



OFPPT

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

Complexe de Formation dans les Métiers des Nouvelles Technologies de l'Information, de
l'Offshoring et de l'Electronique -Oujda

Module : Administration d'un Réseau

Installation et configuration du serveur DNS sous Windows Server 2012R2

Sommaire

1.	Introduction.....	3
1.1	Type de nom	3
1.2	Noms d'hôtes	3
1.3	Noms NetBIOS.....	3
2.	Présentation DNS	3
3.	Requête DNS	4
3.1	Requêtes récursives.....	4
3.2	Les requêtes itératives	5
4.	Fonctionnement du serveur DNS	5
5.	Serveur cache.....	7
6.	Serveur secondaire / Principal (slave/master).....	7
7.	Zones DNS.....	7
7.1	Zones de recherche directe.....	7
7.2	Zones de recherche inversée.....	7
8.	Principaux types d'enregistrements.....	8
9.	Installation DNS sous Windows Server 2012R2 Graphiquement	8
10.	Configuration du serveur DNS sous windows server2012R2 graphiquement	11
10.1	Adresse d'écoute	12
10.2	Redirection des requêtes	12
11.	Création des zones.....	13
12.	Installation et configuration du serveur DNS en PowerShell	20
12.1	Installation.....	20
12.2	Redirection.....	21
12.3	Zone primaire.....	21
12.4	Enregistrement.....	21
13.	Configuration du serveur secondaire graphiquement	23
14.	Configuration du serveur secondaire en PowerShell	26
15.	Mises à jour dynamiques.....	27
16.	Vérification du Cache	27
17.	Résolution des problèmes liés à la résolution de noms.....	28
17.1	Nslookup	28
17.2	DNSCmd.....	28
17.3	Dnslint.....	28
17.4	Ipconfig.....	28
17.5	Test-DNSServer	28
17.6	Clear-DNSClientCache.....	29
17.7	Get-DNSClient.....	29
17.8	Get-DNSClientCache.....	29
17.9	Register-DNSClient.....	29
17.10	Resolve-DNSName	29
17.11	Set-DNSClient	29
18.	Zones intégrées à Active Directory	29
	Annexe.....	30
	Référence :	31

1. Introduction

1.1 Type de nom

Le type de nom (nom d'hôte ou nom NetBIOS) qu'une application utilise est déterminé par le développeur d'applications. Si le développeur d'applications conçoit une application pour demander des services réseau via des sockets Windows, les **noms d'hôtes** sont utilisés. En revanche, si le développeur d'applications conçoit une application pour demander des services via **NetBIOS**, un nom NetBIOS est utilisé.

La plupart des applications actuelles, notamment les applications Internet, utilisent des sockets Windows par conséquent **des noms d'hôtes** pour accéder aux services réseau. NetBIOS est utilisé par de nombreuses applications des versions antérieures du système d'exploitation Windows.

1.2 Noms d'hôtes

Un nom d'hôte est un nom convivial associé à l'adresse IP d'un ordinateur afin de l'identifier en tant qu'hôte TCP/IP. Le nom d'hôte peut comprendre jusqu'à 255 caractères (caractères alphabétiques et numériques, points et traits d'union).

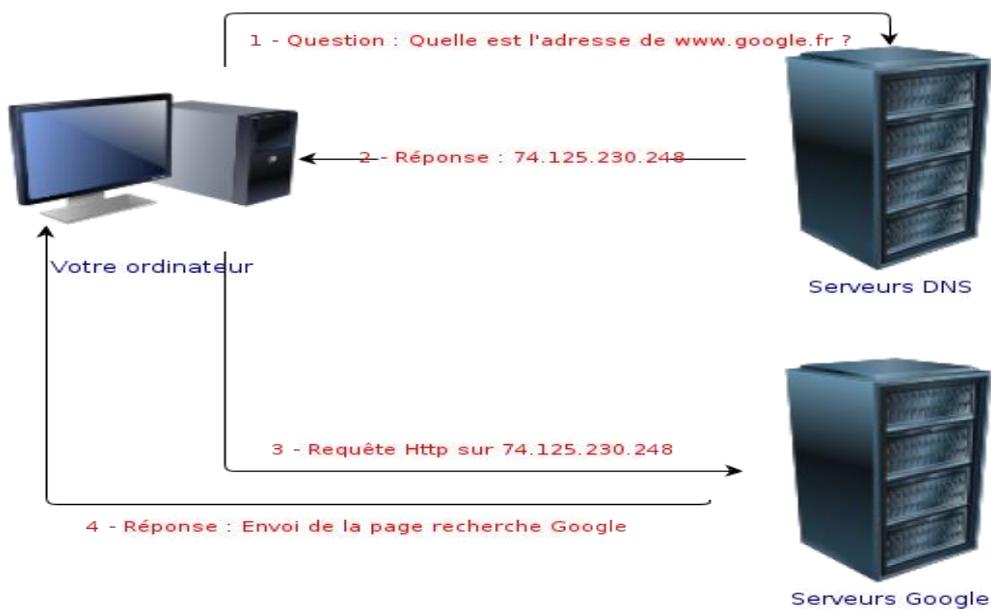
1.3 Noms NetBIOS

Un nom NetBIOS, qui compte 16 caractères, identifie une ressource NetBIOS sur le réseau. Un nom NetBIOS peut représenter un ordinateur unique ou un groupe d'ordinateurs. Les 15 premiers caractères sont utilisés pour le nom, le dernier caractère identifie la ressource ou le service de l'ordinateur auquel il est fait référence.

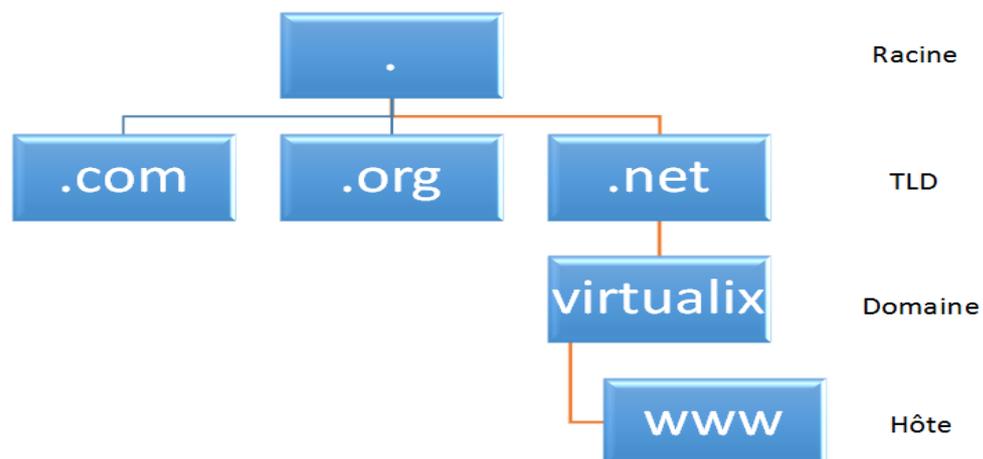
2. Présentation DNS

DNS Domain Name System. C'est un système hiérarchique distribué permettant la résolution des noms de machines en adresses IP et inversement. Le schéma suivant explique comment ça se passe lorsque vous surfez sur Internet et à quel moment intervient le serveur DNS.

Principe d'une requête DNS



Le DNS considère le réseau comme une arborescence de domaines. Voici un schéma sur le fonctionnement de l'arborescence



3. Requête DNS

Une requête est une demande de résolution de noms envoyée à un serveur DNS. Il existe deux types de requêtes : requêtes récursives et requêtes itératives.

3.1 Requêtes récursives

Une requête récursive est une requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur de fournir une réponse complète. Une requête récursive ne peut pas être redirigée vers un autre serveur DNS.

Dans une requête récursive, le serveur DNS renvoie l'une des trois réponses suivantes :

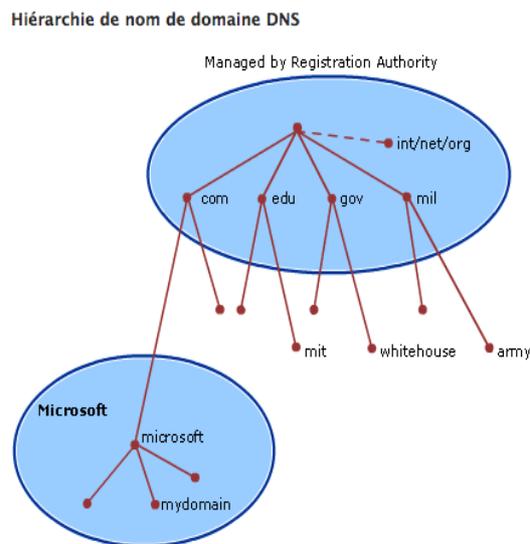
- Les données informatiques demandées.
- Un message d'erreur indiquant que les données informatiques du type demandé n'existe pas.
- Un message indiquant que le nom de domaine spécifié n'existe pas.

3.2 Les requêtes itératives

Une requête itérative est une requête envoyée à un serveur DNS dans laquelle le client DNS demande la meilleure réponse que peut fournir le serveur DNS. Le résultat d'une requête itérative est souvent une référence à un autre serveur DNS situé plus bas dans l'arborescence DNS.

4. Fonctionnement du serveur DNS

L'espace de noms de domaine DNS, comme le montre la figure suivante, est basé sur le concept d'une arborescence de domaines nommés. Chaque niveau de l'arborescence peut représenter une succursale ou une feuille de l'arborescence. Une branche est un niveau où plus d'un nom est utilisé pour identifier un ensemble de ressources nommées. Une feuille représente un nom unique utilisé une seule fois à ce niveau pour indiquer une ressource spécifique.



Type de nom	Description	Exemple
Domaine racine	Il s'agit de la partie supérieure de l'arborescence, représentant un niveau non nommé	
Domaine de niveau supérieur	Nom utilisé pour indiquer un pays/région ou le type d'organisation en utilisant un nom.	« .com », indique un nom enregistré pour l'entreprise pour un usage commercial sur Internet. « .ma », indique un nom enregistré pour le pays maroc
Domaine de	Noms de longueur variable inscrits	« ofppt.ma », qui est le

second niveau	d'un individu ou organisation pour une utilisation sur Internet. Ces noms sont toujours basées sur un domaine de niveau supérieur approprié, selon le type d'organisation ou l'emplacement géographique où un nom est utilisé.	nom de domaine de second niveau inscrit à ofppt par le Registre des noms de domaine DNS Internet.
Sous-domaine	Noms supplémentaires qu'une organisation peut créer que les dérivés du nom de domaine de second niveau inscrit. Ils comprennent les noms ajoutés pour développer l'arborescence DNS des noms dans une organisation et la diviser en services ou emplacements géographiques.	« oujda.ofppt.ma ». qui est un sous-domaine fictif attribué par ofppt à la region d'oujda
Nom d'hôte	Noms qui représentent une feuille dans l'arborescence DNS des noms et d'identifient une ressource spécifique. En règle générale, l'étiquette la plus à gauche d'un nom de domaine DNS identifie un ordinateur spécifique sur le réseau. Par exemple, si un nom à ce niveau est utilisé dans un enregistrement de ressource hôte (A), il est utilisé pour rechercher l'adresse IP de l'ordinateur en fonction de son nom d'hôte.	« « hôte-a .oujda .ofppt.ma », où la première étiquette (« hôte-a ») est le nom d'hôte DNS pour un ordinateur spécifique sur le réseau.

Le tableau suivant présente quelque exemple du niveau TLD

Nom de domaine DNS	Type d'organisation
com	Organisations commerciales
edu	Établissements d'enseignement
org	Organisations à but non lucratif
NET	Réseaux (dorsale d'Internet)
gov	Organisations gouvernementales non militaires
mil	Organisations gouvernementales militaires
arpa	DNS inverse
"xx"	Code de pays à deux lettres (par exemple, us, AOU, autorité de certification, fr)

5. Serveur cache

Pour optimiser les requêtes ultérieures, les serveurs DNS récursifs font aussi office de *DNS cache* : ils gardent en mémoire (*cache*) la réponse d'une résolution de nom afin de ne pas effectuer ce processus à nouveau ultérieurement. Cette information est conservée pendant une période nommée *Time to live* et associée à chaque nom de domaine.



6. Serveur secondaire / Principal (slave/master)

Tout réseau n'étant pas à l'abri d'une panne, il est fortement recommandé d'avoir 2 serveurs DNS dans un réseau : le **DNS Principal** étant celui qui répond aux requêtes en temps normal, le **DNS secondaire** prenant le relais si le principal ne répond pas.

Un serveur est dit secondaire d'une zone quand il obtient toutes les informations de cette zone d'un autre serveur dit serveur primaire. Il télécharge le contenu de la zone régulièrement afin de pouvoir prendre le relai du serveur primaire en cas d'incident.

7. Zones DNS

Une zone DNS est une partie spécifique de l'espace de noms DNS qui contient des enregistrements DNS. Les types de zone DNS les plus couramment utilisés dans le DNS Windows Server sont les zones de recherche directe et les zones de recherche inversée.

7.1 Zones de recherche directe

Les zones de recherche directe résolvent les noms d'hôtes en adresses IP et hébergent les enregistrements de ressources courants, notamment les enregistrements de ressources d'hôte (A), d'alias (CNAME), de service (SRV), de serveur de messagerie (MX), de source de noms (SOA) et de serveur de noms (NS). Le type d'enregistrement de ressource le plus courant est l'enregistrement de ressource d'hôte (A).

7.2 Zones de recherche inversée

La zone de recherche inversée résout les adresses IP en noms de domaine. Une zone inversée fonctionne de la même manière qu'une zone directe, mais l'adresse IP fait partie de la requête et le nom d'hôte représente l'information retournée. Les zones de recherche inversée hébergent les enregistrements de ressources SOA, NS et de pointeur (PTR).

8. Principaux types d'enregistrements

SOA : Permet de définir les informations relatives à la zone. En l'occurrence le nom du serveur DNS primaire et l'adresse mail du contact technique (root.example.com. le @ est remplacé par un point). Il est composé de plusieurs champs :

- **Serial** : C'est le numéro de série à incrémenter à chaque modification du fichier. Il permet au serveur secondaire de recharger les informations qu'ils ont. L'usage général vient à le formater de cette manière YYYYMMDDXX,
- **Refresh** : définit la période de rafraîchissement des données.
- **Retry** : si une erreur survient au cours du dernier rafraîchissement, celle-ci sera répétée au bout du délai Retry.
- **Expire** : le serveur sera considéré comme non disponible au bout du délai Expire.
- **Negative cache TTL** : Durée de vie est la durée de validité des données communiquée par le serveur pour toute requête .

NS : renseigne le nom des serveurs de noms pour le domaine.

MX : renseigne sur le serveur de messagerie. Plusieurs peuvent être définis. Ainsi, il est possible de leur donner une priorité en leur affectant un numéro. Plus bas est le numéro, plus haute est la priorité.

A : associe un nom d'hôte à une adresse ipv4 (32 bits)

AAAA : associe un nom d'hôte à une adresse ipv6 (128 bits)

CNAME : identifie le nom canonique d'un alias, un nom pointant sur un autre nom

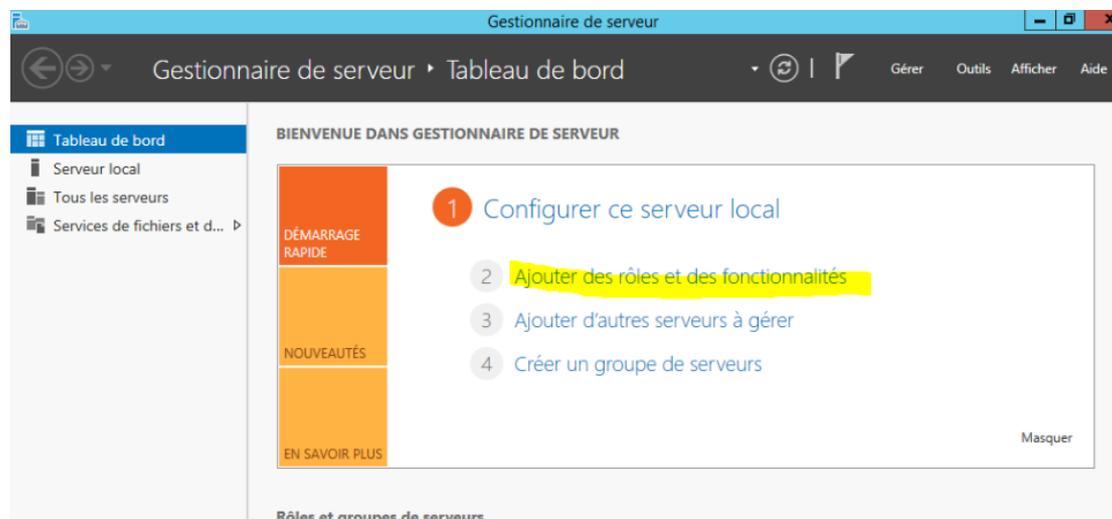
SRV : Renseigne sur le serveur ADDS (Annuaire LDAP)

PTR : c'est simplement la résolution inverse (le contraire du type A).

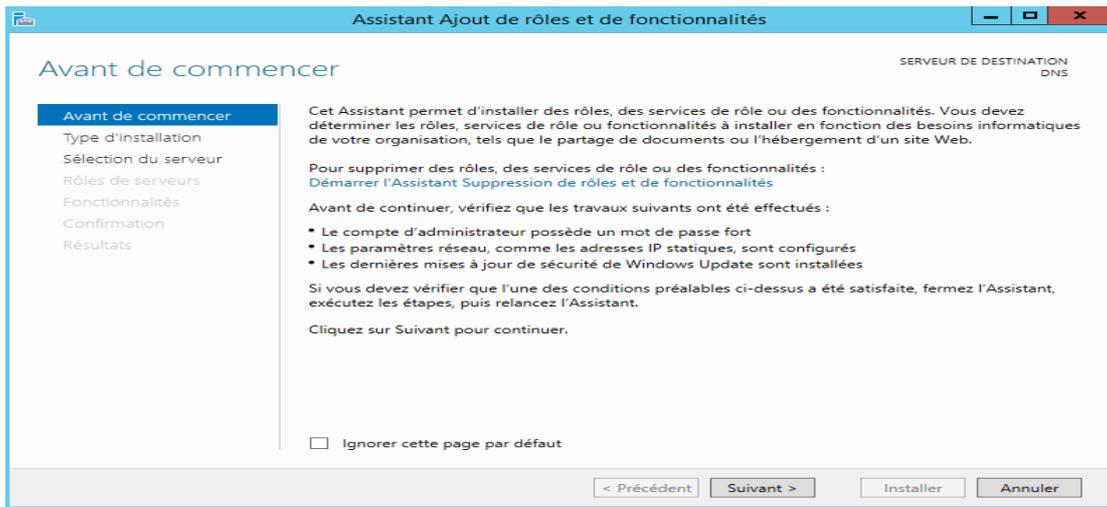
9. Installation DNS sous Windows Server 2012R2 Graphiquement

Ouvrir le "Le Gestionnaire de serveur" et "ajouter des rôles et des fonctionnalités".

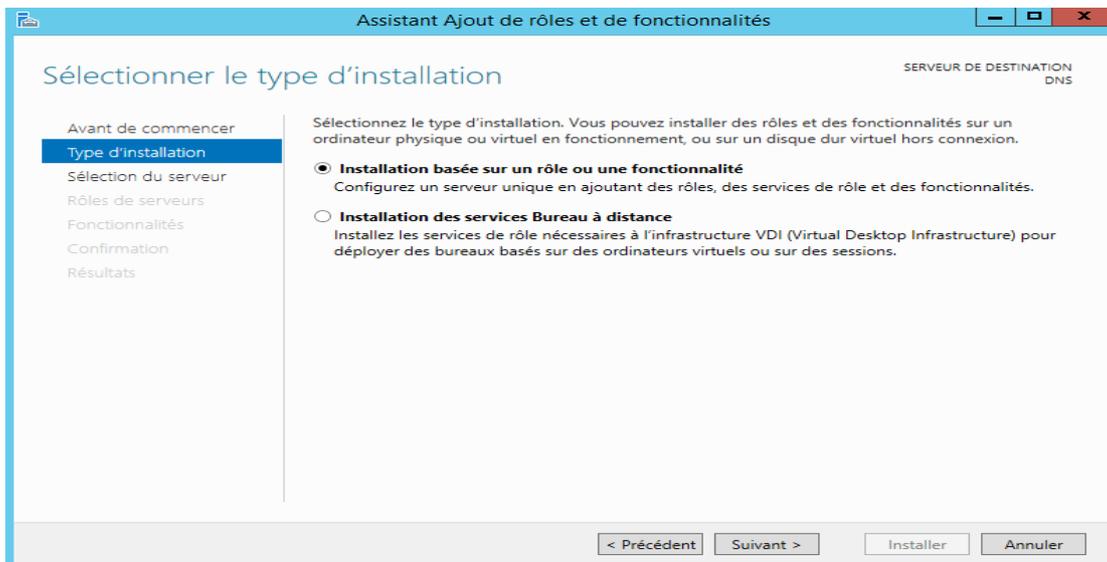
NB : Si vous avez déjà configuré un Active directory sur votre serveur, ce rôle est déjà installé.



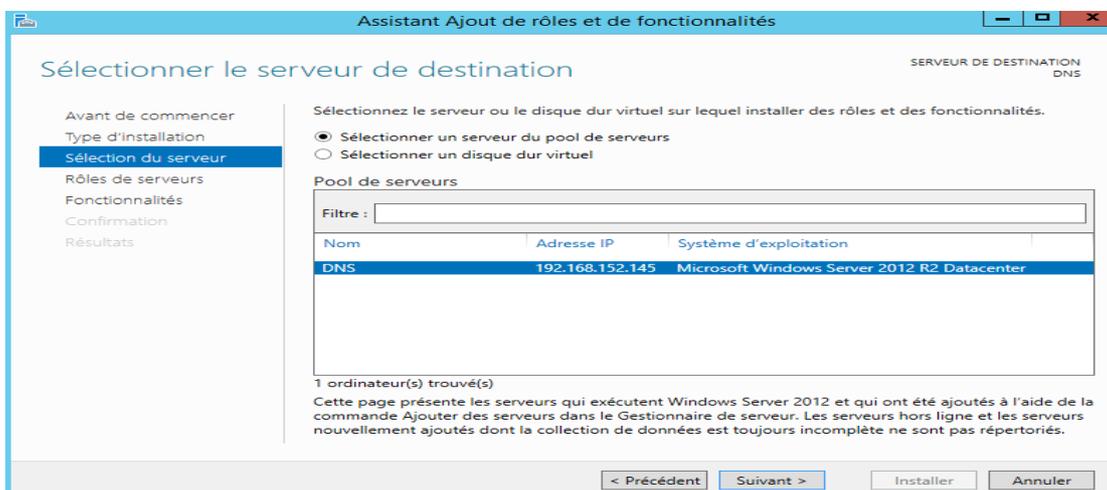
Cliquer sur "Suivant"



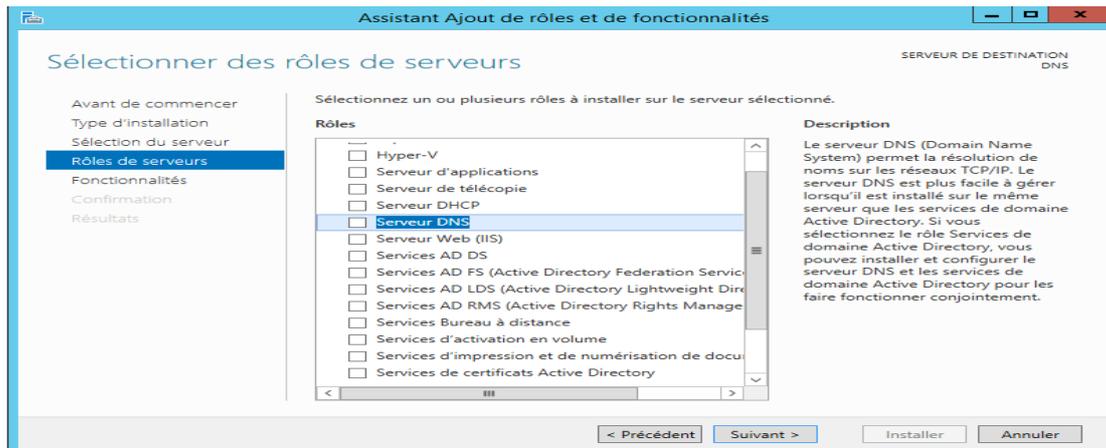
Cliquer sur "Suivant"



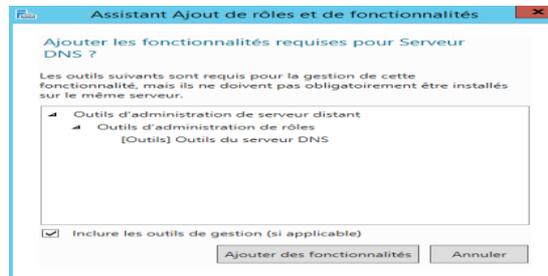
Cliquer sur "Suivant"



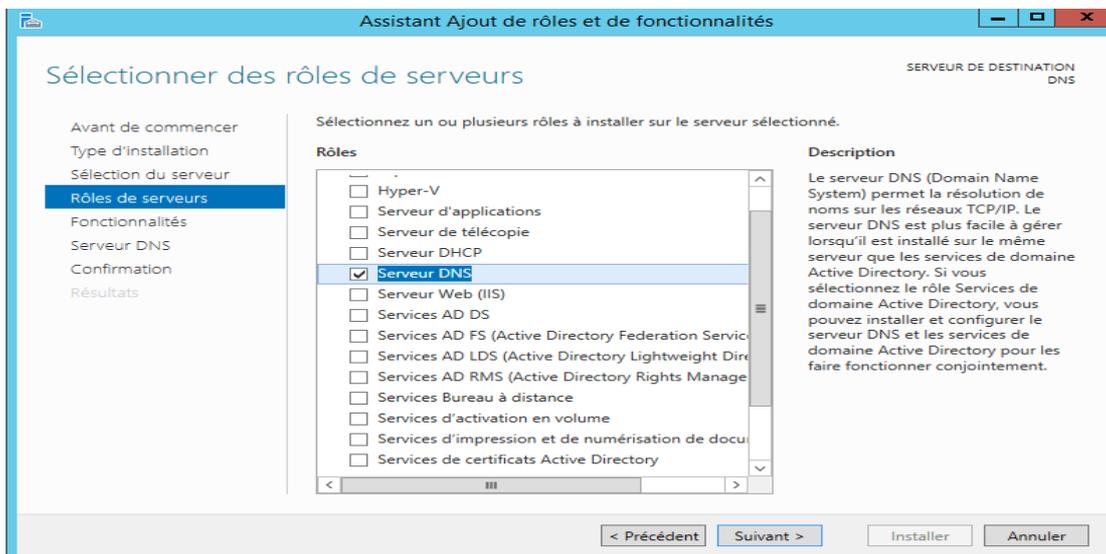
Cocher la case Serveur "DNS" puis cliquer sur suivant



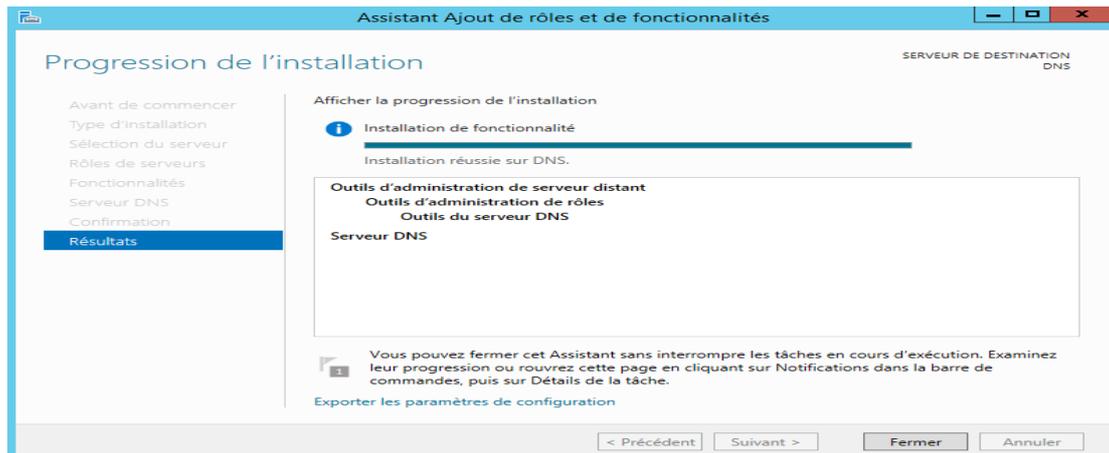
Et cliquer sur "Ajouter des fonctionnalités" pour l'installation d'autre fonctionnalités nécessaires pour serveur DNS



Cliquer sur "Suivant"

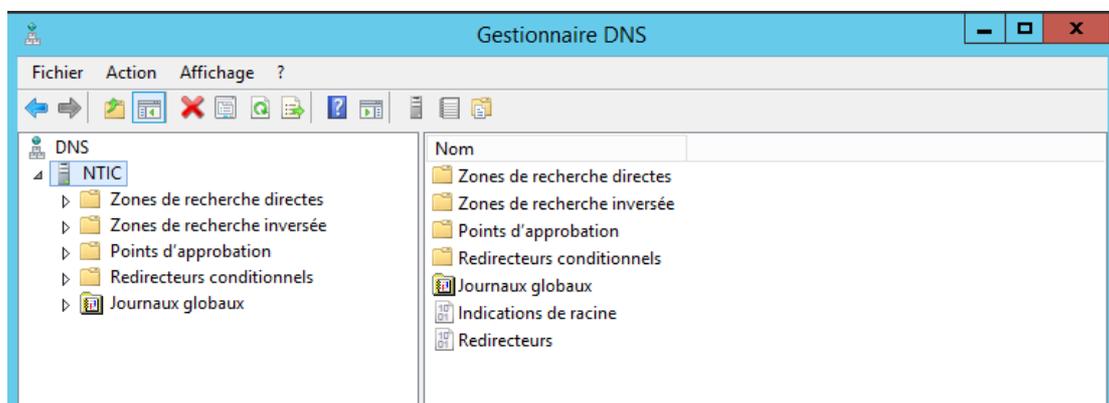
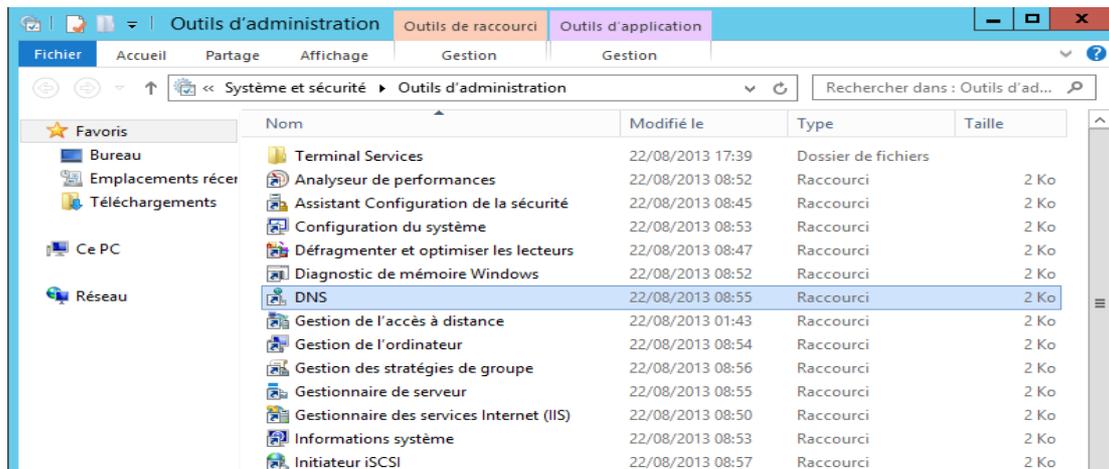


Suivre les étapes jusqu'à la fin de l'installation

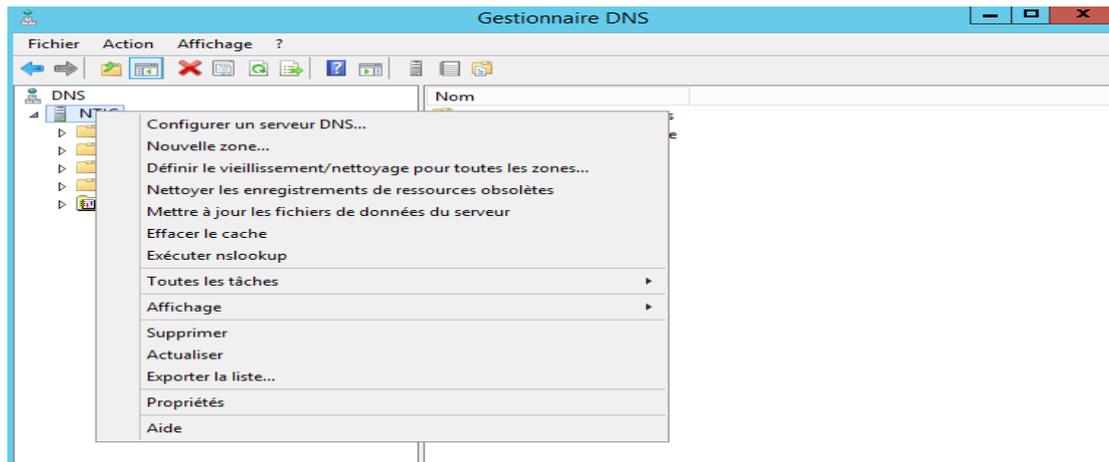


10. Configuration du serveur DNS sous windows server2012R2 graphiquement

Pour configurer une zone DNS (un domaine) il faut ouvrir le menu "Démarrer ", "Outils d'Administration", "DNS". Une fenêtre va alors s'ouvrir, concernant la gestion du rôle DNS auparavant installé

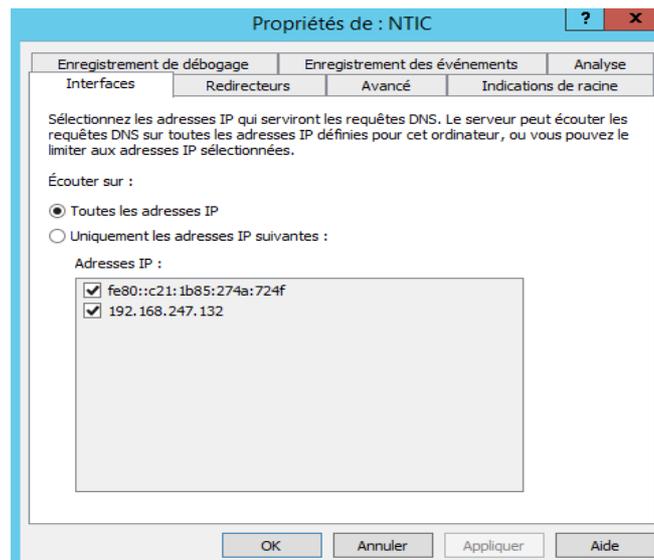


Faites un clic droit sur serveur DNS et cliquez sur "Propriétés".



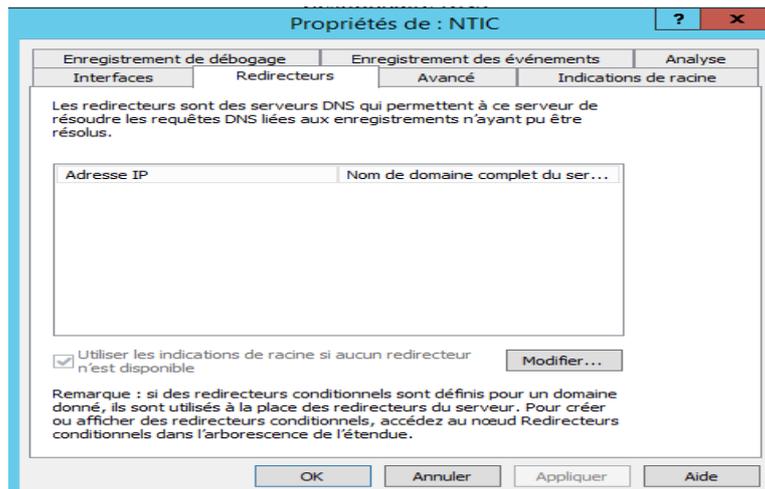
10.1 Adresse d'écoute

Par défaut, le serveur DNS écoute sur toutes les adresses IP (et donc toutes les cartes réseau en IPv4 et IPv6). Pour qu'il écoute uniquement sur certaines adresses IP, sélectionner "Uniquement les adresses IP souhaitées".



10.2 Redirection des requêtes

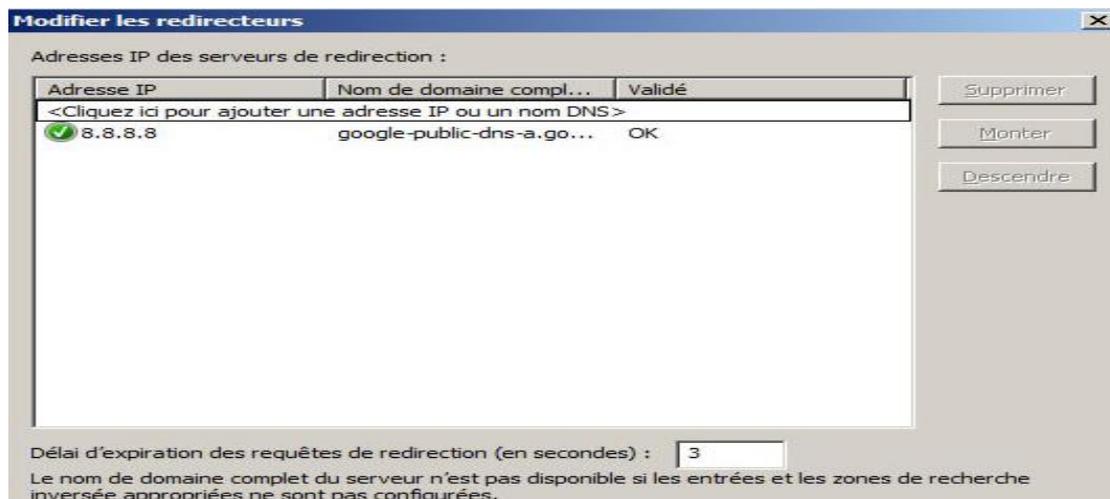
Si le serveur ne peut pas résoudre certains domaines (ou enregistrements de domaines), nous allons devoir rediriger la requête à un autre serveur DNS. Dans notre exemple nous allons rediriger la requête au serveur DNS public de Google. Cliquez sur "Modifier".



Il vous suffit ensuite d'ajouter les serveurs DNS désirés en tapant leurs adresses IP. Les adresses IP des serveurs DNS de Google sont :

- 8.8.8.8
- 8.8.4.4

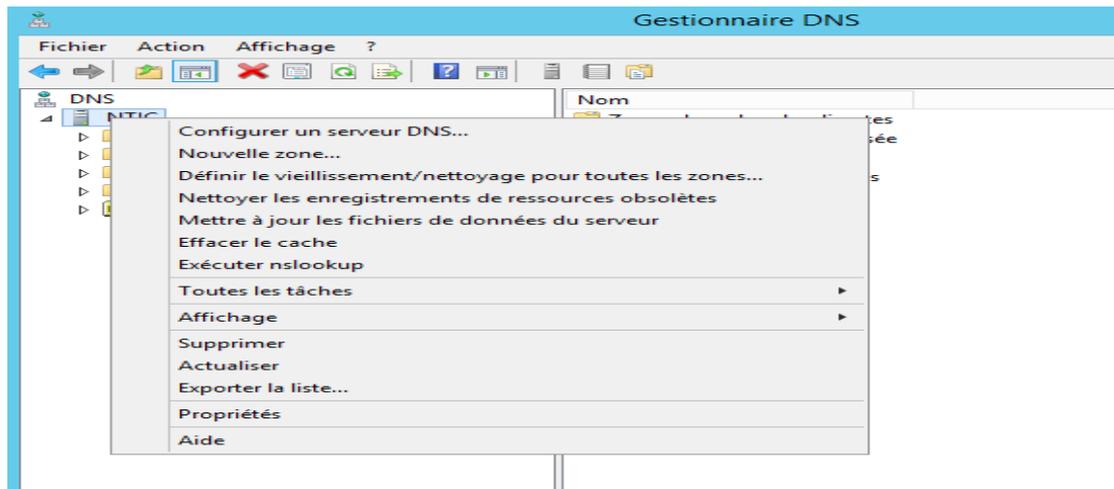
Une fois que vous avez indiqué une adresse IP, le serveur va tenter de résoudre le nom de domaine correspondant à l'adresse IP indiquée. Si tout se passe bien, un "v" vert devraient s'afficher devant celle-ci.



11. Création des zones

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

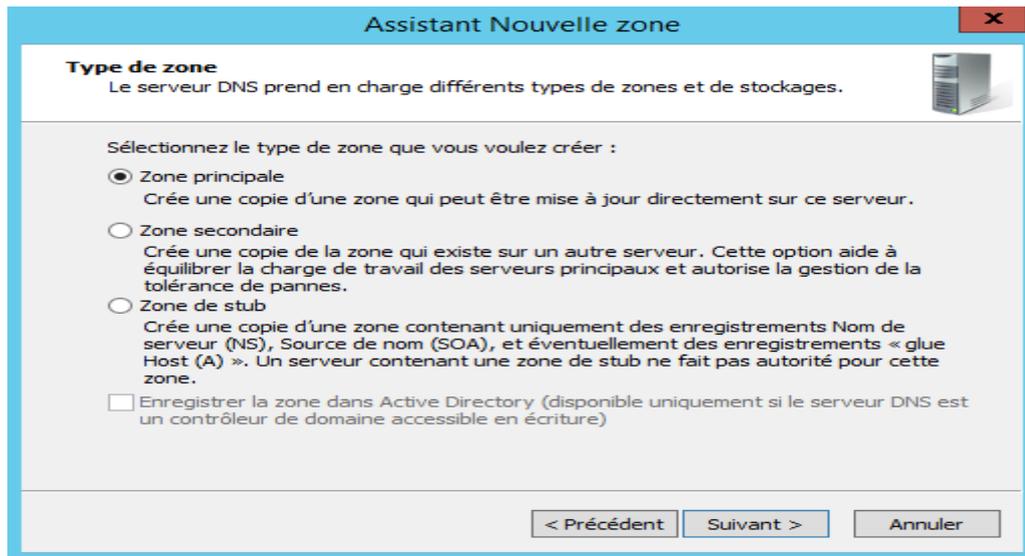
Pour cela **Outils d'administration -> DNS -> Clic droit sur le serveur DNS -> Nouvelle zone.**



Ensuite vous allez arriver sur une fenêtre pour choisir quel type de zone vous souhaitez créer.

Il existe quatre type de zones: zone primaire , zone secondaire et zone de stub.

- **La zone primaire:** quand on définit une zone primaire dans un Serveur DNS, on lui dit que sur cette zone c'est lui le « DNS maître » 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 maître 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 procédé 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.
- **Zone intégrée à Active Directory** Si les services AD DS stockent les données de zone, le serveur DNS peut utiliser le modèle de réplication multimaître pour répliquer les données de la zone principale. Cela vous permet de modifier des données de zone sur plusieurs serveurs DNS simultanément.

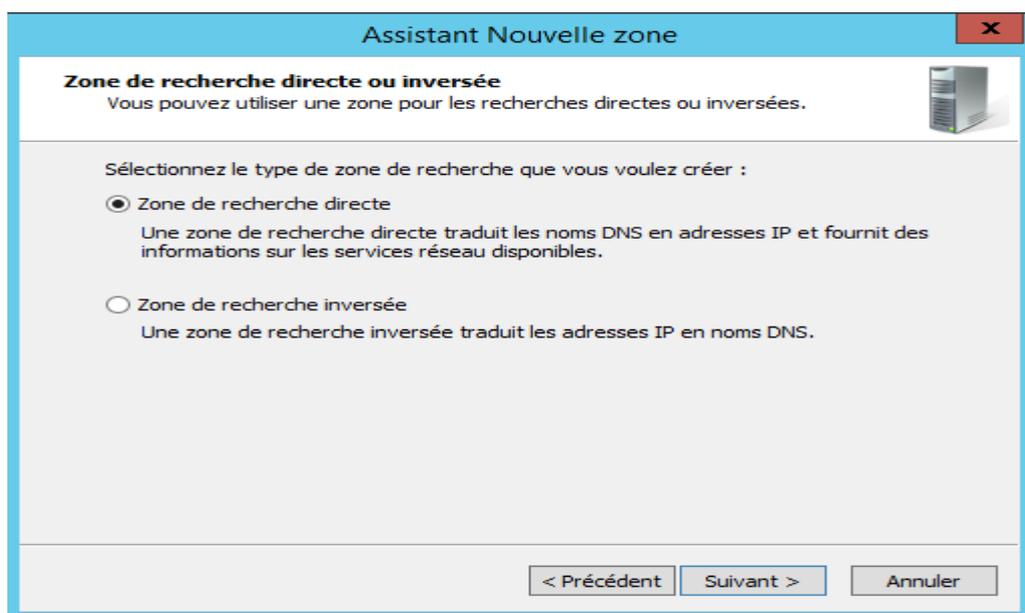


Une fois le type de zone choisie, il nous est demandé de choisir si l'on veut une « zone de recherche directe » ou une « zone de recherche inversée ».

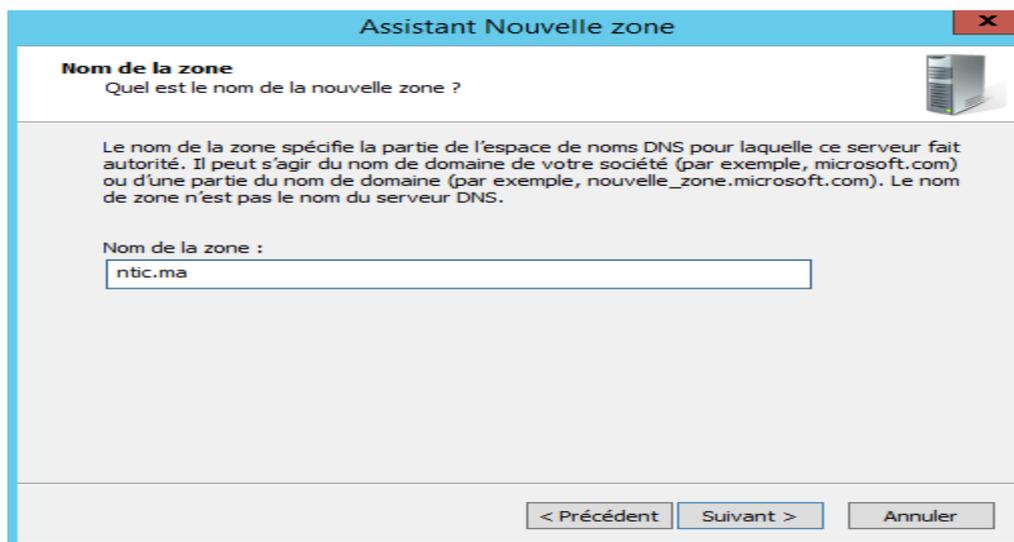
- **Zone de recherche directe:** le serveur DNS fait correspondre les noms de domaine pleinement qualifié (FQDN) en adresse IP.
- **Zone de recherche inversé:** le serveur DNS fait correspondre l'adresse IP en FQDN, pour cela il faut inversé les 3 premiers octets de l'adresse IP et rajouter « in-addr.arpa ». 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.

11.1 Zone de recherche directe

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.



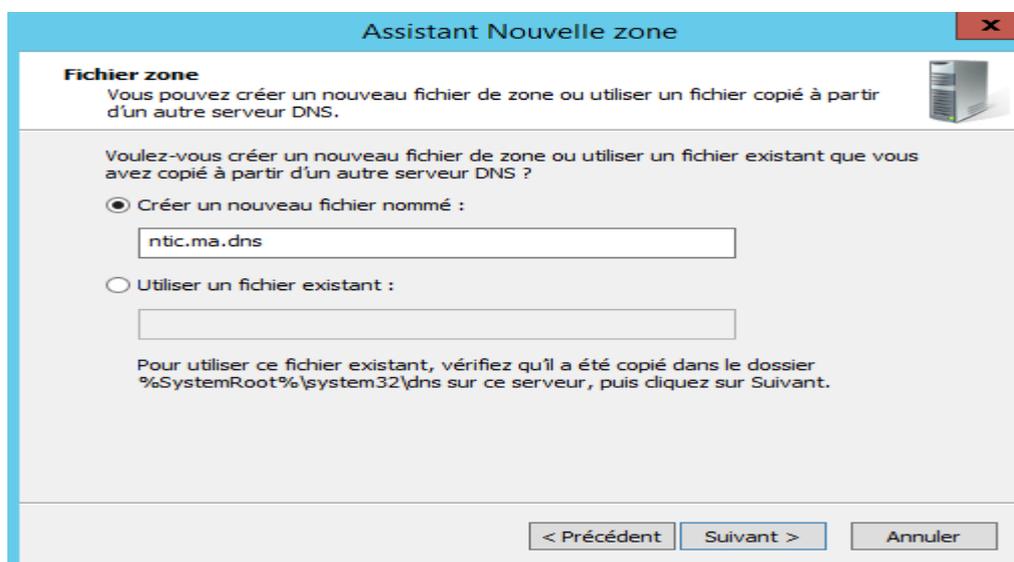
Puis il nous est demandé de choisir le nom de la zone



The screenshot shows a Windows dialog box titled "Assistant Nouvelle zone". The main heading is "Nom de la zone" with the question "Quel est le nom de la nouvelle zone ?". Below this, there is explanatory text: "Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS." A text input field labeled "Nom de la zone :" contains the text "ntic.ma". At the bottom, there are three buttons: "< Précédent", "Suivant >", and "Annuler".

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 ».

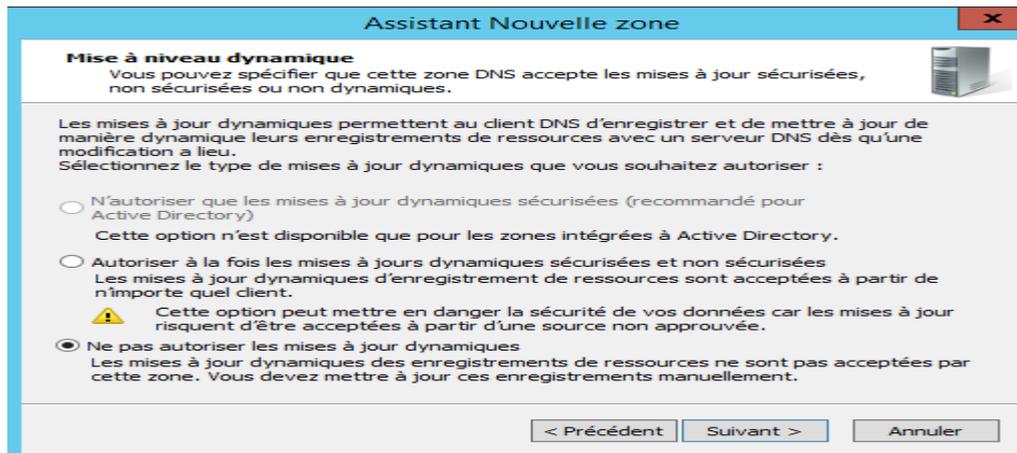
Ensuite l'utilitaire vous propose de créer un fichier de zone ou d'utiliser un fichier existant. Dans notre cas et pour apprendre on demandera de créer un fichier qu'on éditera plus tard.



The screenshot shows the same "Assistant Nouvelle zone" dialog box, but at the "Fichier zone" step. The heading is "Fichier zone" with the text "Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS." Below this, a question is asked: "Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?". There are two radio button options: "Créer un nouveau fichier nommé :" (which is selected) and "Utiliser un fichier existant :". The selected option has a text input field containing "ntic.ma.dns". The unselected option has an empty text input field. Below the options, there is a note: "Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant." At the bottom, there are three buttons: "< Précédent", "Suivant >", and "Annuler".

Une fois le fichier créé, 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.



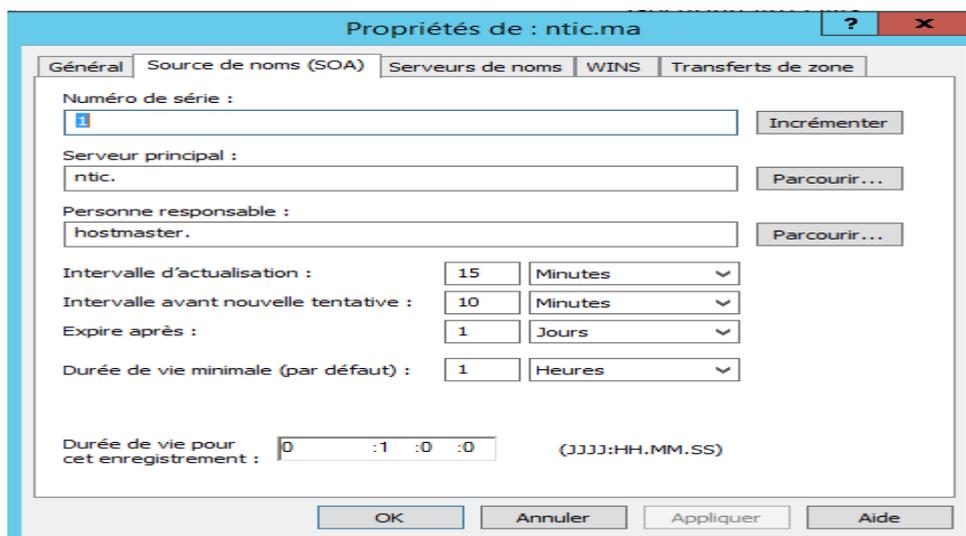
Maintenant notre zone est créée, mais il est indispensable dans une zone d'avoir deux types d'enregistrement le SOA (Start of Authority) et le NS (Name Server).

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

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

Remarque: le numéro de série dans une SOA ne s'invente pas ! Il est incrémenté à chaque modification d'un enregistrement de ressource (serveur messagerie, serveur de nom..).

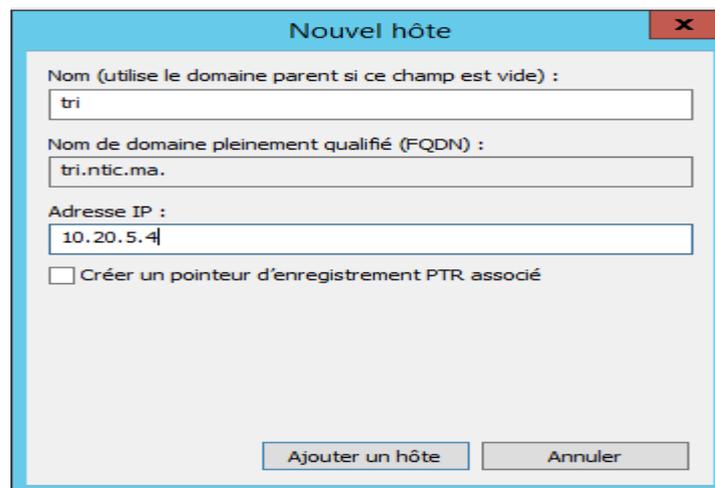
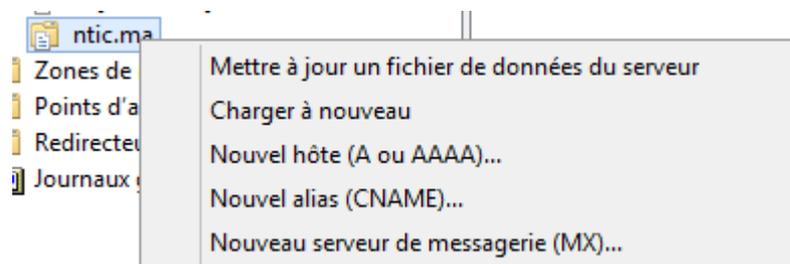
Il est fondamental de ne pas y toucher car cet ID va permettre aux serveurs secondaires de savoir s'ils ont le bon fichier zone. Si les numéros de série ne s'accorde pas le fichier zone du DNS « maître » (DNS où la zone a été configurée comme primaire) est envoyé aux serveurs secondaires.



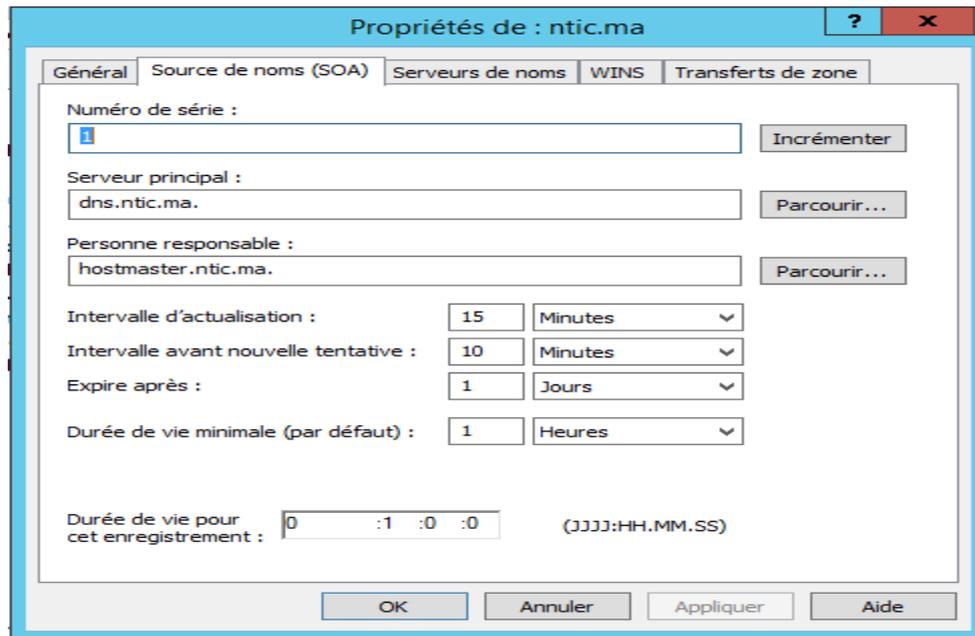
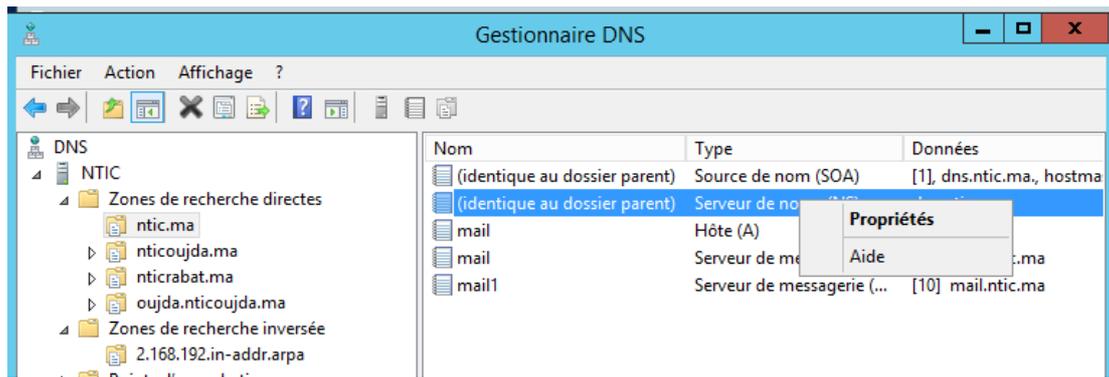
Maintenant que vous avez pu modifier votre SOA et votre NS vous pouvez ajouter les différentes machines que vous avez dans votre réseau. Pour cela vous avez 3 possibilités d'enregistrement de ressource: un hôte A ou AAAA, un alias CNAME ou un échangeur de messagerie MX.

- **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 un enregistrement A, AAAA, CNAME ou hôte ou MX.

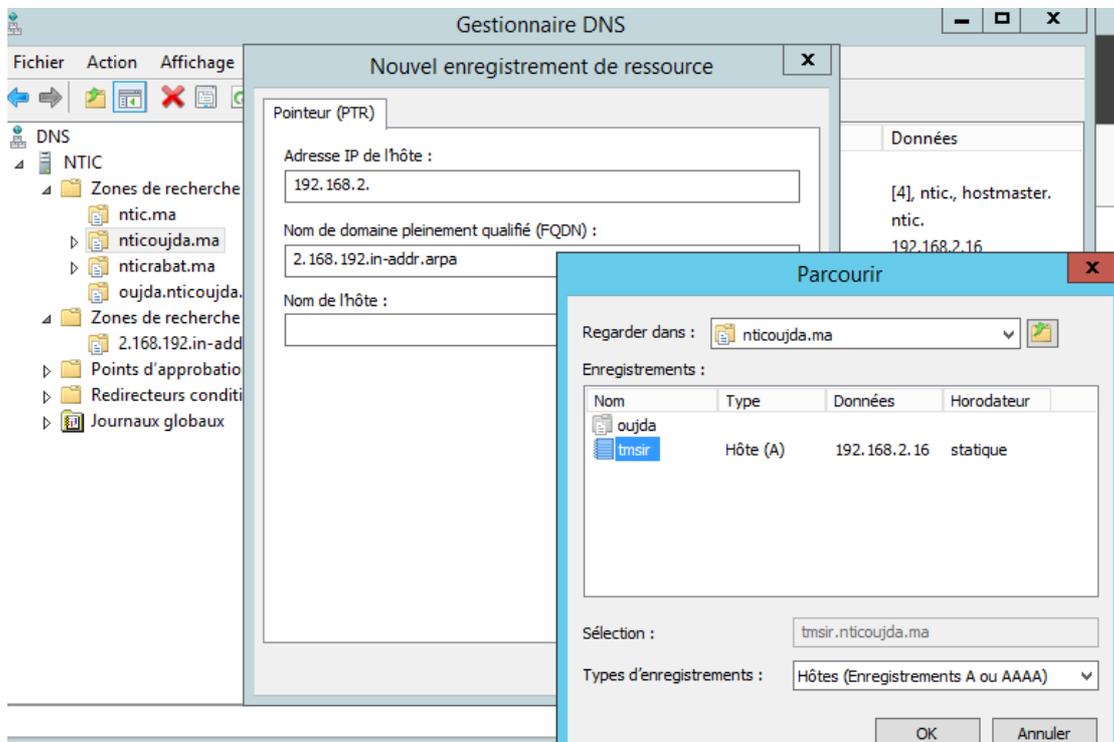
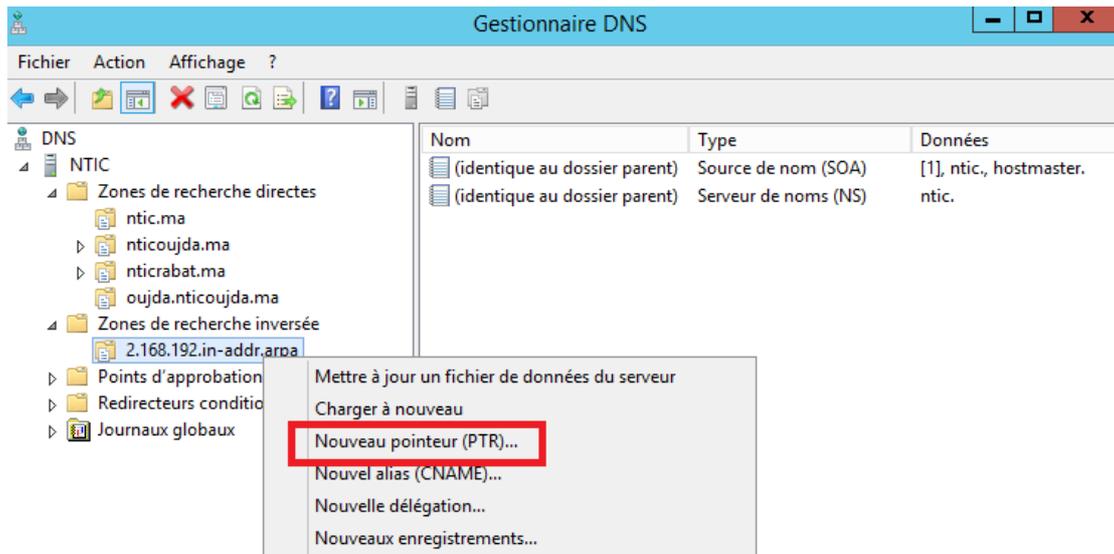


Pour modifier les informations de la zone SOA et NS , il faut faire un clic droit sur « serveur de nom NS » puis « Propriétés »



11.2 Zone de recherche inverse

Pour l'enregistrement PTR, un clic droit sur la zone inverse puis dans le nom du hôte cliquer sur parcourir et sélectionner le nom du domaine associé



12. Test

12.1 Configuration du client

12.2 Interrogation du serveur

13. Installation et configuration du serveur DNS en PowerShell

13.1 Installation

Pour ajouter le rôle du serveur il faut utiliser la commande

```
>Install-WindowsFeature DNS -IncludeManagementTools
```

```
PS C:\Users\Administrateur.WIN-30KPE2K33NE> Install-WindowsFeature DNS -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result
-----
True      No           NoChangeNeeded {}
PS C:\Users\Administrateur.WIN-30KPE2K33NE> _
```

13.2 Redirection

Pour configurer la redirection il faut utiliser la commande

```
Add-DnsServerForwarder -IPAddress 8.8.8.8 -PassThru
```

13.3 Zone primaire

Pour créer une zone Primaire

Directe :

```
Add-DnsServerPrimaryZone -Name "nom de la zone " -ZoneFile
"nomdelazone.dns"
```

Inverse :

```
Add-DnsServerPrimaryZone -NetworkID 85.17.209.0/24 -ZoneFile "209.17.85.in-
addr.arpa.dns"
```

13.4 Enregistrement

Pour ajouter les enregistrements de type A, AAA, MX, PTR, CNAME il faut utiliser les commandes :

Enregistrement A :

```
Add-DnsServerResourceRecord -ZoneName le nom de la zone -Name le nom du
hôte -A -IPv4Address l'adresse IP
```

```
PS C:\Users\Administrateur> Add-DnsServerResourceRecord -zoneName ofppt.ma -Name tmsir -A -IPv4Address 192.168.2.5
PS C:\Users\Administrateur> nslookup.exe tmsir.ofppt.ma
Serveur : Unknown
Address: 192.168.247.146
Nom : tmsir.ofppt.ma
Address: 192.168.2.5
PS C:\Users\Administrateur> _
```

Dans le cas d'enregistrement AAAA, il faut remplacer le A par les quatre A et l'option IPv4Address par IPv6Address

Enregistrement CNAME:

Add-DnsServerResourceRecord -ZoneName le nom de la zone -Name le nom du hôte -CNAME -HostNameAlias le nom du hôte originale

```
PS C:\Users\Administrateur> Add-DnsServerResourceRecord -zoneName ofppt.ma -Name tdi -CNAME -hostnameAlias tmsir.ofppt.ma
PS C:\Users\Administrateur> nslookup.exe tdi.ofppt.ma
Serveur : Unknown
Address: 192.168.247.146

Nom : tmsir.ofppt.ma
Address: 192.168.2.5
Aliases: tdi.ofppt.ma
PS C:\Users\Administrateur>
```

Enregistrement MX

Add-DnsServerResourceRecord -ZoneName le nom de la zone -Name le nom du hôte -MX -MailExchange Le FQDN -Preference la priorité du serveur mail

```
PS C:\Users\Administrateur> Add-DnsServerResourceRecord -zoneName ofppt.ma -Name mail1 -MX -MailExchange mail1.ofppt.ma -Preference 20
```

Enregistrement PTR

Add-DnsServerResourceRecord -ZoneName le nom de la zoneinverse -Name numéro de la machine (IP) -PTR -PtrDomainName le FQDN

```
PS C:\Users\Administrateur> Add-DnsServerResourceRecord -zoneName 2.168.192.in-addr.arpa -Name 8 -PTR -PtrDomainName ntic.ofppt.ma
PS C:\Users\Administrateur> nslookup.exe 192.168.2.7
Serveur : Unknown
Address: 192.168.247.146

Nom : ntic
Address: 192.168.2.7
PS C:\Users\Administrateur>
```

Pour afficher la configuration :

Get-DnsServer

```

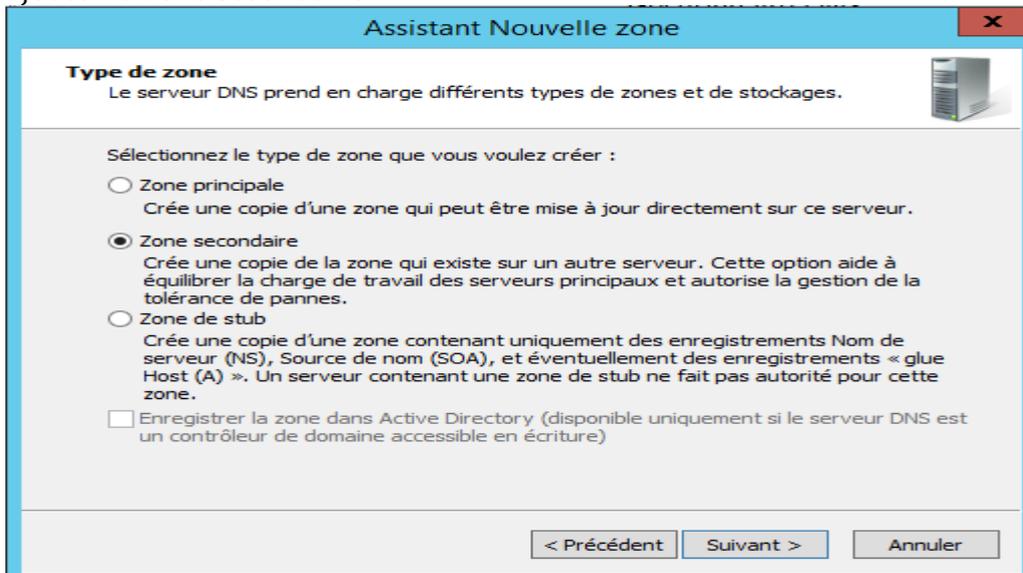
PS C:\Users\Administrateur> Get-DnsServer
AVERTISSEMENT : EnableRegistryBoot non applicable sur la version SLAVE du serveur DNS.

ServerSetting:
=====
EnableOnLineSigning                True
TcpReceivePacketSize               65536
WriteAuthorityNs                   False
SocketPoolSize                     2500
AppendMsZoneTransferTag            False
NameCheckFlag                      2
UpdateOptions                      783
MaximumTrustAnchorActiveRefreshInterval 15.00:00:00
EnableIPv6                          True
RncProtocol                         5
ForestDirectoryPartitionBaseName   ForestDnsZones
AutoCreateDelegation               False
EnableDirectoryPartitions          4294967295
SelfTest                            False
DsAvailable                         True
EnableSendErrorSuppression          True
SilentlyIgnoreCNameUpdateConflicts False
EnableDuplicateQuerySuppression    True
DomainDirectoryPartitionBaseName   DomainDnsZones
ReloadException                     False
AdminConfigured                    True
StrictFileParsing                   False
AllowCNameAtNs                     True
MaximumSignatureScanPeriod         2.00:00:00
IsReadOnlyDC                        False
DisableAutoReverseZone              False
AllIpAddress                       {fe80::5955:75e1:3ca5:e9dc, 192.168.2...}
EnableUpdateForwarding              False
DeleteOutsideGlue                  False
MinorVersion                       3
MajorVersion                       6
LocalNetPriority                    True
RootTrustAnchorsURL                https://data.iana.org/root-anchors/ro...
MaxResourceRecordsInNonSecureUpdate 30
ComputerName                        slave
RemoteIP4RankBoost                  5

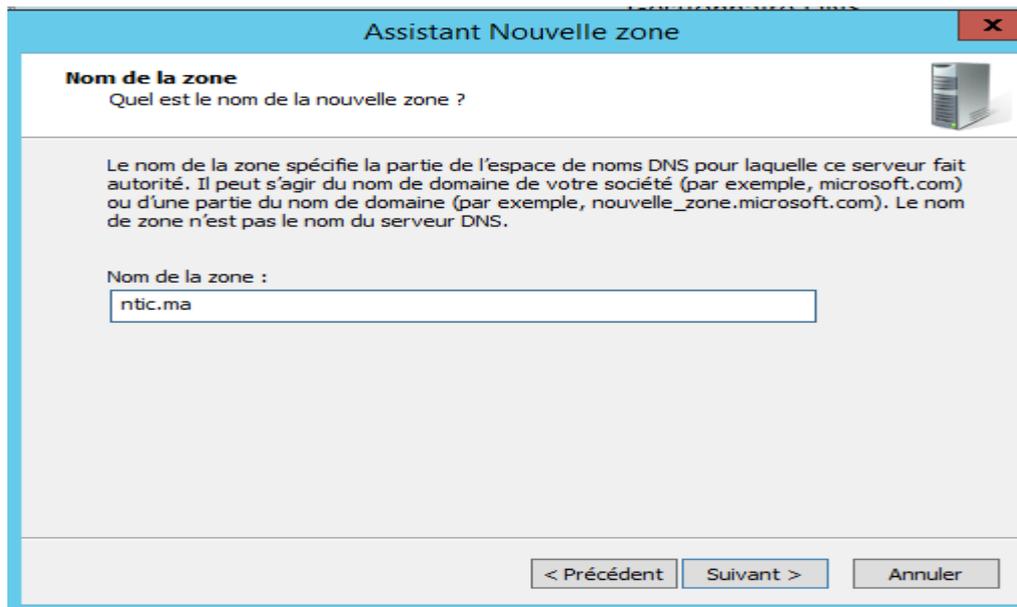
```

14. Configuration du serveur secondaire graphiquement

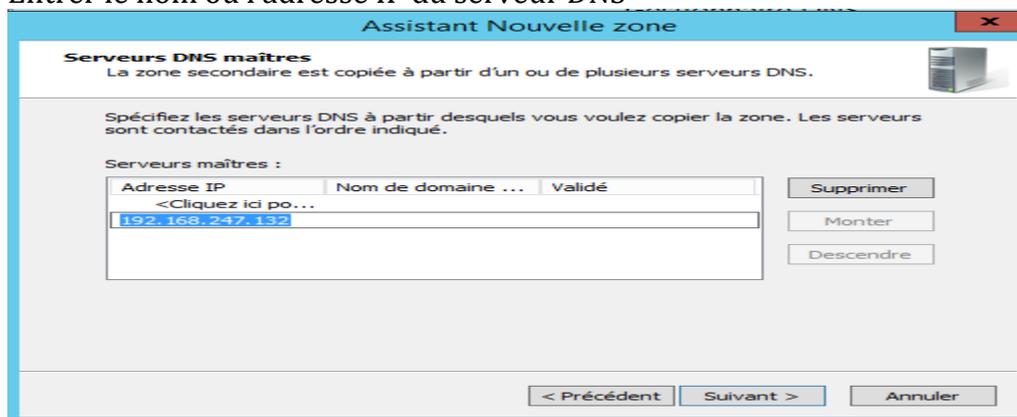
Ajouter le rôle DNS sur le serveur secondaire, puis dans le gestionnaire dns ajouter la zone secondaire



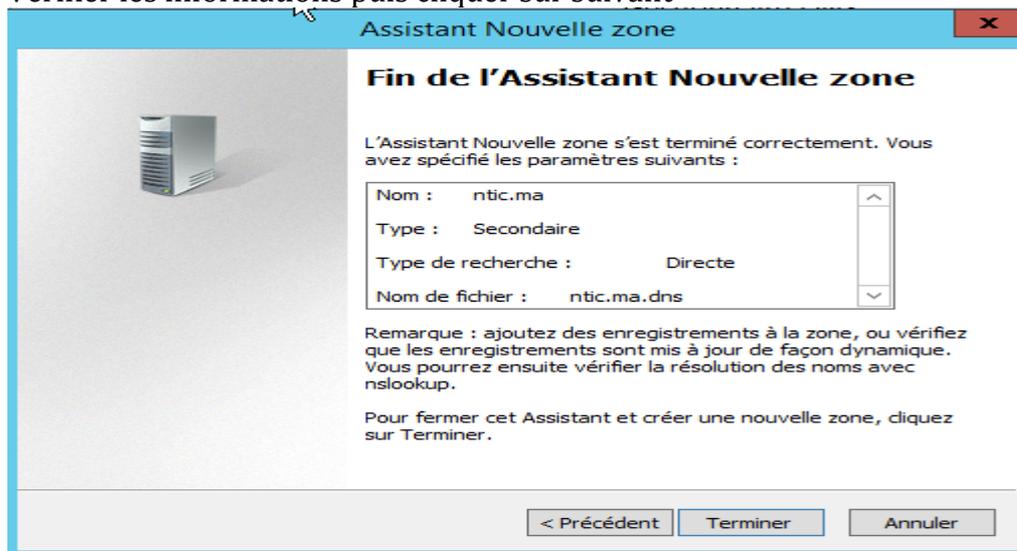
Puis entrez le nom de la zone primaire



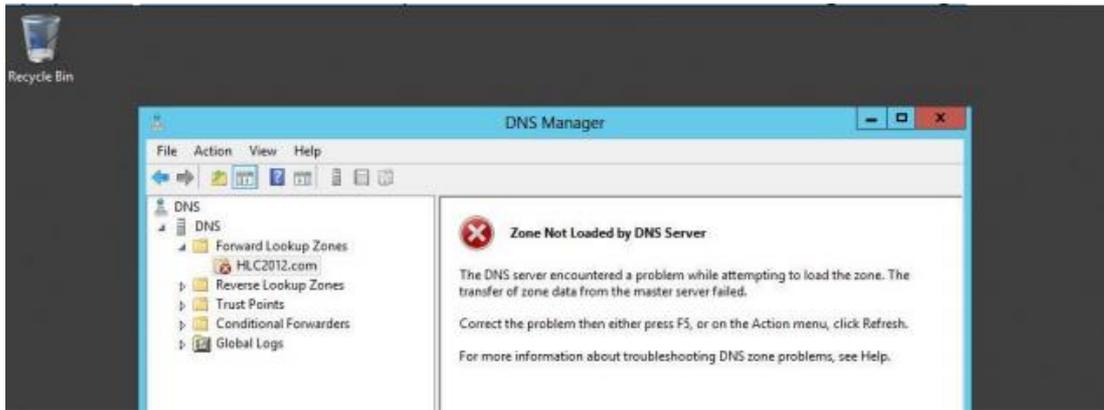
Entrer le nom ou l'adresse IP du serveur DNS



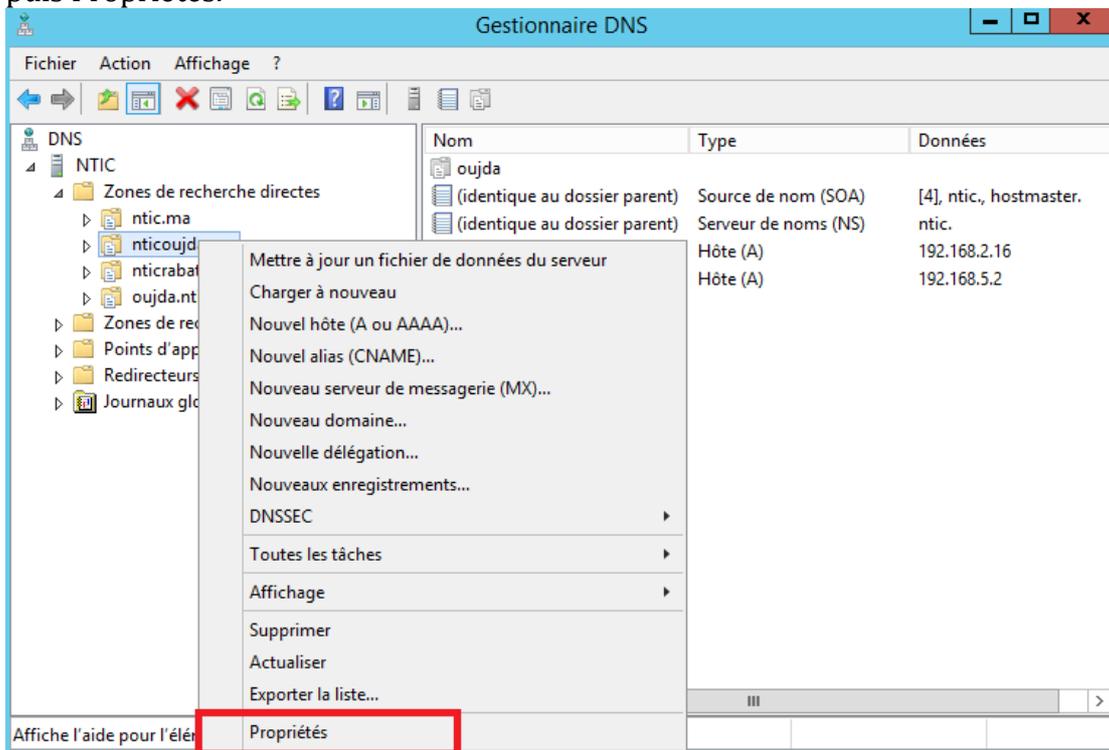
Vérifier les informations puis cliquer sur suivant



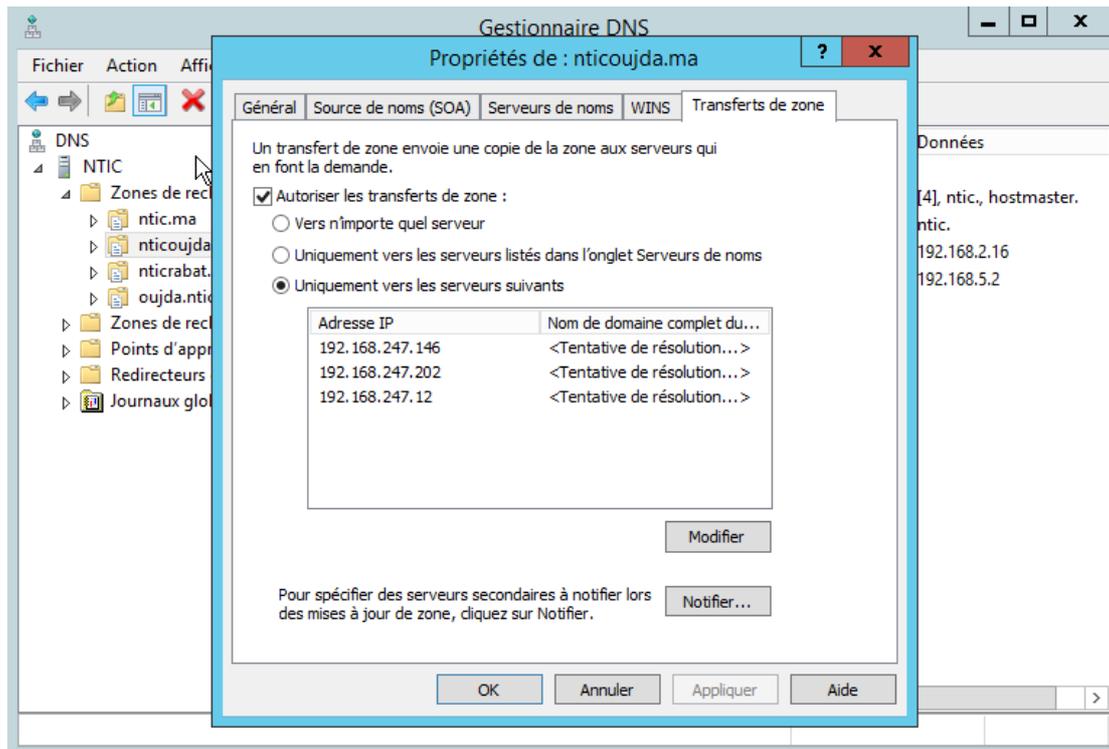
La configuration du DNS est terminée, mais il faut maintenant dire au DNS primaire qu'il faut répliquer les informations. Sinon la réplication échoue et vous obtiendrez ce gros X rouge.



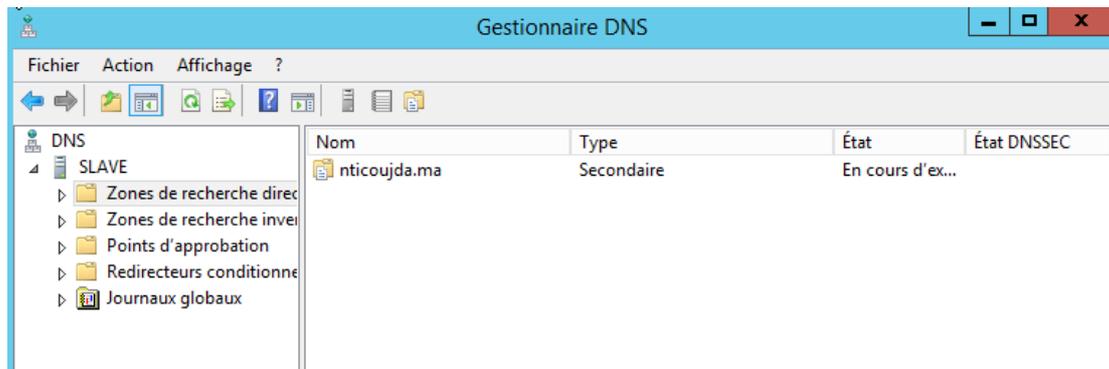
Sur le serveur DNS primaire, lancer le gestionnaire de DNS, clic droit sur la zone puis Propriétés.



Aller à l'onglet "Transferts de zone", par défaut, pour des raisons de sécurité, l'option "Autoriser les transferts de zone:" n'est pas cochée pour protéger vos informations DNS. Nous devons permettre les transferts de zone, si vous tenez à vos enregistrements DNS, vous ne voulez pas sélectionner "Vers n'importe quel serveur», mais assurez-vous que vous cliquez sur «Uniquement vers les serveurs listés dans l'onglet Serveurs de noms"



Le serveur DNS secondaire est maintenant OK. La croix rouge va disparaître et vos zones vont être transférées automatiquement



15. Configuration du serveur secondaire en PowerShell

Il faut commencer par autoriser le transfert au niveau du serveur primaire

```
Set-DnsServerPrimaryZone NomdeZone -SecureSecondaries TransferAnyServer -Notify Notify
```

Ajouter le rôle DNS sur le serveur secondaire

```
Install-WindowsFeature DNS -IncludeManagementTools
```

Ajouter la zone secondaire en indiquant le nom de la zone primaire et l'adresse IP du serveur primaire

```
Add-DnsServerSecondaryZone -Name "nom de la zone primaire" -ZoneFile  
"nom de la zone primaire .dns" -MasterServers @IP du serveur primaire
```

16. Mises à jour dynamiques

Une mise à jour dynamique est une mise à jour de DNS en temps réel. Les mises à jour dynamiques sont importantes pour les clients DNS qui changent d'emplacement, car elles peuvent inscrire et mettre à jour dynamiquement leurs enregistrements de ressources sans intervention manuelle.

Alors pour réinscris les noms DNS utiliser la commande :

```
ipconfig /registerdns
```

Ou exécute l'applet de commande Windows PowerShell

```
Register-DNSClient
```

17. Vérification du Cache

Dans Windows Server 2012, vous pouvez accéder au contenu du cache du serveur DNS en sélectionnant l'affichage Avancé dans la console du Gestionnaire DNS. Lorsque vous activez cet affichage, le contenu mis en cache s'affiche sous la forme d'un nœud dans le Gestionnaire DNS. Vous pouvez également supprimer des entrées spécifiques (ou la totalité) du cache du serveur DNS.

Vous pouvez également utiliser l'applet de commande Windows PowerShell

Pour afficher le cache de résolution du serveur DNS utiliser la commande

```
> Get-dnsservercache
```

Pour afficher le cache de résolution du client DNS utiliser la commande

```
> Get-dnsclientcache
```

Ou En utilisant la commande ipconfig avec les options :

/flushdns: Vide et réinitialise le cache de résolution du client DNS. Cette option est utile pour exclure les entrées de cache négatives ainsi que toutes les autres entrées ajoutées de façon dynamique.

/displaydns: Affiche le cache de résolution du client DNS, qui inclut les entrées préchargées à partir du fichier des hôtes locaux ainsi que tous les enregistrements de ressources récemment obtenus pour les requêtes de noms résolues par l'ordinateur. Le service Client DNS utilise ces informations pour résoudre rapidement les noms fréquemment sollicités, avant d'interroger ses serveurs DNS configurés.

18. Résolution des problèmes liés à la résolution de noms

Les outils en ligne de commande et les commandes que vous utilisez pour résoudre les problèmes de configuration sont les suivants :

18.1 Nslookup

Permet d'interroger des informations DNS. Il s'agit d'un outil flexible, capable de fournir des informations précieuses à propos de l'état du serveur DNS. Vous pouvez également l'utiliser pour rechercher des enregistrements de ressources et valider leur configuration. Vous pouvez, en outre, tester des transferts de zone, des options de sécurité et la résolution des enregistrements MX.

18.2 DNSCmd

Permet de gérer le rôle serveur DNS. Cet outil permet de créer des scripts dans des fichiers de commandes dans le but d'automatiser des tâches de gestion DNS de routine ou de procéder à un simple travail d'installation et de configuration sans assistance de nouveaux serveurs DNS sur votre réseau.

18.3 Dnslint

Permet de diagnostiquer les problèmes DNS courants. Cet outil diagnostique rapidement les problèmes de configuration de DNS et peut générer un rapport au format HTML sur l'état du domaine que vous testez.

18.4 Ipconfig

Permet d'afficher et modifier les détails de la configuration IP que l'ordinateur utilise. Cet outil inclut des options de ligne de commande supplémentaires que vous pouvez utiliser pour dépanner et prendre en charge des clients DNS.

Vous pouvez consulter le cache DNS local du client à l'aide de la commande `ipconfig/displaydns`. En outre, vous pouvez effacer le cache local à l'aide de `ipconfig/flushdns`. Si vous voulez réinscrire un hôte dans DNS, vous pouvez utiliser `ipconfig/registerdns`.

- Analyse du serveur DNS: pour tester si le serveur peut communiquer avec des serveurs en amont, vous pouvez effectuer de simples requêtes locales et récursives à partir de l'onglet Analyse du serveur DNS. Vous pouvez également planifier ces tests pour qu'ils s'exécutent de manière régulière. L'onglet Analyse du serveur DNS est disponible uniquement dans Windows Server 2008 et Windows Server 2012, dans la boîte de dialogue Propriétés de : nom du serveur DNS.

18.5 Test-DNSServer

Permet de vérifier les fonctionnalités du serveur DNS

Dans Windows Server 2012, il existe un nouvel ensemble d'applets de commande Windows PowerShell que vous pouvez utiliser pour la gestion des clients et serveurs DNS. Voici certaines des applets de commande les plus fréquemment utilisées :

18.6 Clear-DNSClientCache.

Cette applet de commande efface le cache client, à l'instar de ipconfig /flushdns.

18.7 Get-DNSClient

Cette applet de commande affiche les détails des interfaces réseau.

18.8 Get-DNSClientCache

Cette applet de commande affiche le contenu du cache client DNS local.

18.9 Register-DNSClient

Cette applet de commande inscrit toutes les adresses IP de l'ordinateur sur le serveur DNS configuré.

18.10 Resolve-DNSName

Cette applet de commande effectue une résolution de noms DNS pour un nom spécifique, à l'instar de Nslookup.

18.11 Set-DNSClient

Cette applet de commande définit les configurations de client DNS spécifiques à l'interface sur l'ordinateur.

19.Zones intégrées à Active Directory

Un serveur DNS peut stocker des données de zone dans la base de données AD DS à condition que le serveur DNS soit un contrôleur de domaine AD DS. Les avantages d'une zone intégrée à Active Directory sont importants :

- Mises à jour multimaîtres. Contrairement aux zones principales (qui ne peuvent être modifiées que par un seul serveur principal), les zones intégrées à Active Directory sont accessibles en écriture à n'importe quel contrôleur de domaine vers lequel la zone est répliquée
- Réplication des données de zone DNS à l'aide de la réplication AD DS.
- Mises à jour dynamiques sécurisées. Une zone intégrée à Active Directory peut appliquer des mises à jour dynamiques sécurisées.

Annexe

Enregistrement A :

```
Add-DnsServerResourceRecord [-ZoneName] <String> [-Name] <String> [-A] -IPv4Address <IPAddress> [-AgeRecord] [-AllowUpdateAny] [-CimSession <CimSession[]> ] [-ComputerName <String> ] [-CreatePtr] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-PassThru] [-ThrottleLimit <Int32> ] [-TimeToLive <TimeSpan> ] [-ZoneScope <System.String> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Enregistrement AAA:

```
Add-DnsServerResourceRecord [-ZoneName] <String> [-Name] <String> [-AAAA] -IPv6Address <IPAddress> [-AgeRecord] [-AllowUpdateAny] [-CimSession <CimSession[]> ] [-ComputerName <String> ] [-CreatePtr] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-PassThru] [-ThrottleLimit <Int32> ] [-TimeToLive <TimeSpan> ] [-ZoneScope <System.String> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Enregistrement CNAME

```
Add-DnsServerResourceRecord [-ZoneName] <String> [-Name] <String> [-CName] -HostNameAlias <String> [-AgeRecord] [-AllowUpdateAny] [-CimSession <CimSession[]> ] [-ComputerName <String> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-PassThru] [-ThrottleLimit <Int32> ] [-TimeToLive <TimeSpan> ] [-ZoneScope <System.String> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Enregistrement NS

```
Add-DnsServerResourceRecord [-ZoneName] <String> [-Name] <String> [-NS] -NameServer <String> [-AgeRecord] [-AllowUpdateAny] [-CimSession
```

```
<CimSession[]> ] [-ComputerName <String> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue |
Stop | Continue | Inquire | Ignore | Suspend} ] [-
InformationVariable <System.String> ] [-PassThru] [-ThrottleLimit
<Int32> ] [-TimeToLive <TimeSpan> ] [-ZoneScope <System.String> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Enregistrement MX:

```
Add-DnsServerResourceRecord [-ZoneName] <String> [-Name] <String> [-
MX] -MailExchange <String> -Preference <UInt16> [-AgeRecord] [-
AllowUpdateAny] [-CimSession <CimSession[]> ] [-ComputerName
<String> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue |
Stop | Continue | Inquire | Ignore | Suspend} ] [-
InformationVariable <System.String> ] [-PassThru] [-ThrottleLimit
<Int32> ] [-TimeToLive <TimeSpan> ] [-ZoneScope <System.String> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Enregistrement PTR:

```
Add-DnsServerResourceRecord [-ZoneName] <String> [-Name] <String> [-
Ptr] -PtrDomainName <String> [-AgeRecord] [-AllowUpdateAny] [-
CimSession <CimSession[]> ] [-ComputerName <String> ] [-
InformationAction <System.Management.Automation.ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ]
[-InformationVariable <System.String> ] [-PassThru] [-ThrottleLimit
<Int32> ] [-TimeToLive <TimeSpan> ] [-ZoneScope <System.String> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Référence :

<http://blog.benjaminperrin.fr/index.php/2014/02/06/dns-bind9-ajout-dun-serveur-secondaire-a-votre-zone/>

<https://4sysops.com/archives/server-roles-in-server-core-part-3-dns-servers/>

<https://technet.microsoft.com/library/jj649925.aspx>

<http://www.joryck-leyes.fr/tuto/DNS.pdf>