Chapitre 3
Intégration des zones DNS dans Active Directory

1. Introduction

Nous venons de voir que les zones DNS standards existent sous la forme de fichiers lesquels sont habituellement stockés dans \System32\dns. L'idée consiste maintenant à abandonner ce stockage pour utiliser celui proposé par les services d'annuaire Active Directory. Avant de rentrer dans les détails de cette intégration, il convient de faire remarquer que l'Active Directory et le DNS manipulent des noms qui semblent être identiques, mais qu'en fait ces noms appartiennent à des espaces bien différents.

Le tableau ci-dessous illustre le parallèle qui existe entre les éléments qui appartiennent au DNS et ceux qui appartiennent à l'Active Directory.

Éléments du DNS	**Éléments et objets de l'annuaire Active Directory**
Stockage de type fichier	Stockage de type base de données
Fichiers de zones dans \System32\dns	Objets containers de type **dnsZone**
Enregistrements de ressources (RR - Resource Record)	Objet de type **dnsNode**

Ainsi, on peut dire que l'espace DNS est composé de zones et d'enregistrements de ressources dans les zones, tandis que l'espace Active Directory, appelé « Forêt » dans sa totalité, est composé de domaines et d'objets au sein de ces domaines.

Les objets et attributs Active Directory utilisés dans le cadre du service DNS sont listés ci-dessous :

DnsZone : il s'agit d'un objet container créé au moment où une zone est créée dans l'Active Directory.

DnsNode : il s'agit d'un objet utilisé pour mapper un nom vers un enregistrement contenant plusieurs données.

DnsRecord : il s'agit d'un attribut de type multivaleurs associé à la classe d'objet dnsNode. Il est utilisé pour stocker les enregistrements de ressources dans l'objet dnsNode.

DnsProperty : il s'agit d'un attribut de type multivaleurs associé à la classe d'objet dnsNode. Il est utilisé pour stocker les informations de configuration de la zone.

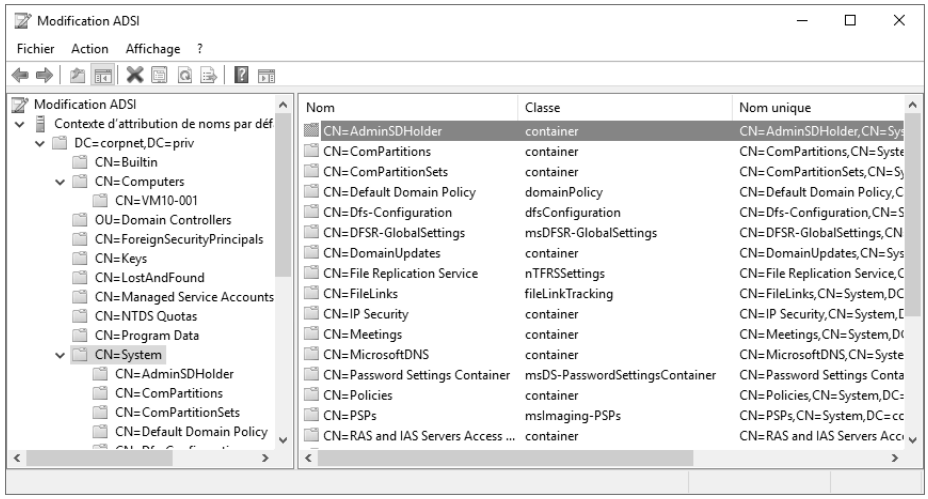
Finalement, chaque zone intégrée à l'annuaire sera stockée dans un objet container de type dnsZone, lequel est identifié par le nom attribué à la zone au moment de sa création.

2. Objets ordinateurs Active Directory et nommages

Chaque ordinateur membre d'un domaine Windows Active Directory existe sous la forme d'un objet de type Computer. La figure ci-après montre un ordinateur appartenant au domaine à l'aide de l'outil ADSI Edit.

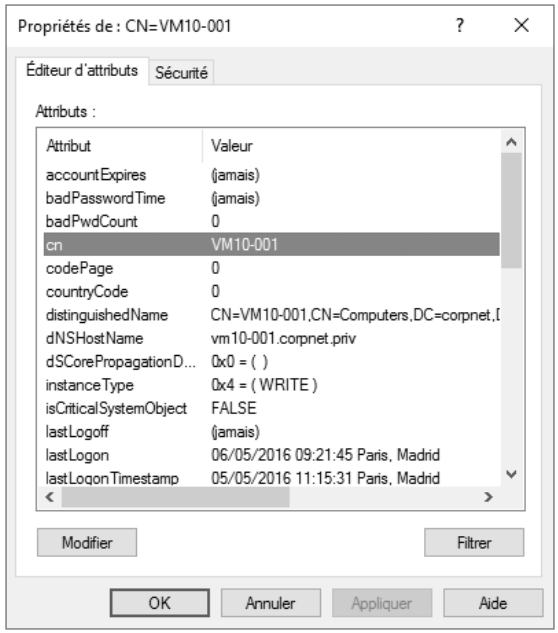
Remarque

Le composant logiciel enfichable ADSI Edit est intégré de base à Windows Server 2016. Vous pouvez y accéder en exécutant Adsiedit.msc ou aussi via le Gestionnaire de serveur. Notez que cet outil d'édition et de modification des objets contenus dans les partitions d'annuaire Active Directory existe depuis de nombreuses années et qu'il faisait partie des Outils de support livrés sur le CD-Rom de Windows Server 2003 et Windows 2000 Server.



L'ordinateur VM10-001 dans le container Computers du domaine Corpnet.priv

En tant qu'objet existant au sein de l'annuaire Active Directory, ses propriétés existent sous la forme d'attributs. Ainsi, ces attributs sont manipulés par l'annuaire lui-même, par les applications ou bien aussi par toute entité habilitée à le faire. La figure suivante montre la fenêtre permettant d'afficher ou de modifier les attributs d'un objet, toujours avec ADSI Edit.



Propriétés de l'objet win7-001 et valeur de l'attribut dNSHostName

Le tableau suivant présente les différents attributs d'un objet appartenant à la classe computer et étant en relation avec la problématique de nommage.

Attributs de l'objet	Désignation et valeur de l'attribut
canonicalName	Représente le nom canonique Active Directory de l'objet corpnet.priv/computers/vm10-001.
cn	Représente le nom commun LDAP de l'objet vm10-001.
displayName	Représente le nom d'affichage LDAP de l'objet vm10-001$.
distinguishedName	Représente le nom distinct complet CN=vm10-001,CN=Computers,DC=corpnet,DC=priv.
dNSHostName	Représente le nom DNS sous la forme d'un FQDN vm10-001.corpnet.priv.
name	Représente le nom vm10-001.
sAMAccountName	Représente le nom SAM (*Security Account Manager*) de l'ordinateur vm10-001$.

Attributs de l'objet	Désignation et valeur de l'attribut
servicePrincipalName	Représente les noms des identités (SPN, *Security Principal Names*) HOST/vm10-001 HOST/vm10-001.corpnet.priv.

Comme expliqué précédemment, ce tableau montre qu'un ordinateur au sein du domaine Windows existe dans plusieurs espaces de nommages distincts. Les attributs les plus importants en termes de sécurité sont le **sAMAccountName** et le **servicePrincipalName**, lequel peut d'ailleurs être contrôlé à l'aide de la commande système **SetSPN.exe**.

Bien entendu, de nombreux autres attributs enrichiront l'annuaire d'informations dont l'usage sera plus perceptible.

Quelques exemples d'attributs sont présentés ci-après :

Attributs de l'objet computer win10-001	Désignation et valeur de l'attribut
objectCategory	CN=Computer,CN=Schema,CN=Configuration, DC=corpnet, DC=priv.
operatingSystem	Windows 10.

3. Avantages de l'intégration des zones DNS dans Active Directory

Les contrôleurs de domaine Windows Server permettent au service DNS de profiter des nombreuses avancées technologiques apportées par l'Active Directory. Ces avantages sont présentés ci-dessous.

3.1 Mise à jour en mode multimaître (ou maîtres multiples)

Dans le modèle habituel de stockage des zones DNS, les mises à jour ne sont possibles que vers le serveur primaire pour la zone. De fait, un seul et unique serveur DNS servant de référence pour la zone est disponible en lecture et écriture. Il s'agit là d'une énorme limitation lorsque l'on souhaite profiter des mises à jour DNS en mode dynamique.

Un autre inconvénient majeur du modèle DNS traditionnel est que toute la disponibilité en écriture de la zone repose sur le seul et unique serveur principal. Si ce serveur n'est pas disponible, alors les requêtes de mise à jour formulées par des clients DNS ne sont pas traitées pour toute la zone. De plus, lorsque la zone arrive à expiration en fonction de la valeur fixée sur l'enregistrement de SOA, celle-ci passe au statut d'expirée et plus aucune demande de résolution DNS n'est traitée.

À l'inverse, lorsqu'une zone DNS est intégrée à l'Active Directory et que la zone est configurée pour supporter les mises à jour dynamiques, alors ces mises à jour peuvent aussi être prises en charge en mode multimaître. En fait, tout serveur DNS de type NS et contrôleur devient une source principale pour la zone. Par conséquent, la zone peut être mise à jour par les serveurs DNS fonctionnant sur tout contrôleur du domaine. Un tel concept permet d'offrir une disponibilité totale, pourvu que l'on dispose de plusieurs contrôleurs de domaine fonctionnant en tant que serveurs DNS. On notera que seuls les contrôleurs de domaine disponibles uniquement en lecture seule, appelés en anglais RODC pour *Read Only Domain Controllers*, font exception à la règle.

3.2 Sécurité avancée des contrôles d'accès sur les zones et les enregistrements

Chaque enregistrement de ressource DNS est un objet Active Directory de type dnsNode. À ce titre il existe et profite, comme tous les autres types d'objets de l'annuaire, des services de sécurité Active Directory. Dans notre cas, il s'agira des authentifications mutuelles utilisant le protocole Kerberos v5 et de l'usage des SPN. Le support des listes de contrôles d'accès vous permet de contrôler qui peut faire quoi sur chaque objet, c'est-à-dire sur chaque enregistrement DNS.

Bien entendu, tous ces objets disposent de permissions par défaut qui sécurisent l'environnement DNS, mais vous pourrez par exemple accéder aux fonctions des ACL (*Access Control List*) pour sécuriser de manière particulière un conteneur dnsZone dans l'arborescence Active Directory. La granularité d'administration est très fine puisque, en fonction des besoins de sécurité, vous aurez toujours la possibilité de gérer chaque zone et chaque enregistrement au sein d'une zone.

Le groupe intégré **Utilisateurs authentifiés** dispose d'une autorisation de type **Créer tous les objets enfants**. Cet ACL permet à tous les ordinateurs Windows supportant les authentifications Kerberos d'être authentifiés.

Remarque

*Le groupe de sécurité **Utilisateurs authentifiés** considère toutes les entités susceptibles d'être contrôlées qu'il s'agisse d'objets utilisateurs, de groupes ou d'objets de type ordinateurs membres du domaine Active Directory ou de tout domaine approuvé.*