Chapitre 5
Configuration et maintenance de DNS

1. Introduction

Le rôle DNS est avec Active Directory un point essentiel. En effet, il permet la résolution de nom en adresse IP. L'arrêt du service DNS empêcherait toute résolution et donc un risque de dysfonctionnement au niveau des applications souhaitant accéder à des ressources partagées (application accédant à une base de données par exemple).

2. Installation de DNS

Comme pour Active Directory ou DHCP, DNS est un rôle dans Windows Server 2019. Il existe deux manières de l'installer : procéder à l'ajout du rôle depuis la console **Gestionnaire de serveur** ou en effectuant une promotion d'un serveur en contrôleur de domaine.

DNS (*Domain Name System*) est un système basé sur une base de données distribuée et hiérarchique. Cette dernière est séparée de manière logique. Ainsi, les noms publics (editions-eni.fr) sont accessibles par n'importe qui quelle que soit sa position géographique.

Il est naturellement plus facile de retenir un nom de domaine ou un nom de poste qu'une adresse IP, de plus l'implémentation d'IPv6 favorise l'utilisation d'un nom plutôt que d'une adresse IP.

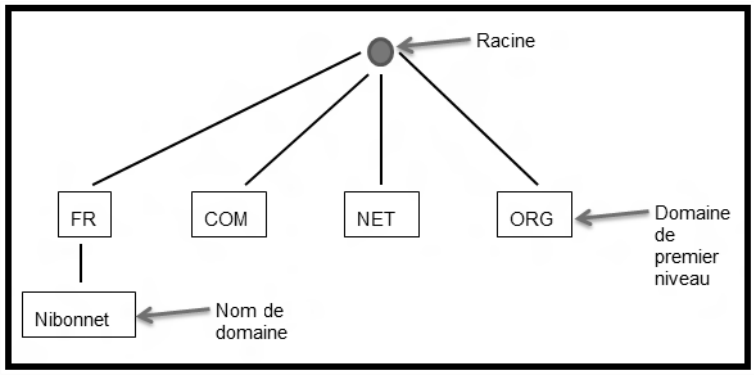
2.1 Vue d'ensemble de l'espace de noms DNS

DNS est construit sur un système hiérarchique. Le serveur racine permet de rediriger les requêtes vers les serveurs DNS juste en dessous de lui. Il est représenté par un point. On trouve en dessous les différents domaines de premier niveau (fr, net, com…). Chacun de ces domaines est géré par un organisme (AFNIC pour le .fr), IANA (*Internet Assigned Numbers Authority*) gère pour sa part les serveurs racines.

Au second niveau se trouvent les noms de domaine qui sont réservés par les entreprises ou les particuliers (editions-eni). Ces noms de domaine sont réservés chez un fournisseur d'accès qui peut également héberger votre serveur web ou tout simplement vous fournir un nom de domaine.

On trouve sur chaque niveau des serveurs DNS différents qui ont autorité sur leur zone. Le serveur racine contient uniquement l'adresse et le nom des serveurs de premier niveau. Il en est de même pour tous les serveurs de chaque niveau.

Il est possible pour une entreprise ou un particulier de rajouter pour le nom de domaine qu'il a réservé des enregistrements ou des sous-domaines (par exemple mail.nibonnet.fr, qui me permet de transférer tout mon trafic mail vers mon routeur, plus précisément à destination de mon adresse IP publique).



Chaque serveur DNS ne peut résoudre que les enregistrements de sa zone. Le serveur de la zone FR peut résoudre l'enregistrement nibonnet, mais il ne sait pas résoudre le nom de domaine shop.nibonnet.fr.

2.2 Séparation entre DNS privé/public

Un système DNS est composé de deux parties, le DNS privé qui a pour charge la résolution de noms DNS dans un réseau local ainsi que le serveur DNS sur les réseaux publics qui résout lui les noms DNS accessibles sur Internet (serveurs web…).

Il est ainsi nécessaire de choisir la politique souhaitée pour les deux serveurs. L'espace de noms interne (privé) peut ainsi être identique à l'espace de noms externe (public). Chaque serveur possède bien sûr ses propres enregistrements. Ce type de solution est valable pour des tailles de réseau restreintes. Il est fréquent de trouver un espace de noms interne différent de l'externe. L'espace de noms se trouve ainsi complètement séparé en deux parties bien distinctes. Enfin une solution hybride consiste à définir au niveau des DNS privés des sous-domaines de l'espace public.

2.3 Déploiement du DNS

Lors de la mise en place d'une solution DNS, il est important de prendre en compte certains paramètres. Dans un premier temps, il est nécessaire de connaître le nombre de zones DNS configurées sur un serveur ainsi que le nombre approximatif d'enregistrements (ceci afin de fractionner si besoin les enregistrements en plusieurs zones). Par la suite, il est également nécessaire de savoir le nombre de serveurs à installer et à configurer, ceci en fonction évidemment du nombre de clients qui communiquent avec les serveurs. Il est utile d'installer un serveur supplémentaire dans le cas où le nombre de postes client est important, ceci afin de pouvoir éviter la surcharge des serveurs. De plus, l'ajout d'un serveur permet également la continuité de service si le premier serveur venait à subir un dysfonctionnement. Il est nécessaire de connaître le positionnement des serveurs, il est fréquent de trouver au minimum un serveur DNS par localisation (si le réseau de l'entreprise s'étend sur quatre agences, soit quatre réseaux locaux reliés par des liaisons WAN, il est judicieux d'avoir au moins quatre serveurs DNS). Ceci est évidemment assujetti à la taille du site.

Enfin, d'autres interrogations peuvent apparaître, comme l'intégration ou non dans Active Directory. Lors de la création d'une zone, le stockage de cette dernière peut être réalisé de deux manières :

– **Utilisation d'un fichier texte** : l'ensemble des enregistrements est stocké dans un fichier. Ce dernier peut évidemment être modifié à l'aide d'un éditeur de texte.
– **Active Directory** : les enregistrements DNS sont contenus dans la base de données Active Directory. Pour procéder à une modification, il est nécessaire d'accéder à la console DNS. Néanmoins l'intégration de la zone à Active Directory nécessite que le rôle DNS soit installé sur le contrôleur de domaine, sans quoi il est impossible d'effectuer l'opération. Cette dernière offre un véritable bénéfice aux administrateurs. En effet, en plus de sécuriser les mises à jour dynamiques, la réplication s'effectue en même temps que celle d'Active Directory. Les administrateurs n'ont donc plus que celle-ci à gérer.

3. Configuration du rôle

Une fois installé, il est nécessaire de procéder à la configuration du rôle. Dans le cas d'une installation lors de la promotion du serveur en contrôleur de domaine, la création de la zone s'opère automatiquement.

3.1 Composants du serveur

Une solution DNS est constituée de plusieurs composants. Les serveurs DNS, pour commencer, ont pour fonction de répondre aux requêtes de leurs clients mais d'assurer également l'hébergement et la gestion d'une ou plusieurs zones. Ces dernières contiennent plusieurs enregistrements de ressources. Les serveurs DNS publics gèrent également des zones et des enregistrements de ressource. Néanmoins ces derniers ne concernent que les ressources qui doivent être accessibles depuis Internet. Enfin les clients DNS ont eux la fonction d'envoyer au serveur DNS les différentes requêtes de résolution

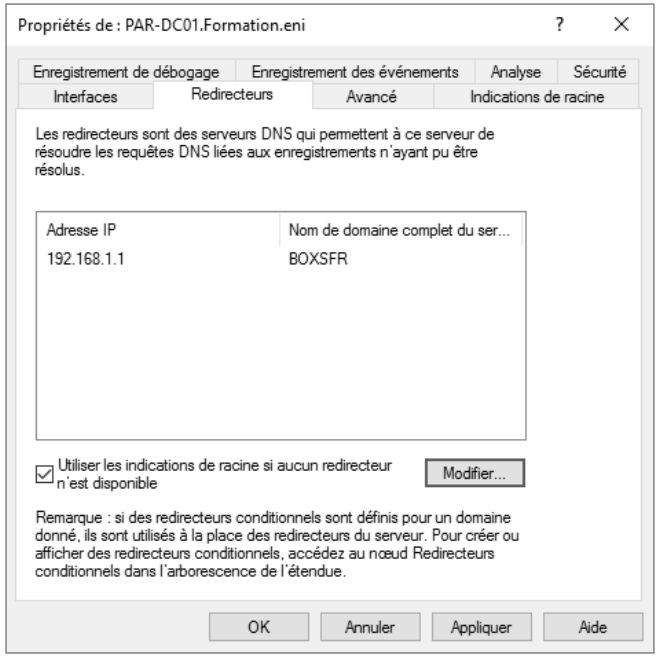
3.2 Requêtes effectuées par le DNS

Une requête permet de demander une résolution à un serveur DNS. Ainsi ce dernier peut apporter deux types de réponses, celles faisant autorité et celles ne faisant pas autorité. Un serveur fournit une réponse faisant autorité si la demande concerne une ressource présente dans une zone sur laquelle il a autorité. Dans le cas contraire, il ne peut répondre au client. Il utilise donc un redirecteur ou des indications de racines afin d'obtenir cette réponse. Deux types de requêtes peuvent donc être utilisés, itératif ou récursif.

Avec les requêtes itératives, le poste client envoie à son serveur DNS une requête afin de résoudre le nom www.editions-eni.fr par exemple. Le serveur interroge le serveur racine. Ce dernier le redirige vers le serveur ayant autorité sur la zone FR. Il peut ainsi connaître l'adresse IP du serveur DNS ayant autorité sur la zone editions-eni. L'interrogation de ce dernier permet la résolution du nom www.editions-eni.fr. Le serveur DNS interne répond à la demande qu'il a reçue au préalable de son client.

Avec les requêtes récursives, le poste client souhaite résoudre le nom www.editions-eni.fr. Il envoie la demande à son serveur DNS. N'ayant pas autorité sur la zone editions-eni.fr, le serveur a besoin d'un serveur externe pour effectuer la résolution. La demande est donc transmise au redirecteur configuré par l'administrateur (le serveur DNS du FAI qui possède un cache plus important par exemple). Si la réponse n'est pas contenue dans son cache, le serveur DNS du FAI effectue une requête itérative puis transmet la réponse au serveur qui lui a transmis la demande. Ce dernier peut maintenant répondre à son client.

La capture ci-dessous montre la configuration d'un redirecteur :

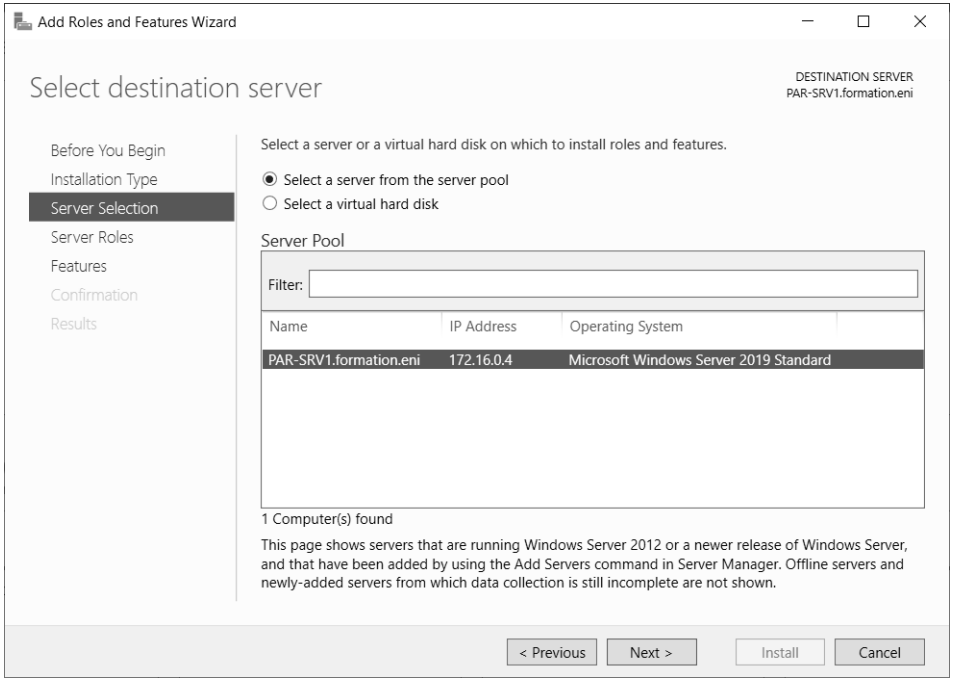


Pour toute demande sur laquelle le serveur n'a pas autorité, le redirecteur est utilisé. Dans certains cas (approbation de forêt AD, etc.), il est nécessaire que la demande de résolution qui va être envoyée à un autre serveur DNS soit redirigée en fonction du nom de domaine (pour le domaine eni.fr envoyer la demande à SRVDNS1). Le redirecteur conditionnel permet d'effectuer cette modification et d'aiguiller les requêtes vers le bon serveur si la condition (nom de domaine) est validée.

Par exemple un redirecteur conditionnel peut être un moyen pour permettre à un administrateur de donner la possibilité de résoudre un nom de domaine par exemple **Formatica.msft**. Dans cet exemple, on installe le service DNS sur un serveur membre du domaine **Formation.eni**.

- Ouvrez une session en tant qu'administrateur du domaine.
- Lancez la console **Gestionnaire de serveur** puis cliquez sur le lien **Ajouter des rôles et des fonctionnalités**.

- Un assistant se lance, cliquez sur **Suivant**.
- Dans les fenêtres **Sélectionner le type d'installation** et **Sélectionner le serveur de destination**, cliquez sur **Suivant** en laissant la valeur par défaut.



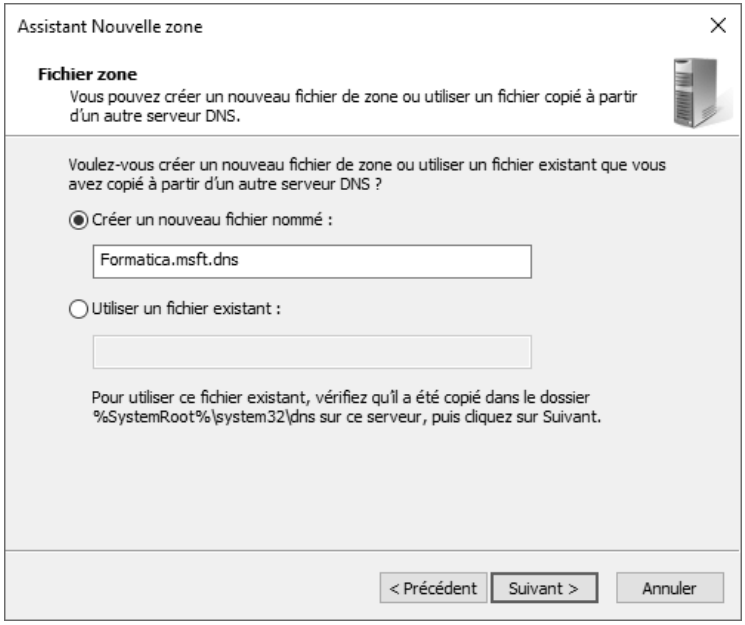
- Cochez le rôle **Serveur DNS** puis cliquez sur **Ajouter des fonctionnalités**.
- Cliquez trois fois sur **Suivant** puis sur **Installer**.
- Fermez la fenêtre une fois l'opération terminée.
- Lancez la console **DNS** depuis les Outils d'administration puis déroulez **PAR-SRV1**.
- Effectuez un clic droit sur **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.
- Dans la fenêtre de bienvenue, cliquez sur **Suivant**.
- Vérifiez que **Zone principale** est coché puis cliquez sur **Suivant**.

- Dans le champ **Nom de la zone**, saisissez **Formatica.msft** puis cliquez sur **Suivant**.

La zone ne peut pas être intégrée à Active Directory car le serveur n'est pas un contrôleur de domaine.

Un fichier est donc créé, ce dernier contient tous les enregistrements de la zone.

- Cliquez sur **Suivant** dans la fenêtre **Fichier zone**.



- Laissez coché **Ne pas autoriser les mises à jour dynamiques** puis cliquez sur **Suivant**.
- Cliquez sur **Terminer** pour effectuer la création de la zone.
- Développez la zone **Formatica.msft** puis effectuez un clic droit sur la zone.
- Dans le menu contextuel, sélectionnez **Nouvel hôte (A ou AAAA)**.
- Saisissez **www** dans le champ **Nom** puis **172.16.0.97** dans le champ **Adresse IP**.