

Le serveur DNS

Objectifs du cours

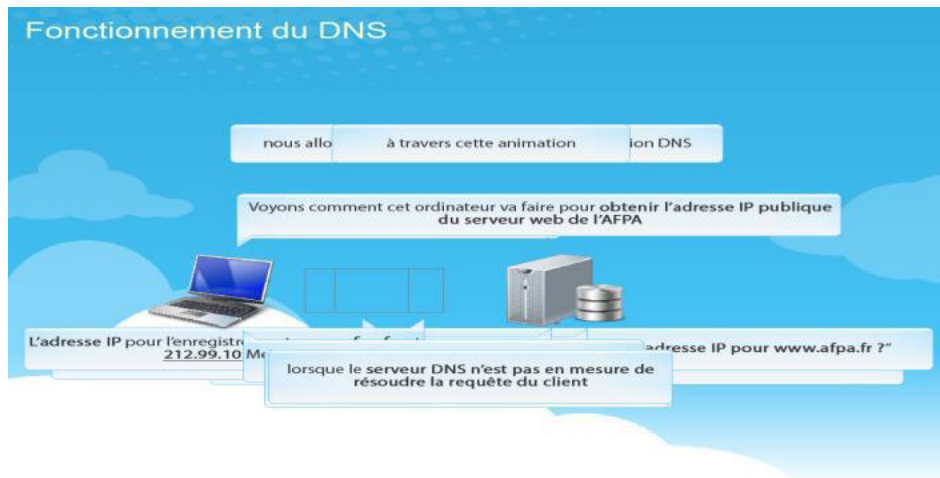
- Démontrer l'intérêt d'utiliser un serveur DNS dans un réseau local
- Expliquer le processus de résolution DNS
- Expliquer la différence entre une zone directe et une zone inversée
- Lister les différents types d'enregistrements

Nous aborderons dans ce cours les techniques que vous emploierez pour configurer et gérer les services DNS (Domain Name System) d'un réseau.

DNS est un service de résolution de noms qui transforme les noms d'ordinateurs en adresse IP.

À l'aide de DNS, le nom d'hôte complet srvad01.contorse.local, par exemple, peut être résolu en adresse IP (192.168.0.1), ce qui permet aux ordinateurs de se trouver réciproquement.

Résolution DNS



Avant d'aborder la configuration du serveur DNS, nous allons d'abord voir le principe de la résolution DNS.

Supposons qu'un ordinateur souhaite accéder au site www.afpa.fr.

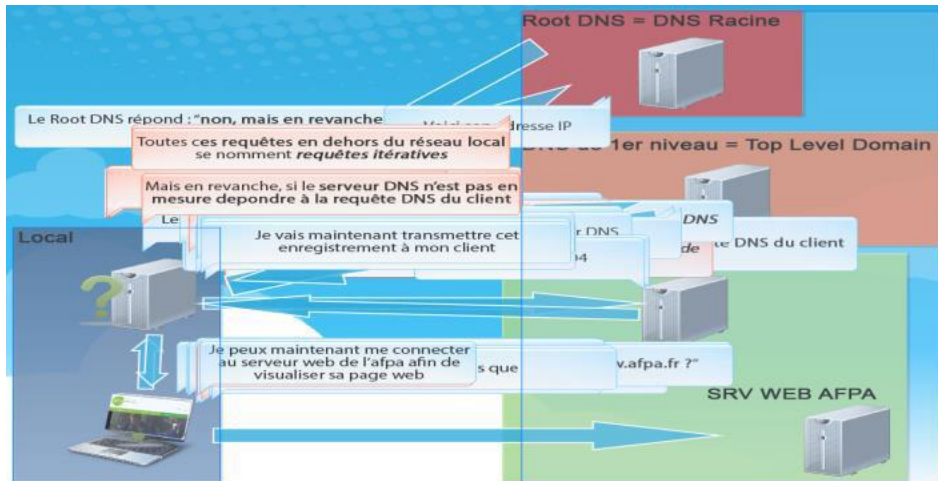
Mais malheureusement, cet ordinateur ne connaît pas l'adresse IP publique du serveur Web de l'AFPA.

Voici comment cet ordinateur va faire pour obtenir l'adresse IP publique du serveur web de l'AFPA :

- Tout d'abord le client DNS, va envoyer une requête UDP sur le port 53 du serveur DNS qui va demander " Quelle est l'adresse IP pour www.afpa.fr ?"
- Le serveur DNS va interroger sa base de données pour voir s'il connaît cette adresse
- Si le serveur connaît cet enregistrement alors il retourne l'adresse IP au client .L'adresse IP pour l'enregistrement www.afpa.fr est 212.99.102.104
- L'ordinateur peut maintenant se connecter au serveur web en utilisant son adresse IP publique.

Comme nous venons de le voir, le fonctionnement de la résolution DNS est simple lorsque le serveur connaît l'adresse.

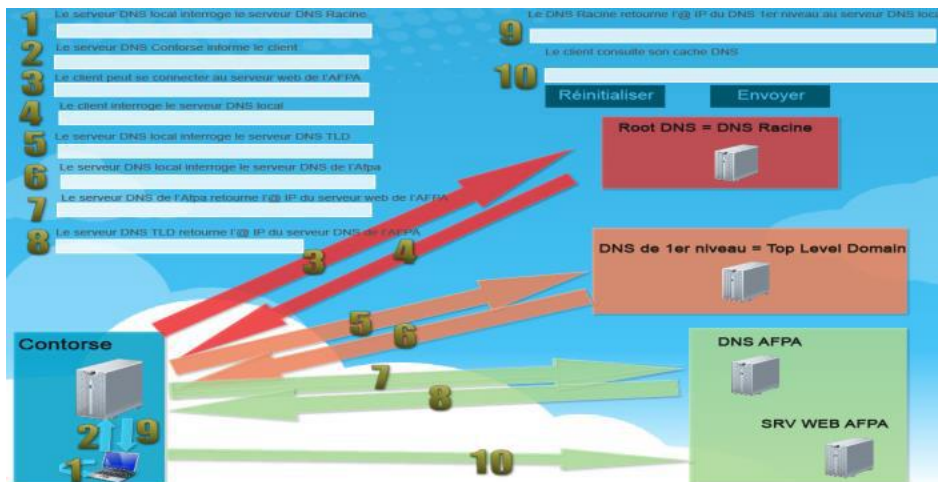
Nous allons maintenant voir en détail le processus des requêtes DNS lorsque le serveur DNS n'est pas en mesure de résoudre la requête du client.



Le poste client souhaite accéder au site web www.afpa.fr .

- Dans un 1er temps, le client consulte son cache DNS afin de voir s'il possède cet enregistrement.
- Si le client ne possède pas cet enregistrement DNS dans son cache, il va interroger le serveur DNS de son entreprise en lui demandant "connais-tu l'adresse IP de www.afpa.fr ?"
- le serveur DNS de Contorse ne possède pas cet enregistrement, il pose alors la question à l'un des Root DNS : « Connais-tu l'enregistrement www.afpa.fr ? »
- Comme les root DNS, qui sont au nombre de 13 et qui sont situés à différents endroits du globe, connaissent les adresses IP des serveurs DNS de 1er niveau (ou TLD), il répond « non, mais en revanche je connais le serveur DNS qui gère le domaine de 1er niveau .fr. Voici son adresse IP »
- Le serveur DNS de Contorse possède maintenant l'adresse IP du serveur DNS qui gère le domaine .fr. Il lui pose cette question : « sais-tu me résoudre l'enregistrement www.afpa.fr ? »
- Le serveur qui gère les .fr répond : « Non, je ne suis pas en mesure de te résoudre cet enregistrement, mais en revanche, je connais l'adresse IP du serveur DNS qui gère le domaine AFPA : là voici »
- Le serveur DNS de Contorse interroge le serveur DNS de l'AFPA : « Connais-tu l'adresse www.afpa.fr ? ».

Afin de vérifier que vous avez bien compris le fonctionnement du processus de résolution DNS vous allez compléter ce schéma en mettant les phrases au bon endroit.

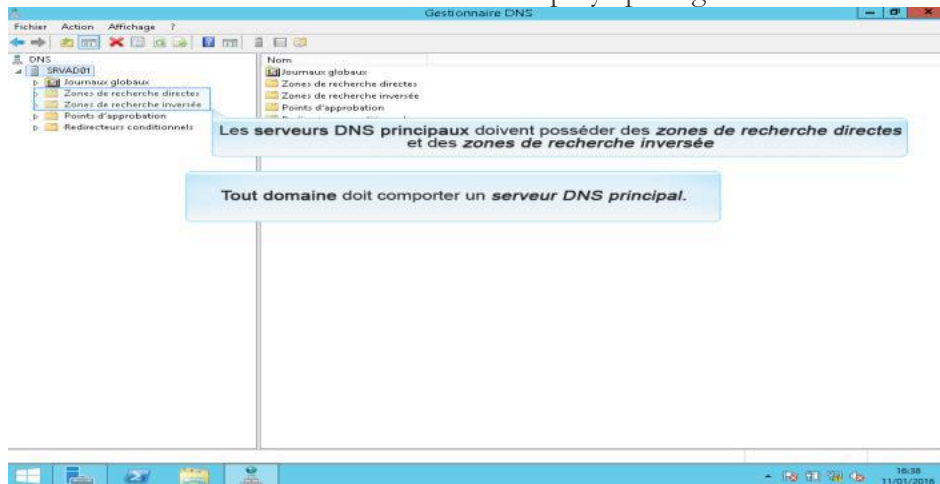


L'outil Gestionnaire DNS

Nous avons vu dans les comment fonctionne la résolution de noms et les termes techniques associés (root dns, tld, etc...).

Il sera ainsi, plus facile d'appréhender le fonctionnement du serveur DNS.

La console Gestionnaire DNS est l'outil employé pour gérer les serveurs DNS locaux ou distants.



Le volet principal de la console est divisé en 2 volets :

- Le volet de gauche donne accès aux serveurs DNS et à leurs zones
- Le volet de droite affiche les détails de l'élément sélectionné

Tout domaine doit comporter un serveur DNS principal.

Les serveurs DNS principaux doivent posséder des zones de recherche directes et des zones de recherche inversées.

Les recherches directes servent à traduire des noms de domaines en adresse IP

Ainsi srvad01 est le nom NetBios du serveur Active Directory et 192.168.0.1 est son adresse IP.

Quand nous ajouterons une station cliente au domaine contorse, un enregistrement supplémentaire apparaîtra correspondant à la station cliente.

Nous reviendrons sur cet aspect du serveur DNS après avoir ajouté notre station cliente.

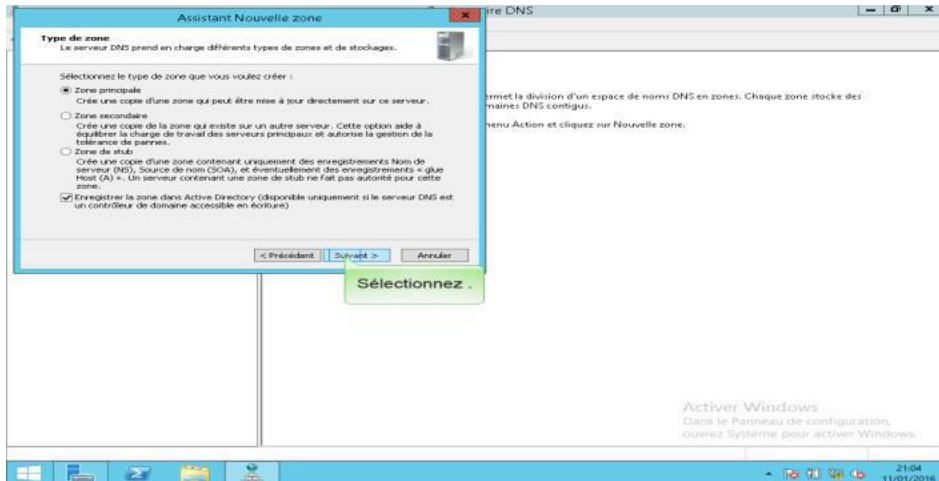
Les recherches inversées servent à résoudre les adresses IP en noms de domaines

La déclaration inversée est importante puisqu'elle est utilisée par certains services.

Ainsi par exemple un serveur de messagerie se présentant en envoi avec une adresse IP n'ayant pas de résolution inversée, a de grandes chances de se voir refuser, par l'hôte distant, la transmission du courrier (erreur de type : IP lookup failed).

Cette résolution est également importante dans le cadre de diagnostics réseaux, car c'est elle qui permet de rendre les résultats de la commande traceroute.

Nous allons maintenant procéder à la création d'une nouvelle zone de recherche inversée.



Comme il s'agit du serveur Active Directory principal, on sélectionne « zone principale » et on vérifie que cette case est bien cochée.

On choisit « Zone secondaire » lorsqu'il s'agit d'un second serveur DNS.

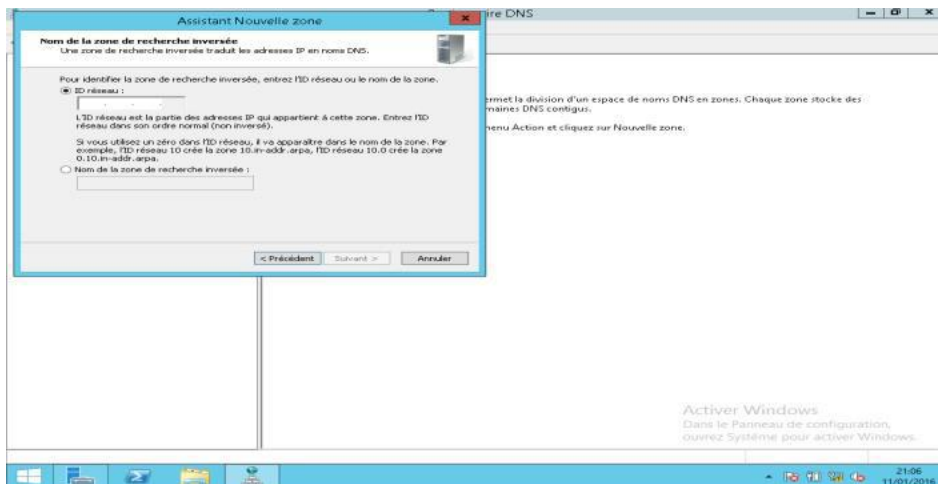
Comme la zone va être intégrée à Active Directory, il faut choisir l'une des stratégies de réplication suivantes :

Choisissez la façon dont les données de la zone doivent être répliquées :

- ☐ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : contorse.local
- ☒ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : contorse.local
- ☐ Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : contorse.local
- ☐ Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

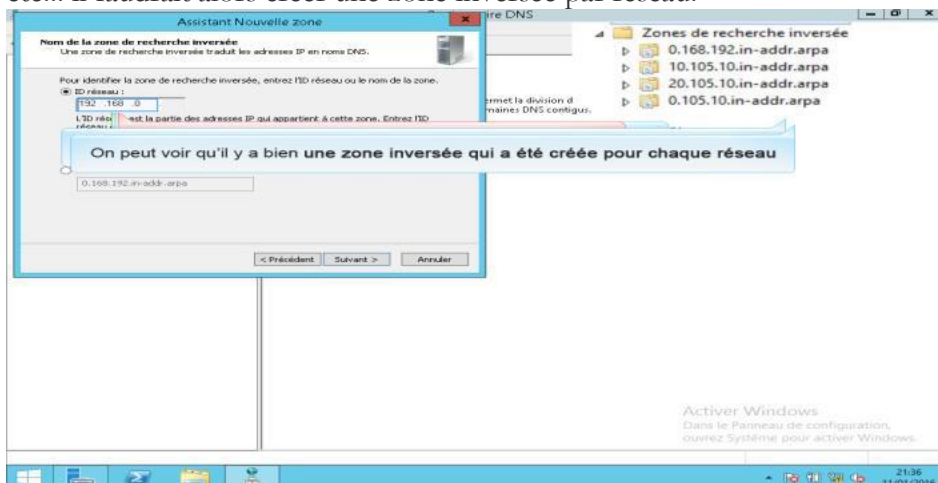
- Option 1 : Cette stratégie permet la réplication la plus large puisque la forêt Active Directory inclut toutes les arborescences des domaines qui partagent les données d'annuaire avec le domaine en cours.
Nous l'avons déjà abordé dans un cours précédent, mais une forêt peut avoir plusieurs domaines : par exemple, contorse.local mais aussi toto.local etc...
Avec cette option, la réplication des enregistrements de la zone inversée se fera sur l'ensemble des serveurs DNS de la forêt.
- Option 2 : Cette stratégie permet de répliquer les informations DNS dans le domaine en cours. Cela signifie que s'il y a un second serveur DNS dans le domaine Contorse, alors les informations des enregistrements de ce serveur DNS seront répliquées sur le second serveur DNS.
- Option 3 : Cette stratégie permet de répliquer les informations DNS sur tous les contrôleurs du domaine en cours, même s'ils ne sont pas serveurs DNS.

Choisissez la deuxième option puisque nous resterons, tout au long de ce cours, dans une configuration mono-domaine.



Saisir l'adresse du réseau.

Dans le cas où il y aurait plusieurs réseaux dans l'entreprise, par exemple, 10.105.10.0, 10.105.20.0 etc... il faudrait alors créer une zone inversée par réseau.



Comme on peut le voir sur cette capture issue d'un serveur en production, il y a bien une zone inversée pour chaque réseau.

Mise à niveau dynamique
 Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.



Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

- ☒ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
 Cette option n'est disponible que pour les zones intégrées à Active Directory.
- ☐ Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
 Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.
- ☐ Ne pas autoriser les mises à jour dynamiques
 Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

Il nous est maintenant proposé de spécifier si les mises à niveau des enregistrements DNS sont autorisées .

En sélectionnant la première option, seuls les clients disposant de comptes d'ordinateurs autorisés et de listes de contrôle d'accès approuvées peuvent dynamiquement mettre à jour leurs enregistrements de ressources sur le serveur DNS.

En clair, pour qu'un ordinateur puisse mettre à jour son entrée DNS, c'est-à-dire lorsqu'il change d'adresse IP par exemple, il doit être intégré au domaine.

On sélectionne la deuxième option lorsque certains postes ne sont pas intégrés au domaine et que ces clients veulent utiliser le serveur DNS de l'entreprise.

Et enfin, on sélectionne la dernière option lorsque le serveur DNS n'est pas intégré à un domaine Active Directory.

Comment tous nos clients et serveurs que nous allons ajouter tout au long de cette progression seront intégrés au domaine Active Directory, nous choisissons la première option.

La zone inversée est maintenant créée.

Pour le moment, seules les entrées correspondant au serveur Active Directory apparaissent.
Nous verrons qu'elle se complétera automatiquement lorsque nous intégrerons des nouveaux ordinateurs dans le domaine.

Après avoir créé les fichiers de zones nécessaires, il est possible d'ajouter des enregistrements aux zones.

Les ordinateurs auxquels les domaines DNS et Active Directory ont besoin d'accéder doivent disposer d'enregistrements DNS.

Bien qu'il existe de nombreux types d'enregistrements DNS différents, la plupart d'entre eux ne sont généralement pas utilisés.

Au lieu de nous intéresser à des types d'enregistrements que vous n'utiliserez probablement jamais, nous allons nous concentrer sur ceux que vous utiliserez.

Les enregistrements de type A mappent un nom d'hôte en adresse IP v4.

Lorsqu'un ordinateur dispose de plusieurs cartes réseau ou adresses IP v4, il doit posséder plusieurs enregistrements d'adresses.

Un enregistrement de type AAA est utilisé pour les adresses IP v6.

Un enregistrement de type Cname définit un alias pour un nom d'hôte.

Cela est très utilisé lorsque votre serveur héberge un site Internet.

Par exemple, le nom d'hôte de ce serveur est srvad0.

Le nom de domaine complet, ou son FQDN (Full Qualified Domain Name) est
srvad01.contorse.local.

Si un poste client souhaite accéder au serveur web de ce serveur, il devra saisir son nom de domaine complet.

Mais il est possible de créer un cname de type WWW qui est un alias de srvad01.

Le poste client pourra saisir www.contorse.local pour accéder au site web du serveur au lieu de
srvad01.contorse.local.

Un **enregistrement de type MX** indique le serveur de messagerie du domaine qui permet de transmettre le courrier électronique aux autres serveurs de messagerie si besoin.

Un **enregistrement de type NS** indique le serveur de noms du domaine, ce qui permet des recherches DNS au sein des diverses zones.

Chaque serveur de noms, principal ou secondaire, doit être déclaré par cet enregistrement.
Comme ce serveur est également serveur DNS, il possède son enregistrement de type NS.

Et enfin un **enregistrement de type SOA (autorité principale)** déclare l'hôte disposant de la plus grande autorité dans la zone et de ce fait, étant la meilleure source d'information DNS de la zone.

Chaque fichier de zone doit avoir un enregistrement SOA.

Il est automatiquement créé lorsque l'on ajoute une zone.

Général Source de noms (SOA) Serveurs de noms

Numéro de série :

Serveur principal :

Personne responsable :

Intervalle d'actualisation : Minutes

Intervalle avant nouvelle tentative : Minutes

Expire après : Jours

Durée de vie minimale (par défaut) : Heures

Durée de vie pour cet enregistrement : : : : (JJJ:HH.MM.SS)

L'enregistrement SOA déclare également d'autres informations relatives à la zone telles que :

- la personne responsable de la zone,
 - la durée de vie minimale d'un enregistrement DNS dans le cache,
 - le numéro de série, qui indique la version des fichiers de la base de données DNS
- Ce numéro est automatiquement mis à jour à chaque modification des fichiers de zone. Il est également possible de le mettre à jour manuellement.

Les serveurs DNS secondaires utilisent le numéro de série pour déterminer si les enregistrements DNS de la zone ont changé.

Si le numéro de série du serveur principal est supérieur à celui du secondaire, cela signifie que les enregistrements DNS ont changé et le serveur DNS secondaire peut demander les enregistrements DNS de la zone principale.

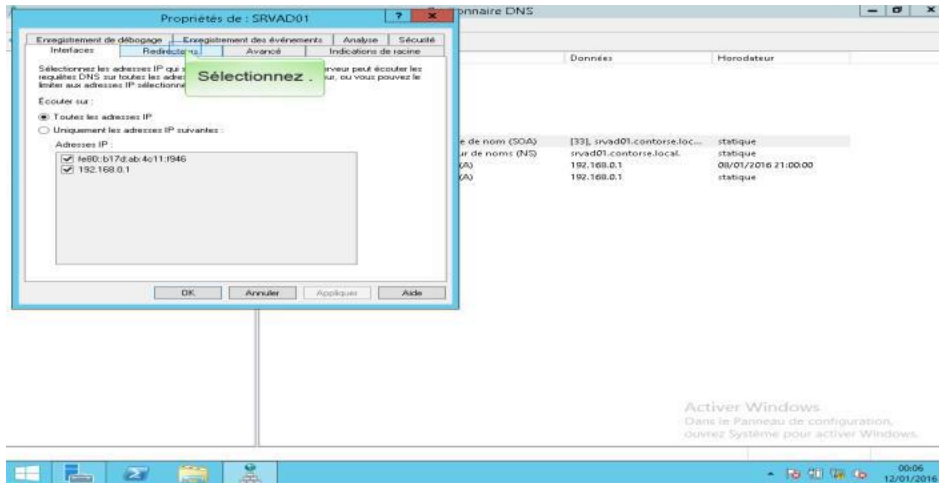
Chaque enregistrement de zone est enregistré dans un fichier texte qui se situe dans le répertoire c:\windows\system32\dns\backup.

Lorsque que vous supprimez une zone ou un domaine, le fichier de zone peut ne pas se supprimer.

Après avoir supprimé votre zone, vous pourrez supprimer ce fichier en toute tranquillité.

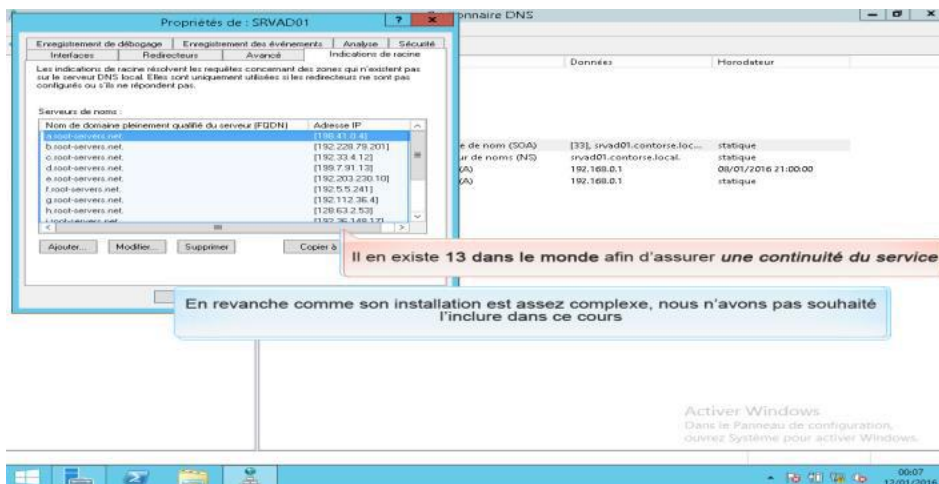
Quelques configurations

Les DNS publics



Cette fenêtre nous permet de saisir les DNS publics du FAI.

Les DNS Racine



Comme nous l'avons vu, lorsque votre serveur DNS n'est pas en mesure de résoudre votre requête DNS, il interroge dans un premier temps, l'un des root DNS indiqués ici.

Il en existe 13 dans le monde afin d'assurer une continuité du service.

Résumé

Nous avons pu voir que le service DNS est automatiquement installé lorsqu'il s'agit du 1er serveur Active Directory

En effet, Active Directory s'appuie sur DNS pour localiser les ordinateurs, mais aussi pour appliquer des stratégies. Nous aborderons ce sujet ultérieurement.