

Chapitre 11 : DNS et Active Directory

Introduction

Principe du DNS

Planification de l'espace de noms pour DNS

Les zones

La hiérarchie des serveurs DNS

La cache DNS

Protocole DNS de modification dynamique : DDNS

Requêtes directe et inverse

Les types d'enregistrement dans la base de données DNS

DHCP

WINS

Introduction :

L'installation (ou la migration) de Windows 2000 serveur en tant que contrôleur de domaine (Domaine Active Directory) nécessite une intégration avec un serveur DNS. Sans un serveur DNS correctement configuré, l'Active Directory ne peut pas fonctionner car DNS est la méthode utilisée par les clients pour localiser les contrôleurs de domaine. De plus, la planification d'une stratégie de nommage pour Active Directory est le point de départ du déploiement de Windows 2000 (2003).

Avec des serveurs NT, le nom de domaine NetBIOS est indépendant du nom de zone DNS. Il est possible de créer un grand nombre de domaines distincts par leur nom mais impossible de créer une arborescence de domaines. La localisation des serveurs (PDC et BDC) se fait via le NetBIOS et/ou grâce à un serveur WINS.

La multiplication des services offerts par l'Active Directory de Windows 2000, la volonté d'interconnecter les réseaux Microsoft, de les organiser en « forêt » et « unité organisationnelle » nécessitent un système de localisation de services plus performant et plus mondial que le WINS. Microsoft a ainsi choisi de développer son Active Directory sur base du DNS, système dont l'arborescence existante reflète généralement fidèlement l'organisation d'une société.

Dans cette optique, le nom de domaine Active Directory est par défaut égal au nom de la zone DNS correspondante. Si le nom donné au domaine Active Directory n'est pas un nom de zone DNS existant, il faudrait alors créer cette zone DNS. On comprend donc que plus l'arborescence DNS est proche de l'organisation d'une société, plus l'implantation d'un réseau Win2000 sera aisée.

Principe du DNS : (RFC 1034 et RFC 1035, RFC 1591 et RFC 2136)

Toute machine connectée à l'Internet est identifiable sans équivoque par son adresse IP. Le nom Internet associé à une adresse IP est plus convivial et plus facile à mémoriser que les adresses IP. (En outre, les valeurs numériques de l'adresse IP peuvent changer si, par exemple, on déplace une machine).

DNS est un **espace de nom** qui contient des noms de domaine complètement qualifiés (**FQDN**, Fully Qualified Domain Name) associés à des adresses IP (**mappage**).

DNS est une base de données distribuée, hiérarchique et extensible qui se décompose en différents **domaines**. Les domaines de niveau supérieur, ou domaines racine, (org, net, edu, les codes de pays...) appartiennent à un organisme appelé InterNic qui délègue la responsabilité des domaines de deuxième niveau inclus dans les premiers. (Désormais, InterNic n'est plus le seul habilité à enregistrer les noms de domaine, visitez le site d'ICANN : <http://www.icann.org>).

Les noms FQDN sont combinés et séparés par des points définissant ainsi une arborescence hiérarchique correspondant à l'arborescence hiérarchique des serveurs DNS, comme nous venons de le voir.

Par exemple, Microsoft est propriétaire d'un domaine de deuxième niveau, microsoft, situé sous le domaine de premier niveau : com

Le FQDN complet est du type « monpc.dpt.bigfirm.com. » où le point terminal est la racine de la hiérarchie DNS.

Remarque : Le terme de domaine, pris dans le contexte DNS ne doit pas être confondu avec la notion de domaine NT4-2000-2003 !

Planification de l'espace de noms pour DNS

Lors de l'installation de serveurs DNS, il est recommandé de choisir et d'enregistrer d'abord un nom de domaine DNS de parent unique pouvant être utilisé pour héberger votre organisation sur Internet, par exemple, « microsoft.com ». Ce nom est un domaine de second niveau à l'intérieur de l'un des domaines de premier niveau utilisés sur Internet. (voir <http://www.dns.be> et <http://www.iana.org/domain-names.htm>)

Avant de choisir un nom de domaine DNS parent pour votre organisation qui sera utilisé sur Internet exécutez une recherche afin de savoir si le nom n'est pas déjà enregistré ! Une fois que vous avez choisi votre nom de domaine parent, vous pouvez combiner ce nom avec un emplacement ou un nom d'organisation utilisé à l'intérieur de votre entreprise pour former d'autres noms de sous-domaine.

Il est fortement recommandé de n'utiliser dans vos noms que des caractères qui font partie du jeu de caractères standard Internet autorisé pour les noms d'hôte DNS. Les caractères autorisés sont définis dans la RFC 1123 comme suit : toutes les lettres majuscules (A-Z), toutes les lettres minuscules (a-z), tous les nombres (0-9) et le tiret (-). La longueur maximale du nom est de 63 octets par libellé et de 255 octets par nom de domaine complet (FQDN)

Les zones :

Pour simplifier le système de nommage (connaître l'appartenance d'un ordinateur à un département via son nom), pour diminuer la charge des serveurs, on divise les domaines en **zones** ayant chacune un DNS responsable qui est nommé « autorité » pour cette zone. C'est la « **délégation** » : le serveur DNS du domaine parent contient un enregistrement qui renvoie vers le serveur DNS de la zone pour les demandes qui la concerne.

Un serveur DNS peut consigner des données pour une ou plusieurs zones et une zone peut avoir plusieurs serveurs DNS : un (seul) serveur principal qui possède le droit de lecture/écriture et des serveurs secondaires qui n'ont que des copies en lecture seule. Le procédé qui consiste à copier des informations de zone d'un serveur à un autre est appelé « **transfert de zone** ».

Avec Active Directory, il y a deux méthodes de stockage et de réplication des zones :

Stockage standard sous forme d'un fichier texte pour la zone.

Stockage intégré à Active Directory pour la zone. Dans ce cas, la réplication de la zone est prise en charge par celle de l'Active Directory.

Une zone doit englober un espace de noms de domaine contigu : On peut créer une zone pour « ventes.microsoft.com » et pour le domaine parent « microsoft.com » car les zones sont contiguës mais pas pour « ventes.microsoft.com » et « pub.microsoft.com »

Un serveur DNS 2003 peut gérer plusieurs types de zone :

Zone principale : Copie de la zone qui peut être updatée directement

Zone secondaire (standard) : Copie d'une zone existante.

Zone intégrée à Active Directory : (non conformes aux spécifications RFC)

Tous les serveurs DNS sont des serveurs principaux.

Seuls les ordinateurs membres d'un domaine Active Directory associé peuvent inscrire dynamiquement des enregistrements avec une zone intégrée à AD.

Zone de stub : (Utile pour le cas du DNS divisé.)

Ce sont des zones secondaires de taille réduite qui ne contiennent que des informations de serveur de nom pour la zone. Ce sont des pseudo zones qui renvoient directement vers les serveurs DNS d'une zone spécifique sans devoir trouver les serveurs en utilisant la procédure de récursivité.

La hiérarchie des serveurs DNS :

Lorsqu'une requête ne concerne pas la zone du DNS, elle est dirigée vers d'autres serveurs DNS de l'Internet jusqu'à ce qu'un serveur « autorité » renvoie la réponse. En pratique, c'est le serveur DNS du domaine parent. Par exemple, pour trouver l'adresse IP de www.bigfirm.com, il faut contacter le DNS de bigfirm.com. Pour localiser celui-ci, il faut contacter les serveurs DNS du domaine parent com. Pour obtenir l'adresse du serveur DNS de com, il faut interroger les serveurs DNS de la racine « . ». Ceux-ci sont référencés dans un fichier appelé « fichier d'indication de racine » qui reprend les adresse IP des 13 serveurs DNS racine. (%SystemRoot%\system32\dns\cache.dns). Cette méthode est dite de « **récurtivité** ».

La cache DNS :

Afin de diminuer le trafic réseau, le serveur de noms place le résultat de ces requêtes dans un cache pendant une durée déterminée (TTL : Time To Live) dont la valeur par défaut est de 60 minutes.

Protocole DNS de modification dynamique : DDNS

Les machines communiquent directement leur adresses IP au serveur DNS, éliminant toute intervention de l'Administrateur.

L'Active Directory étant susceptible de contenir un grand nombre d'informations changeantes il doit également refléter au mieux l'état instantané du réseau. C'est pourquoi Active Directory utilise un DNS dynamique et reflétant par conséquent l'état réel du réseau. Dans la même logique, les clients Windows 2000 professionnel sont par défaut configurés pour s'enregistrer dynamiquement dans le système DNS.

Requêtes directe et inverse :

Un serveur DNS a pour fonction de résoudre un nom Internet en une adresse IP : c'est une requête de recherche directe. Et vice-versa : une requête de recherche inversée effectuée l'opération inverse qui met en correspondance une adresse IP et un nom. Les noms DNS vont du particulier au général : ils commencent par le nom de l'hôte, pour remonter, à la fin, à la racine du domaine : monpc.dpt.bigfirm.com où l'élément le plus à gauche correspond au nom de l'hôte et les autres éléments au domaine DNS dit aussi suffixe DNS (dpt.bigfirm.com est un domaine enfant, un sous-domaine de bigfirm.com) Les adresses IP fonctionnent en sens inverse. Pour faciliter la recherche, on a créé un domaine spécial : le domaine in-addr.arpa : où on inverse les octets de l'adresse IP puis on y ajoute in-addr.arpa. Par exemple, pour résoudre l'adresse IP 10.230.231.232, on interroge 232.231.230.10. in-addr.arpa.

La zone inverse est gérée à partir de la zone directe. Les enregistrements dans la zone inverse sont de type PTR (pointeur) car ils pointent vers un enregistrement de type A (adresse) enregistré dans la zone directe, voir la section « Les types d'enregistrement dans la base de données DNS » Nslookup suivi de l'adresse IP rend en retour le nom du système si l'adresse existe dans la zone inverse.

Les types d'enregistrement dans la base de données DNS :

Il existe plusieurs types d'enregistrements de ressource (ou RR, Resource Record) dans une base de données DNS :

Voici les plus courants :

Type A et PTR : associe un nom de machine à une adresse IP.

Type MX : identifie les serveurs de messagerie.

Type CNAME : enregistrement d'alias.

Type SOA : (Start of Authority) : C'est un enregistrement source de nom qui nomme le serveur principal pour le domaine. (et d'autres données annexes).

Type NS : Les enregistrements de serveurs de noms (NS pour Name Server)

Type SRV :

L'Active Directory localisation les services sur le système DNS : un poste client recherchant un contrôleur de domaine ou un service intégré à l'AD, va pouvoir obtenir l'adresse IP de la machine exécutant ce service par une simple requête DNS.

Dans un réseau un peu important, le nombre d'enregistrements DNS relatifs à l'Active Directory est très vite trop important pour être géré manuellement d'où l'utilité d'un serveur DNS acceptant les mises à jour dynamiques automatiques.

Pour chaque « service », un enregistrement de type « SRV » est inscrit dans la zone DNS adéquate. Ces enregistrements sont stockés dans 4 zones DNS qui présentent une nomenclature de nom « hors standard » toujours sous cette forme:

- _tcp.domain.com
- _udp.domain.com
- _sites.domain.com
- _msdcs.domain.com

Le protocole DHCP :

Dynamic Host configuration Protocol : gère toutes les **configurations** IP depuis un serveur central.

A la connexion au réseau, le poste client envoie une diffusion générale « DHCP Discover » (UDP) qui est interceptée par un serveur DHCP qui y répond. Les requêtes DHCP sont confinées au sous-réseau. Une solution est de mettre un serveur DHCP par sous-réseau. L'autre solution est de configurer les routeurs pour qu'ils laissent passer ces requêtes (voir la documentation du routeur) et de configurer un agent relais DHCP.

Une **étendue** (scope) est un groupe d'adresse IP que le serveur DHCP utilise pour affecter des adresses à ses clients ainsi que d'autres paramètres de configuration.

Exemple : Les adresse IP de 192.168.10.5 à 192.168.10.250

DNS :192.168.10.4

WINS :192.168.10.3

Passerelle par défaut : 192.168.10.1

Certains serveurs doivent avoir une adresse IP statique : DHCP, DNS, WINS, les routeurs....

L'affectation d'une adresse à un client ne dure qu'un laps de temps fini nommé **bail** (lease). A la moitié du bail, le client essaye de le renouveler pour garder la même configuration.

WINS :

Les noms d'hôtes NetBIOS (15 caractères au maximum) doivent être unique sur le réseau. Les diffusions générales NetBIOS ne sont (normalement) pas permises par les routeurs d'où l'impossibilité de résoudre les noms NetBIOS d'hôtes d'un autre sous-réseau. WINS résout le problème en stockant une base de donnée des correspondances « adresse IP – nom NetBIOS ».

WINS reste nécessaire si votre parc informatique contient encore des versions d'OS comme Windows NT et Windows 95/98.