DNS, il est possible de contrôler les points suivants :

- Enregistrements manquants
- Enregistrements incomplets
- Enregistrements mal configurés

Il existe bien des utilitaires vous permettant d'analyser, gérer et de dépanner le système DNS. Ces exécutables sont **Nslookup**, **DNSCmd** et **DNSLint**.

6.5.2. Nslookup

Nslookup est un utilitaire en ligne de commande employé pour diagnostiquer les éventuels problèmes liés à l'infrastructure DNS.

Nslookup permet d'exécuter le test de requête sur des serveurs DNS et de récupérer une liste de réponses détaillées. Ces informations sont utiles lors du dépannage de la résolution de noms ou pour vérifier que des enregistrements de ressources ont été correctement ajoutés ou mis à jour dans une zone.
Vous pouvez utiliser cette commande pour effectuer un déboguage sur d'autres incidents techniques liés au serveur DNS.

Nslookup peut être utilisé en 2 modes :

- *Interactif* : Qui permet de rester dans le prompt de la commande ce qui vous permettra d'effectuer plusieurs requêtes.

- *Non interactif* : Qui permet d'utiliser Nslookup en une simple commande. Par ce moyen, vous pouvez rediriger la sortie de la commande vers un fichier texte.

Pour que Nslookup fonctionne correctement, un enregistrement de ressource PTR doit exister pour le serveur sur lequel vous voulez effectuer une recherche. Au démarrage, Nslookup effectue une recherche inversée sur l'adresse IP du serveur qui exécute le service Serveur DNS et signale une erreur s'il est incapable de résoudre l'adresse en nom. Cette erreur ne nuit pas aux performances normales de Nslookup en ce qui concerne les diagnostics.

6.5.3. DNSCmd

DNSCmd est un outil de support DNS inclus dans les outils de support du CD-ROM Windows Server 2003 **(\Support\Tools\suptools.msi)**.
DNSCmd est une interface de ligne de commande pour la gestion des serveurs DNS. Cet outil permet d'écrire des scripts de fichiers de commandes, pour automatiser la gestion et la mise à jour des configurations existantes de serveur DNS, ou pour effectuer l'installation et la configuration de nouveaux serveurs DNS sur votre réseau.

6.5.4. DNSLint

DNSLint est un outil de support DNS inclus lui aussi dans les outils de support du CD-ROM Windows Server 2003. Cet utilitaire Microsoft Windows peut exécuter une série de requêtes, facilitant ainsi le diagnostic des problèmes courants liés à la résolution de noms DNS.

Afin de faciliter le diagnostic et la résolution des problèmes qu'entraînent des enregistrements DNS manquants ou incorrects, il est utile de s'assurer de la cohérence d'un ensemble particulier d'enregistrements DNS sur plusieurs serveurs DNS.

Par exemple : Certains clients ont des difficultés à ouvrir une session sur le domaine, vérifiez si les enregistrements SRV, utilisés par les clients pour rechercher les serveurs LDAP **(Lightweight Directory Access Protocol)** et **Kerberos,** sont disponibles et exacts. Vous déterminerez ainsi plus facilement si les paramètres DNS sont à l'origine du problème.

DNSLint possède trois fonctions qui vérifient les enregistrements DNS et génèrent un rapport en HTML (Hypertext Markup Language).

- **DNSLINT /d** diagnostique les causes possibles de délégations inappropriées et d'autres problèmes DNS apparentés.
    - La délégation inappropriée survient si un sous-domaine DNS est configuré pour utiliser un serveur DNS qui soit n'existe pas, soit ne fait pas autorité pour ce sous-domaine.

- **DNSLINT /ql** vérifie un ensemble défini par l'utilisateur d'enregistrements DNS sur plusieurs serveurs DNS.

- **DNSLINT /ad** vérifie les enregistrements DNS spécifiquement employés pour la réplication Active Directory.

6.5.5. Comment vérifier la présence d'un enregistrement de ressource à l'aide de Nslookup, de DNSCmd et de DNSLint

Vous pouvez avoir recours à l'un des trois utilitaires DNS (Nslookup, DNSCmd et DNSLint) pour effectuer des tâches d'analyse, comme vérifier l'existence d'un enregistrement de ressource. Par défaut, Nslookup est disponible dans Windows Server 2003. Quant à DNSCmd et DNSLint, ils doivent être installés à partir des outils de support du CD-ROM Windows Server 2003.

Pour pouvoir utiliser les utilitaires DNSCmd et DNSLint, il faut installer **suptools.msi** qui se trouve sur le Cd-Rom de Microsoft Windows Server 2003 dans le dossier /Support/Tools.

Exemple d'utilisation de ces commandes :

- DNSCmd [*nom du serveur*] **/enumzones**: Permet d'afficher la liste complète des zones configurées sur le serveur DNS.

- DNSCmd [*nom du serveur*] **/zoneinfo** [*zone*] : Permet d'afficher les informations d'une zone spécifique.

6.6. Analyse des performances du serveur DNS

6.6.1. Principes d'analyse des performances du serveur DNS à l'aide de la console de performances

Les serveurs DNS ont une importance capitale dans la plupart des environnements, c'est pourquoi l'analyse de leurs performances procurent des avantages certains dans la stratégie d'optimisation de votre infrastructure réseau.

- L'analyse vous donne des informations utiles pour prévoir, estimer et optimiser les performances du serveur DNS.

- L'analyse vous facilite le dépannage des serveurs DNS victimes d'une baisse de performances.

Il est recommandé d'analyser d'une part les phases critiques de l'activité du système DNS, comme les mises à jour dynamiques, les notifications, les transferts de zone complets et incrémentiels, les requêtes, et d'autre part l'intégrité du serveur DNS.

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 de 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 liée aux requêtes imposées 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, cela veut dire que 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 revoir la configuration des transferts de zone.

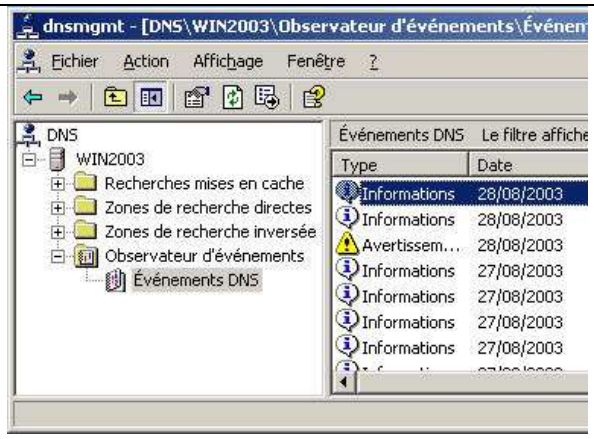
6.6.2. Qu'est-ce qu'un journal des événements DNS ?

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'erreurs du service DNS y sont également enregistrés, par exemple lorsque le serveur démarre et qu'il y a une erreur lors des transferts de zone ou encore lorsque les informations de zone nécessaires au démarrage ne sont pas disponibles.

6.6.3. Qu'est-ce que l'enregistrement de déboguage DNS ?

L'enregistrement de déboguage DNS est un outil journal facultatif pour DNS, qui stocke les informations DNS que vous sélectionnez. Il ne faut pas oublier que l'enregistrement dans un journal nécessite des ressources du serveur, l'enregistrement de déboguage 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.

Vous pouvez capturer un grand nombre de données statistiques DNS à l'aide de l'outil Performances qui vous permet de créer des graphiques. Si vous voulez obtenir des informations encore plus spécifiques, vous pouvez activer l'enregistrement de déboguage DNS, lequel permet de collecter des données DNS spécifiques dans le fichier DNS.Log.

Par exemple, si vous voulez connaître les types de requêtes envoyées par un ordinateur au serveur DNS, vous pouvez configurer l'enregistrement de déboguage DNS pour qu'il recueille uniquement les informations relatives aux requêtes DNS entrantes utilisant les protocoles UDP (User Datagram Protocol) ou TCP (Transmission Control Protocol) à partir d'une adresse IP (Internet Protocol) particulière.

L'enregistrement de déboguage se poursuit jusqu'à ce que la taille de journal spécifiée soit atteinte ou que le lecteur sur lequel se trouve le fichier journal vienne à manquer d'espace disponible. Une fois la limite en terme de taille de fichier est 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.

ATTENTION ! : Le mode déboguage pour DNS altère fortement la disponibilité des ressources de votre système, processeur et mémoire vive. Le temps de réponse pour les requêtes des clients DNS distants sera alors augmenté.

7. Résolution de noms NetBIOS à l'aide du service WINS

Le service WINS a été créé dans le but de limiter le trafic de diffusion et de permettre la résolution de noms NetBIOS sur plusieurs segments de réseau.

Dans Windows 2003, le principal moyen utilisé pour la résolution de noms est le système DNS. Pour les ordinateurs clients démarrant des versions de Windows antérieures à Windows 2000, XP ou 2003, un serveur WINS leur permettra de communiquer efficacement. (ex : Windows NT4)

7.1. Installation et configuration d'un serveur WINS

7.1.1. Composants du service WINS

Le système *WINS* complet de Windows Server 2003 comprend les composants suivants :

- *Serveur WINS* : Ordinateur qui traite les requêtes d'inscription de noms provenant des clients WINS, inscrit les noms et adresses IP du client. Le serveur WINS répond aux requêtes de noms NetBIOS soumises par les clients. Le serveur WINS renvoie ensuite l'adresse IP d'un nom demandé, si ce dernier figure dans la base de données du serveur.

- *Base de données WINS* : La base de données WINS stocke et réplique les mappages des noms NetBIOS aux adresses IP d'un réseau.

- *Client WINS* : Ordinateurs que vous pouvez configurer pour utiliser directement un serveur WINS ; ces ordinateurs possèdent généralement plusieurs noms NetBIOS qu'ils doivent inscrire pour pouvoir être utilisés sur le réseau.

- *Agents proxy WINS* : Ordinateur qui contrôle la diffusion des requêtes de noms et répond aux requêtes clientes lorsque les noms ne figurent pas sur le sous-réseau local. Le proxy communique avec un serveur WINS pour résoudre les noms, puis les met en cache pour une période donnée.

7.1.2. Présentation d'un type de nœud NetBIOS

Les types de nœuds NetBIOS permettent à un administrateur de configurer l'ordre et la méthode utilisée par un client lors de la résolution de noms NetBIOS en adresses IP.

Il y a plusieurs possibilités en fonction du type de nœud :

- **Nœud B** (broadcast-node) : Utilise la diffusion pour l'enregistrement et la résolution de noms.
- **Nœud P** (Peer-to-peer-node) : Utilise un serveur de noms (WINS) pour la résolution.
- **Nœud M** (mixed-node) : Méthode B et P : si aucun résultat par la méthode B (méthode de résolution par défaut), utilisation de la méthode P.

- **Nœud H** (Hybrid-node) : Méthode B et P : si aucun résultat par la méthode P (méthode de résolution par défaut), utilisation de la méthode B.

Windows Server 2003 et Windows XP sont configurés par défaut avec la configuration de type nœuds B.

Lorsqu'un ordinateur exécutant Windows XP, Windows Server 2003 ou Windows 2000 est configuré avec les adresses de serveurs WINS pour la résolution de noms, il utilise automatiquement le nœud. Vous pouvez utiliser les options du protocole DHCP (Dynamic Host Configuration Protocol) pour attribuer ce type de nœud.

7.1.3. Comment un client WINS inscrit et libère des noms NetBIOS

Au démarrage de l'ordinateur, le service **NetBT** sur le protocole TCP/IP va envoyer une demande d'enregistrement du nom NetBIOS à un serveur WINS. Dans le cas où le nom NetBIOS serait déjà approprié, l'ordinateur ne pourra pas utiliser le protocole NetBIOS pour communiquer.

Un nom NetBIOS est inscrit de façon temporaire sur le serveur WINS. Le serveur WINS envoie un message au client lors de son inscription pour l'informer de la durée de l'enregistrement acquis (TTL, Time to Live). Ce dernier devra renouveler son enregistrement à la fin du TTL afin de le conserver.

Si le processus de renouvellement n'est pas effectué dans le temps imparti, l'inscription sur le serveur WINS va être supprimée. Le renouvellement est donc nécessaire pour ce type d'enregistrement contrairement aux enregistrements statiques qui n'utilisent pas le TTL.

La durée du TTL par défaut est de 6 jours. Un renouvellement d'un enregistrement à donc lieu au bout de 3 jours car le client WINS tente son renouvellement à 50% de l'écoulement du TTL.

7.1.4. Fonctionnement de la prise en charge du traitement en rafale

Le traitement de réponse de type rafale est utilisé lorsque le nombre de tentatives simultanées excède la taille de la file d'attente de traitement (**par défaut : 500**). Le principe de ce traitement est de répondre superficiellement aux requêtes clients (par une inscription positive), ce qui permet au client d'utiliser le protocole NetBIOS pour la communication. Afin d'éviter des problèmes d'enregistrements non achevés correctement, le serveur WINS définit une courte durée de vie afin d'effectuer une inscription complète une fois le trafic WINS revenu à la normale.

Par exemple, lorsque le courant est rétabli après une coupure, de nombreux utilisateurs démarrent et inscrivent simultanément leur nom sur le réseau, ce qui engendre un trafic WINS très dense. Avec la prise en charge du traitement en rafale, un serveur WINS peut répondre positivement aux requêtes des clients, avant même de traiter et d'entrer physiquement ces mises à jour dans la base de données du serveur WINS.

7.1.5. Comment un serveur WINS résout les noms NetBIOS

Pour la famille Windows Server 2003, Windows XP et Windows 2000, le service WINS utilise les options suivantes pour résoudre un nom une fois la requête NetBIOS émise :

1. Le client WINS contacte le premier serveur WINS à trois reprises pour résoudre le nom à l'aide du service WINS.

2. Si le premier serveur WINS ne répond pas, le client contacte d'autres serveurs WINS disponibles jusqu'à ce qu'il obtienne une réponse.
3. Si un serveur WINS résout le nom NetBIOS, l'adresse IP est renvoyée au client. Après avoir reçu la réponse, le client utilise cette adresse pour se connecter à la ressource souhaitée.
4. Si aucun serveur WINS ne peut résoudre le nom NetBIOS, le processus de résolution se poursuit en dehors du service WINS. Le client avec nœud H tente une diffusion. Si la diffusion échoue, le client parcourt son fichier Lmhosts local.

7.1.6. Comment installer le service WINS

Pour installer le service WINS, vous pouvez passer par la console habituelle d'**Ajout/Suppression de programmes** pour **Ajouter ou supprimer des composants Windows**. Ensuite dans la rubrique **Services de mise en réseau**, il faut cocher **Service WINS**.
Vous pouvez passer aussi par la console **Gérer votre serveur** pour y ajouter le rôle de serveur WINS. Cette console se trouve dans les outils d'administration.

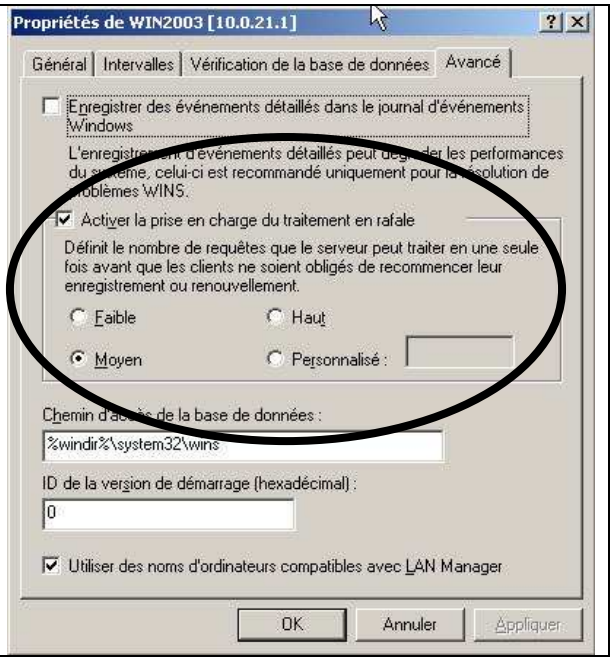
7.1.7. Comment configurer la prise en charge du traitement en rafale

Vous pouvez configurer le niveau de prise en charge du traitement en rafale utilisé par le serveur et adapter ainsi la taille de la file d'attente de transmission en rafale pour des rafales faibles, moyennes ou élevées. La prise en charge du traitement en rafale est activée par défaut et la file d'attente de transmission en rafale est définie sur le niveau moyen.

Pour configurer cette prise en charge, il faut aller dans l'onglet **Avancé** des propriétés du serveur WINS.

Correspondance Niveau et requêtes :

- Faible → 300
- Moyen → 500
- Haut → 1000
- Personnalisé → entre 50 et 5000



7.2. Gestion des enregistrements dans le serveur WINS

7.2.1. Présentation d'un enregistrement client

Un enregistrement client est une entrée contenue dans la base de donnée WINS qui contient des informations détaillées concernant les services NetBIOS exécutés sur le client comme :

- Nom d'enregistrement : Nom NetBIOS inscrit
- Type : Type de service

- Adresse IP
- Etat : Actif, libéré ou désactivé
- Statique : Indique si le mappage est statique
- Propriétaire : Le serveur WINS d'où provient l'entrée
- Version : Numéro unique affecté par le serveur lors de l'enregistrement (utile pour la réplication)
- Expiration

7.2.2. Présentation d'un mappage statique

Un mappage statique est un enregistrement client entré manuellement dans la base de données WINS par l'administrateur afin d'enregistrer les services des clients non-WINS (ex : UNIX).

7.2.3. Comment ajouter une entrée de mappage statique

Pour ajouter une entrée de mappage statique, il est nécessaire de posséder trois éléments concernant ce mappage :

- Nom NetBIOS
- Type de nom (unique, groupe, nom de domaine, …)
- Adresse IP

L'ajout se trouve dans la console WINS : Clic droit sur le dossier *Inscription actives* du serveur WINS \ ***Nouveau mappage statique…***

7.2.4. Méthodes de filtrage et d'affichage des enregistrements du service WINS

Les méthodes de filtrage et d'affichage des enregistrements du service permettent d'afficher l'essentiel des informations nécessaires lors d'une administration à distance par exemple, ou d'isoler un problème plus rapidement.

Lors de la création d'un filtre de recherche, vous pouvez choisir entre 3 catégories de filtres :

- ***Mappage des enregistrements*** **:** Recherche à partir d'un nom NetBIOS complet ou non, et/ou une adresse IP avec ou sans masque de sous réseau.

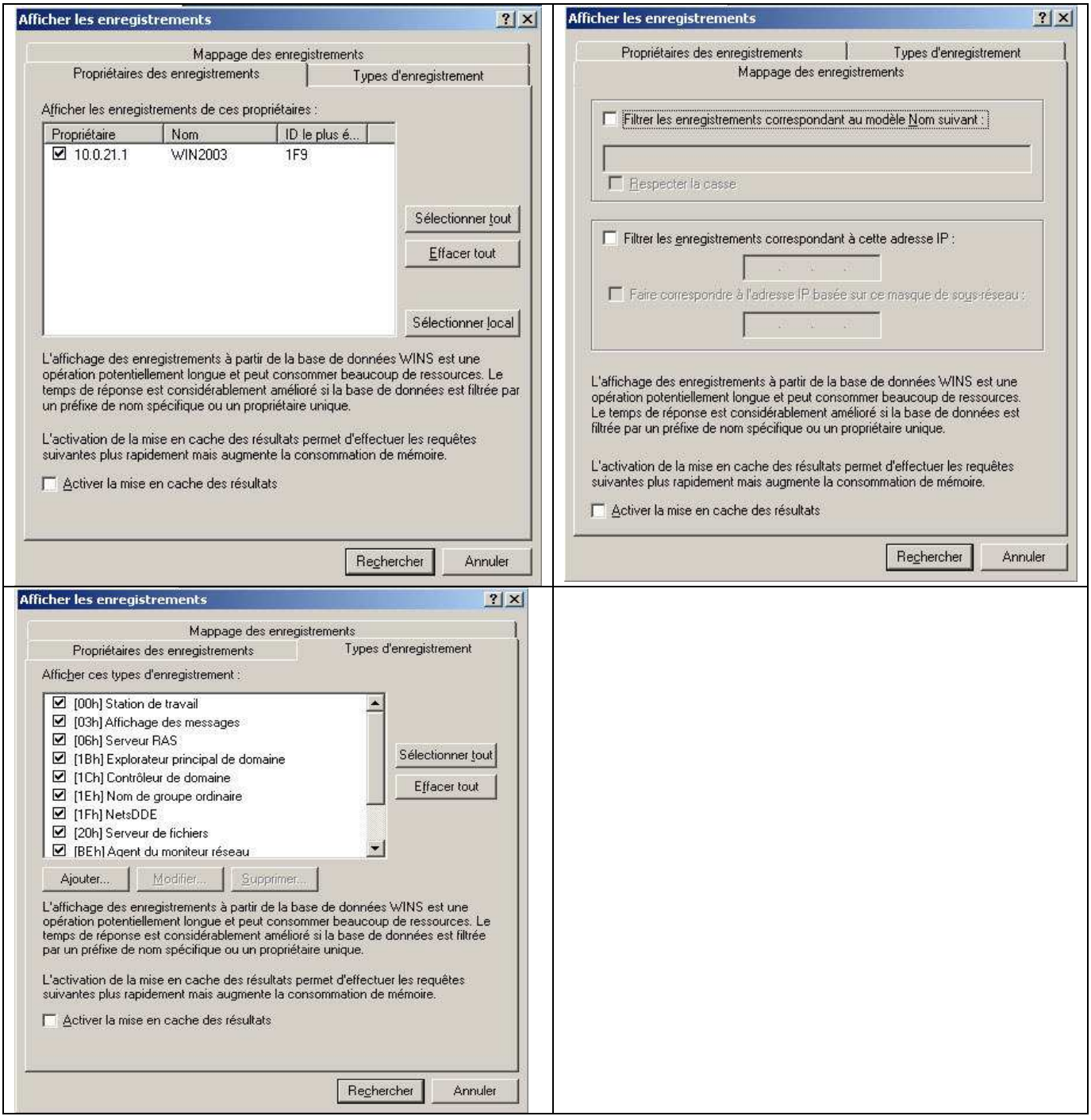
- ***Propriétaires des enregistrements*** : Recherche à partir d'enregistrements dans les enregistrements de noms d'un ou de plusieurs propriétaires d'enregistrements de noms.

- ***Types d'enregistrement*** : Recherche à partir d'enregistrements sur un ou plusieurs types d'enregistrements, grâce au suffixe du nom NetBIOS.

7.2.5. Comment filtrer les enregistrements WINS

Pour accéder aux différentes catégories de recherche, il faut faire un clic droit sur le dossier *Inscriptions actives* puis cliquer sur ***Afficher les enregistrements…***

Une fois le filtre configuré, il ne reste plus qu'à appuyer sur **rechercher**.



7.3. Configuration de la réplication WINS

7.3.1. Fonctionnement de la réplication WINS

La réplication WINS consiste à mettre à jour les données WINS entre plusieurs serveurs afin de synchroniser les données. Lorsqu'un client WINS veut résoudre un nom NetBIOS, il peut passer par n'importe quel serveur du même réseau.

Lorsqu'un réseau utilise plusieurs serveurs WINS, chaque serveur est configuré comme partenaire émetteur ou comme partenaire émetteur/récepteur d'au moins un autre serveur WINS. La configuration par défaut des partenaires de réplication WINS se fait par émission/réception. Cependant, vous pouvez modifier cette configuration en fonction des exigences de votre environnement réseau.

7.3.2. Fonctionnement de la réplication par émission

Un partenaire **Emetteur** avertit ses partenaires de réplication lorsque le nombre de modifications dans sa base de données atteint un seuil que vous pouvez configurer. Ce type de partenaire est utilisé dans le cas de liaisons rapides

7.3.3. Fonctionnement de la réplication par réception

Un partenaire **Collecteur** demande les copies des nouvelles entrées de la base de données à ses partenaires de réplication à intervalles réguliers. Vous pouvez configurer cet intervalle. Ce type de partenaire est généralement utilisé dans le cas de liaisons lentes.

7.3.4. Présentation de la réplication par émission/réception

Un partenaire **Emetteur/Collecteur** demande la copie des nouvelles entrées à intervalles réguliers et avertit ses partenaires de réplication lorsque le nombre de modifications atteint un seuil. Par défaut un serveur WINS est configuré en partenaire Emetteur/Collecteur.

7.3.5. Propriétés des partenaires de réplication WINS

Activer la configuration automatique des partenaires :

Cette option permet à un serveur WINS de configurer automatiquement les autres serveurs WINS comme ses partenaires de réplications.

Vous pouvez paramétrer la configuration automatique des partenaires. Le serveur WINS est alors activé pour contrôler les annonces de multi-diffusions provenant d'autres serveurs WINS et pour effectuer automatiquement les étapes de configuration suivantes.

Lorsque vous configurez l'option « **Activer la configuration automatique des partenaires** », le serveur WINS :

- ajoute l'adresse IP des serveurs découverts à sa liste de serveurs partenaires de réplication
- configure les serveurs découverts à la fois comme partenaires émetteurs et récepteurs
- configure la réplication par réception à des intervalles de 2 heures sur les serveurs découverts

Activer les connexions permanentes :

Généralement, le serveur WINS se déconnecte une fois la réplication effectuée. Lors d'utilisation de liaisons fixes entre les serveurs, il est préférable et plus rapide de rendre ces connexions permanentes. Il ne reste plus qu'à activer le seuil de réplication à 0 et la convergence de base de données sera instantanée.

Activer l'option Remplacer les mappages statiques uniques pour ce serveur (migration) :

Contrairement aux mappages dynamiques qui sont automatiquement supprimés du service WINS au bout d'un certain temps, les mappages statiques peuvent rester inscrits dans la base de données WINS de façon permanente ou jusqu'à ce que l'administrateur réseau les supprime.
Si, au cours d'une mise à jour, le service WINS reçoit une entrée statique et une entrée dynamique portant le même nom, **il conserve par défaut l'entrée de type statique**. Cependant, vous pouvez utiliser le paramètre Remplacer les mappages statiques uniques pour ce serveur pour modifier ce comportement.
Vous pouvez configurer ce paramètre uniquement à partir de la boîte de dialogue des propriétés de l'objet Partenaire de réplication dans la console WINS.

7.3.6. Comment configurer la réplication WINS

Par défaut, les partenaires de réplication WINS sont configurés en tant que partenaires émetteurs/récepteurs. Pour modifier ce paramètre, il faut aller dans la console WINS puis faire un clic droit sur le dossier *Partenaire de réplication* du serveur en cours pour appuyer sur ***Nouveau partenaire de réplication***. Ensuite il ne reste plus qu'à spécifier l'adresse d'un autre serveur WINS valide pour la réplication.

Il est possible de modifier le ***type de partenaire de réplication*** (Emission, Collecte ou Emission/Collecte) dans l'onglet *Avancé* des propriétés du serveur se trouvant dans les partenaires de réplication.

7.4. Gestion de la base de données WINS

7.4.1. Pourquoi sauvegarder une base de données WINS ?

Dans le cas où, il n'est plus possible d'altérer une base de données défaillante à cause d'un virus ou autres problèmes similaires, vous pouvez supprimer la base WINS et en restaurer une « propre ».

La console de gestion WINS fournit des outils de sauvegarde avec lesquels vous pouvez sauvegarder la base de données WINS. Une fois que vous avez spécifié un répertoire de sauvegarde pour la base de données, le service WINS effectue des sauvegardes complètes de la base de données **toutes les 24 heures, par défaut**. La console de gestion WINS fournit également une option de sauvegarde que vous pouvez utiliser pour restaurer une base de données de serveur en cas de défaillance.

Pour restaurer la base :

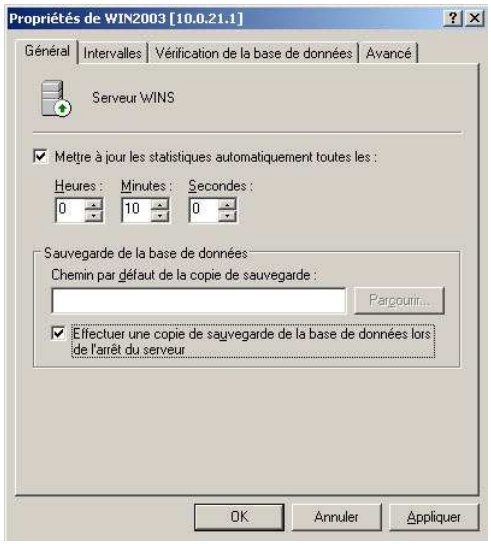
- Arrêtez le service WINS,
- Supprimez tous les fichiers de la base de données actuelle
- Effectuez la restauration à partir de la sauvegarde
- Redémarrez le service.

Attention ! : La base de données à restaurer doit être dans le répertoire de sauvegarde par défaut.

7.4.2. Comment sauvegarder et restaurer une base de données WINS

Pour sauvegarder la base WINS, il faut au préalable spécifier le répertoire de sauvegarde et faire une première sauvegarde manuelle.

Pour spécifier le répertoire de sauvegarde, il faut faire un clic droit sur le serveur WINS (à partir de la console WINS) pour afficher les propriétés de celui-ci. Ensuite dans l'onglet **Général**, il faut entrer le chemin de la sauvegarde dans la zone **Chemin par défaut de la copie de sauvegarde**. Lorsque le service WINS sauvegarde la base de données du serveur, il crée un dossier ***Wins_bak\New*** dans le dossier de sauvegarde spécifié.



Pour initier la première sauvegarde, il suffit de cocher « **Effectuer une copie de sauvegarde de la base de données lors de l'arrêt du serveur »** si nécessaire.

Vous pouvez faire une sauvegarde manuelle en faisant un clic droit sur le serveur WINS puis **Sauvegarder la base de données…**

7.4.3. Présentation de la suppression simple et de la désactivation d'enregistrements

Il est possible de récupérer de la place dans la base de données WINS en supprimant des enregistrements obsolètes. Il existe pour cela plusieurs méthodes disponibles à partir de la console WINS :

- **Suppression simple d'enregistrements** : Il suffit de supprimer des enregistrements que l'administrateur trouve obsolètes sur le serveur. Si vous possédez plusieurs serveurs, il faut veiller à supprimer les enregistrements obsolètes sur les autres serveurs, auquel cas les enregistrements seront de nouveau répliqués.

- **Désactivation d'enregistrement** : Le serveur WINS modifie l'état de l'enregistrement en le mettant **désactivé**. Une fois un enregistrement désactivé, le serveur WINS ne peut plus le résoudre lors de requêtes clientes. Ensuite lors de la réplication, le serveur va indiquer aux autres serveurs le nouvel état de l'enregistrement qui va ensuite expirer et être supprimé.

7.4.4. Comment supprimer un enregistrement WINS

Il y a donc 2 possibilités de suppression d'un enregistrement : la suppression simple et la désactivation.

Pour choisir l'un des deux lors de la suppression d'un enregistrement, il faut faire un clic droit sur l'enregistrement en question puis **supprimer**.

Une boîte de dialogue apparaît alors :

7.4.5. Présentation du compactage dynamique et du compactage hors connexion

Le compactage permet de réorganiser la base de données afin de récupérer la place des enregistrements supprimés.

Dans Windows Server 2003, le service WINS effectue un compactage Jet dynamique de la base de données WINS pendant que le serveur est en ligne. De ce fait, le compactage manuel est beaucoup plus rapide.

Même si le serveur utilise le compactage Jet dynamique, le compactage manuel (jetpack.exe) permet une meilleure récupération d'espace et doit être fait régulièrement. Lors d'un compactage manuel, il suffit de noter la taille du fichier de la base WINS **(%systemroot%\System32\Wins\Wins.mdb)** avant et après le compactage afin de déterminer l'intérêt du compactage manuel et de définir la fréquence d'utilisation de ce procédé.

7.4.6. Comment compacter une base de données WINS

Donc par défaut la base est automatiquement compactée en ligne mais vous pouvez la compactée manuellement en mode hors connexion.

Pour compacter la base de données WINS hors connexion :

1. Arrêtez le service WINS en utilisant la commande **net**. À l'invite de commandes, tapez **net stop wins**.

2. À partir du répertoire *%systemroot%\System32*, exécutez l'utilitaire de ligne de commande jetpack.exe à l'aide de la syntaxe de commande suivante : **jetpack** %systemroot%**\System32\Wins\Wins.mdb** *Nom_Temporaire*.**mdb** (où *Nom_T*emporaire est le nom que vous attribuez au fichier). Cette procédure compacte le contenu du fichier Wins.mdb dans Nom_Temporaire.mdb, copiez le fichier temporaire dans Wins.mdb et supprimez le fichier temporaire.

3. Redémarrez le service WINS en utilisant la commande **net**. À l'invite de commandes, tapez **net start wins**.

7.4.7. Comment fonctionne le nettoyage

Le nettoyage est le processus consistant à supprimer des entrées de base de données WINS qui ont expirées.

Le nettoyage permet de maintenir des informations d'état correctes dans la base de données en contrôlant chaque enregistrement appartenant au serveur WINS, en comparant le datage de l'enregistrement avec l'heure actuelle, puis en modifiant l'état des enregistrements qui ont expirés. Par exemple, le nettoyage modifie l'état d'un enregistrement de l'état « actif » à l'état « libéré ».

Le processus de nettoyage intervient automatiquement à des intervalles définis par la relation entre les configurations d'intervalle de renouvellement et d'extinction. Configurez les propriétés suivantes pour définir cette relation.

Le nettoyage est effectué conformément à une planification définie comme suit :

1. Le minuteur de nettoyage est activé au démarrage du serveur et correspond à la moitié de l'intervalle de renouvellement.

2. Les noms actifs appartenant au serveur WINS et pour lesquels l'intervalle de renouvellement a expiré sont marqués comme étant libérés.

3. Les noms libérés appartenant au serveur WINS et pour lesquels l'intervalle d'extinction a expiré sont marqués pour suppression.

4. Les noms marqués pour suppression et pour lesquels le délai d'extinction a expiré sont supprimés de la base de données.

5. Les noms marqués pour suppression, répliqués à partir d'autres serveurs et pour lesquels le délai d'extinction a expiré sont supprimés de la base de données.

6. Les noms actifs répliqués à partir d'autres serveurs et pour lesquels l'intervalle de vérification a expiré sont revalidés.

7. Les noms marqués pour suppression répliqués à partir d'autres serveurs sont supprimés de la base de données.

7.4.8. Comment nettoyer la base de données WINS

Pour configurer les intervalles, il faut aller dans l'onglet intervalles des propriétés du serveur WINS :

Intervalles	Description de l'intervalle
Intervalle de renouvellement	Fréquence à laquelle un client WINS renouvelle son inscription de nom auprès du serveur WINS. La valeur par défaut est de six jours.
Intervalle d'extinction	Intervalle entre l'heure à laquelle une entrée est marquée comme libérée (plus inscrite) et l'heure à laquelle elle est marquée comme éteinte. La valeur par défaut est de quatre jours.
Délai d'extinction	Intervalle entre l'heure à laquelle une entrée est marquée comme éteinte et l'heure à laquelle elle est effectivement supprimée de la base de données WINS. La valeur par défaut est la même que celle de l'intervalle de renouvellement et ne peut pas être inférieure à 24 heures.
Intervalle de vérification	Intervalle après lequel le serveur WINS vérifie que les noms dont il n'est pas propriétaire (noms dupliqués à partir d'autres serveurs WINS) sont encore actifs. La valeur minimale est de 24 jours.

Enfin pour nettoyer la base de données WINS, il suffit de faire un clic droit sur le serveur WINS puis **Nettoyer la base de données.**

7.4.9. Présentation de la vérification de la cohérence d'une base de données WINS

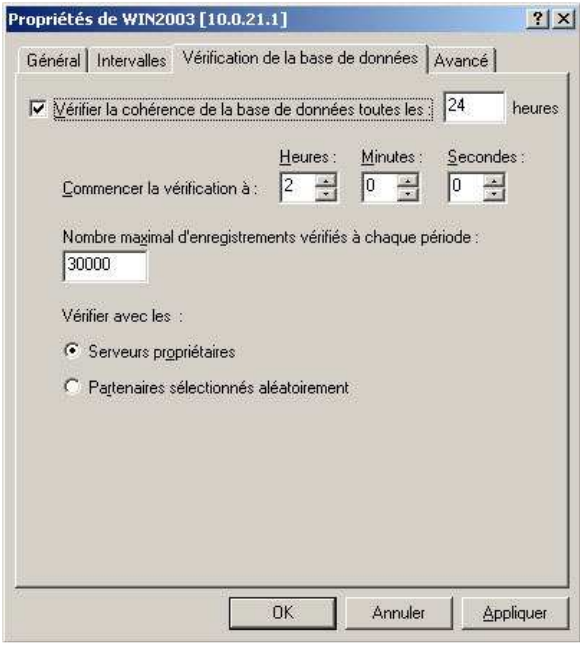
La vérification de la cohérence d'une base de données permet d'obtenir une garantie des informations contenues dans la base auprès des propriétaires et auprès des autres serveurs WINS.
Ce processus permet de garantir l'intégrité des données.

7.4.10. Comment vérifier la cohérence d'une base de données WINS

Vérifier la cohérence est une opération qui peut être effectuée régulièrement pour assurer la cohérence mais il faut noter que ce processus influe beaucoup sur la charge réseau. Il faut donc veiller à effectuer cette opération pendant les heures creuses de l'activité de votre réseau.

Voici l'onglet **Vérification de la base de données** des propriétés du serveur qui va permettre de spécifier l'horaire, la fréquence de réplication, le nombre d'enregistrements maximum et avec qui :

- **Serveur propriétaire :** Vérifie par rapport au serveur qui contient l'enregistrement (propriétaire).
- **Partenaires sélectionnés aléatoirement :** Vérifie par rapport à un partenaire de réplication choisi aléatoirement.



Il est possible de lancer une vérification de la cohérence manuellement. Pour ce faire, il suffit de faire un clic droit sur le serveur WINS puis choisir entre **Vérifier la cohérence de la base de données…** et **Vérifier la cohérence des numéros de versions…**

7.4.11. Instructions concernant le retrait d'un serveur WINS

Vous pouvez retirer (supprimer) un serveur WINS pour réduire ou supprimer l'utilisation du service WINS au sein de votre réseau.

Avant de retirer un serveur WINS de votre réseau, vous devez vous assurer que les clients de ce serveur peuvent interroger un autre serveur WINS afin d'effectuer de la résolution de noms.

Si vous souhaitez retirer tous les serveurs WINS de votre réseau, il faut installer et configurer le service DNS comme étant votre service de résolution de noms principal et configurer tous les clients pour qu'ils l'utilisent.

7.4.12. Comment désinstaller un serveur WINS d'une infrastructure réseau

Procédure pour désinstaller un serveur WINS d'une infrastructure réseau :

1. Dans l'arborescence de la console WINS, clic droit sur **Inscriptions actives**.
2. Cliquez sur **Supprimer le propriétaire.**
3. Dans la boîte de dialogue Suppression d'un propriétaire, cliquez sur l'adresse IP du serveur WINS que vous souhaitez retirer.
4. Sélectionnez **Répliquer la suppression sur les autres serveurs WINS (désactiver)** et cliquez sur **OK**.
5. Dans l'arborescence de la console, clic droit sur **Partenaires de réplication.**
6. Cliquez sur **Répliquer maintenant**.
7. Après avoir vérifié que les enregistrements désactivés lors de l'étape 4 ont bien été répliqués vers d'autres serveurs partenaires, arrêtez le service WINS et supprimez-le du serveur retiré.

8. Protection du trafic réseau à l'aide de la sécurité IPSec et de certificats

8.1. Implémentation de la sécurité IPSec

Pour vous aider dans la compréhension de ce module, nous vous invitons à consulter l'article de Sammy POPOTTE sur le site du laboratoire SUPINFO des technologies Microsoft à l'adresse suivante : **http://www.laboratoire-microsoft.org/articles/network/ipsec/**

8.1.1. Qu'est-ce que la sécurité IPSec ?

Le protocole IPSec est une surcouche réseau qui permet d'authentifier, vérifier ou crypter tout trafic transitant sur le réseau.

La sécurité IPSec permet de protéger les données qui transitent sur le réseau en respectant la *stratégie IPSec*. L'administrateur définit un ensemble de règles qui définissent si un paquet doit être crypté et/ou signé numériquement.
Ce processus est transparent pour les utilisateurs et indépendant du type de données à acheminer sauf pour les données de type diffusion, multi-diffusions et paquets Kerberos qui ne peuvent être cryptés.

La sécurité IPSec présente les avantages suivants :

- Authentification mutuelle avant et pendant les communications.
- Confidentialité grâce au cryptage du trafic IP et à l'authentification numérique des paquets.
- Intégrité du trafic IP en rejetant tout trafic modifié (anti-rejeu).
- Protection contre les attaques de relecture.

8.1.2. De quelle manière la sécurité IPSec protège-t-elle le trafic ?

Comment fonctionne la sécurité IPSec d'une communication entre 2 postes :

1. La configuration IPSec est définie par une stratégie locale ou une stratégie de groupe dans l'Active Directory qui est transmise aux postes clients. Ces stratégies définissent quelles sont les associations de protocole de cryptage et de méthode d'authentification qui vont être utilisées par le client.

2. Le module IKE vérifie l'association de sécurité négociée grâce au protocole **ISAKMP** (Internet Security Association and Key Management Protocol) et au protocole **Oakley Key Determination Protocol**.
   Le module IKE ne peut pas établir d'association de sécurité si les 2 entités utilisent des méthodes d'authentification différentes (Certification et Kerberos par exemple).

3. Une fois l'association établie, le pilote IPSec crypte ou signe, suivant la stratégie employée, le trafic voulu.

8.1.3. Qu'est-ce qu'une stratégie de sécurité IPSec ?

La stratégie IPSec définit le comportement de la sécurité IPSec. Une stratégie est fondée sur l'application d'une ou plusieurs règles. Cependant, seule une stratégie peut s'appliquer à un poste.

Une règle est composée des éléments suivants :

- Un filtre : Spécifie le type de trafic (ex : http ou FTP)
- Une action de filtrage : Spécifie l'action à exécuter sur le trafic rencontré par le filtre (ex : Bloquer, crypter…)
- Une méthode d'authentification : Kerberos, certificats ou clé pré-partagée.

Stratégie par défaut disponible depuis Windows 2000 :

Client (en réponse seule) : L'ordinateur utilisera IPSec uniquement si l'ordinateur distant lui en fait la demande.

Serveur (demandez la sécurité) : L'ordinateur tentera d'imposer IPSec, mais si l'ordinateur distant ne supporte pas IPSec, alors la communication se fera normalement.

Sécuriser le serveur (nécessite la sécurité) : L'ordinateur utilisera toujours IPSec. Si l'ordinateur distant ne peut pas utiliser IPSec, la communication ne se fera pas.

8.1.4. Fonctionnement conjoint des stratégies IPSec

Une stratégie n'est pas à considérer comme une entité seule lors de communications avec d'autres postes. Pour que deux postes négocient une association de sécurité, il faut qu'ils possèdent des stratégies complémentaires comme l'indique le tableau ci-dessous :

Complémentarité pour 2 clients réseau dans un environnement IPSec

	Aucune Stratégie attribuée	Client (en réponse seule)	Serveur (demandez la sécurité)	Sécuriser le serveur (nécessite la sécurité)
Aucune Stratégie attribuée	**Sécurité IPSec inexistante**	**Sécurité IPSec inexistante**	**Sécurité IPSec inexistante**	**Communication inexistante**
Client (en réponse seule)	**Sécurité IPSec inexistante**	**Sécurité IPSec inexistante**	**Sécurité IPSec**	**Sécurité IPSec**
Serveur (demandez la sécurité)	**Sécurité IPSec inexistante**	**Sécurité IPSec**	**Sécurité IPSec**	**Sécurité IPSec**
Sécuriser le serveur (nécessite la sécurité)	**Communication inexistante**	**Sécurité IPSec**	**Sécurité IPSec**	**Sécurité IPSec**

8.2. Implémentation de la sécurité IPSec avec des certificats

8.2.1. Qu'est-ce qu'un certificat ?

Le certificat numérique (**X.509**) est une identification électronique permettant l'authentification et la protection des données sur des réseaux privés ou publiques. Le certificat associe de manière sécurisée une clé publique à une entité détenant la clé privée.

La clé publique : Elle transite sur le segment de réseau non sécurisé (Internet) et permet au **destinataire** de vérifier la signature des données transmises.

La clé privée : Elle est confidentielle et permet à **l'émetteur** de signer le message à transmettre.

L'émetteur du certificat est appelé autorité de certification. Il signe numériquement les certificats pour un utilisateur, un ordinateur ou même un service (IPSec).

L'autorité de certification fournit et affecte les clés de cryptage, de décryptage et d'authentification. Ces clés sont distribuées via des certificats qui font correspondre les clés publiques à des informations comme le nom ou l'adresse e-mail.

Un certificat contient les informations suivantes :

- la clé cryptographique publique de la paire de clés publiques et privées du sujet du certificat
- des informations sur le sujet qui fait la demande de certificat
- le nom unique X.500 de l'utilisateur ou de l'ordinateur
- l'adresse de messagerie du propriétaire du certificat
- des détails sur l'Autorité de certification
- les dates d'expiration
- le hachage du contenu du certificat pour garantir l'authenticité (signature numérique).

8.2.2. Utilisations courantes des certificats

Utilisations des certificats	Description
Signature numérique	Utilise la clé publique dans un certificat pour vérifier que les données ont été signées avec la clé privée correspondante.
Système de fichiers EFS (Encrypting File System)	Utilise la clé publique dans un certificat pour crypter les clés de cryptage des fichiers.
Authentification Internet	Vérifie l'identité d'un serveur Web pour les clients Web. Les serveurs Web peuvent aussi utiliser des certificats pour vérifier l'identité des clients Web.
Sécurité IP (IPSec)	Vérifie l'identité des ordinateurs et crypte les données lorsqu'elles sont transmises sur le réseau.
Messagerie sécurisée	Vérifie les messages électroniques signés et décrypte les messages électroniques.
Ouverture de session par carte à puce	Vérifie l'identité d'un utilisateur à l'ouverture de session par carte à puce. Protocole EAP-TLS
Signature du code logiciel	Vérifie l'identité d'un éditeur de logiciels.

8.2.3. Pourquoi utiliser des certificats avec la sécurité IPSec pour protéger le trafic réseau ?

Les certificats liés à la sécurité IPSec permettent à une entreprise de communiquer avec une autre organisation approuvant la même autorité de certification. Il est utilisé lorsqu'une entreprise nécessite un niveau de sécurité supérieur au protocole Kerberos ou méthode par clés pré-partagées.
Il reste encore un intérêt qui permet d'assurer la sécurité avec des hôtes ne faisant pas partie de l'annuaire Active Directory ou ne supportant pas Kerberos.

Les deux autres méthodes permettant d'authentifier deux hôtes IPSec sont les suivantes :

- Le protocole Kerberos : Assure la façon la plus simple d'authentification pour le trafic entre deux hôtes d'une même forêt.

- Clé pré-partagée : une clé pré-partagée est une chaîne de caractères aléatoires qui sert de mot de passe entre deux hôtes IPSec. Les clés pré-partagées n'offrent pas le même niveau de sécurité que le protocole Kerberos ou les certificats car elles sont stockées en texte clair dans la stratégie IPSec.

8.3. Analyse de la sécurité IPSec

8.3.1. Moniteur de sécurité IP

Le composant logiciel enfichable **Moniteur de sécurité IP** vous permet d'afficher des détails sur les stratégies IPSec locales et les stratégies attribuées au domaine.

Les informations disponibles sont par exemple, les détails de la stratégie IPSec active, notamment le nom, la description, la date de la dernière modification, le magasin, le chemin, l'unité d'organisation et le nom de l'objet Stratégie de groupe. Il y a les filtres avec les filtres génériques du mode principal et du mode rapide, les filtres spécifiques, les statistiques et les associations de sécurité.

8.3.2. Comment arrêter et démarrer les services IPSec

Arrêter et démarrer les services IPSec à l'aide de l'invite de commandes :

	Service routage et accès distant	Service IPSec
Démarrage	**net start remoteaccess**	**net start policyagent**
Arrêt	**net stop remoteaccess**	**net stop policyagent**

9. Configuration de l'accès réseau

9.1. Introduction à l'infrastructure d'accès réseau

9.1.1. Composants d'une infrastructure d'accès réseau

Une infrastructure d'accès réseau est composée de :

- Serveurs d'accès réseau
- Clients d'accès réseau
- Service d'authentification
- Service d'annuaire Active Directory

Un serveur d'accès réseau est un serveur exécutant le service Routage et accès distant de Microsoft. Celui-ci permet aux utilisateurs distants (télétravailleurs, par exemple) de s'authentifier, puis de se connecter au réseau comme s'ils y étaient physiquement connectés.

Un client d'accès réseau permet à un utilisateur d'utiliser à distance toutes les ressources du réseau auquel il se connecte.

Dans une infrastructure d'accès distant utilisant plusieurs serveurs d'accès, l'uniformisation de l'authentification des clients nécessite un Service d'Authentification Internet (IAS). Ce service utilise le protocole RADIUS reconnu par un grand nombre de serveurs d'accès, matériels et logiciels.

Active Directory stocke les informations d'authentification d'un utilisateur ainsi que les propriétés d'accès à distance nécessaires à son authentification. Une fois authentifié, l'utilisateur bénéficie des mêmes fonctionnalités qu'Active Directory offre en environnement de réseau local.

9.1.2. Configuration requise pour un serveur d'accès réseau

Après installation du service Routage et accès distant sur un serveur, l'Assistant Installation du serveur de routage et d'accès distant apparaît. Les informations suivantes devront être connues afin de le remplir correctement :

- Le serveur sera-t-il routeur et/ou serveur d'accès distant ?
- Quelles méthodes d'authentification seront utilisées ?
- Un client réseau a-t-il accès uniquement à ce serveur ou à l'ensemble du réseau ?
- Comment les adresses IP (Internet Protocol) doivent-elles être fournies aux clients ?
- Quelles options de configuration PPP (Point-to-Point Protocol) doivent être utilisées ?
- Quelle est la politique en matière d'enregistrement des événements ?

9.1.3. Qu'est-ce qu'un client d'accès réseau ?

Il existe trois types de clients d'accès réseau :

- Un client VPN se connecte au serveur au travers d'un réseau public non sûr (comme Internet).
- Un client d'accès à distance se connecte au serveur au moyen d'un réseau de communication, tels RTC ou RNIS, pour créer un lien physique à un port sur le serveur.
- Un client sans fil se connecte sur le serveur en utilisant les technologies infrarouges (IR) ou à radiofréquences (RF).

9.1.4. Qu'entend-on par autorisation et authentification de l'accès réseau ?

L'authentification consiste à valider des informations fournies par le client lors de la tentative de connexion (login et mot de passe, par exemple). Ces informations sont transmises par le serveur d'accès à un contrôleur de domaine pour validation.

L'autorisation consiste à vérifier que l'utilisateur en question a effectivement le droit de se connecter, suivant les informations du compte utilisateur et les stratégies d'accès distant.

9.1.5. Méthodes d'authentification disponibles

Différents protocoles permettent d'authentifier les utilisateurs lors des accès distants avec plus ou moins de sécurité :

PAP (Password Authentification Protocol)	Protocole utilisant des logins et des mots de passe en clair.
SPAP (Shiva Password Authentification Protocol)	Dépendant du constructeur matériel Shiva. Les mots de passe sont protégés par un cryptage réversible.
CHAP (Challenge Handshake Authentification Protocol)	Aussi connu sous le nom MD5-CHAP, il permet d'obtenir un niveau de cryptage plus élevé.
MS-CHAP (Microsoft Challenge Handshake Authentification Protocol)	Protocole d'authentification propriétaire à Microsoft permettant d'authentifier les clients utilisant Windows et utilisant le principe de CHAP. Il supporte le MPPE qui permet de crypter l'ensemble des données qui transitent entre le serveur et le client. Tous les OS Microsoft depuis Windows 95 supportent le MS-CHAP.
MS-CHAP v2 (Microsoft Challenge Handshake Authentification Protocol Version 2)	Nouvelle version de MS-CHAP utilisant des clés de cryptage plus robustes ainsi que l'authentification mutuelle. Les ordinateurs sous Windows 95 et antérieur ne supportent pas ce protocole d'authentification (Windows 98 et ultérieur le supportent)
EAP (Extensible Authentification Protocol)	Le client et le serveur négocient la méthode d'authentification qui sera utilisée. Le protocole MD5-CHAP, TLS et des méthodes propriétaires de fournisseurs tiers peuvent être utilisés. Ce protocole garantit la prise en charge des futures méthodes d'authentification.
TLS (Transport Layer Security)	Est utilisé principalement avec des systèmes d'authentification à l'aide de cartes à puce (SmartCard).
PEAP (Protected Extensible Authentication Protocol)	Ce protocole est utilisé par les réseaux 802.1x afin de sécuriser les connexions câblées et sans fil.

9.2. Configuration d'une connexion VPN

9.2.1. Fonctionnement d'une connexion VPN

Un réseau privé virtuel (VPN) permet à un client de se connecter de manière sécurisée à son réseau au travers d'un réseau non sécurisé (tel Internet). Cette technique émule un mode point à point entre les deux machines et assure la confidentialité des données par chiffrement.

Les avantages des tunnels VPN sont :

- Réduction des coûts. Le réseau VPN n'utilise pas de ligne téléphonique ni RNIS et nécessite un minimum de matériel.
- Sécurité accrue. Les données sont incompréhensibles pour les utilisateurs non autorisés, mais les utilisateurs autorisés peuvent y accéder grâce à la connexion.
- Prise en charge des protocoles réseau. Vous pouvez utiliser à distance une application qui dépend des protocoles réseau les plus répandus, dont TCP/IP (Transmission Control Protocol/Internet Protocol).
- Sécurité des adresses IP. Les informations envoyées sur un réseau privé virtuel étant chiffrées, les adresses que vous spécifiez sont protégées et seule l'adresse IP externe est visible depuis Internet. Aucun frais n'est lié à la modification des adresses IP pour l'accès distant sur Internet.

9.2.2. Protocoles de cryptage pour une connexion VPN

Le chiffrement de données va permettre de protéger les données en chiffrant l'ensemble des données qui vont transiter entre le client et le serveur. L'utilisation des protocoles de chiffrement de données est possible uniquement si le protocole d'authentification est **MS-CHAP**, **MS-CHAP v2** ou **TLS**. Deux protocoles de cryptage sont disponibles avec Windows 2003 :

- **MPPE :** MPPE permet de protéger les données sur une connexion PPTP avec 3 niveaux d'encodage (128 bits, 56 bits et 40 bits).

- **IPSec :** IPSec permet de sécuriser les transferts du réseau en cryptant directement les trames IP.

9.2.3. Configuration requise pour un serveur VPN

Apres l'installation du service Routage et Accès distant, l'Assistant Installation de l'accès distant et de routage vous aide à configurer votre serveur VPN. Vous devez connaître les éléments suivants avant de vous lancer :

- Quelle interface réseau assure la connectivité interne et laquelle assure la connectivité externe ?
- Les clients vont ils recevoir leur adresse IP grâce à un serveur DHCP ou grâce au serveur VPN ?
- Les clients vont-ils être authentifiés par un serveur RADIUS ou par le serveur VPN ?

CONNEXION VPN ENTRE 2 CLIENTS

9.3. Configuration d'une connexion d'accès à distance

9.3.1. Comment fonctionne l'accès réseau à distance ?

Un accès réseau à distance est une connexion temporaire à un port physique du serveur d'accès, via des technologies d'accès distant, telles RTC, RNIS ou X25.

L'établissement d'une connexion distante comprend 4 étapes :

1. Le client appelle le serveur distant.
2. Le serveur réceptionne la requête du client et collecte ses informations d'authentification.
3. Le serveur authentifie et autorise le client.
4. Si la connexion est autorisée, le serveur d'accès distant fournit au client la connectivité vers le réseau local auquel il est connecté, jouant le rôle de passerelle.

9.3.2. Configuration requise pour un serveur d'accès distant

Pour configurer un serveur d'accès distant, vous devez connaître les informations suivantes :

- Les clients vont-ils recevoir leur adresse IP grâce à un serveur DHCP ou grâce au serveur VPN ?
- Les clients vont-ils être authentifiés par un serveur RADIUS ou par le serveur VPN ?
- Vérifier que tous les utilisateurs disposent d'un compte configuré pour autoriser l'accès à distance.

9.4. Configuration d'une connexion sans fil

9.4.1. Vue d'ensemble de l'accès réseau sans fil

Les réseaux sans fil permettent à plusieurs périphériques de communiquer entre eux sans connectivité physique, au moyen d'ondes électromagnétiques. Ces réseaux sont particulièrement intéressants pour créer des réseaux temporaires, publics ou dans des locaux où installer une connectivité filaire serait trop onéreuse ou encombrante.

Un réseau sans fil (WLAN) peut fonctionner selon deux modes différents, définis par la norme IEEE **802.11x** :

- ***Infrastructure***. Les clients peuvent communiquer entre eux, ainsi qu'avec un réseau filaire, disponible au travers d'un *point d'accès WLAN*.
- ***Ad Hoc***. Les clients peuvent uniquement communiquer entre eux, sans connectivité filaire.

9.4.2. Normes sans fil

La norme IEEE originale concernant les réseaux WLAN, est la *802.11* (aussi connue sous le nom de Wi-Fi). Elle définit la couche physique (fréquences de fonctionnement, types de modulation) ainsi que la sous-couche MAC du modèle OSI.

La norme ***IEEE 802.11b*** permet des débits plus élevés que la norme originale (5,5 et 11 Mbit/s). Elle admet une portée appréciable, mais est sensible aux interférences. C'est actuellement la norme la plus répandue, car la meilleure marché.

La norme ***IEEE 802.11a*** permet, au prix d'une réduction de la portée, d'augmenter le débit maximum d'un WLAN à 54Mbit/s. Ce standard a l'inconvénient de ne pas être compatible avec les autres normes IEEE 802.11, car opérant dans une bande de fréquences différente.

La norme ***IEEE 802.11g*** cumule les avantages du 802.11b et du 802.11a : il autorise des débits allant jusqu'à 54 Mbit/s, tout en étant compatible avec le 802.11b et en étant moins sensible aux interférences.

La norme ***IEEE 802.1x*** définit des protocoles d'authentification pour l'accès à la connectivité sans fil. Cette norme a été développée dans le but d'augmenter la sécurité des réseaux WLAN, mais peut être implémentée sur les réseaux filaires.

9.4.3. Méthodes d'authentification disponibles pour les réseaux sans fil

Le standard 802.11 définit la confidentialité des données utilisateur sous le terme de **Wired Equivalent Privacy (WEP)**. Il régit le type de chiffrement des données mais pas la manière dont les clés sont échangées. 802.1x apporte une réponse à cette lacune.

Les protocoles d'authentification disponibles dans 802.1x sont :

- **EAP-TLS :** effectue une authentification mutuelle et constitue la solution la plus puissante d'authentification et de détermination des clés. **EAP-TLS** est basé sur des certificats pour le client et le serveur.
- **EAP-MS-CHAP v2 :** effectue une authentification mutuelle basée sur un certificat pour le serveur et un mot de passe pour le client.
- **PEAP (Protected EAP) :** assure une sécurité supplémentaire au protocole EAP en chiffrant les paquets de négociation initiaux. TLS et MS-CHAP v2 sont utilisables avec PEAP.

9.4.4. Configuration requise pour un client Windows XP Professionnel en vue d'un accès réseau sans fil

Windows XP a introduit le service de Configuration Automatique Sans Fil. Ce service inclus dans Windows 2003 permet à l'utilisateur de pré-configurer ses réseaux sans fil préférés sous forme de liste. Si plusieurs réseaux sans fil sont disponibles, c'est le premier à apparaître dans la liste qui sera choisi (une clé WEP peut être paramétrée à l'avance). Si aucun des réseaux disponibles ne figure dans la liste, l'utilisateur en est informé et peut choisir parmi les réseaux à sa disposition.

9.5. Contrôle de l'accès utilisateur au réseau

9.5.1. Autorisations d'appel entrant du compte de l'utilisateur

Dans la version Windows 2003 Server, les autorisations de connexion d'accès distant sont dépendantes des stratégies d'accès distant. Le service Routage et accès distant et le service d'authentification Internet y ont recours pour accepter ou refuser les tentatives de connexion. Les stratégies d'accès distant regroupent plusieurs propriétés nécessaires à l'examen d'une tentative de connexion pour son acceptation ou son refus.
Des autorisations d'appel entrant sont disponibles dans la boite de dialogue « Propriétés » d'un utilisateur dans la console « Active Directory » ou « Utilisateurs et groupes locaux ». Les propriétés sont les suivantes :

- **Autorisation d'accès distant** (Accès à distance ou VPN). Cette propriété autorise ou refuse expressément l'accès distant à l'utilisateur. Cette autorisation peut également dépendre du fait qu'il y ait des règles de stratégie d'accès distant.
- **Vérifier l'identité de l'appelant**. Cette propriété vérifie le numéro de téléphone de l'appelant, dans le cas d'une connexion par modem. Si le numéro réel et le numéro inscrit dans cette propriété diffèrent, la connexion échoue.
- **Options de rappel (callback).** Cette propriété permet à un serveur d'accès de rappeler le client (à un numéro configuré par l'administrateur, ou le client). Fonctionnalité utile pour les utilisateurs itinérants ayant des besoins de connexions à leur structure.
- **Attribution d'une adresse IP statique**. Permet d'attribuer une adresse IP statique à l'utilisateur dès l'établissement de la connexion.
- **Appliquer les itinéraires statiques**. Permet le routage à la demande. Une route configurée ici sera ajoutée à la table de routage du serveur une fois le client connecté.

9.5.2. Qu'est-ce qu'une stratégie d'accès distant ?

Une stratégie d'accès distant est un ensemble de règles définissant les paramètres à respecter pour qu'un utilisateur désigné ou membre d'un groupe désigné puisse établir une connexion d'accès à distance. Chaque règle contient une ou plusieurs conditions, une autorisation d'accès distant, et un profil :

- **Les conditions.** Elles peuvent se baser sur l'adresse IP ou le numéro de téléphone de l'utilisateur, son appartenance à un groupe ou l'heure de l'appel. Les conditions de l'utilisateur sont comparées à celles du serveur, dans l'ordre. La première règle correspondant à ces paramètres est utilisée par le serveur pour valider l'appel. Si aucune règle ne respecte les conditions de l'appel, celui-ci est refusé.
- **L'autorisation.** Définit si l'appel entrant est accepté ou refusé.
- **Le profil.** Il comprend plusieurs paramètres à appliquer à la connexion, tels que les protocoles d'authentification et de cryptage.

9.5.3. Qu'est-ce qu'un profil de stratégie d'accès distant ?

Le profil de stratégie d'accès distant est un ensemble de paramètres à appliquer à une connexion, une fois que celle-ci a été acceptée.

Ces paramètres sont :

- **Contraintes pour les appels entrants**. Définissent le délai d'attente avant déconnexion, la durée maximum de la session, les jours, les heures, les numéros de téléphone et les types de supports (RNIS, VPN, etc.) autorisés.
- **Propriétés IP**. Configurent l'attribution d'adresses IP statiques et le filtrage des paquets TCP/IP. Vous pouvez définir des filtres distincts pour les paquets entrants ou sortants.
- **Liaisons multiples**. Permet d'agréger plusieurs liaisons physiques sous forme d'une seule liaison logique.
- **Authentification**. Définit les protocoles d'authentification à utiliser parmi les protocoles supportés par Windows 2003. MS-CHAP et MS-CHAP v2 sont activés par défaut.
- **Cryptage**. Détermine les chiffrements requis, permis ou interdits.
- **Paramètres avancés**. Permet d'indiquer des paramètres supplémentaires à passer au serveur RADIUS.

9.5.4. Traitement des stratégies d'accès distant

Le processus mis en œuvre pour accepter les connexions à distance commence par la comparaison des conditions de la stratégie d'accès à distance avec celle de la tentative de connexion courante. La première stratégie dont les conditions correspondent est utilisée pour déterminer l'accès.
Si aucune stratégie ne correspond, l'accès est refusé.
Ensuite, le serveur vérifie si l'utilisateur est, de manière explicite, autorisé ou non à se connecter (ce paramètre se trouve dans son compte utilisateur) ou si cette tâche est laissée à l'appréciation de la stratégie d'accès distant.
Enfin, le service Routage et accès distant applique le profil de la stratégie à la connexion entrante.

9.6. Centralisation de l'authentification de l'accès réseau et de la gestion des stratégies en utilisant IAS

9.6.1. Que signifie RADIUS ?

RADIUS (Remote Authentication Dial-In User Service) est un protocole très répandu destiné à l'authentification, l'autorisation et la comptabilisation centralisée de l'accès réseau. Il repose sur le modèle client/serveur et peut valider des connexions d'accès à distance, VPN ou sans fil.

9.6.2. Que signifie IAS ?

Le service IAS (Internet Authentification Service) est l'implémentation du serveur RADIUS incluse dans Windows 2003. Il permet une gestion centralisée des autorisations d'accès au réseau, l'intégration totale avec l'environnement Windows 2003, et la compatibilité avec tous les périphériques d'accès compatibles RADIUS.

9.6.3. Fonctionnement de l'authentification centralisée

La procédure de connexion au réseau faisant appel à un serveur d'authentification RADIUS se déroule comme suit :

- Un utilisateur se connecte à un serveur d'accès réseau (exécutant le service Routage et accès distant) en utilisant une connexion d'accès à distance, VPN ou sans fil.
- Le serveur d'accès réseau transfère la demande d'autorisation à un serveur RADIUS (IAS), le serveur d'accès se comporte alors comme un client RADIUS.
- Le serveur RADIUS (IAS) fait appel à un contrôleur de domaine pour accéder aux informations d'authentification de l'utilisateur. Le serveur vérifie les informations d'authentification de l'accès à distance.
- Si les informations d'identification de l'utilisateur sont authentifiées, le serveur IAS examine la tentative de connexion par rapport aux stratégies d'accès distant configurées localement. Le traitement des stratégies se comporte comme s'il était fait par un service Routage et accès à distance. Si la demande de connexion correspond à une stratégie autorisée, le serveur IAS répond à un message d'acceptation au serveur d'accès réseau, et un message de rejet dans le cas contraire.

10. Gestion et analyse de l'accès réseau

10.1. Gestion des services d'accès réseau

10.1.1. Instructions relatives à la gestion des services d'accès réseau

Parfois, il est inévitable de devoir arrêter le serveur d'accès distant. Pour cela, il faut respecter les points suivant pour minimiser l'impact de cet arrêt :

- Prévoir un serveur de remplacement
- Planifier l'arrêt du serveur au moment où il y a le moins d'activité.
- Prévenir les utilisateurs du réseau d'une perturbation possible du service.
- Déconnecter les éventuels clients du service.

10.2. Configuration de l'enregistrement sur un serveur d'accès réseau

10.2.1. Types d'enregistrements du service Routage et accès distant

Un serveur exécutant le service routage et accès distant prend en charge trois types d'enregistrements :

- ***l'enregistrement des événements*** : Permet d'enregistrer dans le journal d'événements système les erreurs et les avertissements. Une fois l'enregistrement des événements activé, l'ordinateur créer des fichiers journaux dans ***%systemroot%\Tracing*.**

- ***l'enregistrement de l'authentification locale et de la gestion des comptes*** : Surveille et enregistre les tentatives de connexion avec la stratégie qui a acceptée ou refusée l'authentification.

- ***l'enregistrement de l'authentification et de la gestion des comptes RADIUS*** : Ce type d'enregistrement est utilisé par le service d'accès distant pour faire le suivi des connexions.

10.2.2. Enregistrement de l'authentification et de la gestion des comptes

Ce type de processus enregistre les informations détaillées sur les requêtes de connexion au service d'accès distant. Ce type d'information est utile pour :

- Effectuer un suivi de l'utilisation et des tentatives de connexions pour l'accès distant.
- Conserver les enregistrements afin d'établir des facturations.
- Localiser un problème quelconque.

Il est possible de spécifier les éléments ci-dessous lors de la configuration de l'enregistrement :

- les requêtes à enregistrer
- le format du fichier journal
- la fréquence de création de nouveaux journaux
- la détection automatique du journal le plus ancien lorsque le disque est plein
- l'emplacement des fichiers journaux (par défaut : ***%systemroot%\System32\LogFiles***)
- les informations contenues dans les enregistrements du fichier journal.

Par défaut, les types d'enregistrement de requêtes sont désactivés.

10.2.3. Fichiers journaux pour des connexions spécifiques

Il existe d'autres fonctions d'enregistrements d'informations liées au fonctionnement du service d'accès distant :

- **PPP :** *journal PPP*, recense les informations liées au fonctionnement PPP (série de fonctions et messages de contrôle)

- **L2TP/IPSec** :

  - ***Journal d'audit,*** accessible depuis la console observateur d'événements, il enregistre les événements liés à la sécurité IPSec.

  - ***Journal Oakley*** : recense les détails sur le processus d'association de sécurité. Ce journal doit être activé dans le registre (mettre à 1 la clé de registre HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent\Oakley\EnableLogging) .Ce journal est stocké dans ***%systemroot%\Debug***.

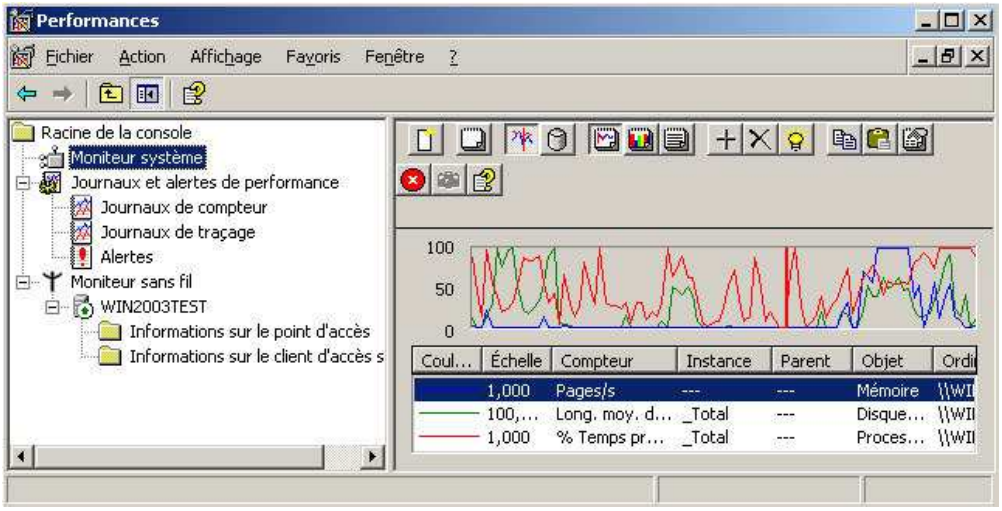
10.3. Collecte et analyse des données d'accès réseau

10.3.1. Pourquoi collecter des données de performance ?

Pour maintenir un niveau correct de fonctionnement, il est nécessaire d'analyser les performances du système en évaluant la charge de travail sur le serveur et en observant ces changements et ces tendances. Cette collecte d'informations apporte un support pour prévoir les futures évolutions, permet d'anticiper des défaillances et fait ressortir les différences lors de modifications de configurations ou de réglages.

10.3.2. Outils de collecte des données d'accès réseau

Windows Server 2003 inclut les outils permettant la collecte de ses données afin de prévoir et identifier les problèmes liés aux accès réseaux.



Moniteur système
Cet outil permet d'afficher les données des performances des composants sélectionnés en temps réel.

Journaux et alertes de performances
Cet outil permet de faire des captures de données dans des fichiers pendant une période. Vous pouvez définir des alertes permettant de déclencher un envoi de message, le démarrage de programme ou l'exécution de script, etc…

Moniteur sans fil
Le service Configuration sans fil enregistre des informations dans le Moniteur sans fil.
Vous pouvez utiliser les informations du journal pour isoler les problèmes que vous rencontrez avec votre service sans fil.