Mise en place d’un serveur DNS sous Windows Server 2008 ou 2008 R2

taochy.samuel | 27 mars 2012

Introduction

Au cour de ce billet, je vous propose de voir la mise en place d’un serveur DNS sous Windows Server 2008 ou 2008 R2. En effet 2008 ou 2008 R2 les manipulations sont relativement les mêmes.

Tout d’abord et en guise d’introduction je vous propose de voir ou de revoir les solutions proposées par Windows Serveur pour la résolution de nom. Bon nombre d’entre vous ont déjà le mot DNS à la bouche. Mais Windows propose pas seulement DNS comme solution il y a trois solutions bien distinctes !

La première solution est LLMNR soit *Link Local Multicast Name Resolution*. Cette solution vient pâlir deux faiblesses du DNS (Domain Name System). La premiere faiblesse est que pour avoir une résolution de nom via DNS, il faut toute une infrastructure DNS (clients et serveur(s)). Or dans un réseau local, en entreprise, il peut s’avérer intéressant d’être capable de se connecter à une machine via son UNC (*Universal Naming Convention*) plutôt que son adresse IP. LLMNR propose cela, en activant l’iPv6 et la « Découverte du réseau » (peut être activer dans le centre de réseau eet de partage). Donc une fois ses IPv6 et la découverte du réseau activé LLMNR est capable de faire la résolution de nom. Pour se connecter à une machine nommé PC-Lolokai il suffit de taper « \\PC-Lolokai » (C’est l’UNC de la machine).

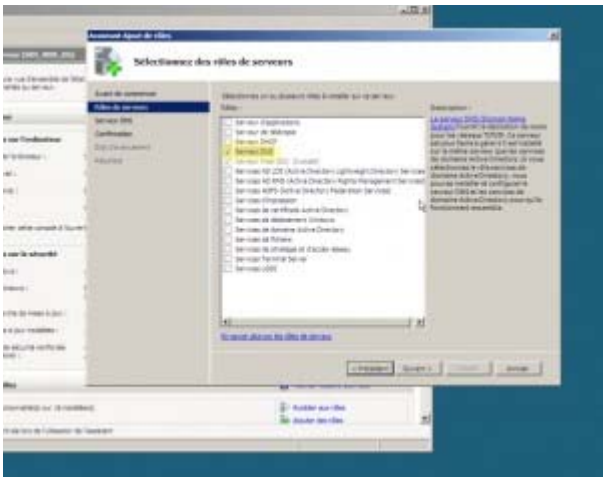
La deuxième solution est NetBios, qui a le meme but que LLMNR mais qui fonctionne avec des adresses IPv4, et surtout avec des machines sous XP ou meme antérieur. NetBios est un service de dénomination et un protocole qui va servir à la compatibilité avec les anciens services réseaux de Windows. Comme LLMNR il fonctionne en local permet de faire la résolution nom de machine en d'adresse IPv4, il permet aussi de « pinguer » une machine via son UNC. NetBios est activer par défaut sur une machine Windows.

La dernière solution et la plus répandue est DNS: *Domain Name System*. DNS lui résout les noms internet et prend en charge les services de domaines Active Directory. Cette solution est fondamentale dans un réseau d'entreprise plus ou moins conséquent. C'est pour cela que nous allons voir pas à pas comment mettre en place un Serveur DNS. Pour ce billet on partira d'un Serveur membre autonome c'est à dire qu'on installera pas notre Serveur DNS sur un controleur de domaine Active Directory.

Dans la rédaction de ce billet j'ai eu quelques petit soucis au niveau de VmWare. J'ai donc du utilisé une machine dans le cloud et merci pour cette invention génial qu'est le cloud ! 😀 Ne soyez pas choqué si vous voyez que dans ce billet les screenshots montre un système en anglais. J'utilise donc une machine sous Windows Server 2008 R2 insérer dans un Workgroup nommé lolokai.local et la machine se nomme ServeurDNS.

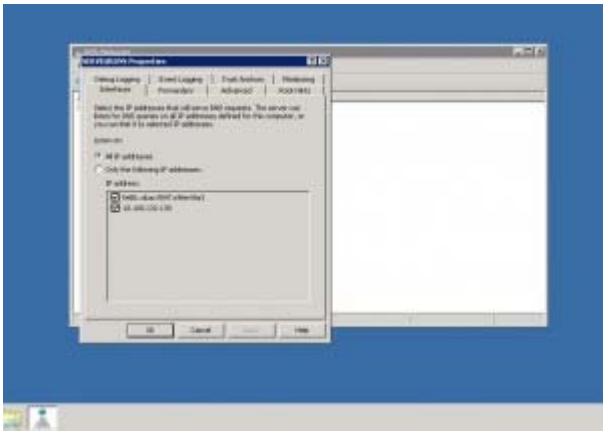
Installation

Tout d'abord il faut ajouter le role « Serveur DNS » à notre Serveur. Pour cela ***Démarrer -> Tous les programmes -> Outils d'administration -> Gestionnaire de serveur.*** Vous faites « Ajouter un rôle » et sélectionnez Serveur DNS:

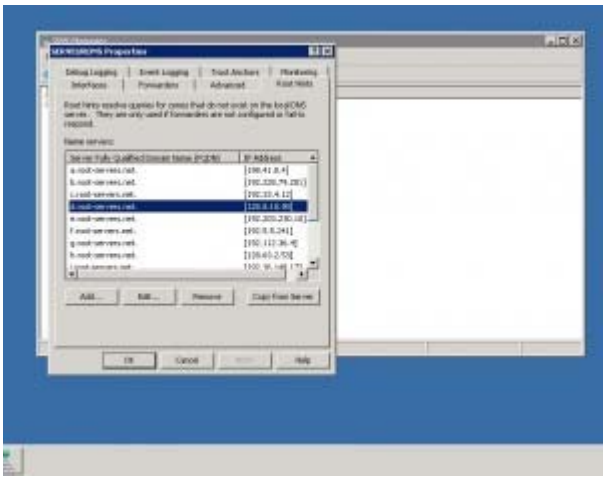


Maintenant le role est installé il suffit juste de le configurer.

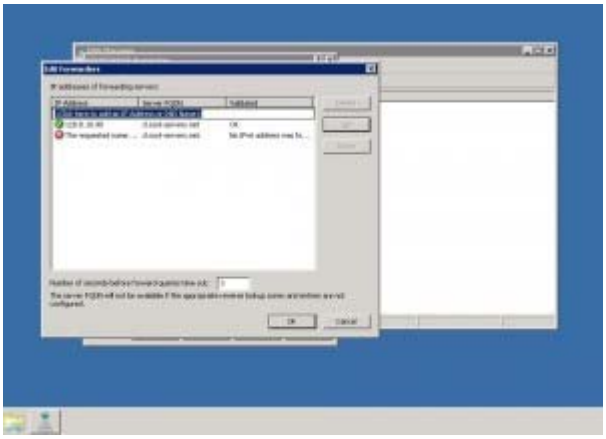
Tout d'abord on vérifie sur quelle interface écoute notre serveur DNS. Par défaut, il écoute toutes les adresses IP associées à l'ordinateur local. S'il est important pour vous de le modifier : **Démarrer -> Tous les Programmes -> Outils d'administration -> DNS ->** Clique droit sur votre serveur DNS **-> Propriété -> Onglet interface.**



Ensuite on regarde si il y a des serveurs racines, car si notre serveur DNS n'a pas de serveur racine recensé, il ne peut que résoudre les adresses de son réseau ou sous réseau. Pour cela onglet « indicateur de racine ».

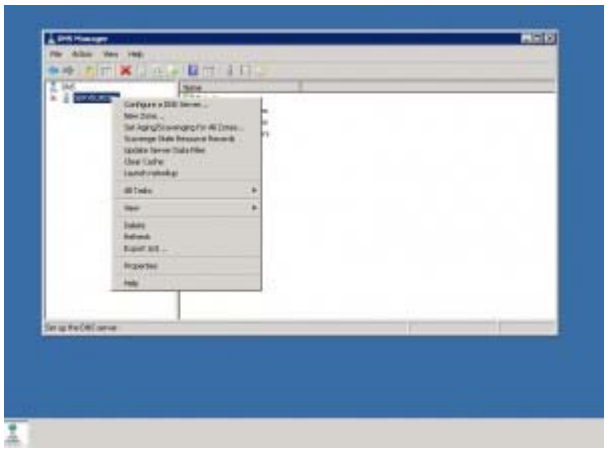


Puis il faut configurer une redirection, c'est à dire si notre serveur DNS ne peut répondre à la requête il redirige la requête vers un autre serveur DNS. Donc il faut renseigner l'adresse IP du serveur redirecteur DNS. Rendez-vous sur l'onglet « Redirecteur ».



Nous allons passer à une des étapes la plus importante, la création de zone. En effet, le serveur DNS fonctionne avec des zones, on crée une zone ou un espace de nom où on renseignera le DNS sur les adresses qu'il doit être en mesure de résoudre.

Pour cela **Démarrer -> Tout les Programmes -> Outils d'administration -> DNS ->** Clic droit sur votre serveur DNS **-> Nouvelle zone**.



Ensuite vous allez arriver sur une fenêtre pour choisir quel type de zone vous souhaitez créer. Il est donc important de savoir quelles zones existent et pourquoi ?

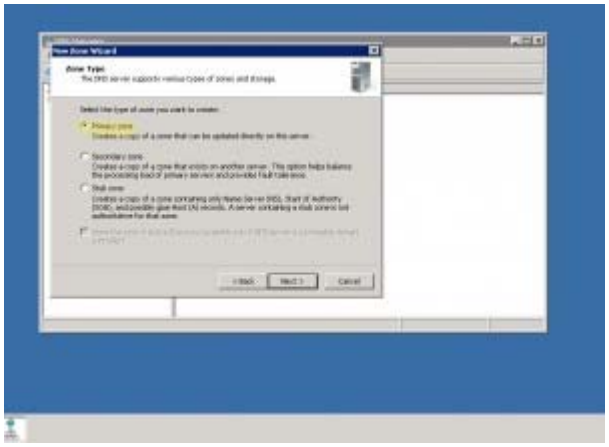
Il y a 3 zones: zone primaire, zone secondaire et zone de stub.

La zone primaire: quand on définie une zone primaire dans un Serveur DNS, on lui dit que sur cette zone c'est lui le « DNS maitre » de la zone. C'est à dire que sur cette zone c'est ce serveur DNS qui possède le fichier de zone maître (« le fichier exemple »). Le Serveur DNS a pleine autorité sur le fichier de zone c'est lui qui l'édite et il peut le lire pour répondre au requête.

La zone secondaire: c'est quand on renseigne notre DNS sur une zone déjà créée. On lui indique la zone et le fichier de zone maitre qu'il a le seul droit de lire pour répondre au requête. Seul le DNS ayant créer la zone en tant que primaire a le droit d'écriture. On utilise ce procedé pour alléger le trafic quand on a un zone où se fait beaucoup de requête DNS.

La zone de stub: Cette zone ressemble beaucoup à la zone secondaire, la seule différence c'est qu'elle garde seulement une copie du fichier de zone. Elle ne fait pas de résolution de nom, son but est juste d'avoir une copie du fichier à jour.

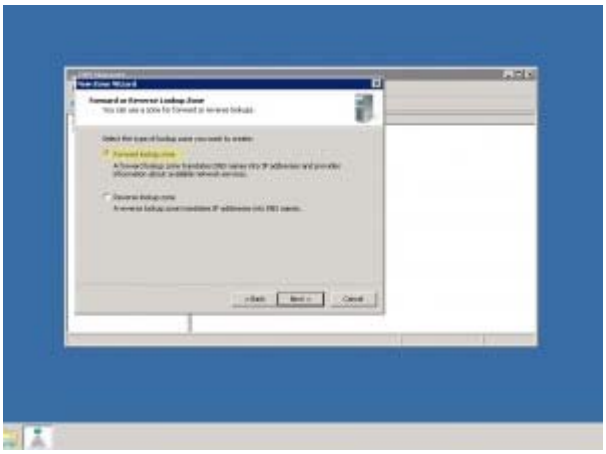
On choisira pour exemple de créer une zone primaire et on désactivera l'enregistrement dans l'Active Directory car ma machine n'est liée à aucun AD.



Une fois le type de zone choisie, il nous est demandé de choisir si l'on veut une « zone de recherche directe » ou une « zone de recherche inversée ».

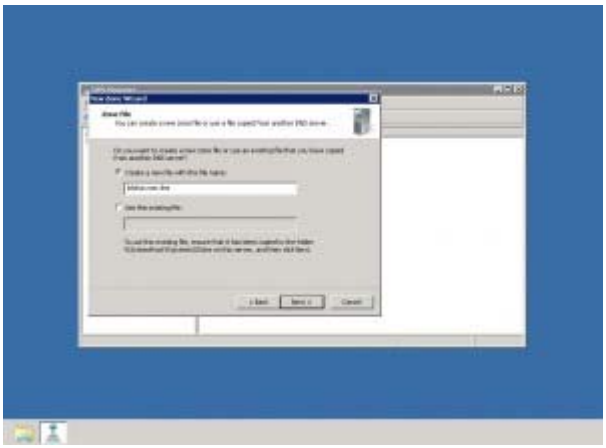
> **Zone de recherche directe**: le serveur DNS fait correspondre les noms de domaine pleinement qualifié (FQDN) en adresse IP.
>
> **Zone de recherche inversé:** le serveur DNS fait correspondre l'adresse IP en FQDN, pour cela il faut inversé les 3 premiers octets de l'adresse IP et rajouter « in-addr.arpa ». Ex: pour créer une zone inversée sur le sous réseau 192.168.1.0/24 on fait une zone inversée dont l'adresse sera 1.168.192.in-addr.arpa.

Pour la bonne résolution de nom dans une zone il est fortement conseillé de faire une zone et sa zone inversée. Donc pour commencer on choisi zone de recherche directe.



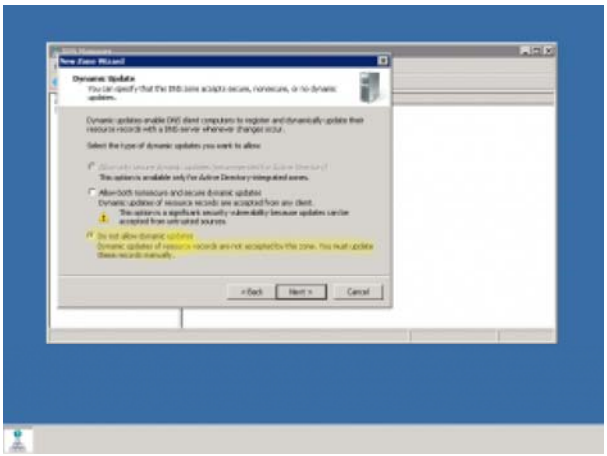
Puis il nous est demandé de choisir le nom de la zone, vous pouvez remarquer sur vos machines que le nom du domaine succède notre nom de zone. Dans ma machine exemple on est intégré à aucun domaine donc il est succéder de « .dns ».

Ensuite l'utilitaire vous propose de créer un fichier de zone ou d'utiliser un fichier existant. Dans notre cas et pour apprendre on demandera de créer un fichier qu'on éditera plus tard.



Une fois le fichier créer, nous arrivons sur une fenêtre qui nous propose de faire des mise-à-jour. En fait, il s'agit de faire des mises-à-jour de notre fichier de zone. On peut autoriser les mises à jour dynamique soit on autorise les machine membres de l'Active Directory et seulement elles à transmettre des mises-à-jour du fichier de zone. Soit on autorise toutes les

machines à le faire. Ou sinon on demande de ne pas faire de mise-à-jour du fichier de zone c'est ce que nous ferons dans l'exemple.



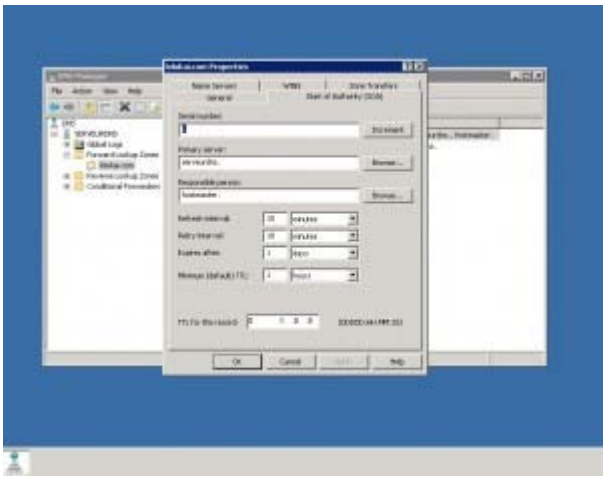
Maintenant notre zone est créée, mais il est indispensable dans une zone d'avoir deux types d'enregistrement le SOA (Start of Authority) et le NS (Name Server).

> **SOA:** Définit les propriétés fondamentales de notre zone. En effet quand une zone est créer il faut aussi créer ses propriété: ID, serveur principale…
>
> **NS:** Définit les serveurs de noms faisant autorité sur la zone, serveur secondaire, serveur racine…

Pour accéder à ces enregistrement : clic droit sur la zone dans le gestionnaire DNS **-> Propriétés**. Dans la fenêtre vous pouvez modifer les paramètres par défaut de SOA ou rajouter manuellement des serveur de noms.

/!\ ATTENTION: le numero de serie dans une SOA ne s'invente pas ! Il est incrémenté à chaque modification d'un enregistrement de ressource (serveur messagerie, serveur de nom..). Il est fondamental de pas y toucher car cet ID va permettre aux serveurs secondaires de savoir s'ils ont le bon fichier zone. Si les numéros de série ne

s'accorde pas le fichier zone du DNS « maitre » (DNS où la zone à été configurée comme primaire) est envoyé aux serveurs secondaires.



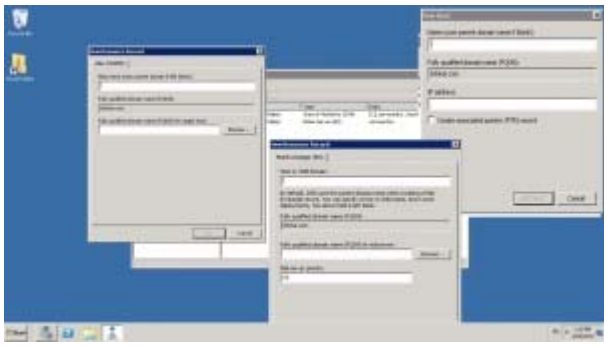
Maintenant que vous avez pu modifier votre SOA et votre NS vous pouvez ajouter les différentes machines que vous avez dans votre réseau. Pour cela vous avez 3 possibilités d'enregistrement de ressource: un hôte A ou AAAA, un alias CNAME ou un échangeur de messagerie MX.

Hôte A ou AAAA: permet simplement de résoudre le nom d'une machine via son adresse IP. A signifie juste qu'on parle d'une adresse IPv4 et AAAA d'une adresse IPv6.

Alias CNAME: comme son nom l'indique il permet de créer des alias. En effet il permet d'appeler une ressource par un alias par exemple récupérer le serveur ftp « ftp1.lolokai.com » en « ftp.lolokai.com ».

Echangeur de messagerie MX: permet simplement de déterminer un serveur de messagerie.

Pour cela il vous suffit de faire un clic droit sur la zone et faire ajouter CNAME ou hôte ou MX.



Voila nous avons mis en place un DNS et un fichier de zone primaire. Vous devriez être capable de le refaire avec vos machines, vos IP, vos enregistrements. Dernière mise en garde nous avons fait qu'un fichier de zone mais cela est que la moitié du travail ! Pour que le DNS fasse la résolution IP -> FQDN et FQDN -> IP il est indispensable de créer une zone inversée ! Pour cela comme indiqué au début il faudra faire les mêmes enregistrements en inversant les 3 premiers octet et rajouter « in-addr.arpa ».

Conclusion

Nous avons vu au travers de ce billet la mise en place d'un serveur DNS sous Windows 2008 Server, ainsi que les différents enregistrements que nous pouvons lier.