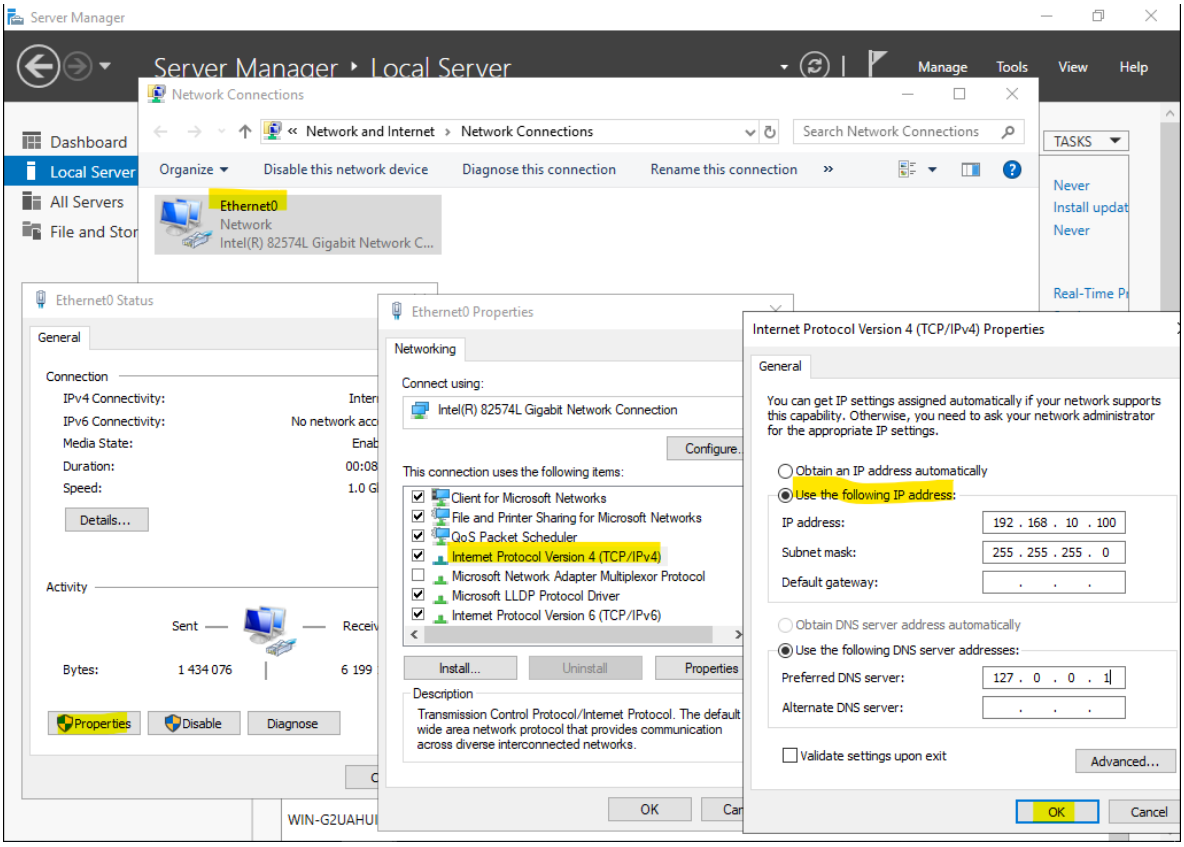
Installation et Configuration d'un Serveur DNS sur Windows Server (Interface Graphique)

1 – Installation d'un Serveur DNS sur Windows Server 2019 :

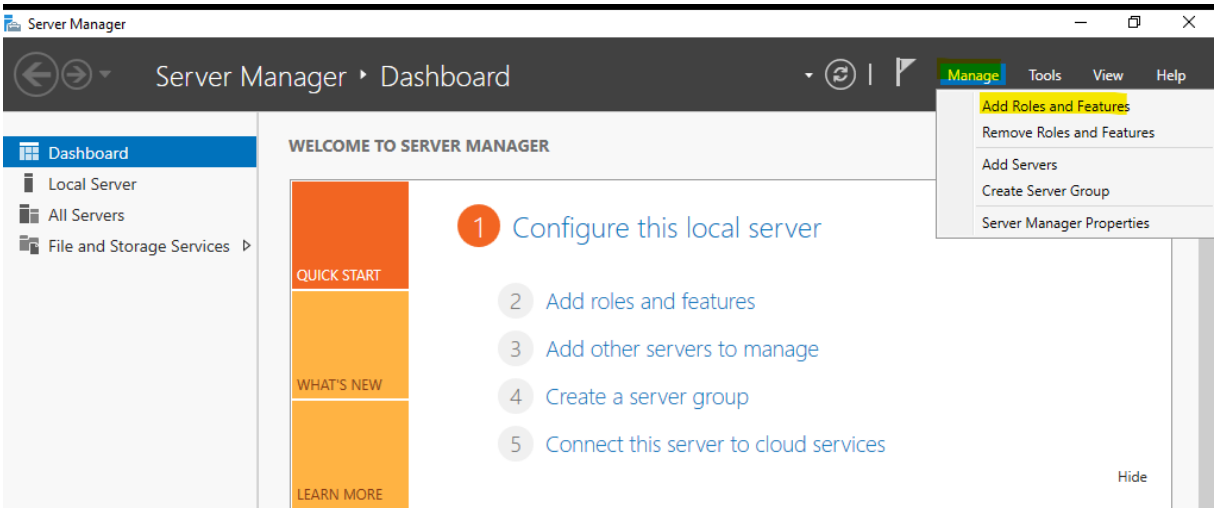
C’est quoi le DNS ?

Le DNS (Domain Name System) est un système qui traduit les noms de domaine lisibles par l’homme (comme *www.example.com*) en adresses IP numériques (comme *192.168.1.1*). Il sert à faciliter l’accès aux sites web et aux services en réseau en permettant aux utilisateurs d’utiliser des noms simples au lieu de devoir mémoriser des adresses IP complexes.

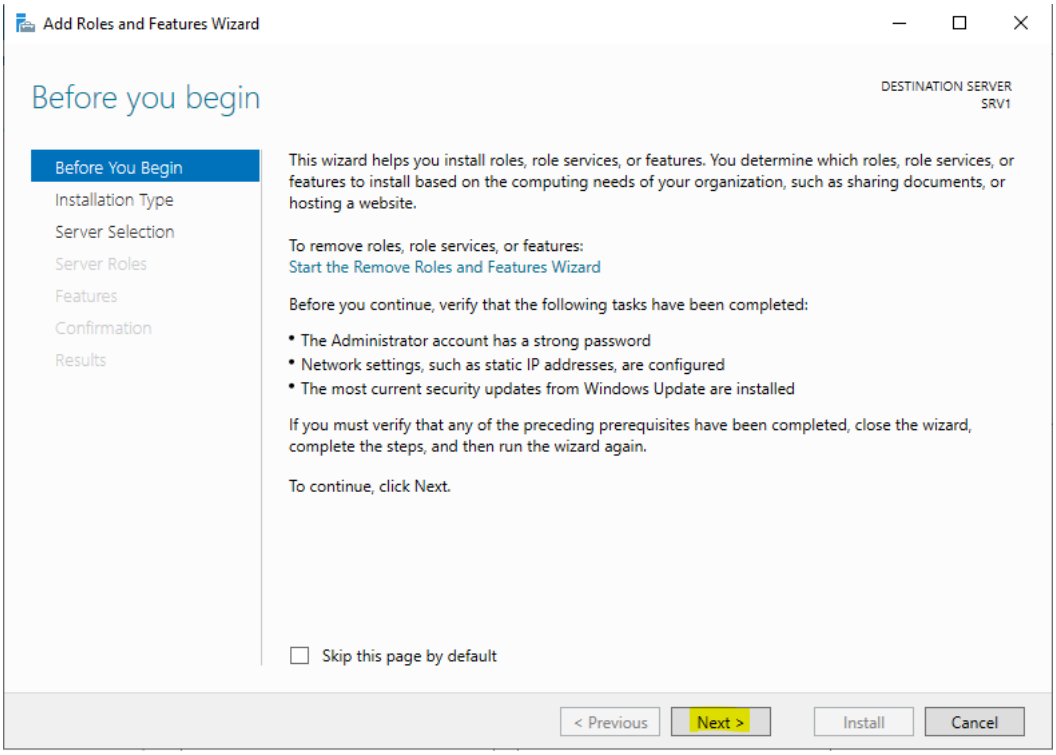
1 – Local server > ethernet > ethernet0 > propersties > internet protocole version 4 > use the following ip address : Cela consiste à attribuer une adresse IP statique à l'interface réseau du serveur local en accédant aux paramètres d'Ethernet, puis en sélectionnant le protocole IPv4 et en saisissant l'adresse IP manuellement, ce qui garantit une connexion stable.



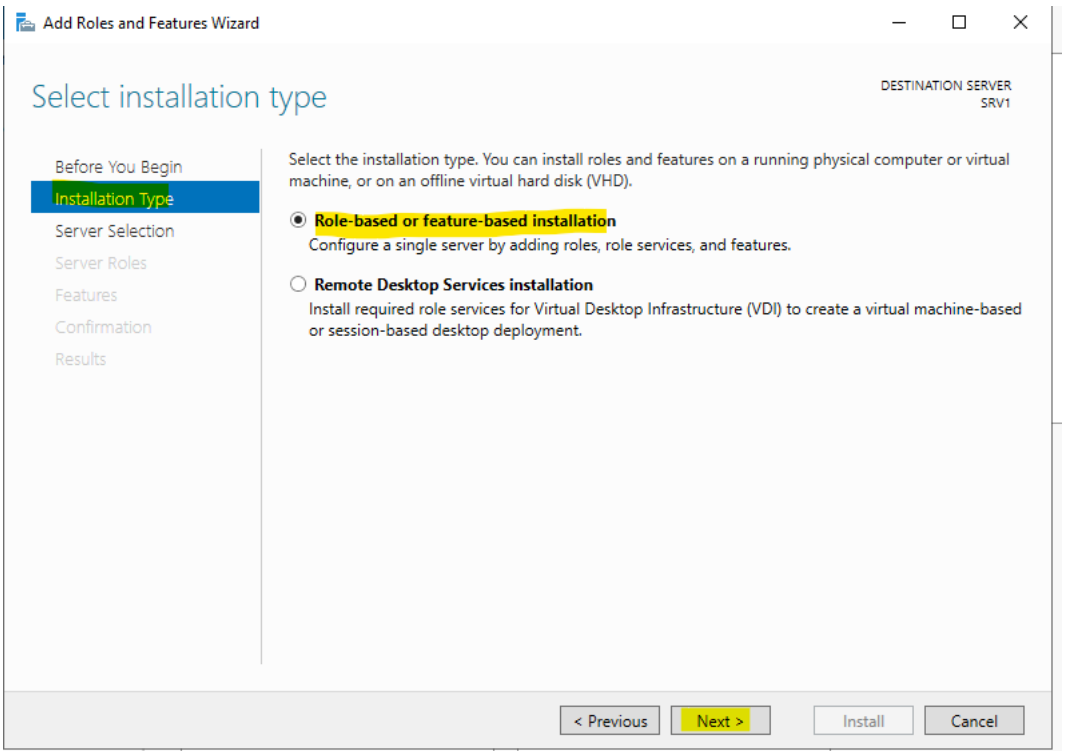
2 – Manager > add roles and feaures : Cela permet d'ajouter des rôles et des fonctionnalités supplémentaires à un serveur Windows.



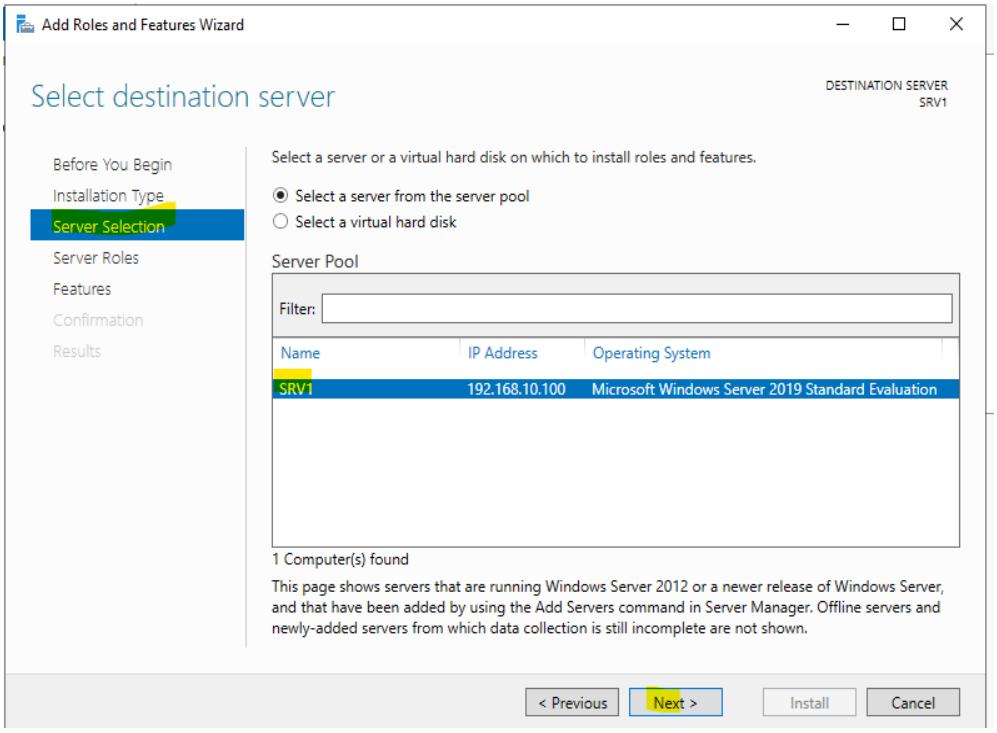
3 – Before you begin > next : Cela signifie que vous devez cliquer sur "Next" (Suivant) après avoir lu la section "Before you begin" (Avant de commencer), pour passer à l'étape suivante de la configuration.



4 – Installation type > role-based or feature-based installation > next : Cela signifie choisir le type d'installation "Role-based or feature-based installation" pour installer un rôle ou une fonctionnalité spécifique sur le serveur, puis cliquer sur "Next" pour continuer.

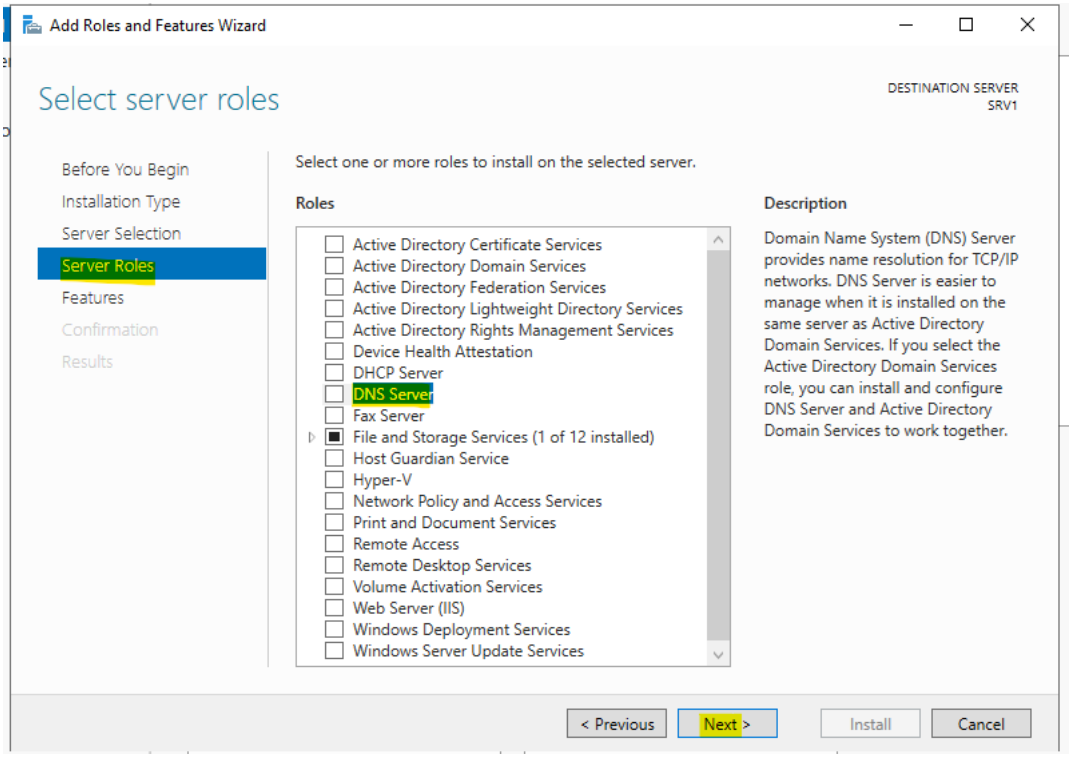


5 – Server selection > SRV1 > next : Cela signifie sélectionner le serveur "SRV1" pour l'installation, puis cliquer sur "Next" pour passer à l'étape suivante.

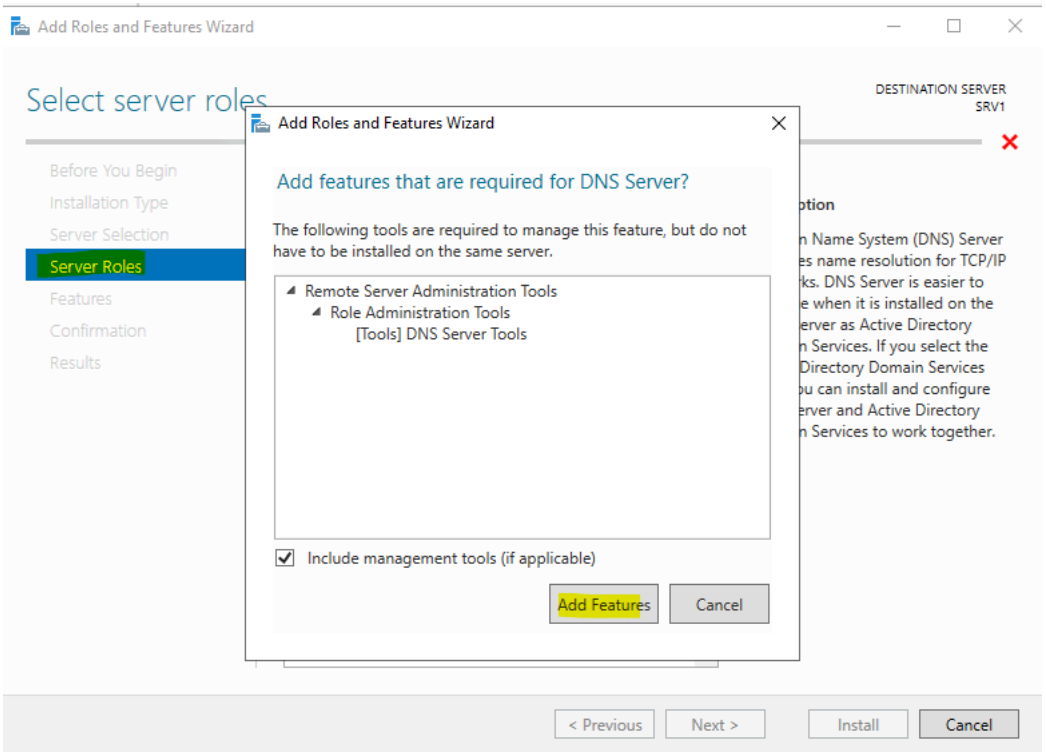


6 – Server roles > dns server > next : Cela signifie sélectionner le rôle "DNS Server" pour l'installer sur le serveur, puis cliquer sur "Next" pour

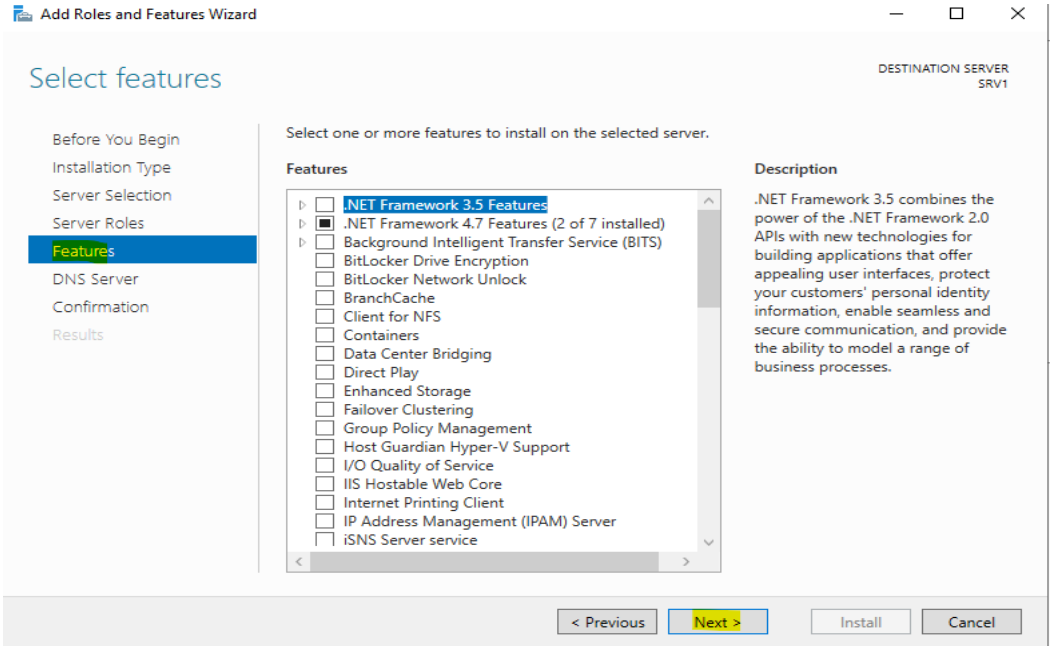
continuer.



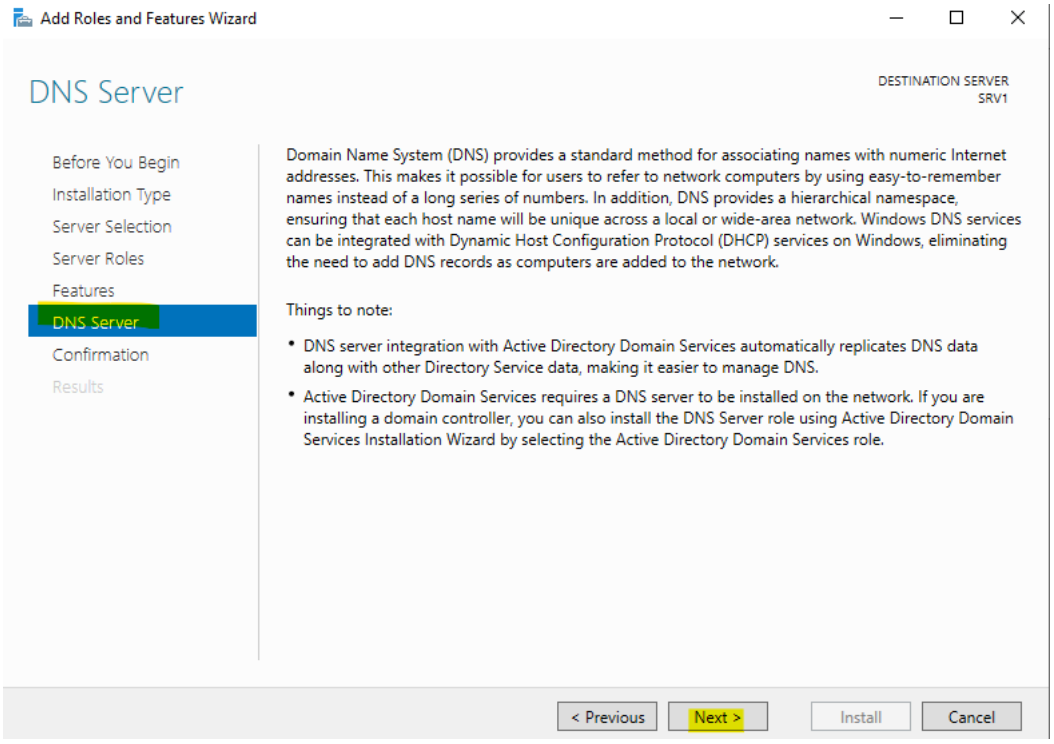
7 – Server roles > add features : Cela signifie ajouter des fonctionnalités supplémentaires nécessaires pour le rôle sélectionné (dans ce cas, le serveur DNS), avant de continuer l'installation.



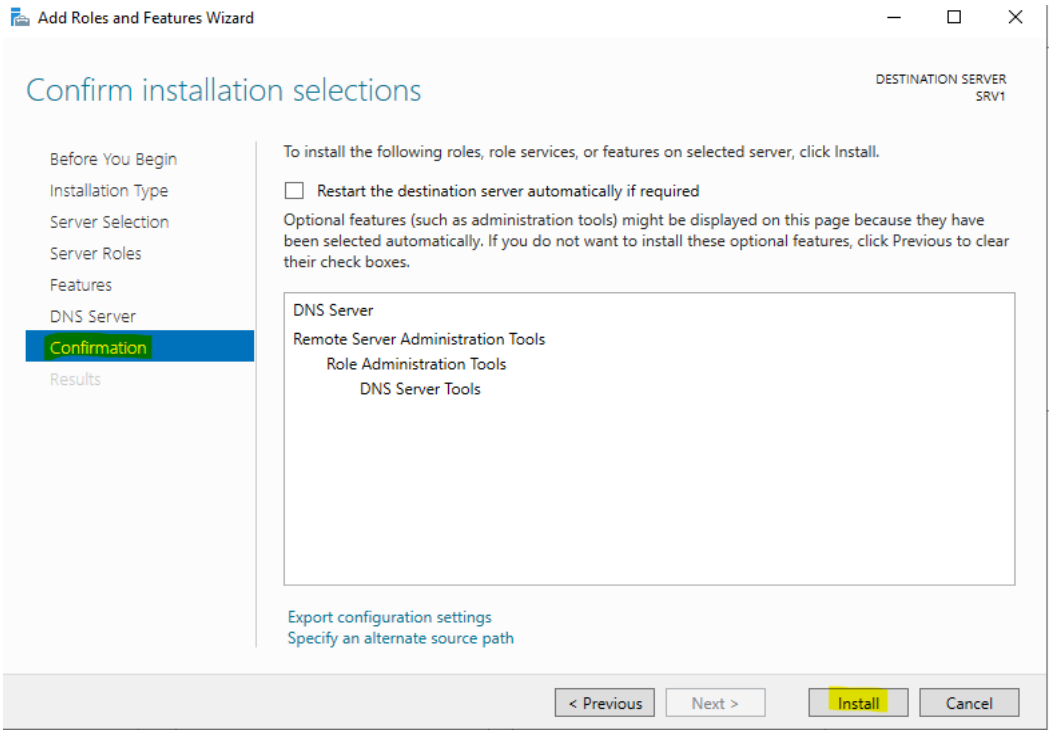
9 – Features > net framework 3.5 features > next : Cela signifie sélectionner la fonctionnalité ".NET Framework 3.5" si elle est nécessaire pour le rôle ou la fonctionnalité que vous installez, puis cliquer sur "Next" pour continuer.



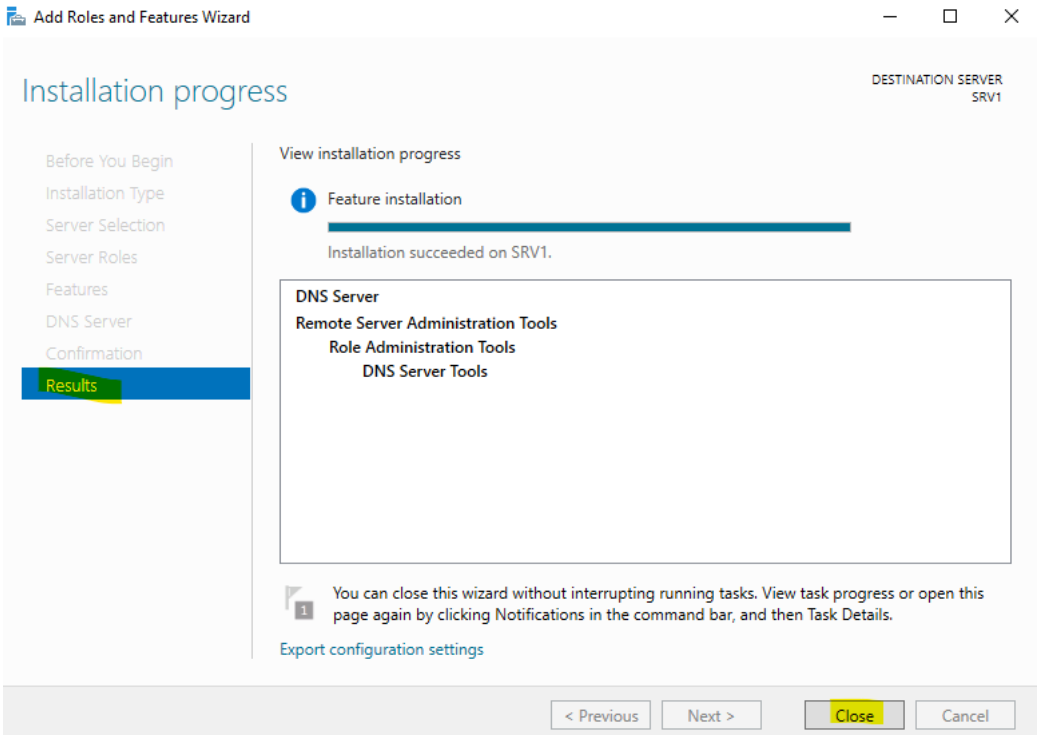
10 – Dns server > next : Cela signifie que vous avez sélectionné le rôle "DNS Server" et que vous devez cliquer sur "Next" pour continuer avec l'installation.



11 – Confirmation > install : Cela signifie que vous devez vérifier les sélections effectuées pour l'installation, puis cliquer sur "Install" (Installer) pour commencer l'installation du rôle ou des fonctionnalités sélectionnées.



12 – Results > close : Cela signifie que l'installation est terminée et vous devez cliquer sur "Close" (Fermer) pour terminer le processus et fermer la fenêtre des résultats.

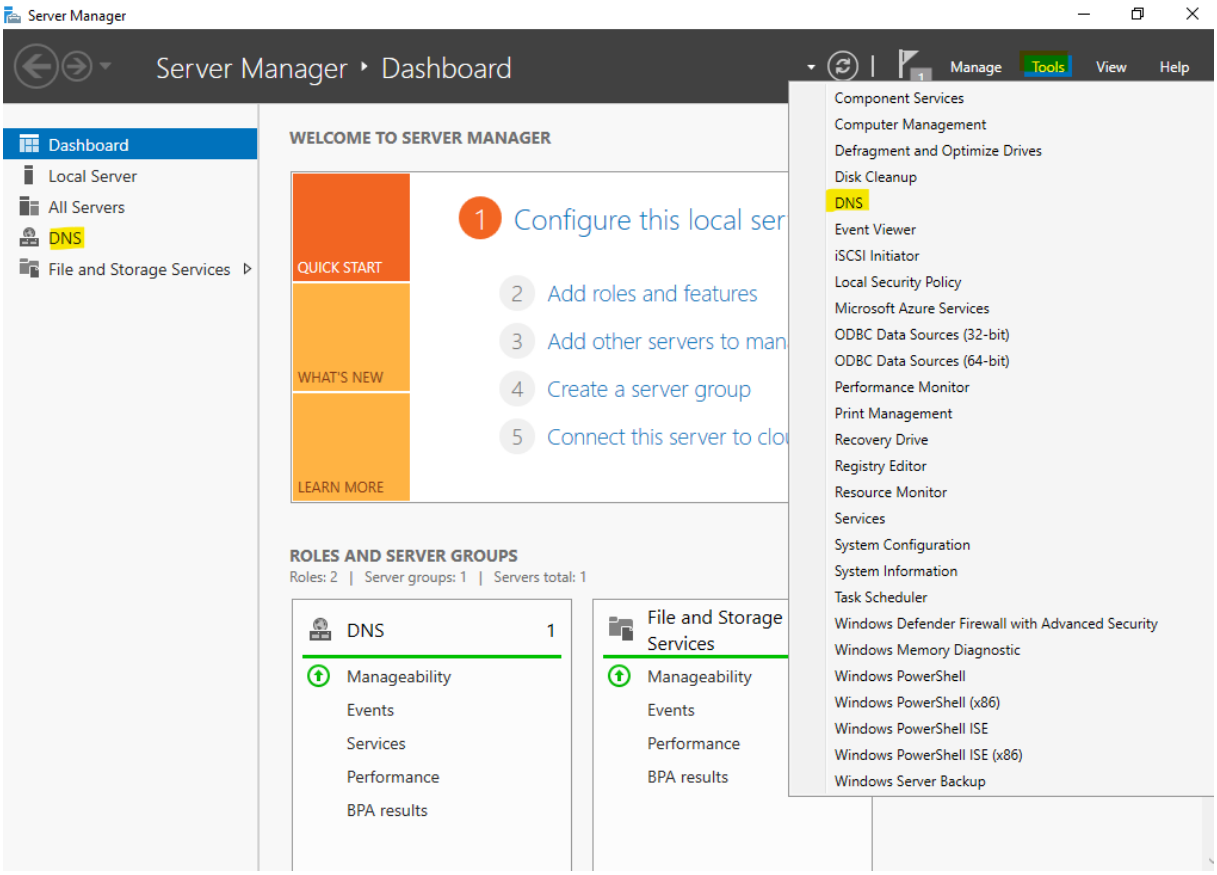


2 – Installation d'une zone directe DNS primaire sur Windows Server :

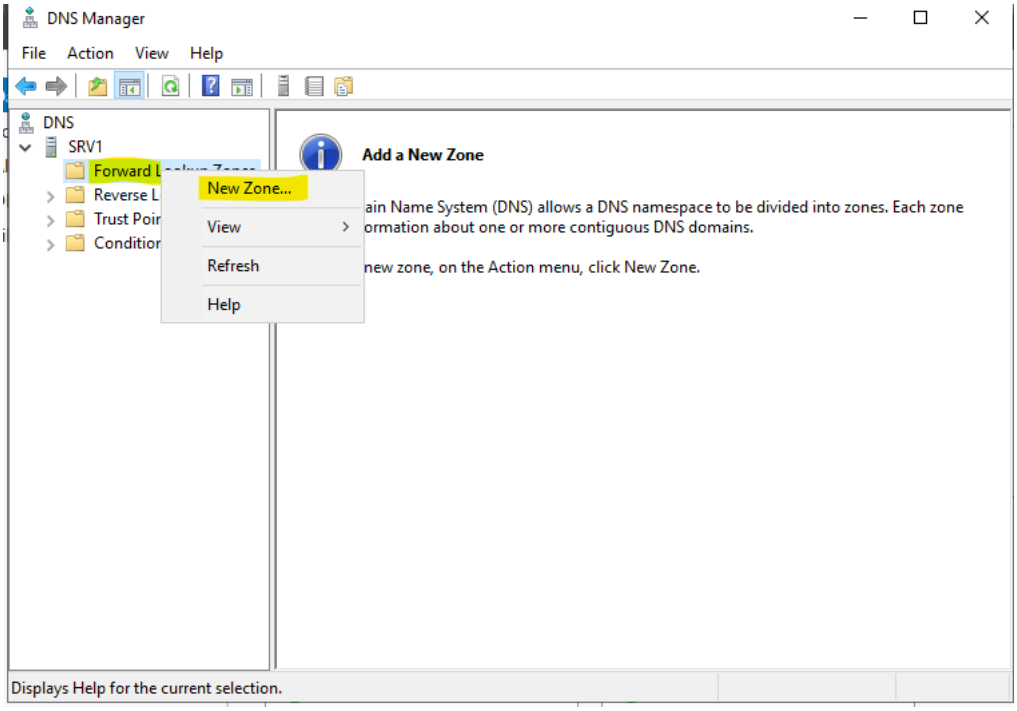
Qu'est-ce qu'une zone directe dans DNS ?

Une zone directe est la base de données principale contenant les enregistrements DNS d'un domaine, où les informations sont directement mises à jour.

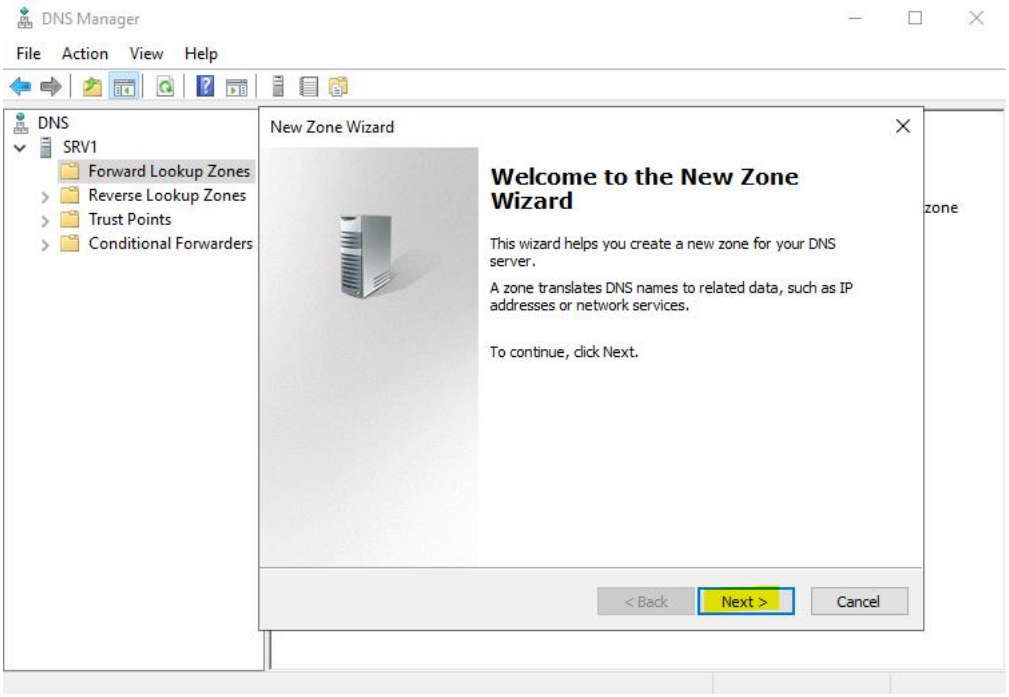
1 – Tools > dns : Cela signifie accéder à l'outil DNS dans le gestionnaire de serveur pour gérer les paramètres et configurations du serveur DNS.



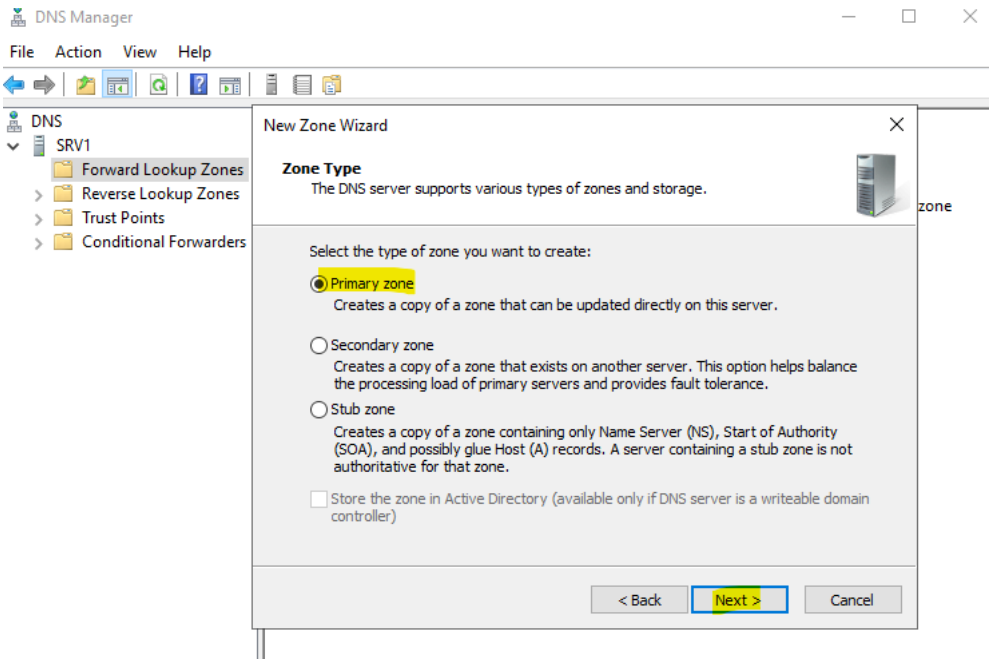
2 – Forward Lookup Zones > New Zone : Créer une nouvelle zone de recherche directe dans le serveur DNS pour résoudre les noms de domaine en adresses IP.



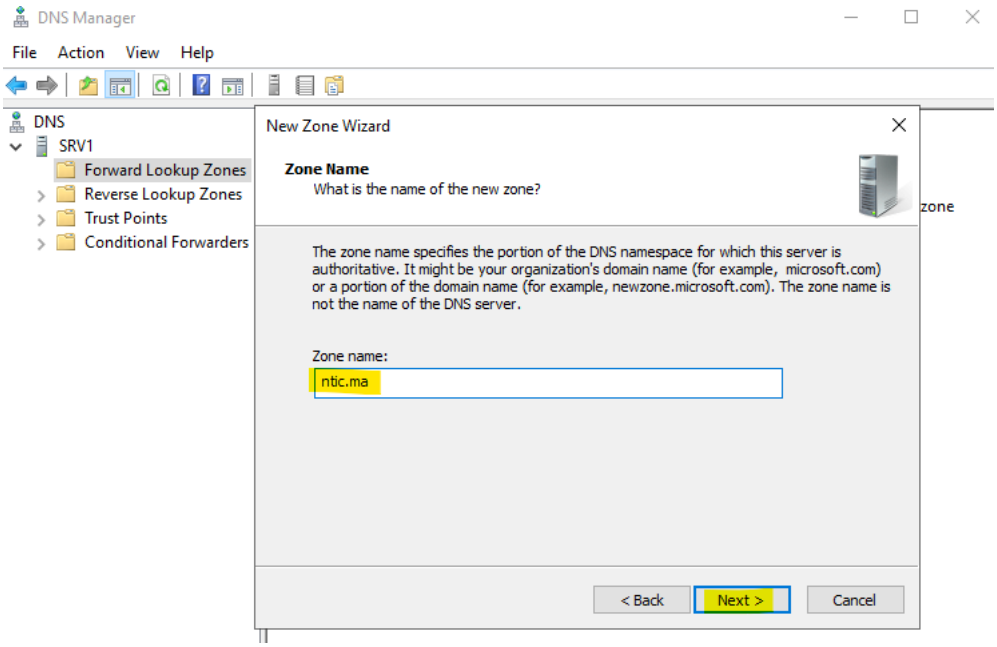
3 – Cliquer sur "**Next**" pour passer à l'étape suivante de la configuration de la zone.



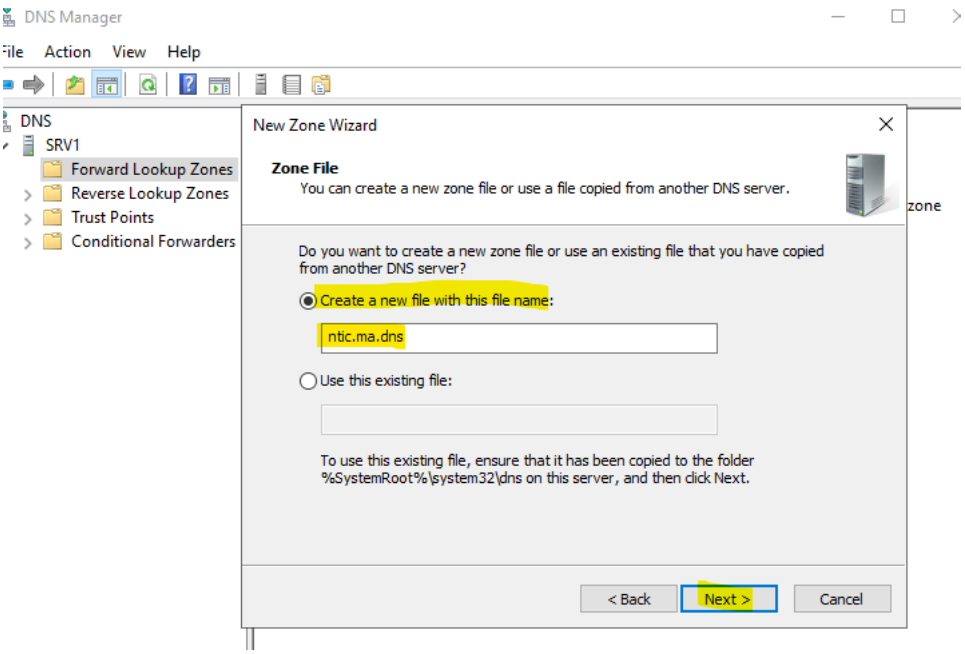
4 – Sélectionner "**Primary Zone**" pour créer une zone primaire, puis cliquer sur "**Next**" pour continuer.



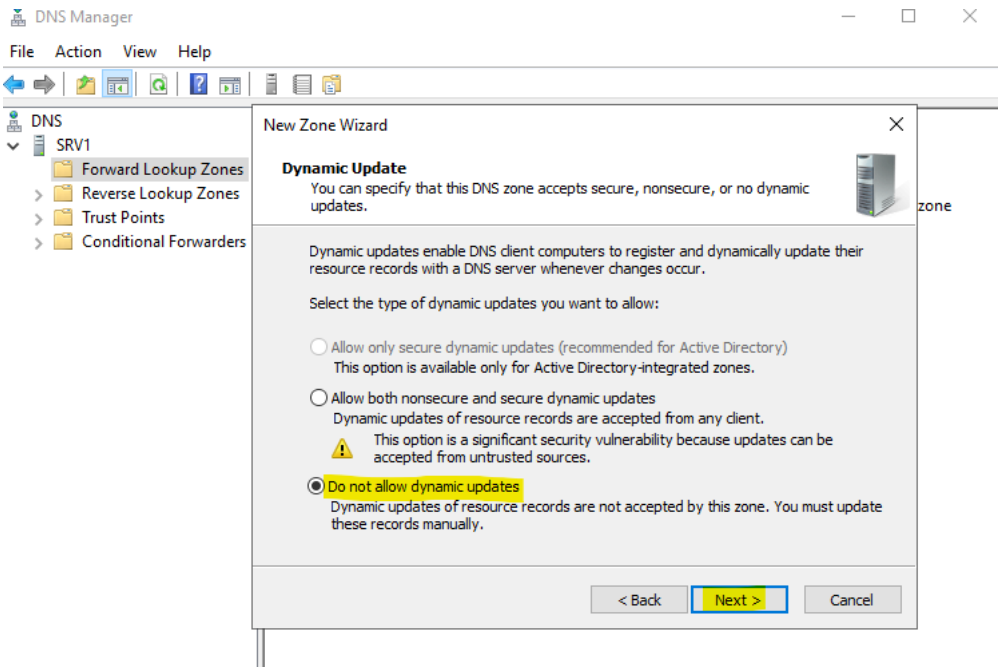
5 – Entrer le nom de la zone, ici "**ntic.ma**", puis cliquer sur "**Next**" pour continuer.



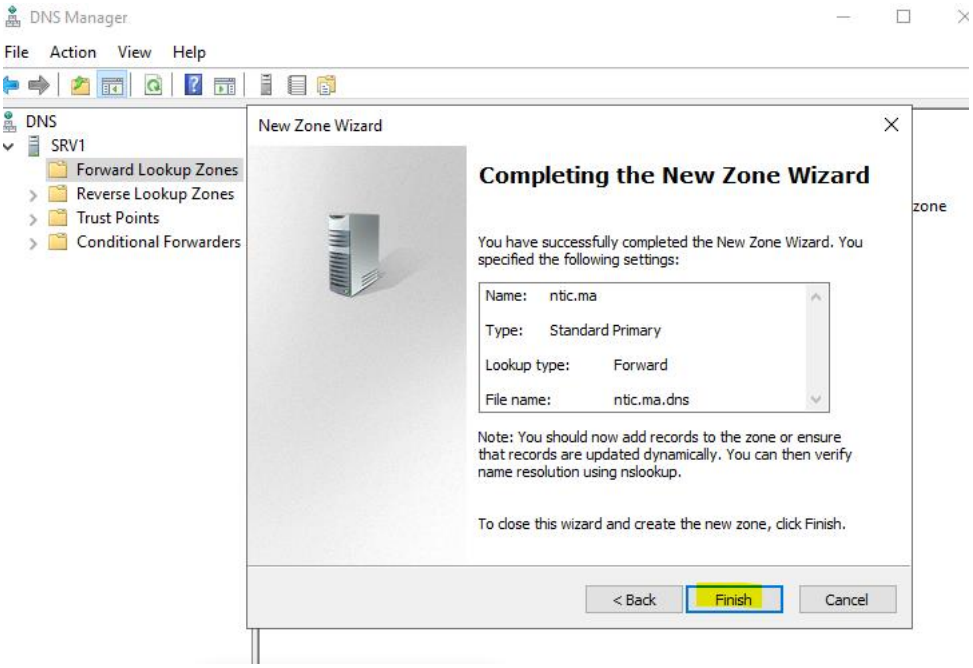
6 – Créer un nouveau fichier avec le nom "**ntic.ma.dns**", puis cliquer sur "**Next**" pour continuer.



7 – Sélectionner l'option "**Do not allow dynamic updates**" pour empêcher les mises à jour dynamiques, puis cliquer sur "**Next**" pour continuer.



8 – Cliquer sur "**Finish**" pour terminer la configuration de la zone primaire DNS.

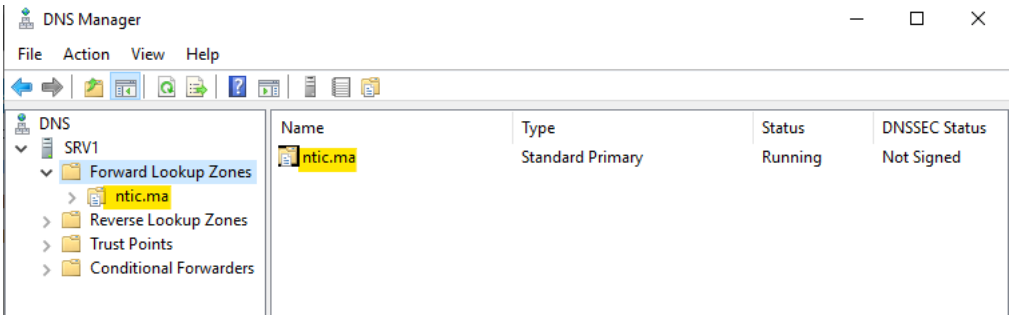


3 – Création d'enregistrements dans la zone directe d'une DNS primaire :

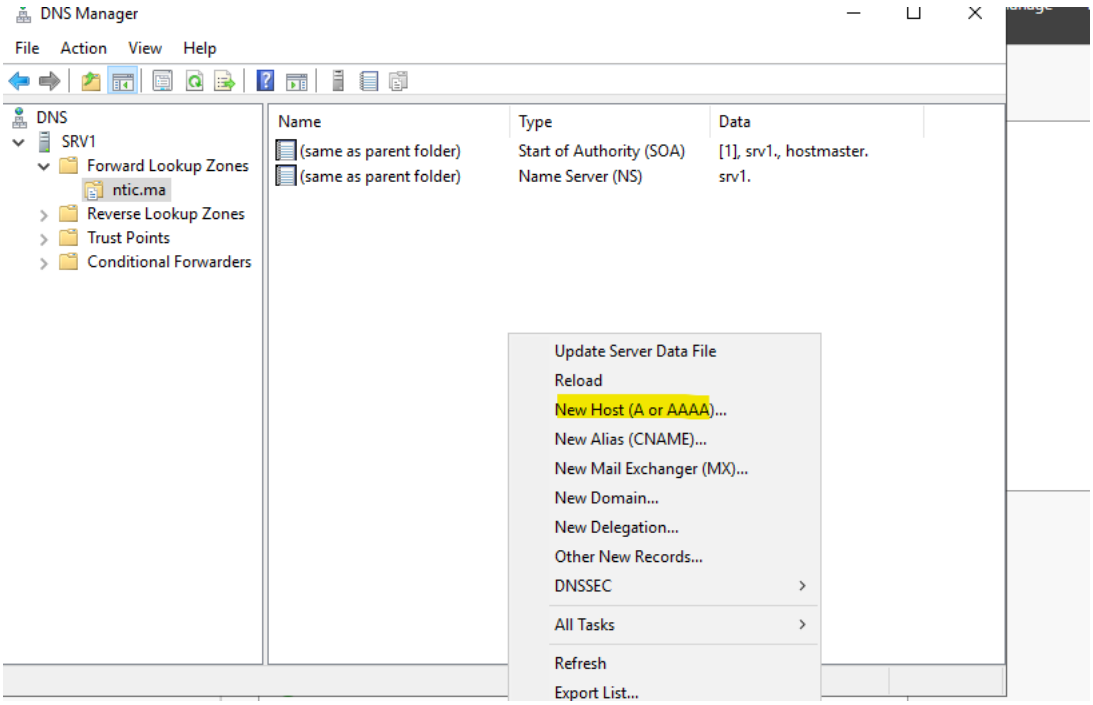
Qu'est-ce qu'un enregistrement DNS ?

Un enregistrement DNS lie un nom de domaine à une adresse IP ou à d'autres services, comme les enregistrements A, MX, et CNAME.

1 – Forward Lookup Zone > ntic.ma : Sélectionner la zone de recherche directe pour le domaine "ntic.ma" afin de gérer les enregistrements DNS associés.



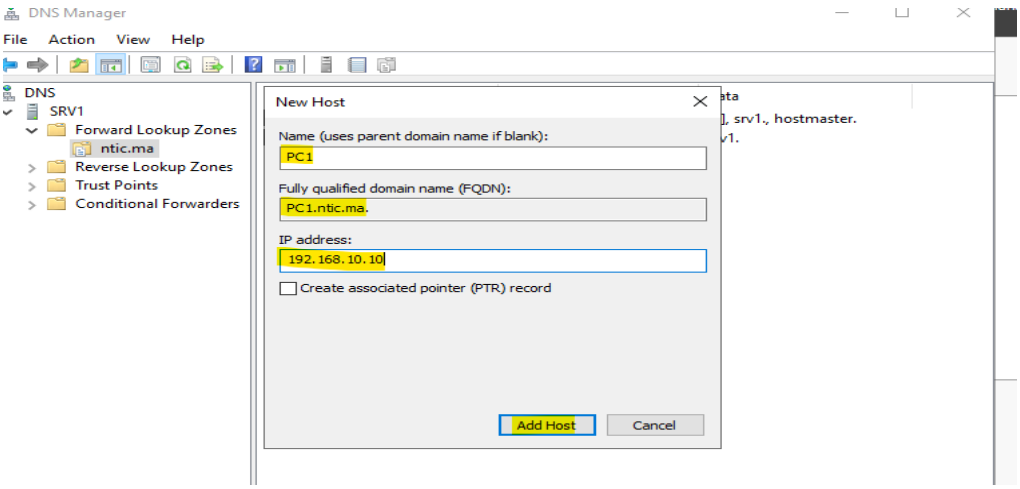
2 – Je choisis "**New Host**" : Ajouter un nouvel enregistrement d'hôte pour le domaine.



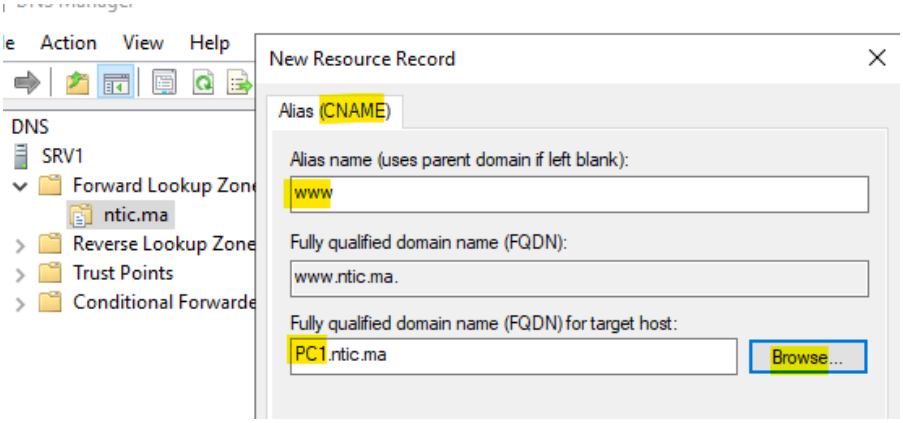
- **A** : Associe un nom de domaine à une adresse IPv4.
- **AAAA** : Associe un nom de domaine à une adresse IPv6.
- **CNAME** : Crée un alias pour un autre nom de domaine.

 MX : Définit les serveurs de messagerie pour un domaine.

3 – **Pc1 > pc1.ntic.ma > 192.168.10.10 > add host** : Cela signifie créer un enregistrement DNS pour l'hôte "**pc1**" avec le nom "**pc1.ntic.ma**" et l'adresse IP "**192.168.10.10**", puis cliquer sur "**Add Host**" pour ajouter l'enregistrement.



4 – Cela signifie créer un enregistrement **CNAME** pour l'alias "**www**" avec le nom "**www.ntic.ma**", redirigeant ce nom vers "**pc1.ntic.ma**". Ensuite, cliquez sur **"Browse"** pour vérifier ou sélectionner l'hôte de destination.

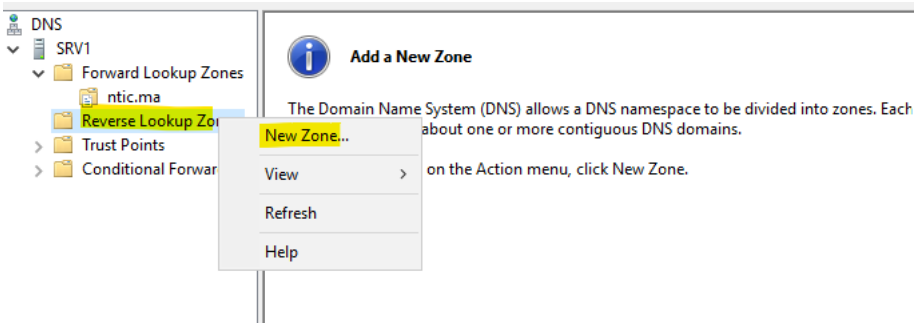


4 – Création d'une zone inversée DNS :

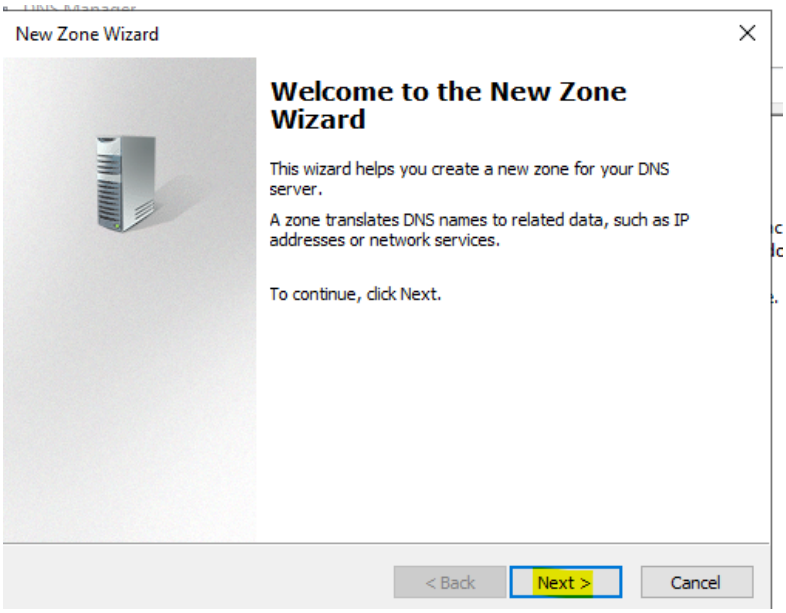
Qu'est-ce qu'une zone inversée DNS ?
Une **zone inversée DNS** est utilisée pour résoudre les adresses IP en noms de domaine. Elle permet de faire une recherche inverse à l'aide

des enregistrements **PTR** pour obtenir le nom de domaine associé à une adresse IP.

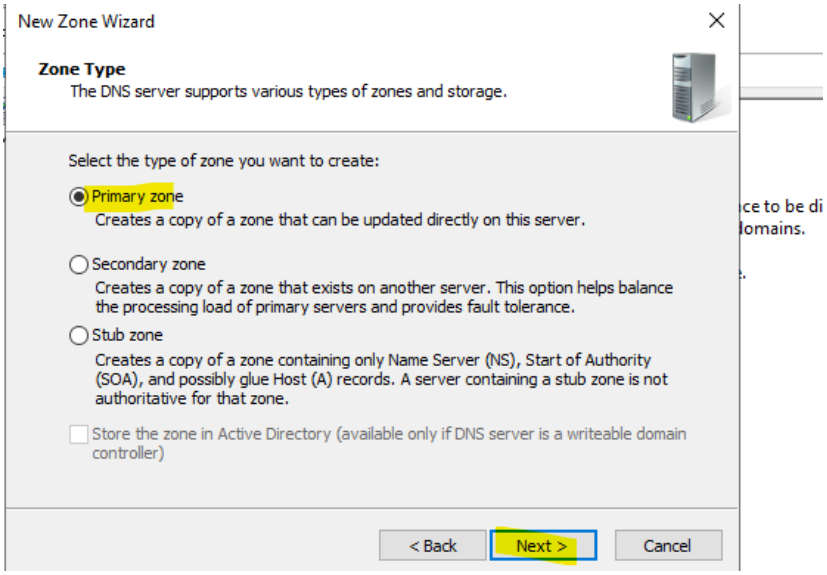
1 – Reverse Lookup Zone > New Zone : Créer une nouvelle zone de recherche inversée pour résoudre les adresses IP en noms de domaine.



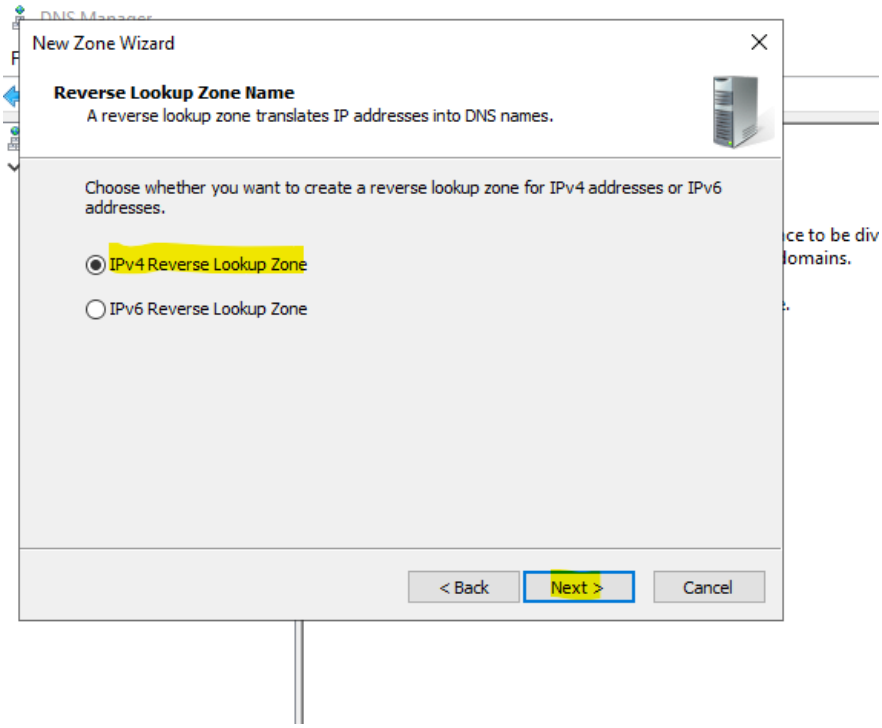
2 – Cliquer sur "**Next**" pour continuer la configuration de la zone de recherche inversée.



3 – Sélectionner "**Primary Zone**" pour créer une zone inversée primaire, puis cliquer sur "**Next**" pour continuer.

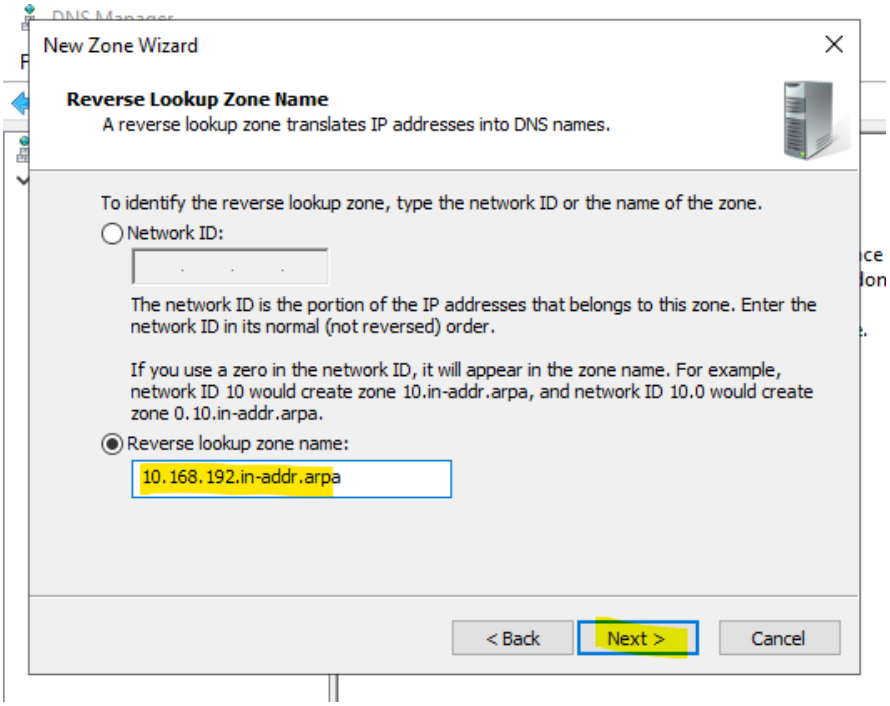


4 – Sélectionner "**IPv4 Reverse Lookup Zone**" pour créer une zone de recherche inversée pour les adresses IPv4, puis cliquer sur "**Next**" pour continuer.

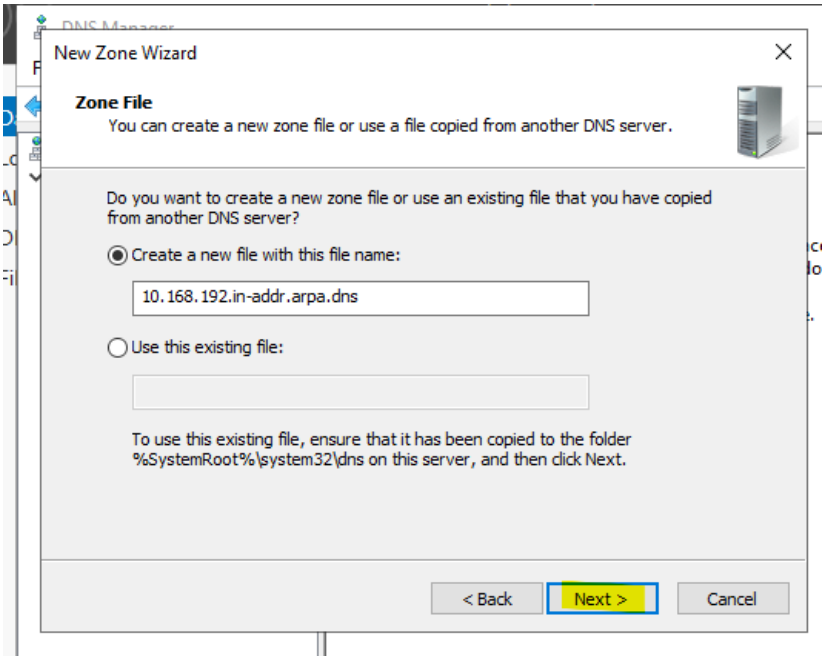


5 – Entrer "**10.168.192.in-addr.arpa**" comme nom de la zone inversée, puis cliquer sur "**Next**" pour continuer (**in-addr.arpa** est un domaine spécial dans DNS utilisé pour les recherches inversées d'adresses IP. Il permet de convertir une adresse IP, comme 192.168.10.1, en un format

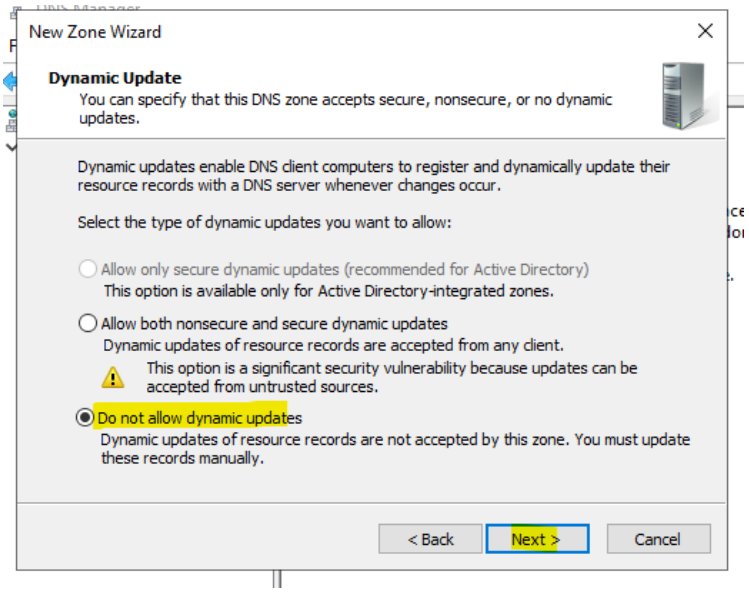
comme **1.10.168.192.in-addr.arpa** pour retrouver le nom de domaine associé)



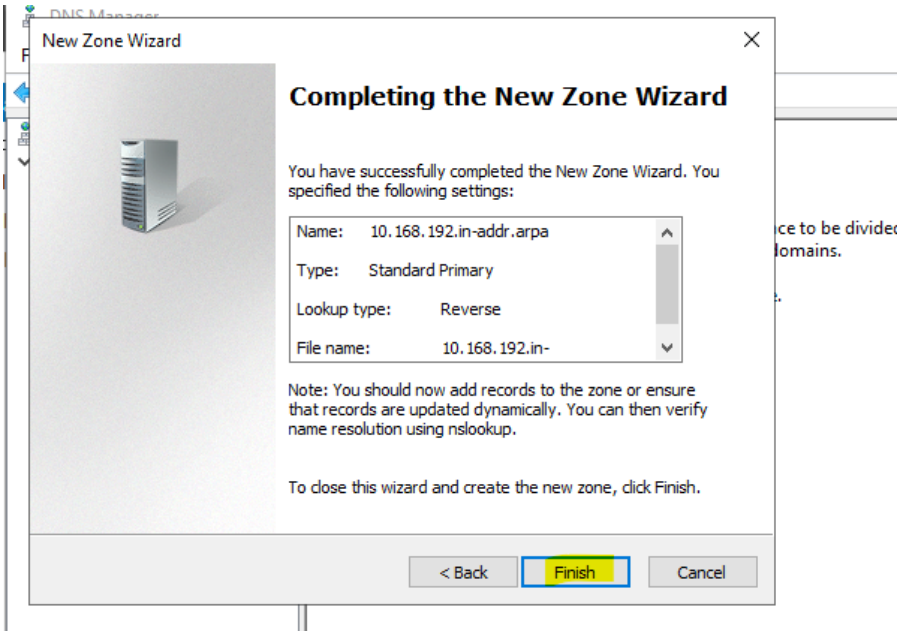
6 – Créer un nouveau fichier avec ce nom, puis cliquer sur "**Next**" pour continuer.



7 – Sélectionner l'option "**Do not allow dynamic updates**" pour empêcher les mises à jour dynamiques, puis cliquer sur "**Next**" pour continuer.

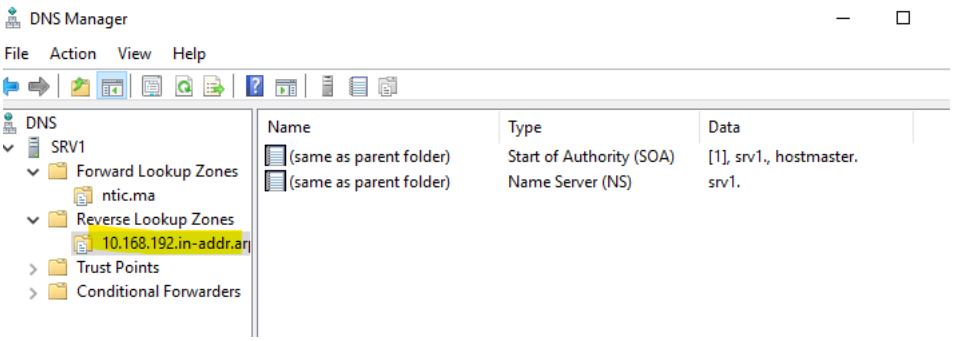


8 – Cliquer sur "**Finish**" pour terminer la création de la zone inversée DNS.

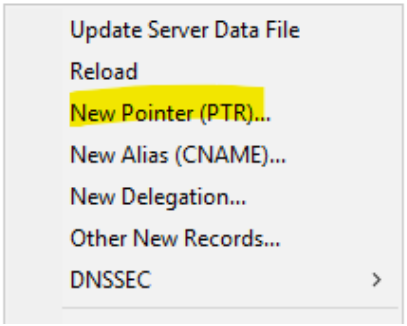


5 – Création d'enregistrements dans la zone inverse d'une DNS primaire :

1 – Reverse Lookup Zone > 10.168.192.in-addr.arpa : Sélectionner la zone de recherche inversée pour l'adresse IP dans le domaine **10.168.192.in-addr.arpa** afin de gérer les résolutions inversées des adresses IP associées.

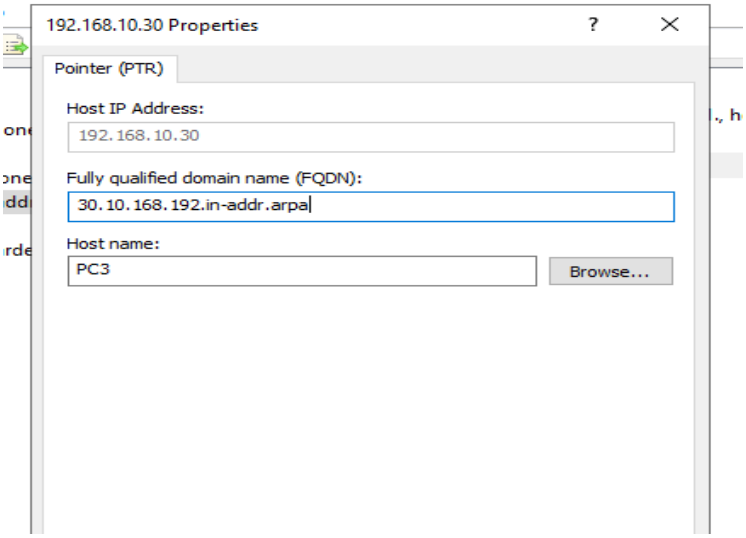


2 **– New PTR** : Créer un nouvel enregistrement **PTR** (Pointer Record) dans la zone inversée DNS. Un enregistrement **PTR** associe une adresse IP à un nom de domaine dans une recherche inversée. Cela permet de résoudre une adresse IP en son nom de domaine correspondant.

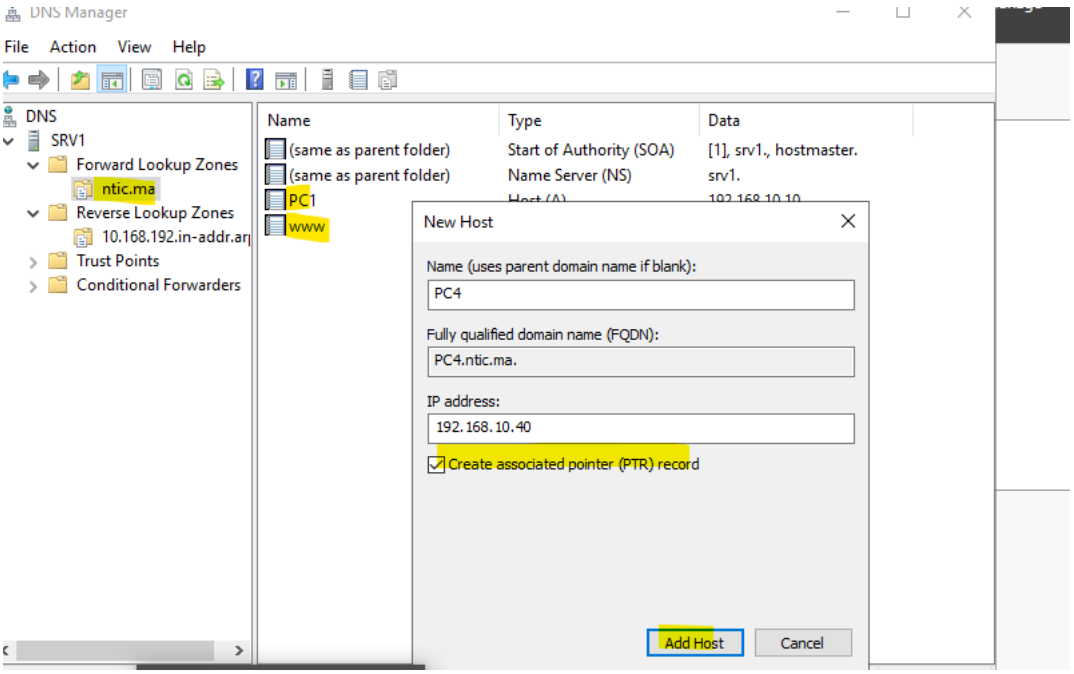


PTR : Enregistrement DNS utilisé pour résoudre une adresse IP en un nom de domaine. Il permet de lier une IP, comme **192.168.10.1**, à un nom de domaine, comme **pc1.ntic.ma**.

3 – Cela signifie créer un enregistrement **PTR** dans la zone inversée **30.10.168.192.in-addr.arpa**, associant l'adresse IP **192.168.10.30** au nom de domaine **pc3**.



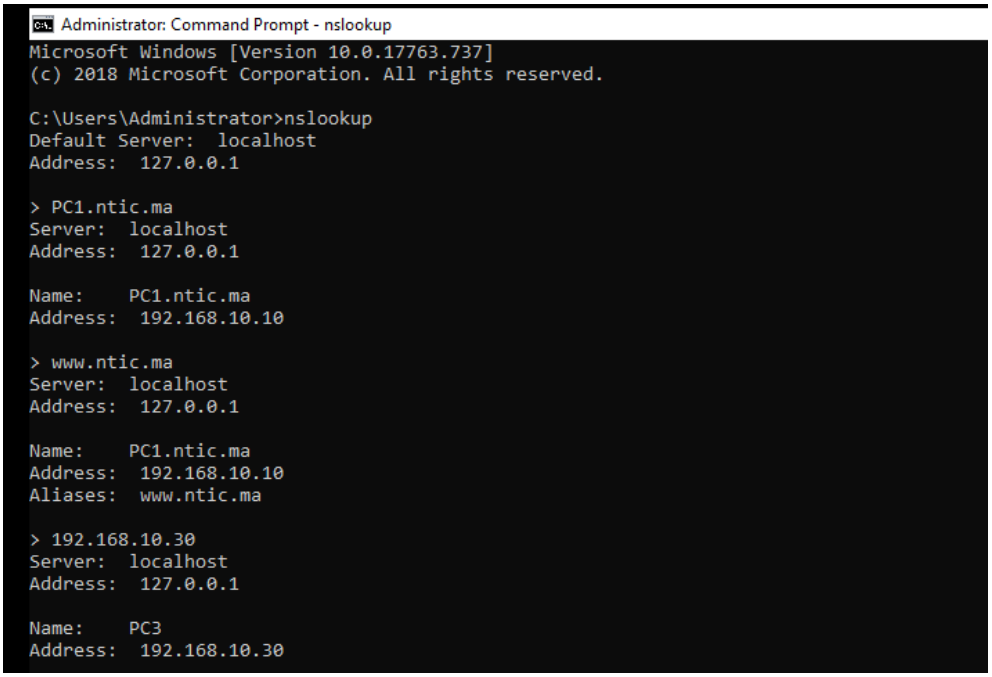
4 – Cela signifie créer un enregistrement d'hôte pour **pc4** dans le domaine **ntic.ma** avec l'adresse IP **192.168.10.40**, et créer également un enregistrement **PTR** associé pour effectuer une recherche inversée, puis cliquer sur "**Add Host**" pour ajouter l'enregistrement.



6 – Vérification du bon fonctionnement des zones DNS primaire directe et inversée :

nslookup est un outil en ligne de commande utilisé pour interroger les serveurs DNS et obtenir des informations sur les enregistrements DNS

d'un domaine. Il permet de vérifier la résolution des noms de domaine et de tester les zones DNS, qu'elles soient directes ou inversées.

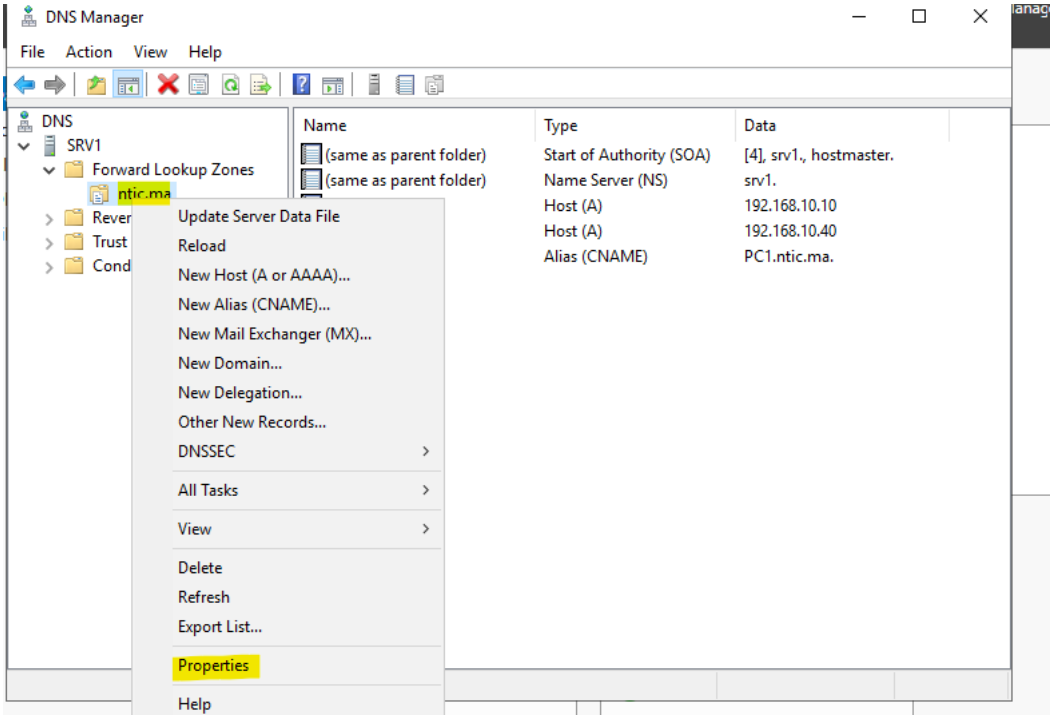


7 - Activation de la transmission sur SRV1 vers SRV2 :

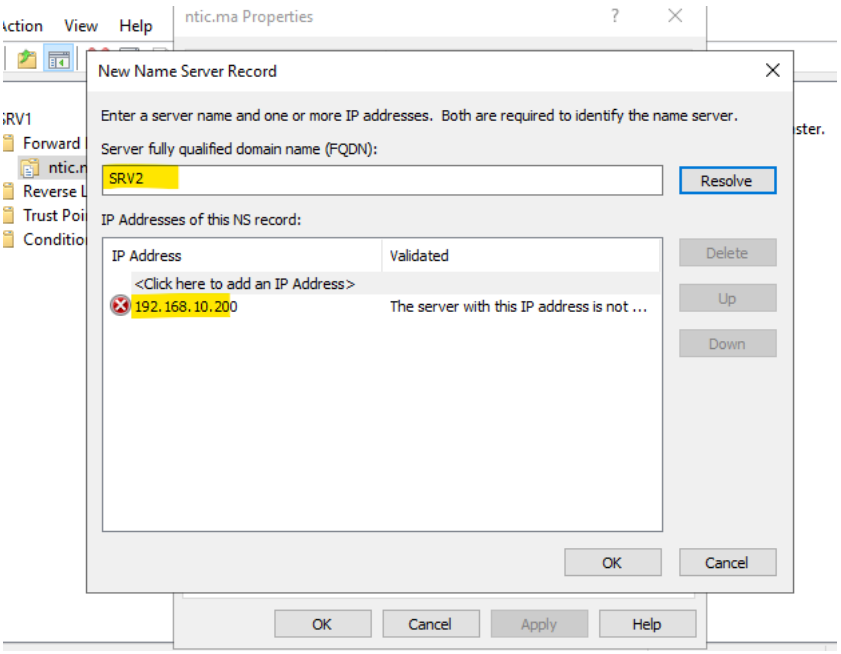
Comment la transmission dans DNS nous aide-t-elle ?

La **transmission** permet au serveur DNS secondaire de recevoir les mises à jour de la zone depuis le serveur DNS primaire, assurant ainsi la redondance et la disponibilité des données DNS.

1 – Lorsque vous accédez aux **Propriétés** de **ntic.ma** ou de **10.168.192.in-addr.arpa**, vous pouvez configurer la **transmission** des données DNS entre le serveur primaire et secondaire. Cela garantit que les informations de zone DNS sont correctement répliquées et mises à jour sur le serveur secondaire, assurant ainsi la disponibilité et la redondance des données en cas de besoin.



2 – Lorsque vous configurez le **Fully Qualified Domain Name (FQDN)** sur **SRV2**, cela permet de garantir que **SRV2** peut recevoir et transmettre les mises à jour DNS depuis **SRV1**, assurant ainsi la synchronisation correcte des zones entre les serveurs.

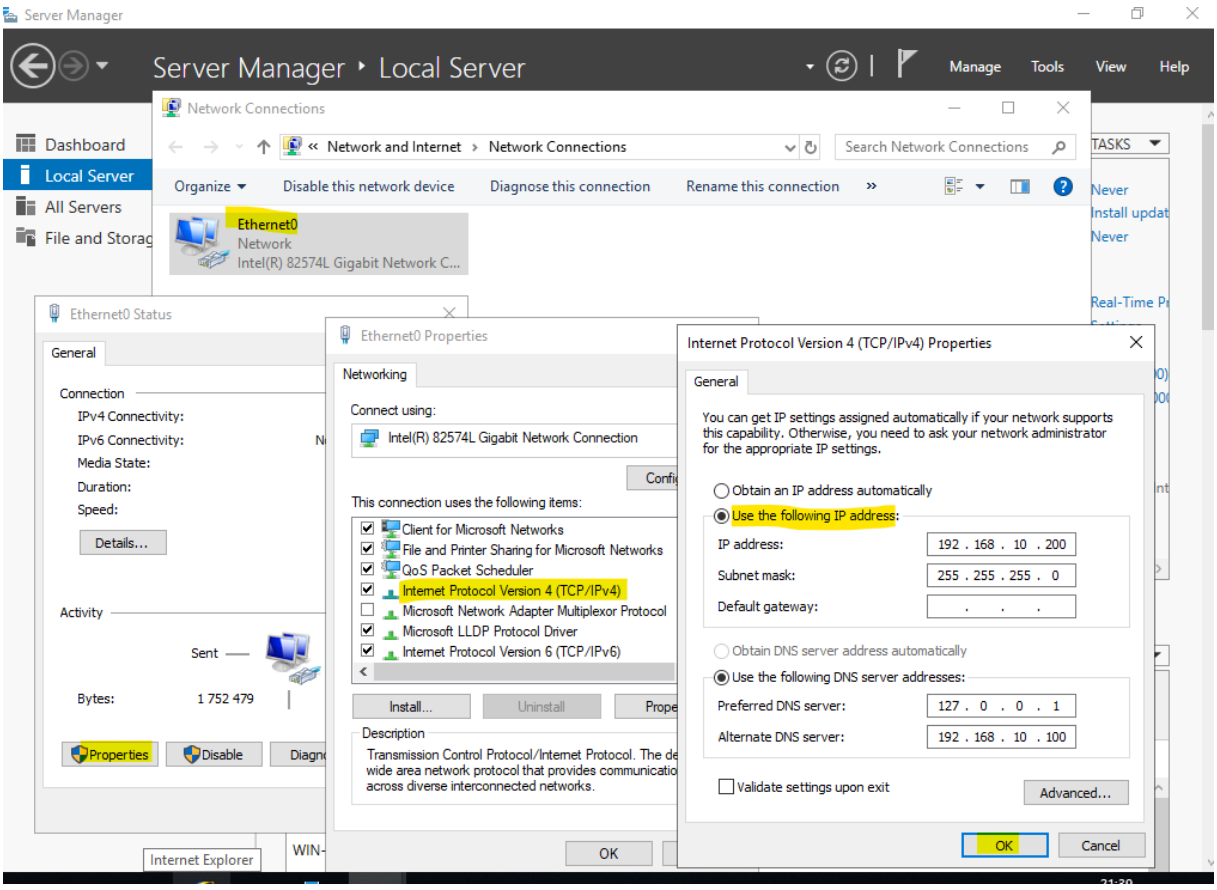


8 – Configuration d'un serveur DNS secondaire :

Qu'est-ce que le DNS secondaire ?

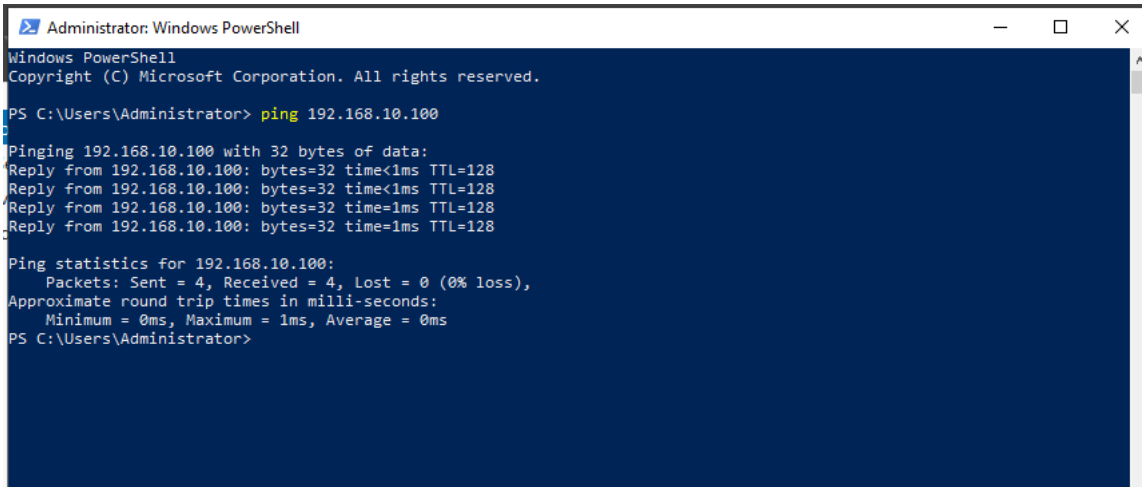
Le **DNS secondaire** est un serveur DNS qui contient une copie de la zone DNS gérée par le serveur principal. Il est utilisé pour assurer la redondance et la disponibilité en cas de défaillance du serveur principal. Lorsque le serveur principal ne peut pas répondre aux requêtes, le serveur secondaire fournit les réponses à partir de la copie de la zone.

1 – Pour configurer le **DNS secondaire** sur **SRV2**, il faut d'abord commencer par la **configuration réseau**. Cela inclut la définition des paramètres IP, la connexion du serveur au réseau, et l'assurance que les communications entre les serveurs DNS primaire et secondaire fonctionnent correctement.



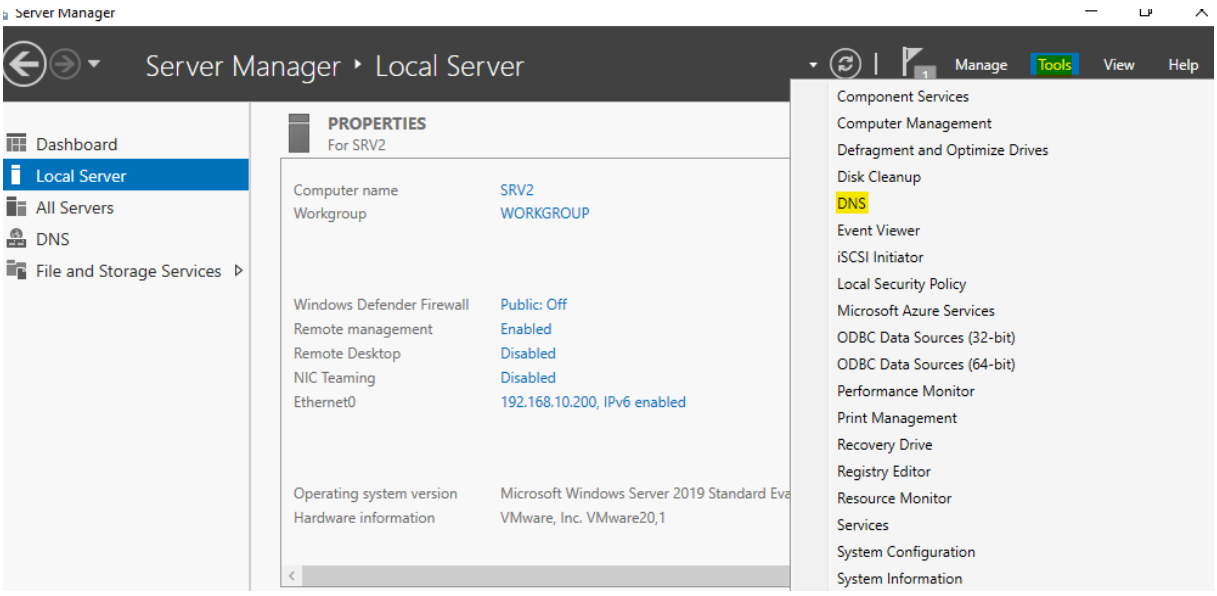
2 – Il faut vérifier la connexion entre **SRV1** (DNS primaire) et **SRV2** (DNS secondaire) en effectuant un test **ping**. Cela permet de s'assurer que les deux serveurs peuvent communiquer correctement sur le réseau. Si le

test de **ping** est réussi, cela signifie que la communication entre les deux serveurs DNS est établie.



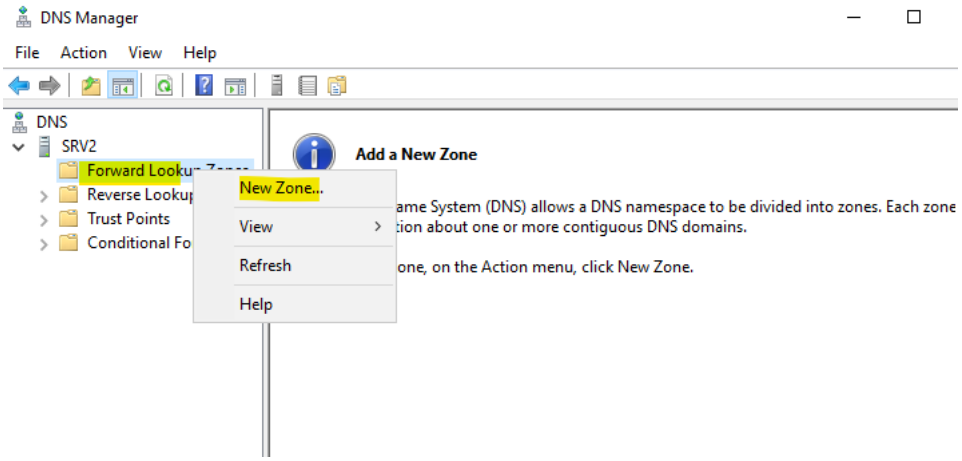
3 – Vous pouvez installer le **DNS** sur **SRV2** de la même manière que sur **SRV1**. Il suffit de suivre les mêmes étapes d'installation, en sélectionnant le rôle **DNS Server** et en configurant le serveur pour qu'il fonctionne en tant que **DNS secondaire** pour la zone correspondante.

4 – **Tools > DNS** : Permet d'accéder à l'outil de gestion DNS pour configurer et gérer les zones et enregistrements DNS.

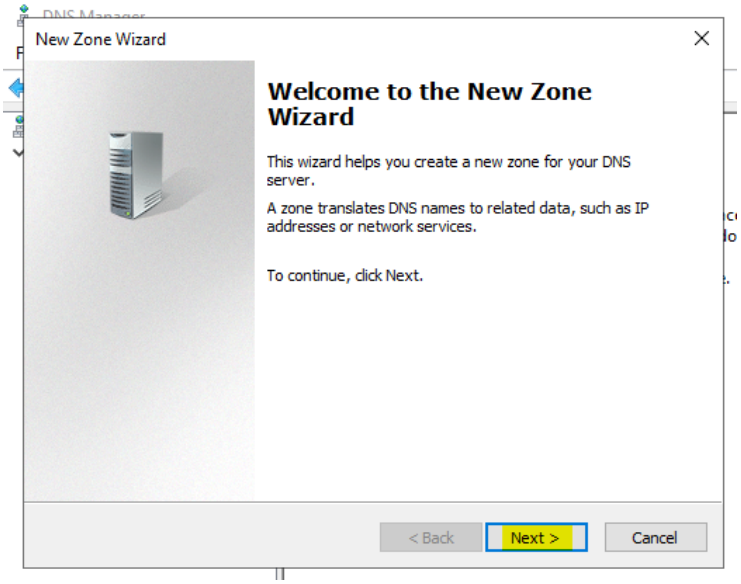


9 – **Création d'une zone directe DNS secondaire** :

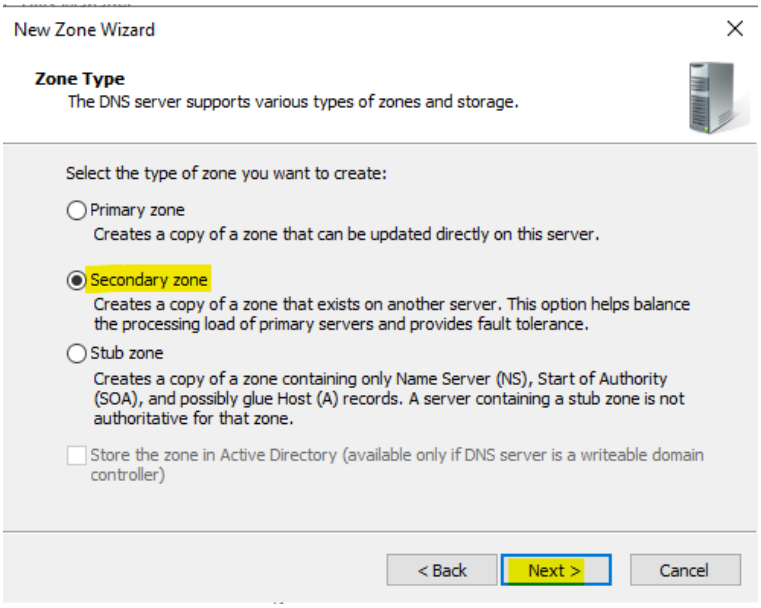
1 – **Forward Lookup Zone > New Zone** : Cela permet de créer une nouvelle zone de recherche directe dans le DNS, où les noms de domaine sont associés à leurs adresses IP correspondantes.



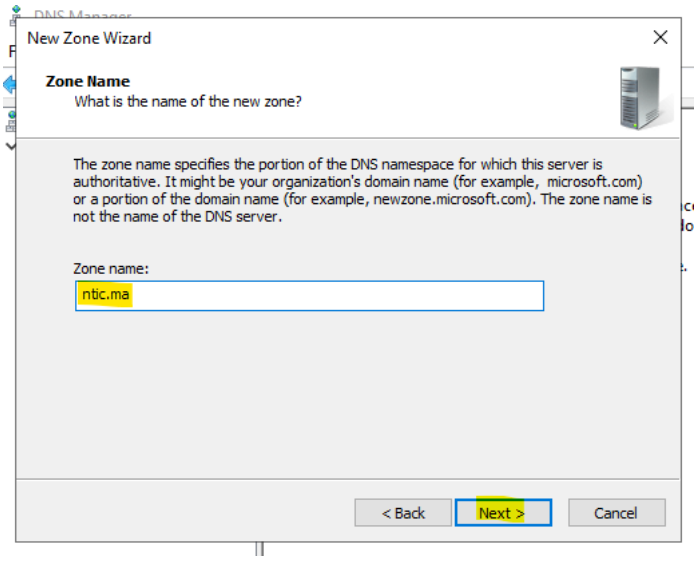
2 – Next : C'est l'option pour passer à l'étape suivante dans un processus de configuration ou d'installation.



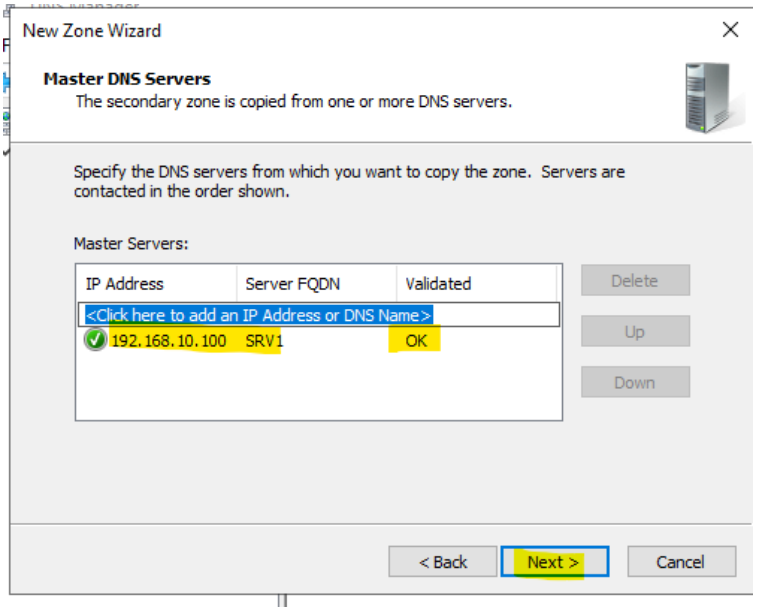
3 – Secondary Zone > Next : Cela vous permet de créer une **zone secondaire** dans le serveur DNS.



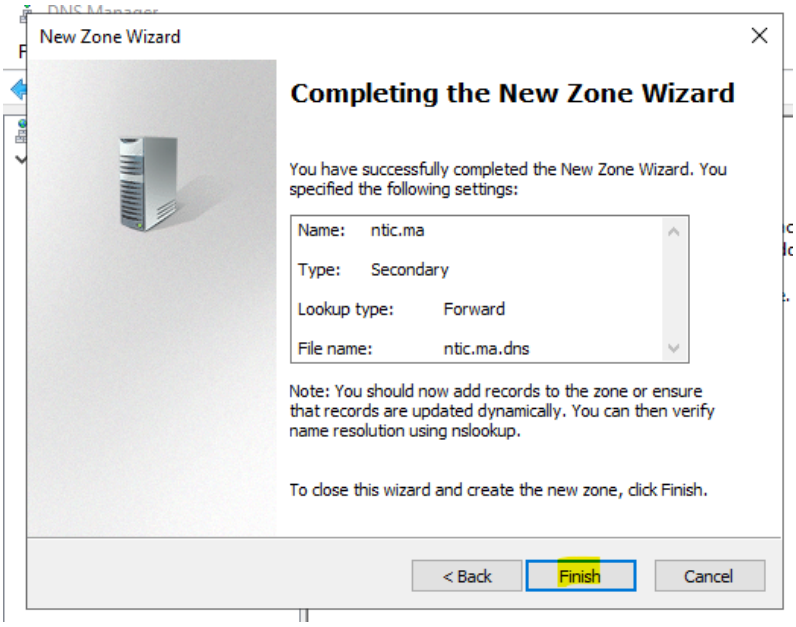
4 – Ntic.ma > Next : Le nom du domaine doit être le même que celui du domaine primaire.



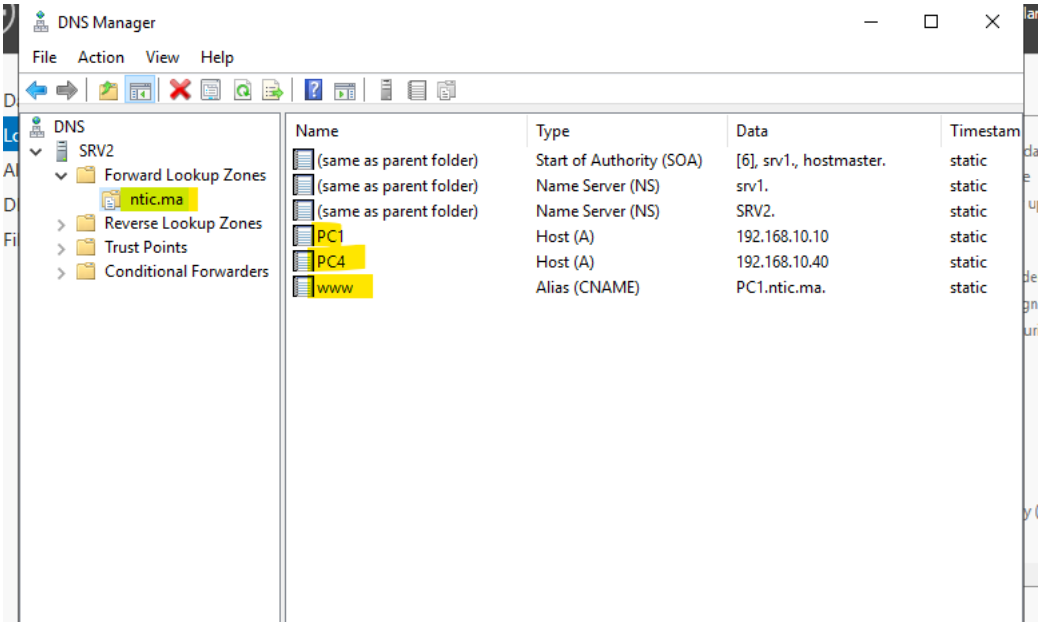
5 – Master server > 192.168.10.100 > Next : Ici, vous spécifiez le **serveur maître** en utilisant son adresse IP **192.168.10.100**. Cela indique que le serveur secondaire va récupérer les données du serveur principal lorsque nécessaire.



6 – Finish : Cela indique que vous avez terminé la configuration et que vous avez terminé le processus d'ajout de la zone secondaire dans le serveur DNS.

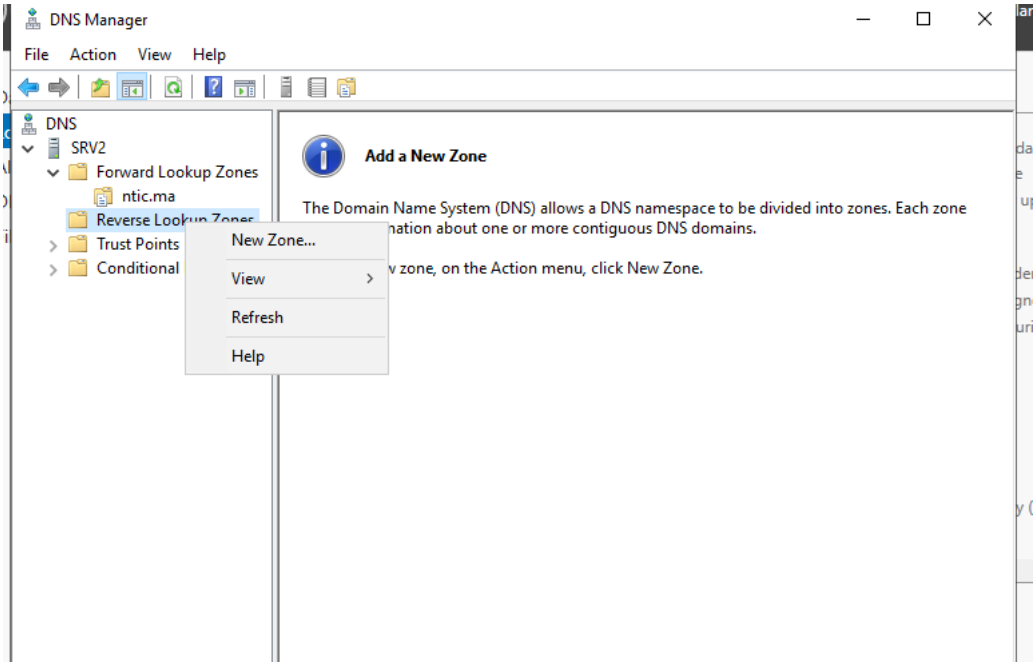


7 – Si tout est bien configuré, **SRV2** doit récupérer les enregistrements de **SRV1** et les synchroniser automatiquement.



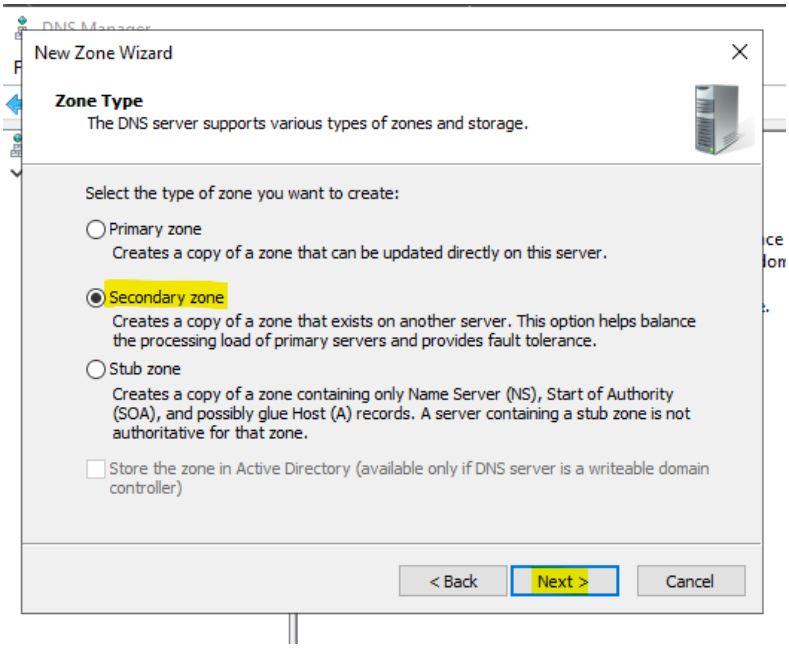
10 – Création d'une zone inversée DNS secondaire :

1 – Reverse lookup zone > New zone : Cette étape permet de créer une nouvelle zone de recherche inversée dans le serveur DNS, utilisée pour résoudre les adresses IP en noms de domaine.

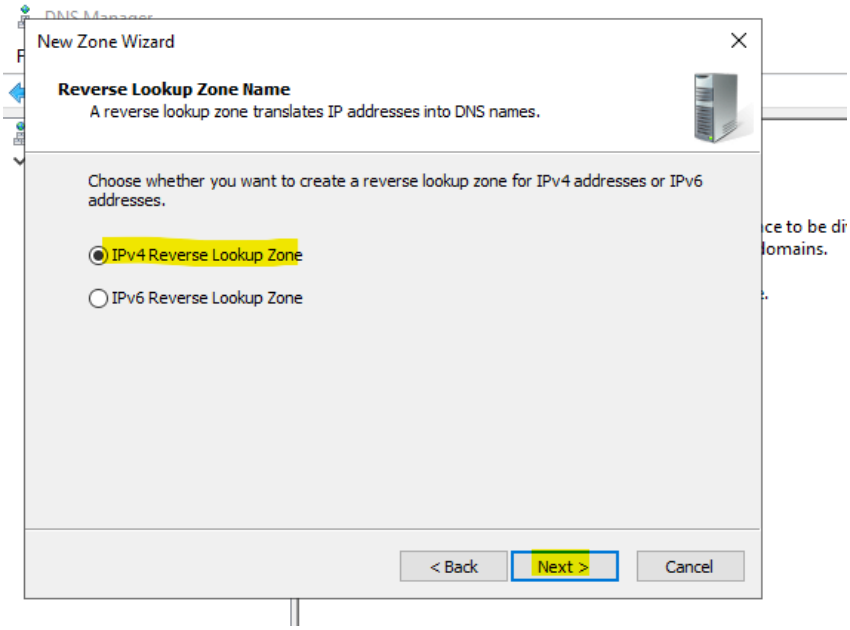


2 – Secondary Zone > Next : Cette étape permet de créer une **zone secondaire inversée**. Le serveur secondaire va récupérer les

enregistrements inversés de la zone primaire pour assurer la redondance et la disponibilité des informations.

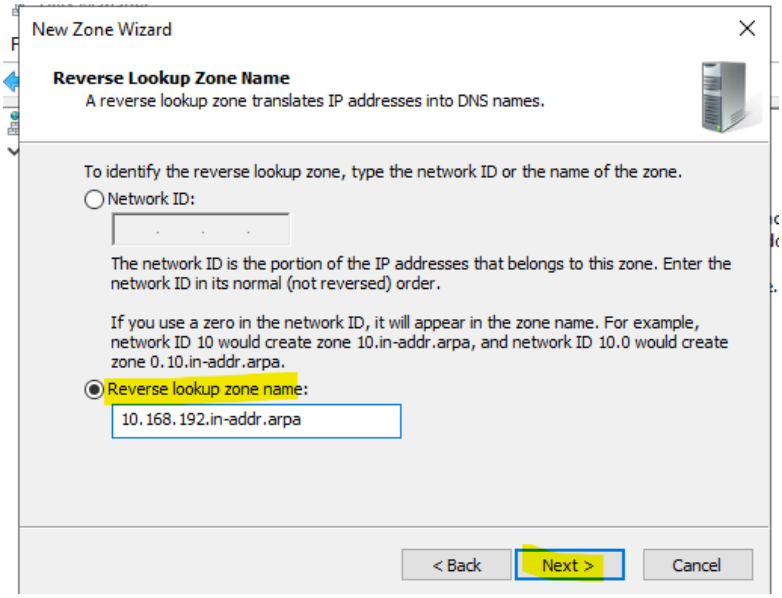


3 – IPv4 Reverse Lookup Zone : Zone DNS qui permet de résoudre les adresses IPv4 en noms de domaine.

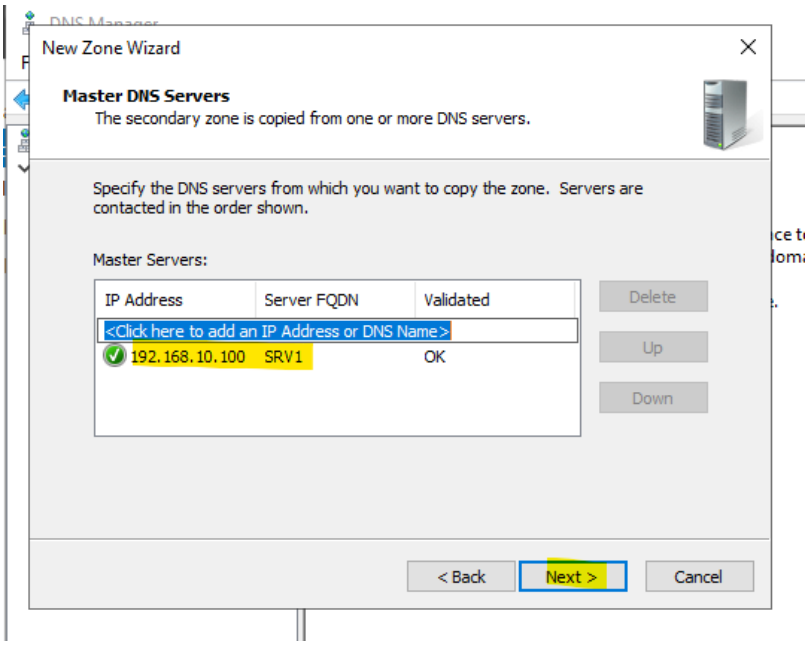


4 – Reverse Lookup Zone Name > 10.168.192.in-addr.arpa > Next : Cette étape permet de définir le nom de la zone de recherche inversée

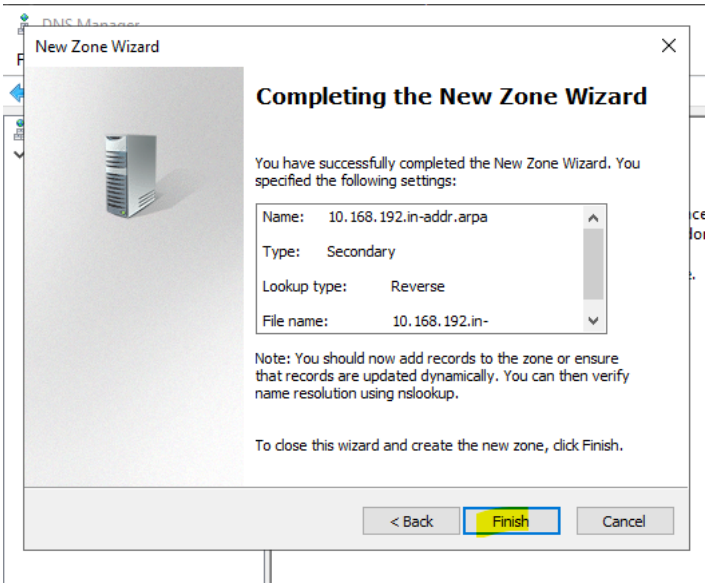
pour l'adresse IP **10.168.192.x**, afin de pouvoir résoudre les adresses IP en noms de domaine.



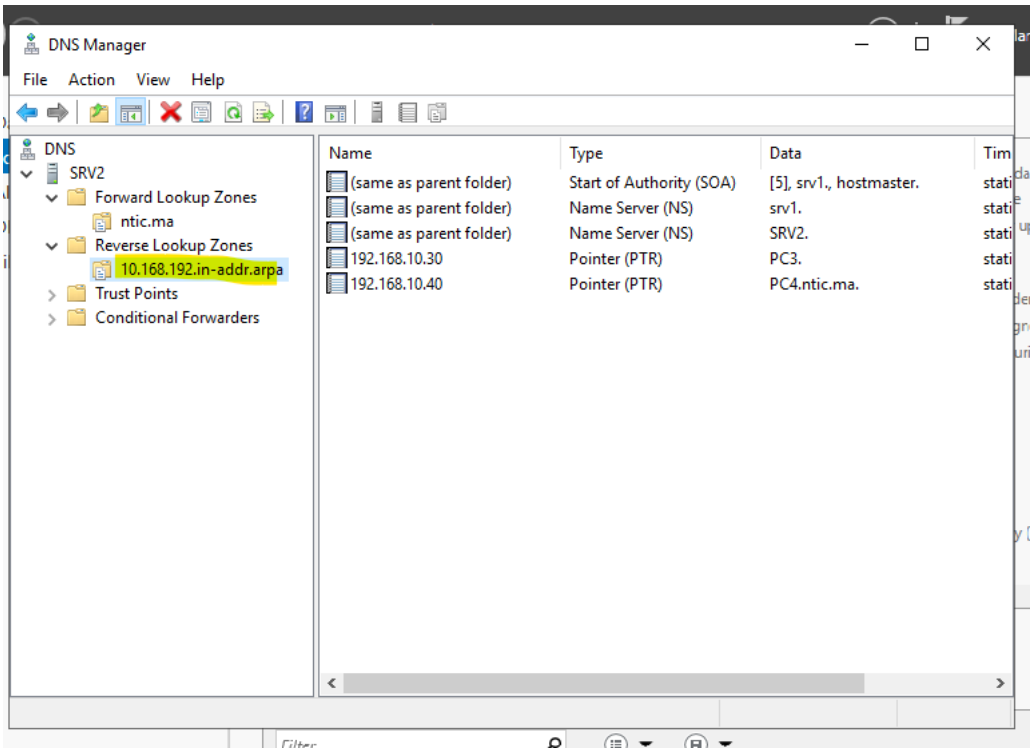
5 – Master Server > 192.168.10.100 > Next : Spécifie l'adresse IP du serveur principal pour la zone inversée, permettant au serveur secondaire de récupérer les données.



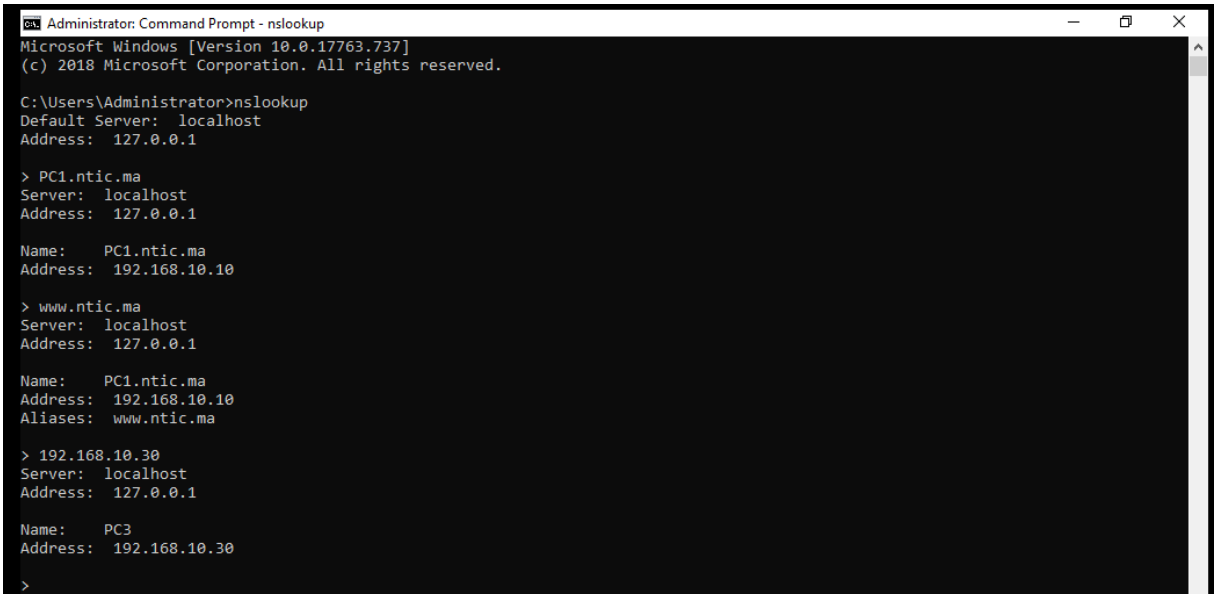
6 – Finish : Terminer la configuration de la zone inversée DNS secondaire.



7 – Si tout est configuré correctement, le serveur secondaire va récupérer les enregistrements de **SRV1** automatiquement.



8 – Vérification DNS : Utilisez la commande **nslookup** pour vérifier si le serveur secondaire récupère les enregistrements du serveur primaire. Si tout est correct, les résultats doivent être identiques.



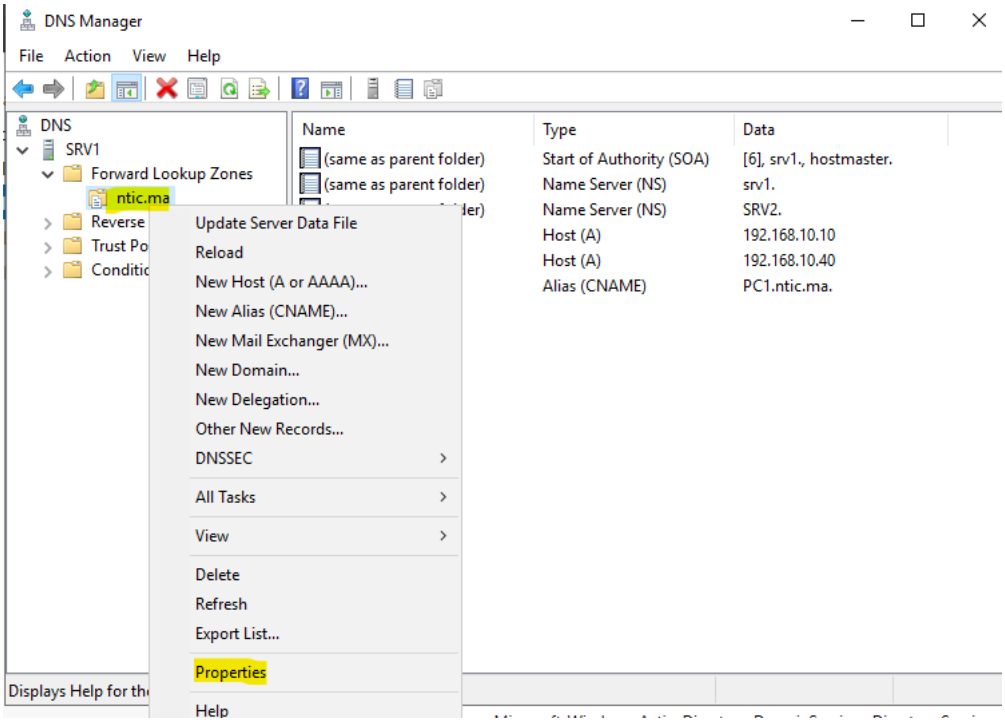
11 – Intégration du DNS dans Active Directory :

Quelle est l'importance de l'intégration du DNS dans Active Directory ?

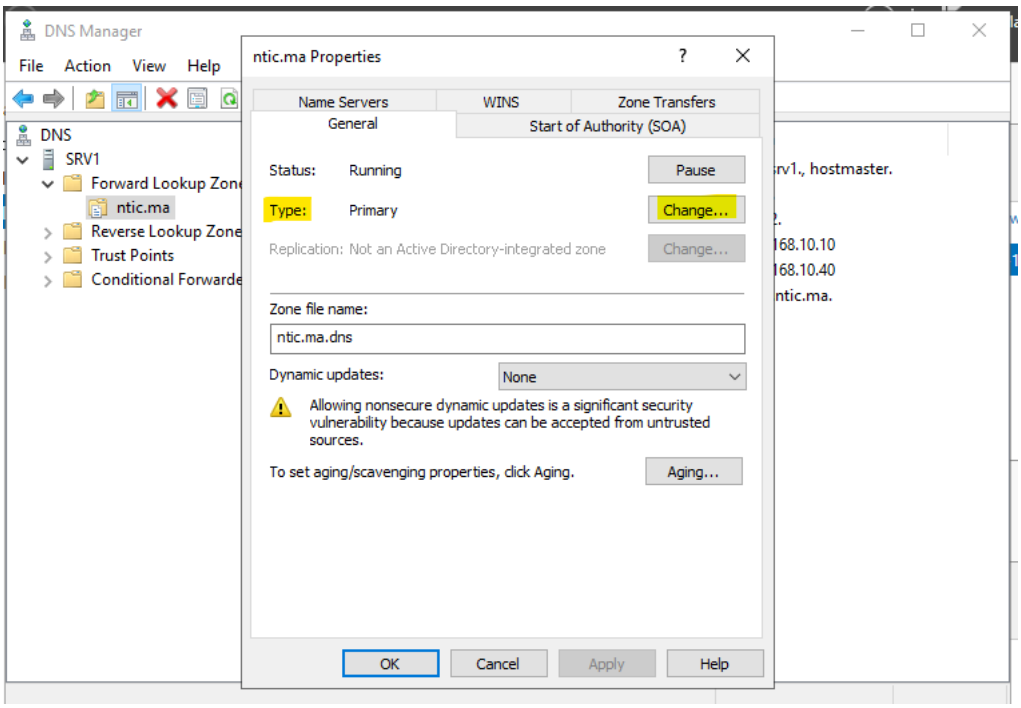
L'intégration du DNS dans Active Directory permet une résolution rapide et fiable des noms de domaine pour les services AD, assurant ainsi le bon fonctionnement de l'authentification, de la réplication et de la gestion des ressources dans le réseau. Elle facilite également la gestion centralisée et améliore la sécurité et la disponibilité des services.

1 – **Premièrement, il faut s'assurer que le rôle AD DS (Active Directory Domain Services) est bien installé sur votre serveur Windows.**

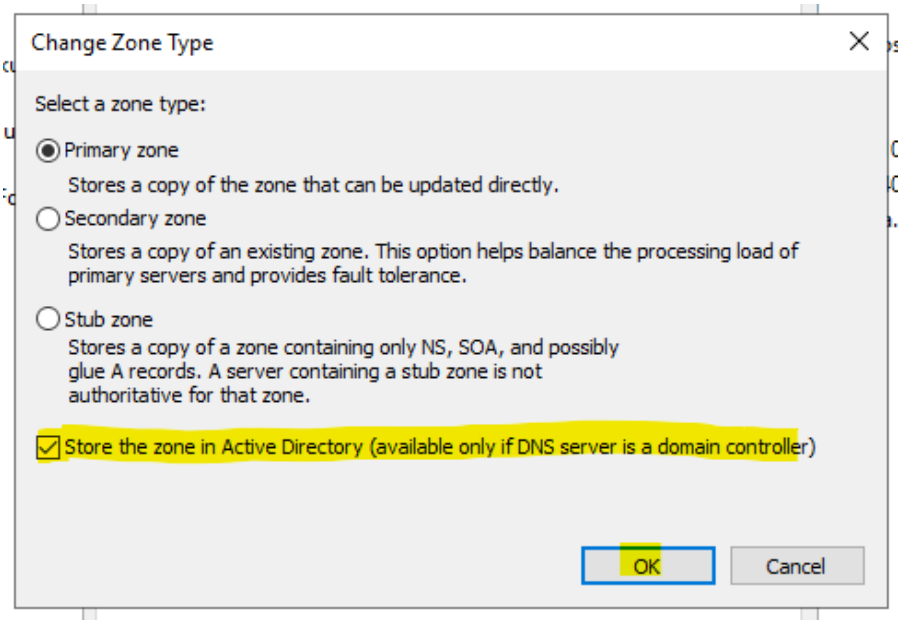
2 – Zone > Properties : Lors de l'intégration du DNS dans Active Directory, cette option permet de configurer les paramètres nécessaires pour l'intégration, tels que la réplication de la zone DNS avec Active Directory et la gestion des mises à jour dynamiques sécurisées.



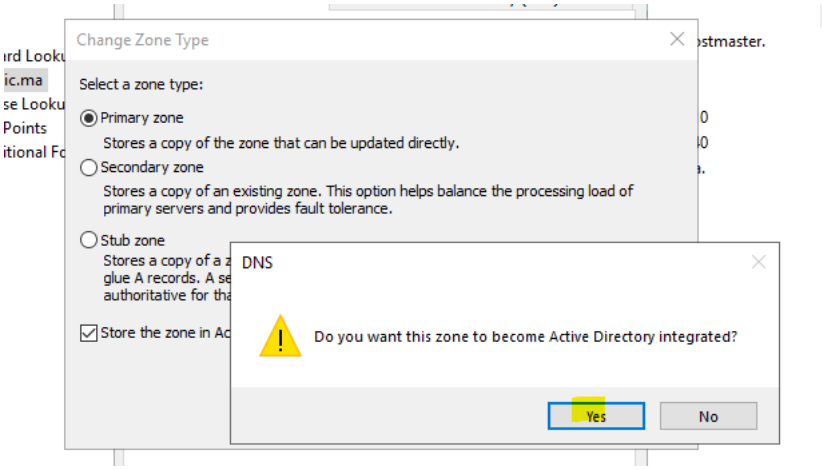
3 – Type > Change : Cette option permet de modifier le type de la zone DNS, par exemple, passer d'une zone normale à une zone Active Directory intégrée .



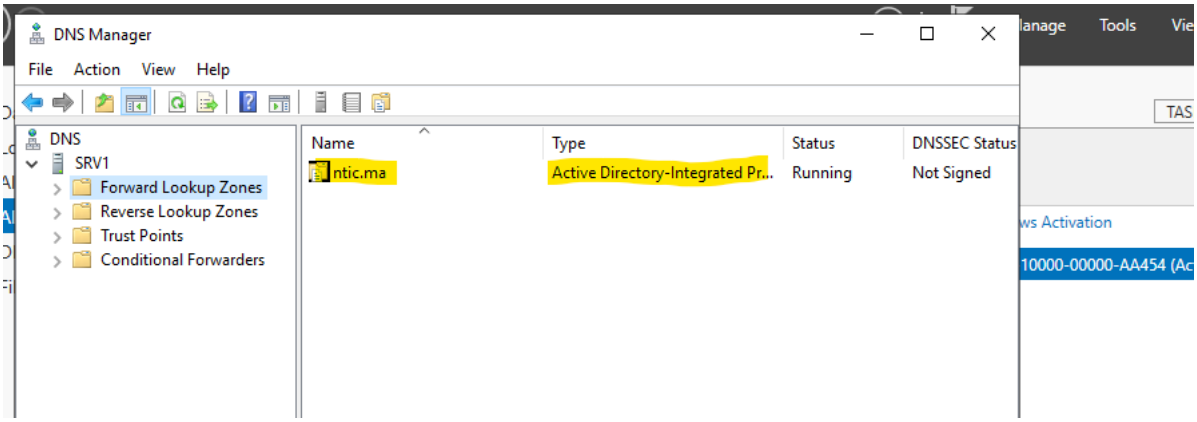
4 – Store the zone in Active Directory > OK : Cette option permet de stocker la zone DNS dans Active Directory .



5 – Do you want this zone to become AD integration > Yes : En sélectionnant cette option, vous intégrez la zone DNS à Active Directory



6 – Ntic.ma > Active Directory-Integrated : Cela signifie que la zone DNS "ntic.ma" est désormais intégrée à Active Directory, ce qui permet une réplication sécurisée et automatique de la zone DNS entre les contrôleurs de domaine dans le réseau, assurant une gestion centralisée et une plus grande sécurité des informations DNS.


DNS Manager
File Action View Help
DNS
SRV1
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
Status
DNSSEC Status
ntic.ma
Active Directory-Integrated Pr...
Running
Not Signed
Tools
TAS
ws Activation
10000-00000-AA454 (Ac