Etude d’Active Directory

Emmanuel le Chevoir
Hervé Schauer Consultants

Cet article présente une étude détaillée de l’annuaire Microsoft™ Active Directory™ dans Windows 2000 et des technologies qui y sont liées.

Y sont abordés en détail les concepts d’annuaire électronique, de domaine Windows 2000, ainsi que l’implémentation DNS de Microsoft et les nouveaux mécanismes d’authentification.

Table des matières

1.1. Introduction

Avec Windows 2000, Microsoft a introduit un ensemble complet de nouveaux outils et méthodes qui changent considérablement l'approche de l'administration et de la sécurisation d'un système ou d'un réseau, rendant son précédent système, Windows NT, obsolète.

Ces nouveautés ont pour but avoué de combler les lacunes de NT en matière de sécurité, d'une part, et d'homogénéiser toute l'administration des domaines tout en renforcant la sécurité globale du réseau, d'autre part. L'ensemble de ces changements s'articule autour d'un point, d'une clé de voûte : Active Directory™.

1.2. Active Directory : un annuaire

1.2.1. Pourquoi un annuaire ?

Active Directory est avant toute chose un annuaire, comme le sont également NDS, de Novell, ou iPlanet, de Sun. Avant d'aller plus loin dans l'étude d'Active Directory, il faut définir ce qu'est exactement un annuaire.

Avec le développement des réseaux, les services offerts se sont multipliés. On trouve ainsi couramment sur un même réseau un service de messagerie, un serveur de fichiers, un agenda partagé, etc. Avant d'accéder à un quelconque service, il est souvent demandé aux utilisateurs de s'authentifier, afin de se faire reconnaitre du service en question. De même, chaque utilisateur d'un service disposera de ses propres données, de ses propres paramètres, pour l'utilisation du service.

En prenant l'exemple de la messagerie, un utilisateur devra donc :

- s'authentifier auprès du serveur de messagerie, au moyen d'un identifiant et d'un mot de passe, par exemple
- pouvoir accéder à son courrier
- éditer ses données personnelles (au minimum nom, prénom et adresse personnelle).

Les mêmes besoins se font sentir si l'utilisateur utilise un service d'agenda, par exemple. Là encore, il devra pouvoir se faire reconnaitre du service, stocker des informations le concernant, enregistrer ses rendez-vous, etc...

Historiquement, chaque service implémentait les mécanismes nécessaires à chaque opération lui étant propre (identification, stockage de données, etc...). Plus le réseau est vaste et plus les services se multiplient. Il est par conséquent difficile, sur un réseau étendu, de contrôler finement et efficacement l'ensemble des resources avec une telle approche.

C'est là que le concept d'annuaire prend son sens. Un annuaire va permettre de centraliser les informations d'un utilisateur, d'un service, etc... pour en simplifier l'administration. Chaque utilisateur disposera d'une entrée dans l'annuaire, entrée dans laquelle seront conservées toutes les données le concernant. Les services n'auront alors plus qu'à consulter l'annuaire pour fournir à l'utilisateur les données qu'il attend.

1.2.2. Contraintes

Il est intéressant de se pencher sur les contraintes qui se trouvent derrière le concept d'annuaire électronique.

1.2.2.1. L'aspect dynamique

Un annuaire électronique doit avant tout être dynamique. Il doit pouvoir être mis à jour rapidement, et ces modifications doivent être accessibles immédiatement, ce dans le but de diminuer le délai de diffusion de l'information sur le réseau. L'aspect dynamique d'un annuaire permet également de faciliter la délégation des responsabilités. C'est le propriétaire d'une information qui met celle-ci à jour ; l'information se trouve ainsi rapprochée de sa source afin de la rendre toujours plus pertinente.

1.2.2.2. La flexibilité

Un annuaire électronique doit également répondre à une deuxième contrainte, celle de la flexibilité. Pour qu'il soit efficace, la structure d'un annuaire doit pouvoir être modifiée pour s'adapter aux nouvelles entrées qui doivent y être enregistrées. L'ajout d'un attribut, d'une structure de données complète ou d'une entrée dans un annuaire électronique doit pouvoir se faire sans altérer les informations existantes pour le reste de l'annuaire.

De même, il doit être possible de modifier l'organisation des données au sein de l'annuaire. La fonction principale d'un annuaire est d'organiser les données de telle façon qu'elles puissent être retrouvées le plus rapidement possible. Pour ce faire, un annuaire met en place un classement qui lui est propre, susceptible d'évoluer en fonction des informations qui sont ajoutées à l'annuaire.

1.2.2.3. La sécurité

Un annuaire électronique doit être en mesure de contrôler les données qu'il fournit, et ce en fonction de différents critères, qui peuvent aller de la localisation géographique de l'utilisateur demandant une information à son identité complète. Des mécanismes d'authentification doivent être présent afin de permettre, par exemple, d'interdire l'accès à un sous-ensemble de l'annuaire, ou à certains attributs. Il doit également être possible de restreindre l'accès à certaines informations en fonction de relations établies ou non dans les données existant dans l'annuaire. Par exemple, un administrateur local devra pouvoir accéder aux profils des utilisateurs locaux, mais pas à ceux des utilisateurs du domaine. De même, un utilisateur local ne pourra pas accéder aux informations concernant l'administrateur.

Il est également envisageable de filtrer les informations en fonction de l'endroit d'où une personne accède à l'annuaire. Par exemple, un annuaire peut avoir une interface privée et une interface publique. Les informations dites publiques étant accessibles depuis Internet, et les informations privées seulement depuis un intranet.

Enfin, recoupant la contrainte de flexibilité, il doit être possible de contrôler précisément la délégation des responsabilités.

1.2.3. Particularités d'un annuaire

Les annuaires sont souvent comparés à des bases de données. La comparaison, si elle est justifiée, créé pourtant une ambiguïté qu'il faut lever. Si un annuaire est effectivement une base de données, la réciproque est fausse. Quelles sont donc les particularités d'un annuaire ?

1.2.3.1. Sollicitations

Un annuaire est beaucoup plus sollicité en lecture qu'en écriture. C'est le but premier d'un annuaire que d'être consulté, d'offrir des informations. Même s'il faut mettre à jour un annuaire, et que, comme cela a été décrit auparavant, la nature dynamique d'un annuaire implique la régularité de ces mises à jour, les écritures dans un annuaire sont négligeables face aux lectures.

1.2.3.2. Nature des transactions

Les transactions gérées par un annuaire sont de nature simple. Un annuaire n'a pas pour vocation de gérer de multiples transactions en concurrence, ou de traiter de gros volumes de données. De par l'organisation des données dans un annuaire, il n'est pas nécessaire de mettre en place des mécanismes complexes de vérification de l'intégrité des données.

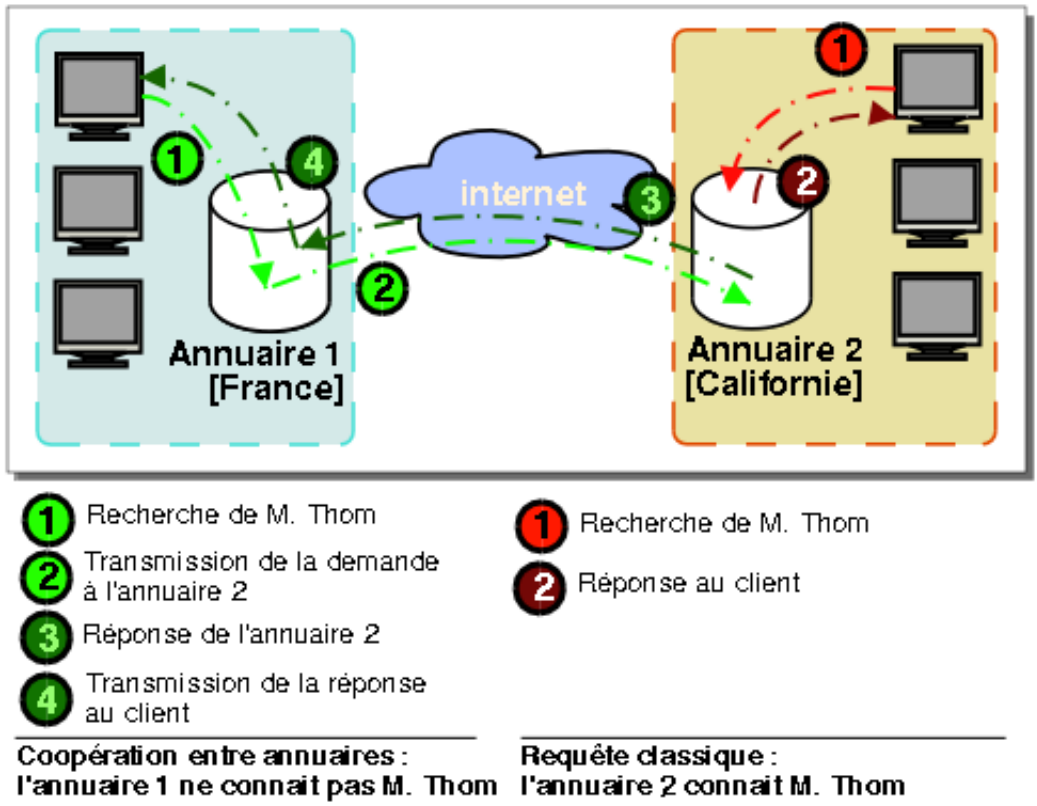
1.2.3.3. Accès à l'information

Le but d'un annuaire est d'être consulté, de fournir des informations. Ces informations doivent être accessibles quelle que soit la distance séparant la personne demandant l'information et l'annuaire lui-même. De même, quel que soit le débit de la liaison entre l'annuaire et le client, la consultation, disons, d'un numéro de téléphone, doit pouvoir se faire rapidement.

1.2.3.4. Communication entre annuaires

Répondant au besoin de flexibilité, la communication inter-annuaire est une caractéristique importante. Elle permet, entre autre, de mettre en place efficacement la délégation de l'administration des données servies. L'intérêt de disposer de plusieurs annuaires électroniques dans une multinationale est aisément compréhensible. Les informations concernant les employés français, par exemple, seront conservées dans un premier annuaire, et celle des employés de Californie dans un second. Ces deux annuaires seront en mesure de communiquer entre eux, si bien qu'une demande d'informations sur un employé californien à l'annuaire français aboutira, de façon totalement transparente. Cette coopération est illustrée Figure 1.

Figure 1. Coopération de deux annuaires



1.2.4. Compatibilité avec les autres annuaires

1.2.4.1. LDAP

Microsoft n'est en rien un pionnier. En effet, bien avant lui, Novell proposait son annuaire, NDS, et le concept même d'annuaire avait été formalisé par une norme, X.500, qui définit précisément la façon d'accéder à un service d'annuaire.

La norme X.500 étant un peu lourde et s'adaptant assez mal aux besoins existant, une version allégée de X.500, appelée *LDAP* fut normalisée par la suite.

Historiquement, de nombreux annuaires s'appuient sur LDAP. Microsoft n'échappe pas à la règle, et les accès à Active Directory se font avec des requêtes LDAP classiques.

1.2.4.2. Microsoft ADSI

Afin de faciliter les accès à un ensemble d'annuaires hétérogènes, Microsoft a développé une couche d'abstraction, appelée *ADSI* (Active Directory Service Interface) [w2kadsi], permettant d'interroger de façon transparente et homogène un ensemble de services d'annuaire, au moyen de scripts ou de programmes écrits en C/C++.

Cette couche d'abstraction rend la manipulation de données appartenant à un annuaire très simple, quelque soit le service d'annuaire sous jacent. Nativement, ADSI supporte les annuaires de type :

- LDAP
- Windows NT
- NDS™
- Netware™ 3

Il est également possible d'ajouter le support d'autres services d'annuaire à ADSI en développant des connecteurs ADSI spécifiques.

Enfin, certains produits Microsoft tels que Exchange et IIS, bien qu'il ne s'agisse pas d'annuaires, disposent d'une interface ADSI.

1.2.5. Spécificités

La précédente partie a présenté Active Directory comme un service d'annuaire électronique classique. Cependant, Active Directory pousse le concept d'annuaire dans ses retranchements. En effet, tout ou presque, dans Windows 2000, peut être enregistré dans l'annuaire. De plus, les mécanismes de réplication, nécessaires à la tolérance de panne, entre autres, lui sont propres.

1.2.5.1. Réplication

Active Directory est fortement basé sur LDAP, ce qui soulève un problème : LDAP ne définit pas le mécanisme de réplication entre annuaires. Actuellement, les mécanismes de réplication d'un annuaire LDAP sont en cours de normalisation à l'*IETF* [ldup], mais à ce jour, rien n'est encore finalisé.

Microsoft a donc fait le choix d'implémenter son propre mécanisme de réplication d'annuaire. A ce jour, les détails du protocole de réplication multi-maître créé par Microsoft ne sont pas connus. La

réplication de l'annuaire Active Directory sera traitée plus en détail dans la partie 3 de ce document, qui traite des contrôleurs de domaine.

1.2.5.2. Un annuaire pour tout enregistrer

Active Directory est bien plus qu'un simple annuaire. En effet, toutes les informations concernant le domaine contrôlé par la machine qui héberge l'annuaire sont stockées dans ce même annuaire. S'y trouvent, par exemple, la liste complète des utilisateurs ainsi que leur mot de passe, mais également toutes les zones DNS, si l'hôte a des fonctions de Serveur de Noms [Section 1.5], les certificats numériques utilisés pour la gestion du domaine, la politique sécurité des groupes du domaine, les règles de filtrage IP du pare-feu Microsoft, ISA server, etc...

Il est même possible de stocker dans l'annuaire des règles spécifiques aux routeurs ou commutateurs Cisco, qui viendront chercher leur configuration d'eux même en utilisant Active Directory. Le but étant clairement de centraliser au maximum l'administration du réseau.

1.2.5.3. Des mécanismes de sécurité complexes

Bien entendu, une telle volonté de centraliser l'administration ne saurait être viable sans une solide politique de sécurité. Afin de pouvoir établir de telles politiques, Active Directory repose entièrement sur le concept d'ACL (Access Control List).

L'annuaire Active Directory possède une structure arborescente, chaque élément étant soit un conteneur, soit une propriété. Chaque objet de l'annuaire dispose de ses propres permissions. Il est donc possible de définir complètement les permissions que l'on souhaite donner à l'ensemble des éléments de l'annuaire.

Active Directory pouvant contenir des millions d'entrées, il est bien entendu inconcevable de définir les permissions pour chaque objet de l'annuaire. Chaque entrée hérite donc des permissions de son parent, à moins que cela ne soit changé de façon explicite.

Cette approche sécurité permet d'atteindre un niveau de granularité sans précédent. Cependant, il faut veiller à toujours utiliser au maximum les propriétés d'héritage, l'ensemble de permissions étant assez difficile à auditer compte tenu du nombre d'entrées de l'annuaire.

1.3. Les domaines Active Directory

1.3.1. Introduction : avant Active Directory

Active Directory regroupe sous un seul nom un ensemble considérable de services, et désigne en fait, plus qu'un produit ou qu'un composant logiciel, un ensemble de standards et de protocoles complétant la base de données qui constitue l'annuaire intégré à Windows 2000. Avant Windows 2000, et plus particulièrement dans Windows NT4, cet annuaire existait plus ou moins, sous la forme d'un ensemble de composantes logicielles et de bases de données éparses. On peut citer, parmi ces composantes :

- IIS 4.0
- La base d'utilisateurs
- La base de données d'Exchange

Un effort était déjà fait pour homogénéiser cet ensemble d'outils et de bases. Ainsi en témoigne l'API *ADSI*, permettant non seulement d'unifier l'accès aux différents annuaires existant, avant même que Microsoft ne mette en production sa propre solution, mais également d'étendre cet accès aux composantes de Windows NT 4.0, telles que celles qui viennent d'être citées.

L'intégration complète de ces diverses composantes dans le système n'a pourtant réellement été réalisée qu'avec l'apparition d'Active Directory.

Windows NT a également introduit et étendu le concept de Contrôleur de Domaine. Ce concept, s'il est aujourd'hui très lié au concept même d'annuaire (un annuaire Active Directory se trouve obligatoirement sur une machine faisant office de Contrôleur de Domaine), était un peu différent.

Sous Windows NT 4.0, deux types de Contrôleur de Domaine existaient :

- Les PDC, ou Primary Domain Controler - Contrôleur de Domaine Principal
- Les BDC, ou Backup Domain Controler - Contrôleur de Domaine Secondaire

La différence entre ces deux types de Contrôleur de Domaine est assez importante. Un domaine ne pouvait avoir qu'un seul PDC, mais plusieurs BDC. Le PDC était le Contrôleur autoritaire pour le domaine, et le seul sur lequel il était possible d'ajouter une machine ou un utilisateur au domaine. Les BDC n'étaient là qu'en cas de problème sur le PDC, pour prendre le relais. Cette notion de serveur primaire autoritaire unique et de serveurs secondaires dits de recopie, de sauvegarde, ressemble beaucoup à l'organisation classique des serveurs DNS.

1.3.2. Le Contrôleur de Domaine de Windows 2000

1.3.2.1. NTDS.DIT : la base de données d'Active Directory

Active Directory est un annuaire, il lui faut donc enregistrer les informations qu'il contient dans une base de donnée. Cette base de données est modélisée sous la forme d'un seul fichier, appelé ntds.dit, et localisé dans `%systemroot%\NTDS\ntds.dit`

L'extension de ce fichier, DIT, signifie Directory Information Tree, ou arborescence d'informations de l'annuaire.

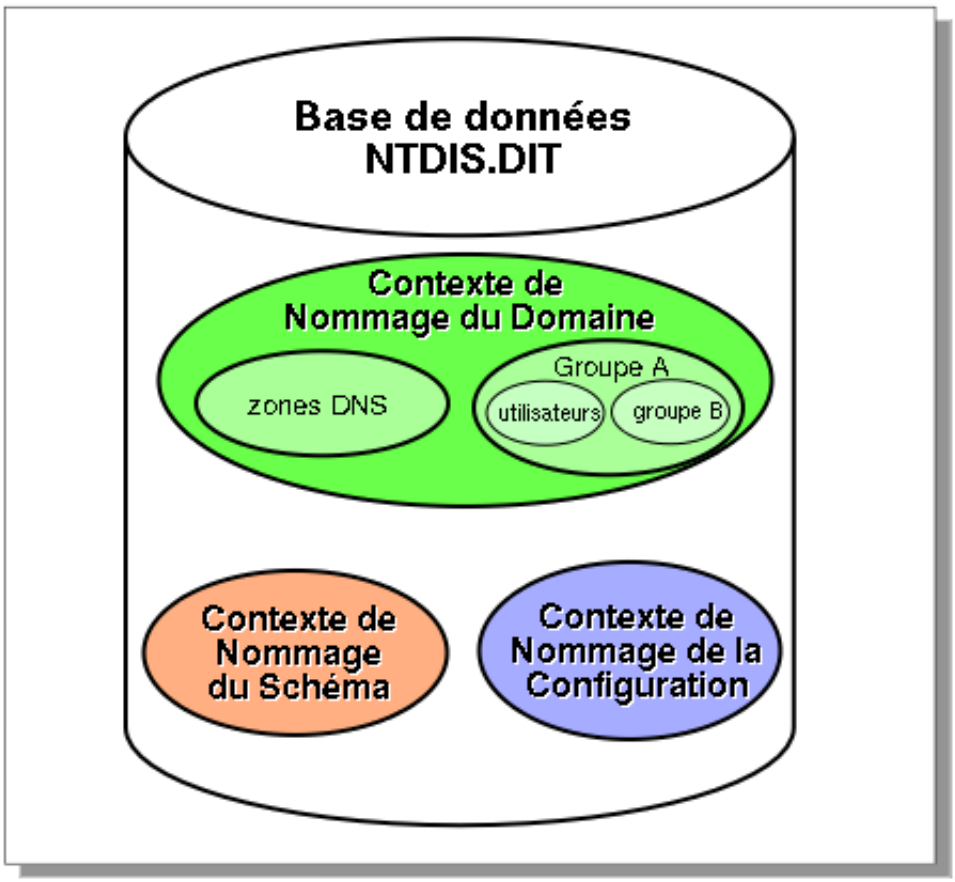
Cette base de données est basée sur la base *ESE* (Extensible Storage Engine), créée à l'origine pour Microsoft Exchange Server. Elle peut stocker plusieurs millions d'objets, et atteindre une taille maximale théorique de 70To. En comparaison, la base utilisée pour stocker les utilisateurs de Windows NT 4.0 pouvait au maximum contenir 40 000 entrées.

Dans le répertoire accueillant la base de données d'Active Directory, se trouvent également les journaux des transactions (ebd*.log). Ces journaux sont circulaires, ce qui peut être assez déroutant pour un administrateur venant du monde Unix. Afin d'éviter une perte des journaux dans le cas où le système viendrait à manquer d'espace disque, Windows 2000 créée deux fichiers de journaux réservés, `res1.log` et `res2.log`.

1.3.2.2. L'organisation des données dans Active Directory : contenu et schema

Active Directory est une base de données, et par conséquent contient de nombreuses informations. Ces informations sont structurées de la façon la plus adaptée, afin de respecter au mieux les contraintes d'un annuaire électronique.

Figure 2. Contenu de la base de données Active Directory



Trois sections, ou partitions, composent donc la structure d'Active Directory. Ces sections sont appelées *Naming Contexts*, ou Contextes de Nommage. Ces trois contextes sont :

- Le *Domain Naming Context*, Contexte de Nommage du Domaine
- Le *Configuration Naming Context*, Contexte de Nommage de la Configuration
- Le *Schema Naming Context*, Contexte de Nommage du Schéma

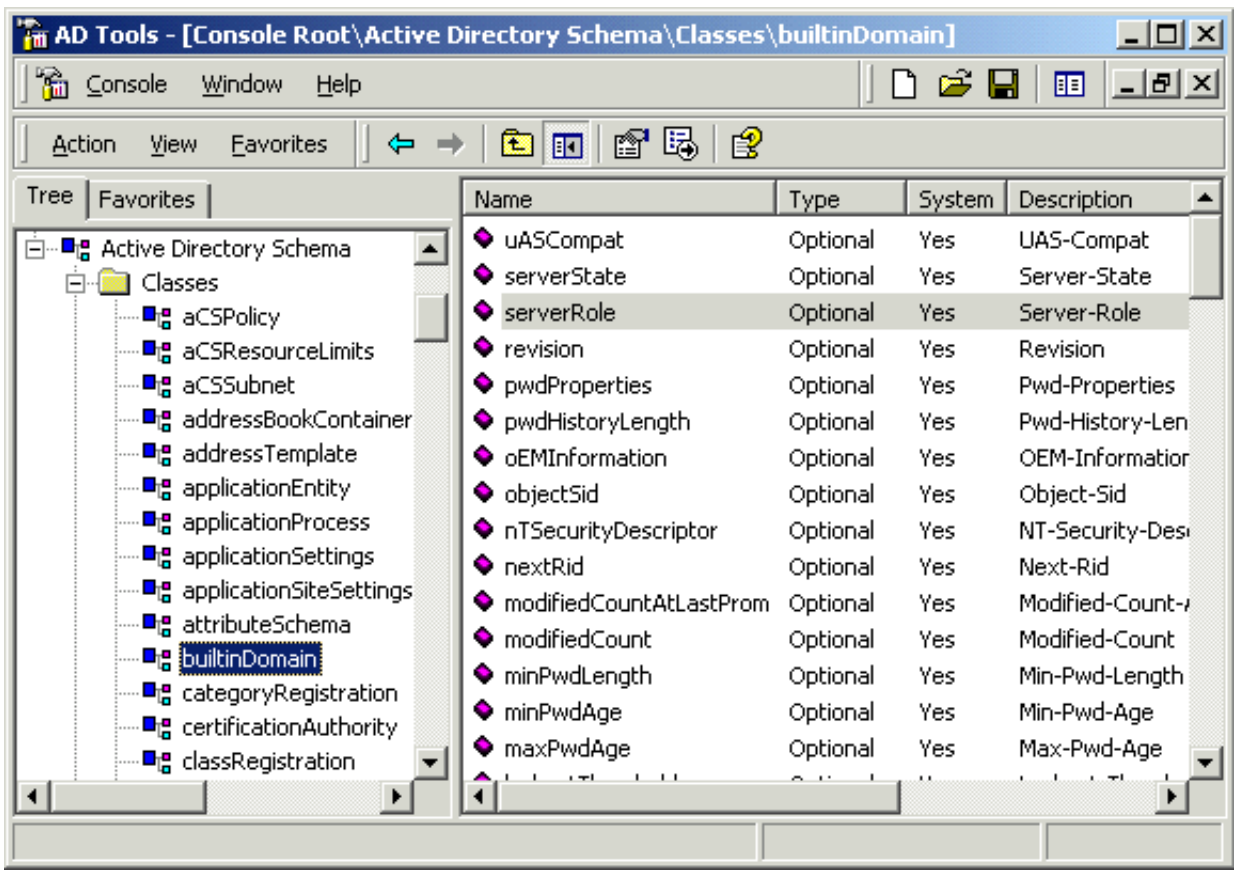
La première section contient les informations qui, la majorité du temps, sont assimilées à Active Directory. C'est à dire la partie concrète de l'annuaire, les informations auxquelles Active Directory permet d'accéder, telles que la description des domaines et des Unités d'Organisation.

La deuxième section, le Contexte de Nommage de la Configuration, contient les informations concernant les sites, les sous-réseaux, les media de réplication [Section 1.3.2.6], les permissions, les données de configuration du service de réplication de fichiers, du service Active Directory, ainsi que la configuration de divers autres services reposant sur Active Directory.

La troisième section, le Contexte de Nommage du Schéma, définit la structure abstraite d'Active Directory. Cette structure est extrêmement importante, c'est grâce à elle que les informations sont organisées de façon consistente à l'intérieur de l'annuaire. Y sont définis les structures et les types de données des objets et des propriétés contenus dans Active Directory. Un parallèle simple peut être fait entre le schéma d'Active Directory et la définition des classes d'un programme orienté objet.

Windows 2000 permet de modifier le schéma de l'annuaire au moyen d'un outil intégré dans une *console MMC* (Figure 3). Par exemple, supposons qu'un administrateur souhaite stocker la configuration de ses routeurs dans l'annuaire, il faudra modifier le schéma afin de lui ajouter de nouveaux types d'objets et d'attributs, à même d'accueillir ces données spécifiques.

Figure 3. Édition du schéma Active Directory



Cisco et Microsoft ont beaucoup travaillé ensemble afin de rendre possible ce type d'utilisation. De ce travail commun est né, dans un premier temps, DEN (Directory Enabled Networking) [DEN98], puis CNS/AD (Cisco Networking Services for Active Directory), qui étend le schéma Active Directory standard avec un ensemble de primitives permettant d'intégrer à l'annuaire de nombreuses données de configuration spécifiques aux équipements Cisco.

Cependant, s'il est intéressant de pouvoir modifier le schéma de l'annuaire Active Directory, cela reste une opération exceptionnelle. Une modification inadaptée du schéma est susceptible de rendre l'annuaire moins efficace. De plus, les modifications du schéma Active Directory sont irréversibles.

1.3.2.3. Notions d'Arbre et de Forêt

Deux nouvelles notions sont apparues avec Windows 2000 et Active Directory, qui n'existaient pas sous Windows NT 4.0. Ces notions viennent compléter le concept de domaine, et s'inscrivent dans le prolongement de la volonté de Microsoft d'utiliser au maximum les conventions de nommage classiques en place sur Internet [Section 1.5].

La première notion est la notion d'arbre. Un arbre représente un ensemble de domaines composant une structure hiérarchique, où un domaine fait office de domaine racine. Par exemple, les domaines stagiaires.hsc.fr, tech.hsc.fr, et hsc.fr forment un arbre, tech.hsc.fr et stagiaires.hsc.fr étant des sous-domaines du domaine racine hsc.fr.

Les concepts de domaines Windows 2000 et de domaines DNS étant encore séparés, il est ici supposé que le domaine DNS hsc.fr est également un domaine racine Windows 2000.

Tous les domaines d'un arbre partagent un espace de nommage commun. Ils disposent également du même schéma, de la même configuration, et le Catalogue Global [Section 1.3.2.8] est répliqué entre tous les contrôleurs de domaine appartenant à l'arbre. Seul le Contexte de Nommage du Domaine n'est pas répliqué dans tout l'arbre.

La seconde notion est la notion de forêt. Une forêt est un ensemble de domaines qui ne sont pas sous-domaines les un des autres, mais qui sont liés par une relation de confiance bidirectionnelle transitive [Section 1.3.2.5]. Par exemple, les domaines stages.hsc.fr et zork.glou.net pourraient appartenir à la même forêt (mais pas au même arbre). L'un pourrait être un domaine racine Windows 2000, et le second lui faire confiance et le répliquer. Une forêt ne nécessite pas de domaine DNS racine commun (à l'exception de ".", bien entendu), mais n'aura qu'un seul domaine racine Windows 2000. Le premier domaine appartenant à une forêt est automatiquement promu domaine racine. Dans une même forêt, les contrôleurs de domaine partagent le schéma, le Contexte de Nommage de la Configuration, et le Catalogue Global.

1.3.2.4. Domaine racine

Un domaine Windows 2000 est constitué du Contexte de Nommage du Domaine dans Active Directory. Il représente l'essentiel du contenu accessible de l'annuaire, des utilisateurs, groupes, machines, etc., mais également des empreintes de mot de passe, des SID, ...

Le premier domaine Windows 2000 mis en place diffère un peu des suivants. Il est appelé domaine racine Windows 2000, et est *de facto* le seul à pouvoir modifier les Contextes de Nommage du Schéma et de la Configuration de l'arbre ou de la forêt desquels il est domaine racine.

De ce fait, un domaine racine Windows 2000 ne peut être supprimé, et ne peut pas être rattaché à un domaine existant.

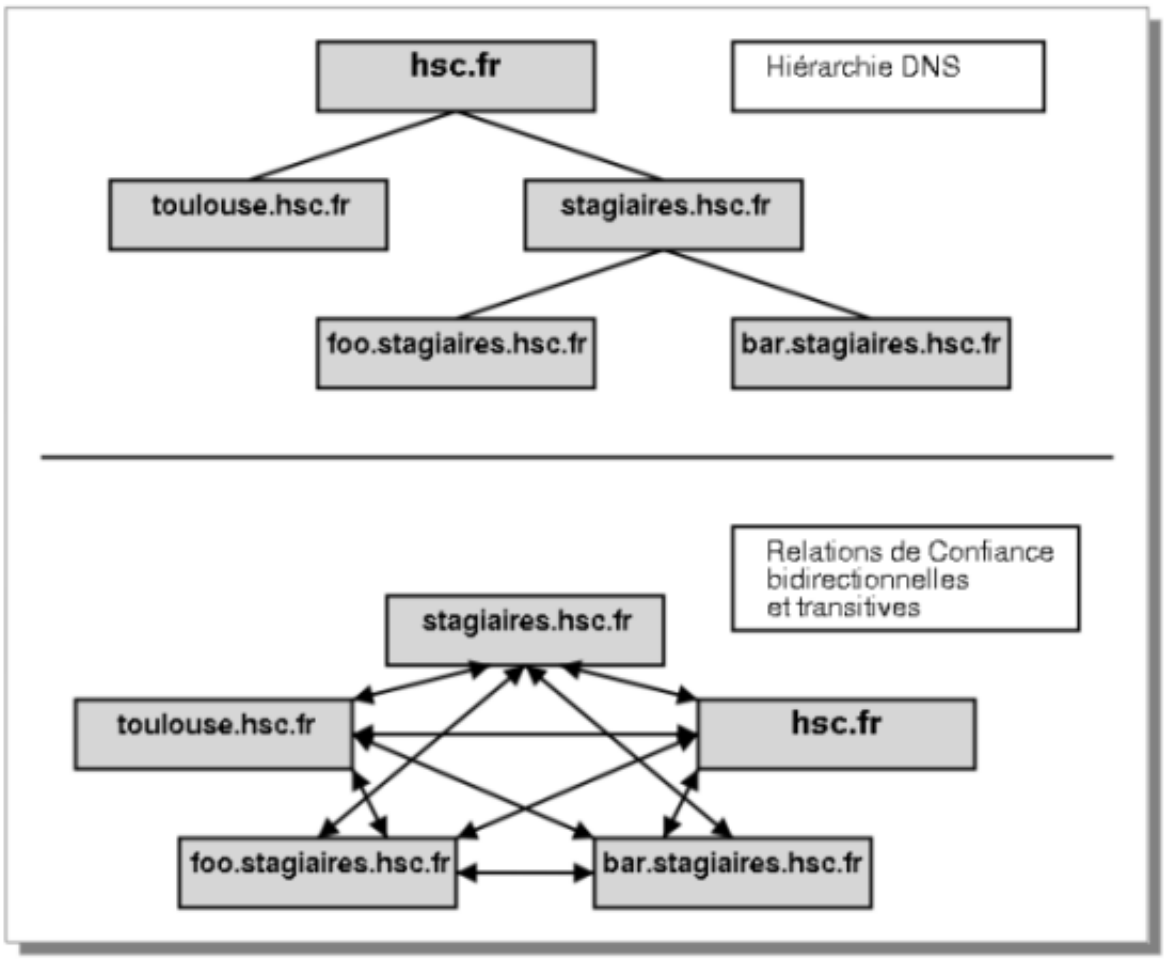
1.3.2.5. Relations de confiance entre domaines

Les domaines marquent les limites de la réplication. Les domaines rattachés, que ce soit dans une forêt ou dans un arbre, partagent des données communes, mais les données propres à un domaine particulier ne sont pas répliquées ailleurs que sur les contrôleurs de ce domaine. La création de domaines permet donc de contrôler en partie le trafic de réplication sur un réseau.

Cependant, malgré cette limite de réplication, il est possible de définir des relations de confiance entre plusieurs domaines. Par défaut, tous les domaines d'un arbre ou d'une forêt sont liés par une relation de confiance bilatérale transitive. Un utilisateur du domaine HSC, par exemple, pourra donc s'authentifier sur n'importe quelle machine de la forêt ou de l'arbre auquel appartient le domaine HSC, même si cette machine appartient à un domaine différent.

Sous Windows NT 4.0, les relations de confiance étaient assez différentes, puisqu'unilatérales, et non transitives. Windows 2000 permet toujours d'établir ce type de relations de confiance, désormais appelées Confiance Explicite. Cela dit, ces relations doivent être créées manuellement. Ce type de relation permet de lier un domaine Windows 2000 à un domaine Windows NT, voire un autre domaine Windows 2000. Ce type de relation, contrairement aux relations bilatérales et transitives, n'implique aucune réplication entre les domaines. Par conséquent, un domaine lié à un domaine racine par ce type de relation n'y est pas « rattaché ».

Figure 4. hiérarchie de domaines et relations de confiance



1.3.2.6. réplication multi-maîtres

Un même domaine peut contenir plusieurs contrôleurs de domaine. Comme on l'a vu précédemment [Section 1.3.2.4], un seul de ces contrôleurs est authoritaire, et contrôle, entre autre, le schéma de l'annuaire. Pourtant, chacun des annuaires peut se voir ajouter des entrées, entrées qui devront être accessibles par tous les autres contrôleurs de domaine si l'on souhaite que le domaine conserve son intégrité.

Afin de s'assurer que tous les contrôleurs disposent des mêmes données, Microsoft a donc mis

en place un système efficace de réplication, dit multi-maître. Cette réplication entre contrôleurs de domaine permet de répartir la charge de façon transparente, mais aussi d'augmenter la tolérance aux pannes.

La réplication multi-maître est un concept complètement nouveau dans Windows 2000. Jusqu'ici, Windows NT s'appuyait sur les notions de PDC et de BDC [Section 1.3.1], où seul le PDC était maître des informations. Windows 2000 assoupli considérablement ce concept en permettant à chacun des contrôleurs d'un domaine de propager les changements qui y ont été fait à tous les autres contrôleurs. La notion de contrôleur principal disparaît donc.

Avec ce type de réplication se pose bien sûr le problème des conflits. Pour résoudre ceux-ci quand ils arrivent, Windows 2000 utilise des horodatages, ainsi que des numéros de séquence de mise-à-jour (*USN* - Update Sequence Number) et des *GUID* (Globally Unique Identifier).

Grâce à ces mécanismes, Windows 2000 remplace les enregistrements les plus anciens par les plus récents. De plus, ces mêmes mécanismes permettent également de ne répliquer que le nécessaire.

La réplication, pour être encore plus efficace, ne considère pas les objets Active Directory, mais leurs propriétés. Ce niveau de granuralité supplémentaire permet de réduire considérablement le trafic de réplication.

La réplication Active Directory s'effectue uniquement dans un « site ». Un site est un ensemble de machines ou de sous-réseaux connectés entre eux avec une liaison disposant d'une bande passante minimum. Cette bande passante doit être au minimum de 256Kbps sur le réseau, et au minimum de 128Kbps entre deux machines. Souvent, un site correspond donc à un réseau Ethernet, ou Token-Ring, par exemple.

La notion de site est purement matérielle. Un domaine peut s'étendre entre plusieurs sites, mais la réplication, par défaut, ne se fera pas entre ces sites. Pour qu'elle aie lieu, il faut mettre en place un lien explicite, Inter-Site. Ce lien peut utiliser deux types de transports :

- RPC sur TCP/IP, sur un lien rapide
- SMTP, sur un lien lent

Seul le transport RPC sur TCP/IP est utilisable pour lier deux sites dans le même domaine. Cela signifie donc que les différents sites composant un même domaine doivent être relié physiquement avec des liaisons rapides.

Le transport SMTP, quant à lui, ne peut être utilisé qu'entre deux sites appartenant à deux domaines différents. Le protocole SMTP n'étant absolument pas sécurisé, Windows 2000 chiffre toutes les données transitant sur ce lien, il faut donc, pour utiliser ce type de transport, une infrastructure complète de PKI, comprenant entre autres le composant logiciel Windows 2000 Enterprise Certification Authority.

1.3.2.7. Le FSMO

Certains services sont très peu adaptés au concept de réplication multi-maîtres. Ce type de services tourne donc dans un mode particulier, au sein même d'Active Directory. Ce mode est appelé *FSMO*, *Flexible Single Master Operation*. Dès qu'un contrôleur de domaine fait tourner un tel service, il devient le « maître FSMO » de ce service, et détient alors un rôle FSMO.

Dans Windows 2000, il existe cinq rôles FSMO principaux :

1. L'émulateur PDC
2. Le serveur RID
3. Le serveur d'Infrastructure
4. Le serveur maître du Schéma
5. Le serveur maître du Nommage du Domaine

L'émulateur PDC

Il en existe un par domaine. Ce service est nécessaire pour permettre de maintenir une compatibilité descendante avec les contrôleurs de domaine NT 4.0. L'émulateur PDC réplique sa base sur les BDC NT 4.0 et joue le rôle de « Master Browser ».

Le serveur de RID

Il en existe également un par domaine. Ce serveur a en charge d'allouer des groupes de *RID* (Relative Identifier) à chacun des contrôleurs du domaine. Quand un contrôleur n'a plus qu'une centaine de RID à sa disposition, il contacte le serveur de RID pour obtenir un nouveau groupe de RID.

Le serveur d'Infrastructure

Il en existe un par domaine. A l'exception du Catalogue Global, la base Active Directory n'est pas répliquée entre deux domaines différents. Cependant, il se peut qu'un objet dans un domaine donné référence d'autres objets dans d'autres domaines. Par exemple, un groupe dans un domaine peut contenir un utilisateur appartenant à un autre domaine. Quand un objet change dans un domaine, si cet objet est référencé par d'autres objets dans un autre domaine, ces objets doivent mettre à jour leurs références. C'est le rôle du serveur d'Infrastructure que de scruter de tels changements et de mettre à jour ces références.

Le serveur maître du Schéma

Ce service est le seul à pouvoir effectuer des changements sur le schéma de la base Active Directory [Section 1.3.2.2]

Le serveur maître du Nommage du Domaine

Seul ce serveur est autorisé à ajouter ou supprimer un domaine d'une fôret Active Directory.

1.3.2.8. Le Catalogue Global

Toujours dans le but d'améliorer, d'une part, l'efficacité des mécanismes de réplication, et d'autre part, la rapidité des requêtes aux annuaires de tous les domaines composant le réseau, Active Directory implémente un composant appelé Global Catalog (GC), ou Catalogue Global. Ce catalogue contient la partie des données de l'annuaire qui doit être répliquée entre domaines, ainsi que les données les plus souvent demandées à tous les annuaires de tous les domaines composant le réseau.

Ce Catalogue Global fait partie intégrante de la base de l'annuaire. Il ne représente pas une quatrième division complétant les trois premières [Section 1.3.2.2], mais est composé à partir des données de l'annaires marquées comme appartenant au GC. Les données du Catalogue Global représentent approximativement 55% de la taille totale de la base complète.

Chaque site contient obligatoirement un Catalogue Global. Afin de rendre ce catalogue encore plus efficace, il est possible de lui ajouter des éléments. Bien entendu, si le catalogue devient trop important, tous les avantages qu'il apporte *a priori* sont perdus.

1.4. Vers un nouveau mécanisme d'authentification : Kerberos

Windows 2000 utilise désormais Kerberos 5 comme mécanisme d'authentification. Kerberos 5 et Active Directory sont intimement liés dans Windows 2000.

La partie qui suit expose les principes, les bases et les origines de Kerberos dans Windows 2000, ainsi que les liens entre Kerberos et Active Directory. Une étude complète de Kerberos, complémentaire de celle-ci, est également disponible sur le site d'HSC (http://www.hsc.fr)

1.4.1. Avant Kerberos : NTLM

Il est intéressant, avant toute chose, de chercher à comprendre pourquoi Microsoft a décidé d'utiliser Kerberos 5, un mécanisme d'authentification développé par le MIT, qui existe de longue date sous Unix.

Avant Kerberos, et avant Windows 2000, par conséquent, l'algorithme d'authentification utilisé par Microsoft dans Windows NT était NTLM.

Le principe de NTLM est simple ; basiquement, le principe consiste à stocker une empreinte du mot de passe utilisateur, à partir de laquelle il est impossible de retrouver le mot de passe originel. Ceci

est obtenu au moyen d'une transformation irréversible (One Way Function, OWF). Voici les étapes de l'algorithme :

1. Le mot de passe est converti en unicode, et peut contenir jusqu'à 128 caractères.
2. La chaine obtenue est alors passée en entrée d'une fonction de hachage, MD4, pour obtenir en sortie une empreinte de 128 bits.

Cet algorithme semble assez robuste, mais quelques points méritent d'être soulignés :

- Cet algorithme est très vulnérable à une attaque par dictionnaire. Les empreintes transitant sur le réseau, ce type d'attaque n'est pas négligeable.
- NTLM ne permet qu'une authentification du client au serveur. Le client prouve bien son identité au serveur, mais ne peut avoir aucune garantie quant à l'identité de ce serveur.
- NTLM ne permet pas la délégation d'accréditation. Un service utilisant NTLM comme mécanisme d'authentification ne pourra donc pas représenter un client auprès d'un autre service. Dans Windows 2000, cette délégation est nécessaire afin de rendre possible les relations de confiance transitives entre contrôleurs de domaine.

Malgré cela, il semble que NTLM soit une solution viable pour gérer l'authentification. Pourquoi dans ce cas passer à Kerberos 5 ? Pour une raison simple. Il est impossible, avec NTLM, de mettre en place une authentification unique (*Single Sign On*). Chaque service nécessitant une authentification demandera donc à l'utilisateur d'entrer son mot de passe pour pouvoir le comparer à l'empreinte dont il dispose.

1.4.2. Kerberos 5 : une authentification unique, un protocole éprouvé.

Kerberos 5 permet donc effectivement de palier le problème de NTLM en ce qui concerne l'authentification unique. Il présente cependant de nombreux autres avantages et inconvénients ;

Kerberos est développé par le MIT depuis dix ans. Le protocole est éprouvé, et déjà relativement répandu.

1.4.2.1. Principe

Kerberos repose sur un principe original. Il est architecturé autour de deux éléments clef : l'AS (Authorization Service) et le KDC (Key Distribution Service), respectivement le serveur d'authentification et le centre de distribution des clés. Ces deux éléments sont deux entités logiques distinctes, mais sont très souvent modélisés par la même entité physique. C'est le cas dans

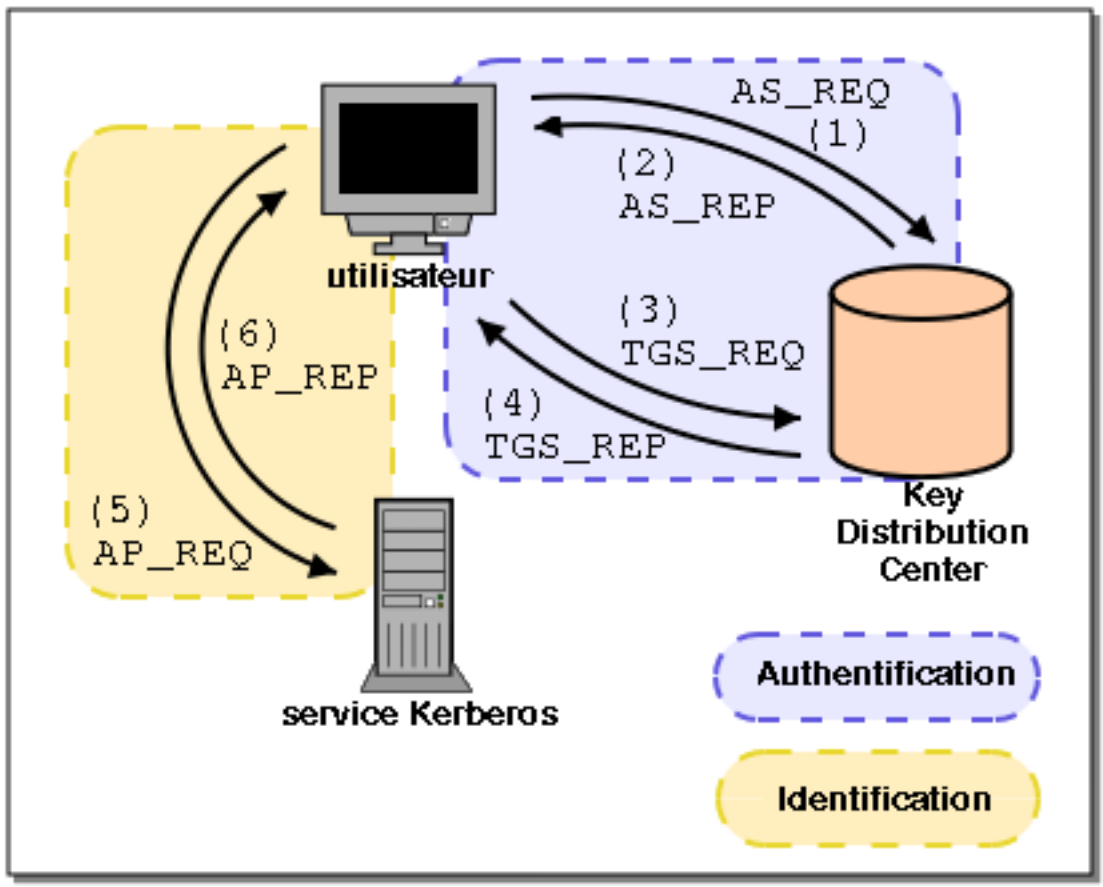
Windows 2000. Pour simplifier, l'AS et le KDC seront assimilés à un seul terme, le KDC. Un troisième élément est utilisé : le TGS (Ticket Granting Service), service de délivrement de ticket.

Quand un utilisateur souhaite s'authentifier, il envoie une demande au KDC (AS-REQ). Lors de cette demande, l'utilisateur va entrer son mot de passe, qui va être transformé, puis utilisé comme clé de chiffrement pour chiffrer la demande d'authentification. A aucun moment, donc, le mot de passe ou une représentation de ce mot de passe ne transitera sur le réseau.

Le KDC recoit cette demande. Il est le seul a connaître le mot de passe de l'utilisateur. Grâce à ce mot de passe, il va pouvoir déchiffrer la demande d'authentification. Si le déchiffrement réussi, c'est que l'utilisateur a chiffré sa demande avec le bon mot de passe ; il vient donc de prouver son identité. Le KDC renvoie alors une réponse positive (AS-REP), comprenant une clé de session, qui servira à valider tous les échanges entre l'utilisateur et le KDC. Si le déchiffrement échoue, le KDC renvoie une erreur (KRB-ERROR). Une fois authentifié, l'utilisateur utilisera sa clé de session pour communiquer avec le KDC et demander des tickets, tickets qui serviront de preuve auprès des services sur lesquels l'utilisateur souhaite s'authentifier.

La Figure 5 résume la demande d'identification d'un utilisateur.

Figure 5. Authentification Kerberos



1.4.2.2. Limitations de Kerberos 5 dans Windows 2000.

Kerberos apporte incontestablement une réponse élégante au problème de l'authentification unique. Pourtant, Kerberos possède également des inconvénients notables, qui sont détaillés dans une étude complète de Kerberos, également disponible sur le site d'HSC (http://www.hsc.fr) Un bref résumé de ces problèmes est fait ici :

Un point central de faille.

Tout repose en effet sur un point central, le KDC. Tout le monde fait confiance au KDC, et c'est la

seule autorité qui règne sur le réseau. Si le KDC est compromis, c'est donc l'ensemble du réseau qui se trouve compromis avec lui.

Une distribution difficile

Le KDC étant le seul à pouvoir prendre en charge l'authentification, il est impossible de répartir les demandes sur d'autres serveurs sans découper le domaine principal en sous-domaines et établir des relations de confiance entre les différents KDC. Microsoft a résolu ce problème au moyen de son système de réplication multi-maître. Cependant, cette solution ne fait qu'aggraver le constat précédent, démultipliant les points sensibles du réseau.

1.4.3. Intégration dans Active Directory

Il est intéressant d'observer de quelle façon Microsoft a intégré Kerberos 5. L'approche est originale, et assez différente de ce que l'on peut trouver dans le monde Unix.

Toutes les entités Kerberos (*principals*) sont enregistrées dans la base Active Directory, avec les clés correspondantes. Toutes ces entrées sont protégées par des ACL spécifiques, qui permettent entre autre d'éviter qu'un administrateur quelconque ne puisse accéder aux clés des entités, malgré ses privilèges.

Active Directory fait un usage intensif de Kerberos pour authentifier tous les accès à la base. Cependant, par soucis de compatibilité avec les versions précédentes de Windows, les outils souhaitant accéder à Active Directory utilisent une couche d'abstraction appelée *SSPI* (Security Support Provider Interface), qui prend en charge l'authentification. Kerberos est le mécanisme d'authentification par défaut, mais il existe aussi un SSP (Security Support Provider, un module d'authentification utilisant l'interface SSPI) permettant d'utiliser NTLM.

Un client LDAP faisant une requête sur une base Active Directory, plutôt que de se connecter de façon classique avec un couple BaseDN/mot de passe, va utiliser des mécanismes génériques pour s'authentifier. De façon transparente, le ticket Kerberos de l'utilisateur sera utilisé pour l'identifier auprès du KDC. Selon que l'identification réussi ou non, la requête sera faite. En fonction des permissions associées à l'utilisateur faisant la requête, le client pourra récupérer les informations qu'il demande ou non.

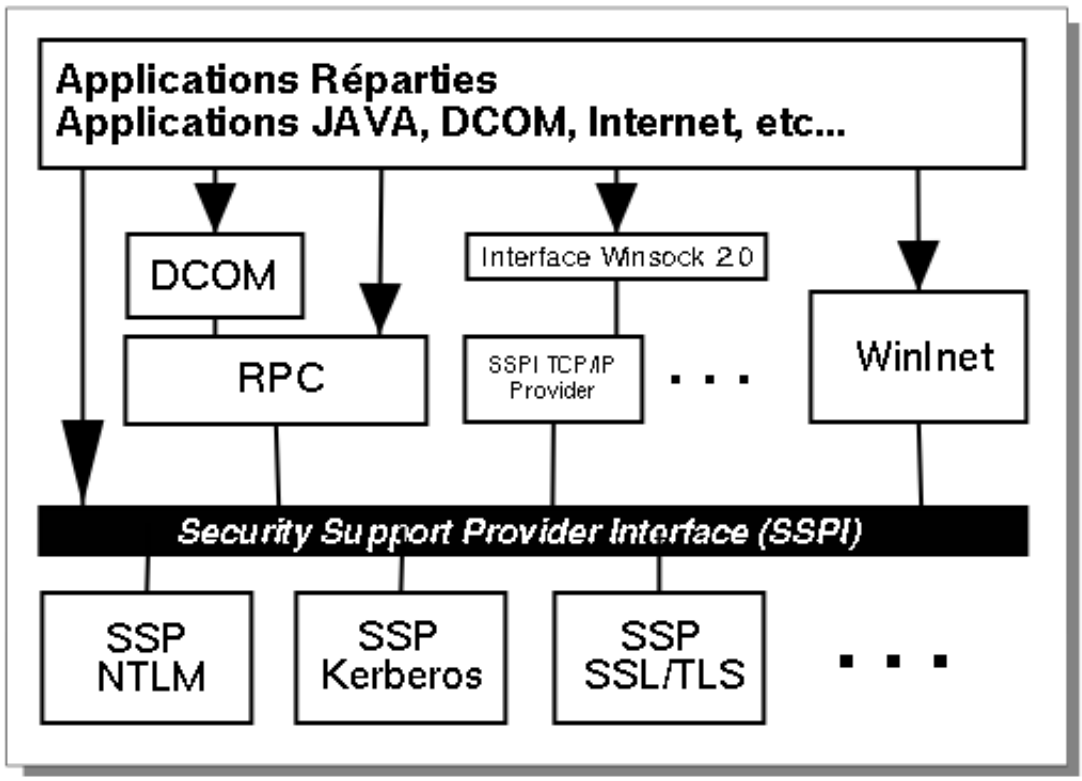
SSPI est une interface très importante dans Windows 2000, et joue un rôle très important dans les interactions avec Active Directory. Ce mécanisme témoigne, comme ADSI, d'une volonté de la part de Microsoft de rendre les accès à l'annuaire aussi souples que possibles. La Figure 6 illustre parfaitement le rôle de SSPI dans le modèle de sécurité Windows 2000.

Cependant, le SSP privilégié dans Windows 2000 est Kerberos 5. De nombreux services utilisent ainsi Kerberos à travers l'interface SSP, dont :

- les services d'impression
- CIFS/SMB
- le service LDAP permettant d'accéder à Active Directory
- IPSec
- la gestion de la QoS (Quality of Service)
- etc.

L'interface SSP est décrite en détail dans [sspi2000].

Figure 6. SSPI et le modèle de sécurité Windows 2000



1.4.4. Compatibilité

Une étude détaillée d'interopérabilité des différentes implémentations Kerberos est réalisée dans un document également disponible sur le site d'HSC () (http://www.hsc.fr)

1.4.5. Spécificités de l'implémentation Microsoft

L'implémentation Kerberos 5 de Windows 2000 diffère quelque peu de l'implémentation traditionnelle décrite dans [rfc1510].

Selon la spécification officielle de Kerberos, les échanges entre clients et KDC se font au moyen de datagrammes UDP (User Datagram Protocol), les datagrammes en question contenant la plupart du temps un ticket, ou des informations visant à l'obtention d'un ticket. Or, à cause de la complexité des tickets émis par le KDC de Windows 2000, il est impossible de faire tenir ceux-ci dans un seul datagramme UDP, ceci à cause de la taille réduite (1500 octets) du MTU Ethernet [6]. Ce qui est particulièrement gênant, puisque, UDP étant un protocole non connecté, les trames UDP ne contiennent aucune information relative à l'ordonnancement des datagrammes. Rien ne garantissant que les datagrammes arrivent dans l'ordre où ils ont été transmis, il est a priori impossible de reconstituer de façon fiable un ticket émis par Windows 2000.

Pour résoudre ce problème, la transmission des tickets d'autorisation de Windows 2000 se fait en TCP, et non en UDP. Afin de garantir l'interopérabilité avec les implémentations classiques de Kerberos, le KDC de Windows 2000 est capable de générer des tickets standards qu'il envoie en UDP. Bien entendu, ces tickets sont très différents des tickets utilisés entre deux Windows 2000.

Cette utilisation de TCP au lieu d'UDP pour l'autorisation Kerberos est très brièvement décrite dans [w2k-kerberos]. Elle est décrite de façon complète dans [draft-brezak-win2k-krb-authz-00], se basant lui-même sur les propositions faites dans [draft-ietf-krb-wg-kerberos-clarifications-00].

1.5. DDNS : le DNS selon Microsoft

1.5.1. Mort programmée de NetBIOS

DDNS (Dynamic Domain Name Service) est l'implémentation DNS de Microsoft. Son objectif est de remplacer à la fois le DNS de Windows NT 4.0, et le service WINS (Windows Internet Naming Service). Pourtant, le service WINS reste présent dans Windows 2000. En effet, WINS est nécessaire si on souhaite utiliser *NetBIOS* sur TCP/IP[rfc1001]. Si les intentions de Microsoft sont claires - faire disparaitre les échanges NetBIOS du réseau - la transition n'est pas aisée.

Historiquement, les clients Windows utilisaient NetBIOS pour communiquer entre-eux. NetBIOS est un protocole de niveau session, pouvant utiliser plusieurs protocoles de transport, tel qu'IP. Afin

de transporter les données NetBIOS sur le réseau, plusieurs protocoles de transports peuvent être utilisés, principalement NetBT (NetBIOS sur TCP/IP) et *NetBEUI*.

Les machines utilisant NetBIOS s'identifient les unes aux autres en utilisant un nom composé de caractères, et non une adresse IP. Microsoft a défini trois type de services au dessus de NetBIOS :

- le service de nommage
- le service de session
- le service de datagramme

Chaque fois qu'une machine souhaite enregistrer un nom ou un service, elle envoie un broadcast sur le réseau. Si le service ou le nom existe déjà sur le réseau, la machine à qui il appartient renvoie alors un message d'erreur sur le réseau, annulant ainsi la demande d'enregistrement.

Il apparait clair que cette façon de procéder surcharge le réseau de façon conséquente, le protocole se reposant sur le broadcast pour l'envoi de messages. Le service WINS tente de résoudre ce problème en centralisant les informations NetBIOS. Ainsi, une machine souhaitant enregistrer un service ou un nom adressera sa demande au WINS plutôt qu'à tout le monde, limitant ainsi les échanges.

Le service WINS permet également d'utiliser NetBIOS sur différents sous-réseaux, à condition bien sûr que la machine faisant office de WINS dispose d'une interface sur chacun des sous-réseaux à relier.

Cependant, même avec un serveur WINS, NetBIOS semble aujourd'hui bien mal conçu, et peu adapté aux réseaux actuels et aux besoins d'interconnexion. D'où la volonté de Microsoft de supprimer NetBIOS. DDNS, la nouvelle implémentation DNS de Microsoft, veut donc concilier la nature statique du service DNS avec la nature dynamique du WINS, ceci au moyen d'un mécanisme de mise à jour dynamique du DNS qui sera détaillé plus loin.

Bien sûr, cette migration n'est pas sans poser problème. Historiquement, NetBIOS était utilisé pour tous les transferts de fichiers via SMB. Même si SMB peut désormais fonctionner directement au dessus de TCP sous Windows 2000, l'interopérabilité avec les anciens systèmes ne peut être maintenue qu'en conservant NetBIOS. Windows 2000 tente donc de faire la transition, en permettant d'activer ou de désactiver NetBIOS.

1.5.2. Intégration Active Directory

Le DDNS de Microsoft s'intègre complètement dans l'environnement Active Directory. Il bénéficie ainsi de la structure sous-jacente de l'annuaire, ce qui lui donne plusieurs avantages ;

- Les enregistrements DNS sont des objets Active Directory. Par conséquent, il est possible

d'appliquer à chaque enregistrement des permissions particulières via les ACL, autorisant ainsi une granularité sans précédent dans la gestion des enregistrements DNS.

- Les zones DNS sont répliquées en même temps que l'annuaire. En plus du concept traditionnel de DNS primaire et secondaire, il est donc possible d'avoir plusieurs DNS autoritaires pour une zone. Cela présente des avantages comme des inconvénients, lesquels sont discutés plus en détail dans la partie 5. concernant le contrôle de domaine.

L'intégration du DNS dans Active Directory pose toutefois un problème dans le cas où l'on souhaite mettre en place un DNS secondaire. En effet, cela n'est tout simplement pas possible (Il faudrait exclure tous les objets Active Directory créés par le DNS de la réplication de l'annuaire, ce qui n'est pas réalisable avec Windows 2000).

1.5.3. Compatibilité de l'implémentation

Microsoft n'est pas à l'origine, loin s'en faut, du concept de DNS. Il est donc naturel de se demander dans quelle mesure l'implémentation de Microsoft est compatible avec les DNS existants. Cette compatibilité est très importante, le DNS étant à la base même du fonctionnement d'Internet.

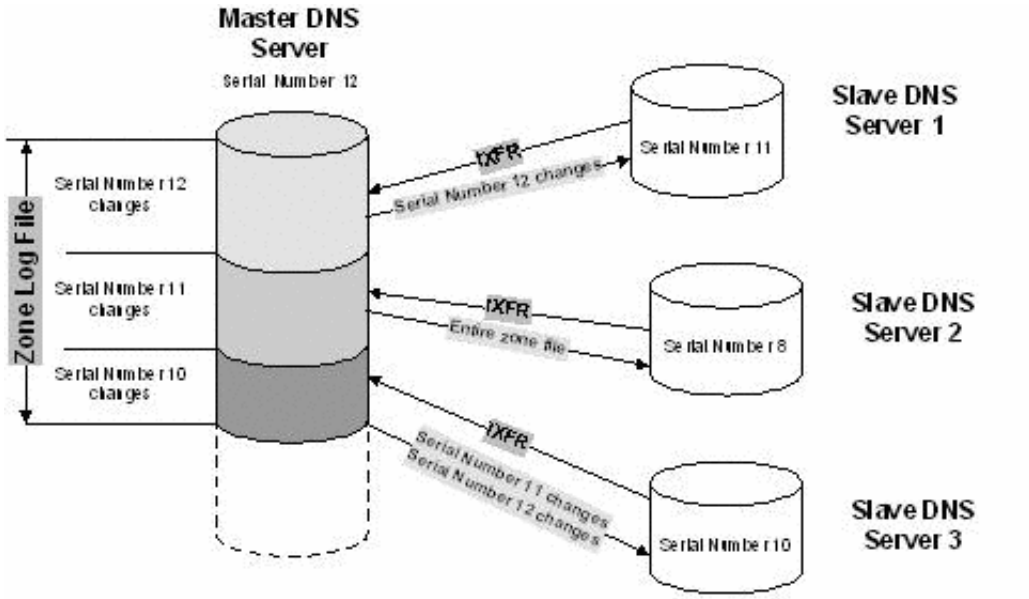
Le DDNS de Microsoft interopère sans problème avec BIND 8.2 et supérieur. Il a besoin, pour pouvoir fonctionner correctement, d'un DNS supportant :

- les enregistrements SRV [rfc2052]
- les mises à jour dynamiques [rfc2136]
- les transferts de zone.

De plus, il supporte les fonctionnalités suivantes :

- le transfert de zone incrémental [rfc1995]
- DNSSec [rfc2535]

Figure 7. Transfert de zone incrémental (IXFR)



1.5.4. Spécificités

1.5.4.1. Mise à jour Dynamique

Bien que compatible avec les implémentations classiques DNS, le DDNS de Microsoft utilise une méthode qui lui est propre pour palier le problème de l'authentification dynamique. Cette mise à jour sécurisée repose sur un ensemble de travaux d'étude menés par des groupes de travail à l'IETF, en particulier sur [draft-ietf-dnsext-gss-tsig-05], travaux s'appuyant eux-même sur GSS-API [rfc2078].

La mise à jour du DDNS se passe en plusieurs temps ;

1. Le client fait une recherche du serveur autoritaire pour la zone qu'il souhaite mettre à jour.
2. Le client tente de faire une mise à jour non sécurisée, en premier lieu. Si le serveur DDNS est configuré pour accepter ce genre de mise-à-jour, l'opération se poursuit de façon non sécurisée. La mise à jour sécurisée rendue possible par DDNS n'est donc efficace que si le serveur est explicitement et correctement configuré.

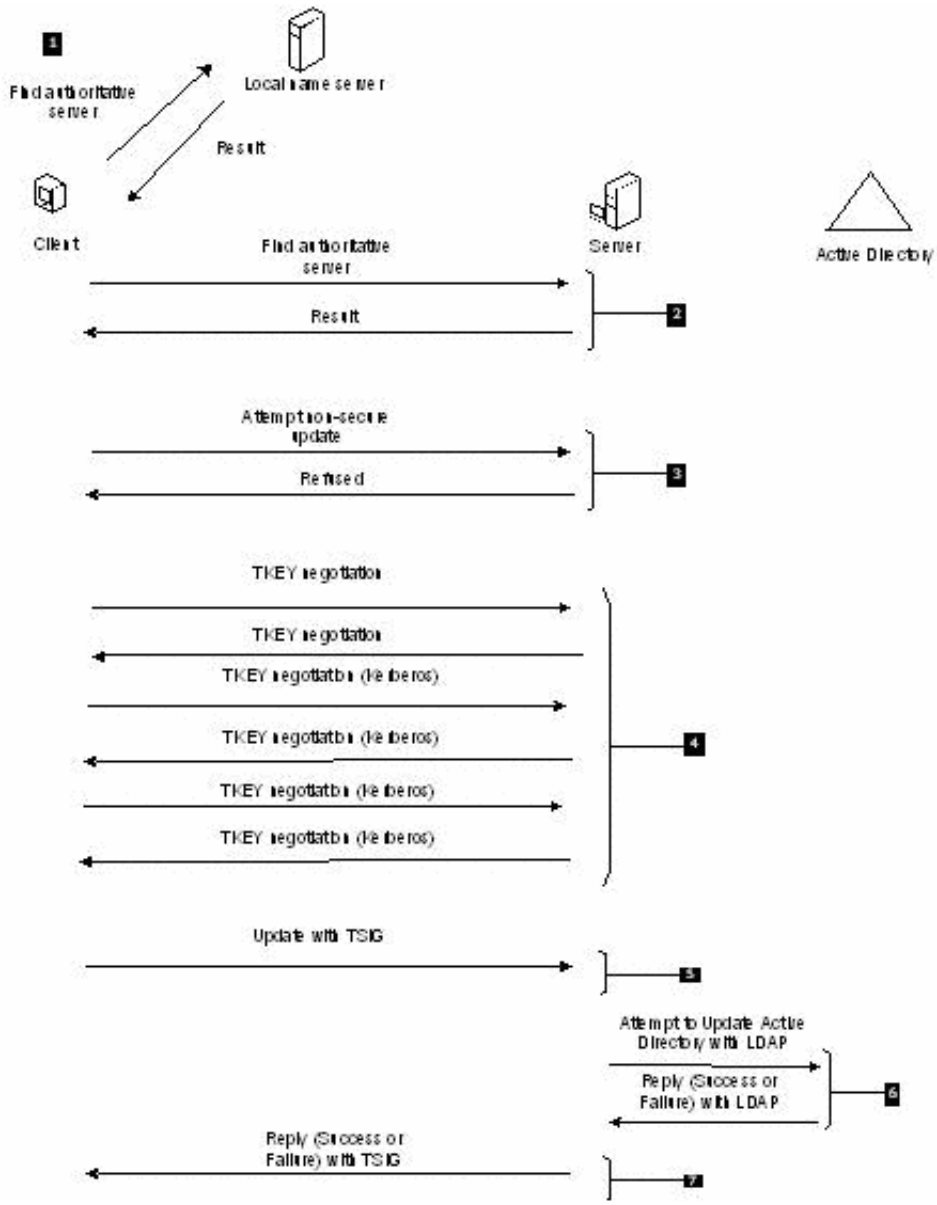
3. La mise à jour non sécurisée ayant échouée, le client et le serveur négocient alors un contexte de sécurité. Le client présente ses privilèges au serveur, au moyen d'un enregistrement TKEY, défini dans [rfc2930].

   Le client commence par négocier le mécanisme de sécurité utilisé pour la négociation. Par défaut, Windows 2000 propose Kerberos. Ce mécanisme de sécurité est ensuite utilisé pour vérifier l'identité des deux parties.

   Une fois le contexte de sécurité défini, il sera utilisé pour créer et vérifier les signatures de chaque transaction DNS.

4. Le client envoie ensuite ses mises-à-jour, signées. Pour cela, il utilise un enregistrement TSIG, défini dans [rfc2845].
5. Si les privilèges du client sont suffisant pour effectuer l'opération, DDNS réalise alors la mise à jour. Il renvoie alors une réponse signée, dans un enregistrement TSIG, dans lequel il informe le client du succès ou non de l'opération.

Figure 8. Déroulement d'une mise à jour Dynamique sécurisée



1.5.4.2. Suppression des enregistrements obsolètes

Grâce aux mises à jour dynamiques permises par DDNS, les enregistrements sont automatiquement ajoutés aux zones DNS quand une machine ou un contrôleur de domaine sont ajoutés. Dans certains cas, toutefois, ces enregistrements ne sont pas supprimés automatiquement, alors qu'ils n'ont plus de raison d'exister.

Le fait d'avoir des enregistrements inutiles n'est pas sans poser problème. Ces enregistrements occupent inutilement de la place sur le serveur, et rendent les informations renvoyées par le serveur moins pertinentes ; en effet, si une machine n'existe plus, il est tout à fait souhaitable que l'entrée correspondante du DNS disparaisse également. Ces enregistrements obsolètes peuvent donc poser un problème de performance du serveur DDNS.

Afin de résoudre ce problème, le DNS de Windows 2000 est capable de supprimer lui même les enregistrements dit « expirés », ou obsolètes. En fait, il est en mesure de chercher dans ses zones les enregistrements qui ont expiré et de les supprimer. Il est possible de contrôler les paramètres d'expiration et de purge des enregistrements en précisant :

- Quels serveurs sont en mesure de supprimer des enregistrements obsolètes
- Quelles zones peuvent être purgées
- Quels enregistrements doivent être supprimés s'ils deviennent obsolètes.

Le DNS de Windows 2000 utilise un algorithme garantissant qu'aucun des enregistrements qui doivent être conservés ne sera supprimé, à la condition que le serveur soit correctement paramétré. Par défaut, le mécanisme de purge est désactivé. Il peut être activé globalement pour un serveur DNS, pour une zone donnée, ou sur un ensemble restreint d'enregistrements.

Durée de vie d'un enregistrement

Au moment de la création ou de la mise à jour d'un enregistrement DNS, un horodatage est effectué sur cet enregistrement. A cause de la présence de cet horodatage, une zone pour laquelle l'expiration automatique des enregistrements est activée diffère légèrement d'un fichier de zone classique. Une telle zone ne peut pas être exportée directement vers un serveur DNS (de type BIND, par exemple). Cependant, le transfert de zone reste possible, l'incompatibilité est donc mineure.

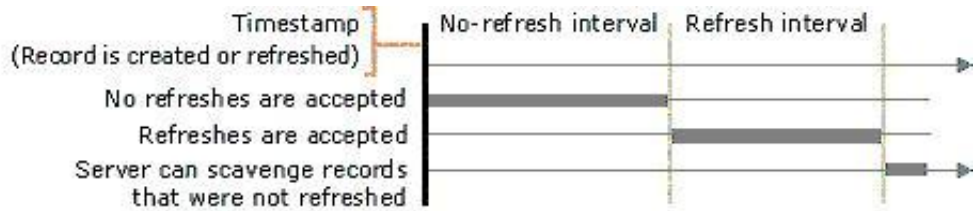
Si un enregistrement est créé autrement que par une mise à jour dynamique, l'horodatage de cet enregistrement vaut 0. Sinon, sa valeur correspond à la date de création ou de mise à jour. Par mesure de protection, les enregistrements dont l'horodatage est nul ne sont pas expirés et purgés par défaut. Il faut forcer l'expiration de tels enregistrements si on souhaite les purger eux aussi.

Le DNS de Windows 2000, s'il est intégré à Active Directory, est automatiquement répliqué entre les différents contrôleurs de domaine. Afin d'éviter une augmentation inutile du trafic lié à cette

réplication, chaque enregistrement dispose d'un paramètre appelé *no-refresh interval*, intervalle de non rafraichissement. Ce paramètre indique le délai nécessaire avant que l'enregistrement puisse de nouveau être raffraichi. Il est toutefois possible de modifier un enregistrement pendant ce délai (si une mise à jour dynamique requiert le raffraichissement, c'est à dire la simple mise à jour de l'horodatage, elle sera ignorée. Si elle requiert une modification de l'enregistrement lui-même, elle sera acceptée).

Le paramètre *refresh* (rafraichissement) d'un enregistrement est pris en compte une fois le délai de non rafraichissement expiré. Durant le délai fixé par le paramètre *refresh*, un enregistrement peut-être mis à jour. Une fois ce délai expiré, si l'enregistrement est marqué comme expirable, il pourra alors être supprimé de la zone DNS lors d'une purge.

Figure 9. Cycle de vie d'un enregistrement expirable



Algorithme de purge

Le serveur effectue les purges à intervalles réguliers. Il est également possible de démarrer une purge à tout moment. Une purge réussira sur une zone si les conditions suivantes sont réunies :

- La zone est une zone primaire
- Le paramètre EnableScavenging est défini pour le serveur et vaut 1
- Le paramètre EnableScavenging est défini pour la zone et vaut 1
- Les mise à jour dynamiques sont autorisées pour la zone
- Le paramètre ScavengingServers est absent, ou contient l'adresse IP du serveur
- L'heure et la date définies par le paramètre StartScavenging sont antérieures à la date et l'heure actuelles.

Le serveur débute une purge dès qu'un des évènements suivant arrive :

- La mise à jour dynamique est activée
- Le paramètre EnableScavenging est passé de 0 à 1 sur la zone
- La zone est chargée

1.5.4.3. Support des caractères Unicode

[rfc952] et [rfc1123], définissant les standards auxquels doit répondre un DNS, restreignent le jeu de caractères utilisables dans un nom à un intervalle bien précis, [a-z0-9]*.

En revanche, les noms NetBIOS posent beaucoup moins de restrictions et autorisent l'usage d'un jeu de caractères plus vaste. Windows 2000 ayant pour ambition de faire disparaître la résolution de noms NetBIOS au profit d'une résolution par DNS, ces différences ne sont pas sans poser problème.

La solution retenue pour permettre une migration simple s'appuie sur un document récent, *Clarifications to the DNS specification* [rfc2181], qui élargi le jeu de caractères autorisés dans les noms DNS ; un nom DNS peut désormais être une chaine binaire, et n'a pas nécessairement à être interprété comme une chaine ASCII. Partant de cela, Microsoft a décidé d'étendre l'espace de nommage DNS au jeu de caractères UTF-8, qui inclue les caractères de la plupart des langues écrites dans le monde.

Toutefois, l'utilisation de ce jeu de caractère peut poser des problèmes de compatibilité avec des applications qui vérifient les noms qui leurs sont passés et qui ne prennent pas en compte cet élargissement du jeu de caractères. De plus, l'utilisation de noms en UTF-8 doit se limiter à un réseau local. Tous les noms qui doivent être visible sur Internet, par exemple, sont dans l'obligation de répondre aux spécifications faites dans [rfc1123].

Références Web

[rfc952] *http://www.ietf.org/rfc/rfc952.txt*.

[rfc1001] *http://www.ietf.org/rfc/rfc1001.txt*.

[rfc1123] *Requirements for Internet Hosts -- Application and Support http://www.ietf.org/rfc/rfc1123.txt*.

[rfc1510] *The Kerberos Network Authentication Service (V5), http://www.ietf.org/rfc/rfc1510.txt*.

[rfc1995] *IXFR, Incremental Zone Transfert, www.ietf.org/rfc/rfc1995.txt*.

[rfc2052] *A DNS RR for specifying the location of services (DNS SRV)*.

[rfc2078] *http://www.ietf.org/rfc/rfc2078.txt*.

[rfc2136] *Dynamic Updates in the Domain Name System, http://www.ietf.org/rfc/rfc2136.txt*.

[rfc2181] *Clarifications to the DNS Specification http://www.ietf.org/rfc/rfc2181.txt*.

[rfc2535] *Domain Name Security Extensions, http://www.ietf.org/rfc/rfc2535.txt*.

[rfc2845] *Secret Key Transaction Authentication for DNS (TSIG),*.

[rfc2930] *Secret Key Establishment for DNS (TKEY RR),*.

[w2kadsi] *http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/w2kadsi.asp*.

[ldup] *http://www.ietf.org/html.charters/ldup-charter.html*.

[sspi2000] *http://www.microsoft.com/windows2000/techinfo/howitworks/security/sspi2000.asp*.

[w2k-kerberos] *http://www.microsoft.com/windows2000/techinfo/howitworks/security/kerberos.asp*.

[draft-brezak-win2k-krb-authz-00] *http://www.ietf.org/internet-drafts/draft-brezak-win2k-krb-authz-00.txt*.

[draft-ietf-krb-wg-kerberos-clarifications-00] *http://www.ietf.org/internet-drafts/draft-ietf-krb-wg-kerberos-clarifications-00.txt*.

[draft-ietf-dnsext-gss-tsig-05] *http://www.ietf.org/internet-drafts/draft-ietf-dnsext-gss-tsig-05.txt*.

[BELLOVIN91] Steven M. Bellovin et Michael Merritt, Winter, 1991, *Limitations of the Kerberos Authentication System, http://www.research.att.com/~smb/papers/kerblimit.usenix.pdf* .

[DEN98] 1998, *Directory Enabled Networks http://www.cisco.com/warp/public/cc/techno/network/dirserv/den/prodl*

Glossaire

A

ADSI

Active Directory Service Interface, interface unifiée d'accès à un annuaire, créée par Microsoft afin de simplifier et généraliser l'accès à un annuaire. ADSI permet ainsi d'accéder à un annuaire Novell, LDAP, iPlanet, etc. avec les mêmes primitives. Se référer à [1.2] pour plus de détails.

authentification mutuelle

Authentification permettant de garantir à la fois l'identité d'un client au serveur et l'identité dudit serveur au client.

Authentication Server - serveur d'authentification

Première entité logique composant le KDC. Le serveur d'authentification prend en charge l'identification d'une entité Kerberos, et fournit un Ticket de délivrement de ticket

Voir aussi : Ticket-Granting Ticket.

E

ESE

Extensible Storage Engine, moteur de base de données créé par Microsoft et utilisé par Exchange Server.

F

FSMO

Flexible Single Master Operation, voir Section 1.3.2.7

G

GUID

Globally Unique IDentifier, identifiant unique. L'unicité de cet identifiant est garantie par l'algorithme de génération.

I

IETF

Internet Engineering Task Force, http://www.ietf.org

K

KDC

Key Distribution Center. Ce service est en fait composé de deux composantes logiques, l'AS et le TGS, qui ensemble constituent l'autorité d'authentification du protocole Kerberos. Seul le KDC est apte à authentifier une entité Kerberos, c'est donc l'élément crucial du protocole Kerberos.

Voir aussi : Authentication Server - serveur d'authentification, Ticket-Granting Server.

L

LDAP

Lightweight Directory Access Protocol

M

MMC

Microsoft Management Console, service de présentation standardisée des applications de gestion. Toute l'administration d'Active Directory se fait par l'intermédiaire de modules s'intégrant dans une MMC.

MTU

Maximum Transmission Unit

N

NetBEUI

Network Basic Extended User Interface

NetBIOS

Network Basic Input/Output System, le protocole utilisé par les versions précédentes de Windows pour communiquer entre elles. Le protocole NetBIOS sur TCP/IP est décrit en détail dans la RFC 1001,

R

RID

Relative IDentifier - Partie d'un SID qui est unique pour chacun des membres d'un domaine.

Voir aussi : RID.

S

RID

Security IDentifier - Nombre unique assigné à chacun des utilisateurs, groupe, ou machine d'un domaine.

SSPI

Security Support Provider Interface - Interface générique d'accès aux mécanismes de sécurité de Windows 2000. Figure 6

T

Ticket-Granting Server

Serveur de délivrement de ticket. C'est la seconde entité logique composant le KDC. Le TGS fournit des tickets de service aux client souhaitant s'authentifier sur un service Kerberos.

Voir aussi : Ticket-Granting Ticket.

Ticket-Granting Ticket

Ticket délivré par le serveur d'authentification, nécessaire pour obtenir les tickets de service délivrés par le TGS.

Voir aussi : Authentication Server - serveur d'authentification, Ticket-Granting Server.

U

USN

Update Sequence Number, numéro de séquence de mise à jour. Les USN sont utilisés lors de la réplication des contrôleurs de domaine, afin de régler les problèmes de conflit.