

Tuto DNS Windows server

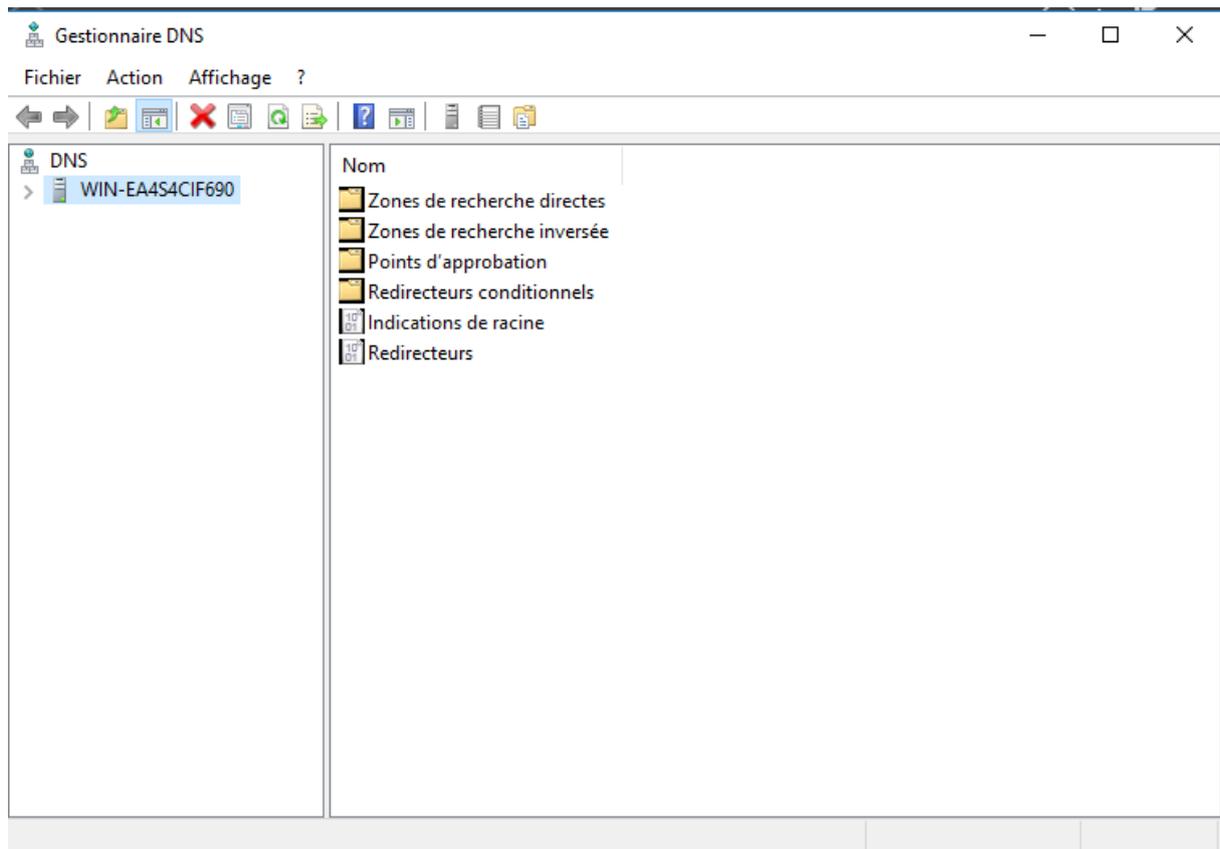
Le protocole DNS (Domain Name System) permet de résoudre des noms de domaines en adresse IPv4 et IPv6.

L'installation d'un serveur DNS local est obligatoire pour utiliser les services Active Directory, mais peut aussi être utile dans d'autres cas. Et notamment pour indiquer quelle machine agit en tant que serveur d'e-mails dans votre réseau.

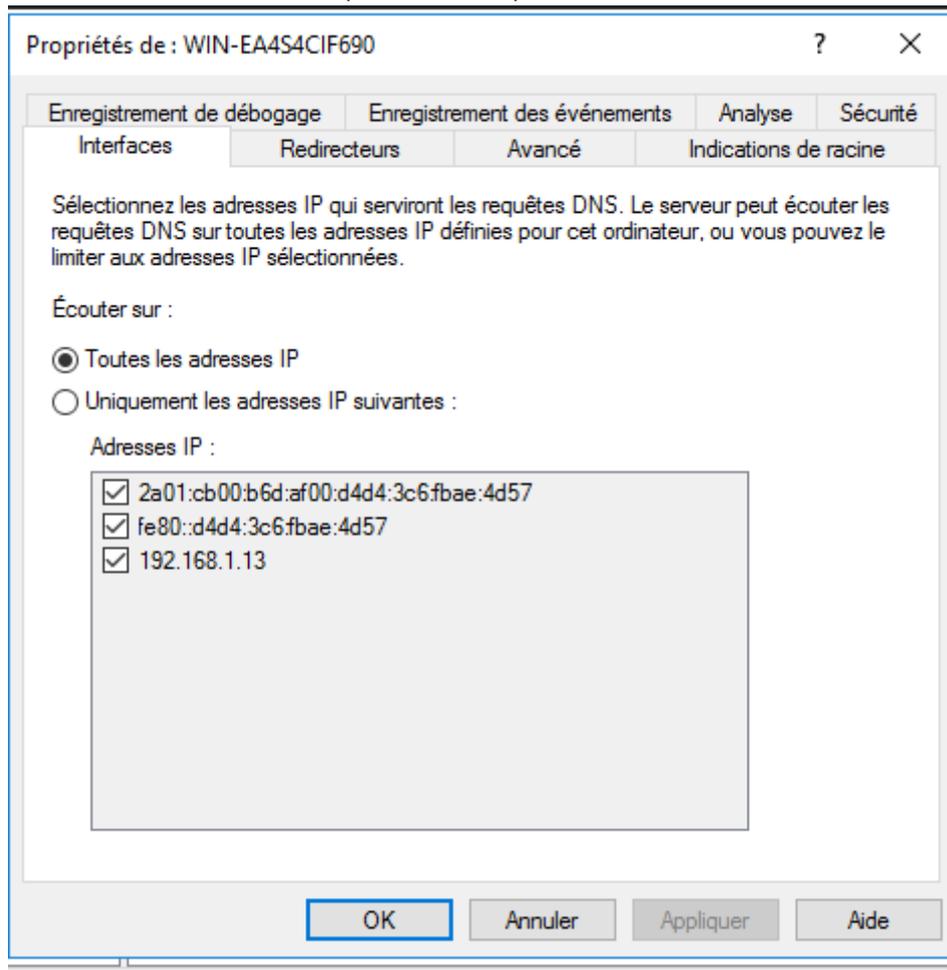
Dans ce tutoriel, nous allons vous montrer comment configurer un serveur DNS sous Windows Server, mais aussi vous expliquer les différents types d'enregistrements DNS et les différentes options disponibles sous Windows Server.

L'ajout des services AD DS a entraîné l'installation automatique d'un serveur DNS. Or, ce serveur DNS n'est pas pleinement fonctionnel. Il faut paramétrer le serveur DNS. Les redirecteurs permettent de transférer des requêtes DNS pour des noms DNS externes vers des serveurs DNS situés à l'extérieur du réseau de l'entreprise.

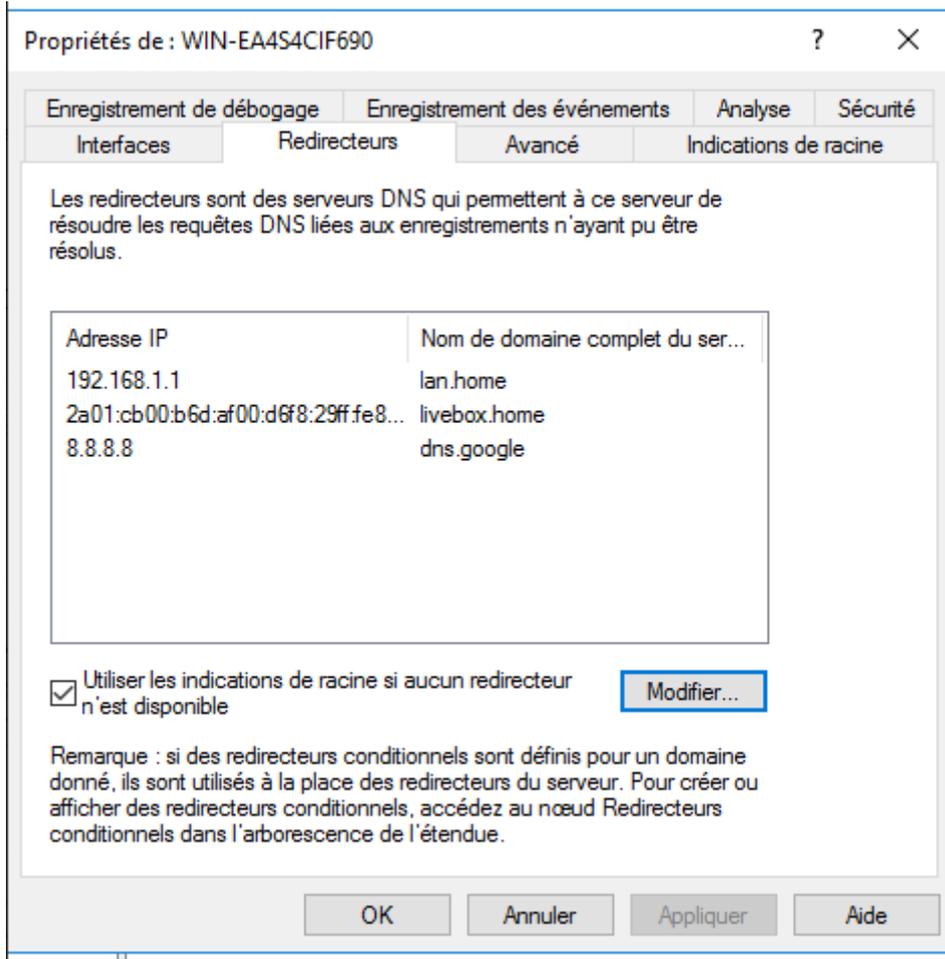
Gestionnaire de serveur / Outils / DNS



Sélectionnez le serveur / clique droit / Propriétés / Interfaces.



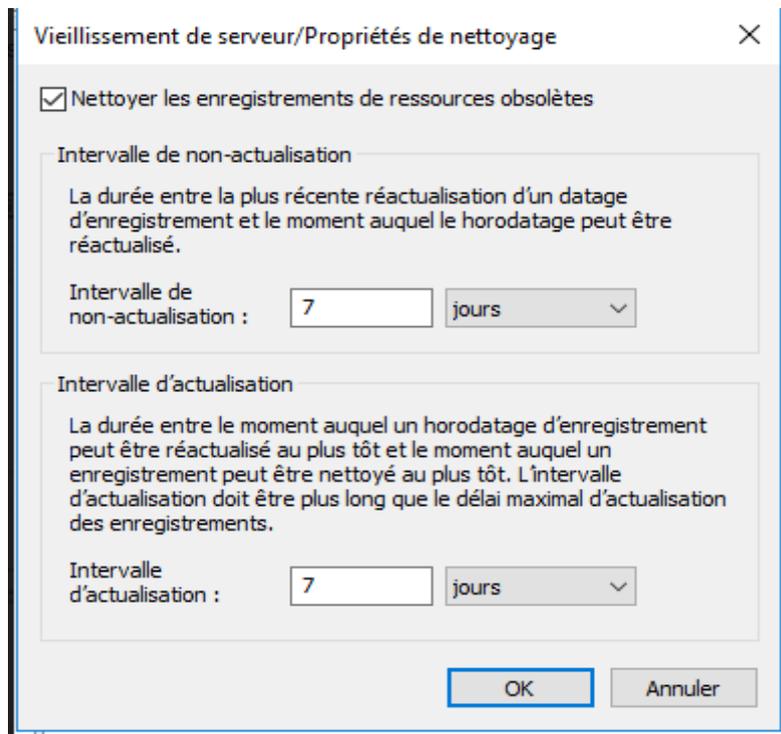
Sélectionner Redirecteur. Vérifiez la présence des DNS de votre FAI. Ajoutez-les si nécessaires. Ajouter le DNS Google. Validez vos choix ;cliquez sur le bouton « ok ».



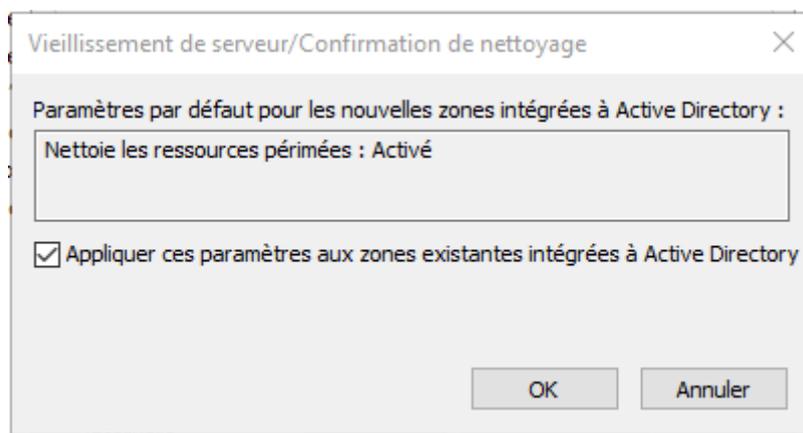
Le vieillissement et le nettoyage permettent de supprimer automatiquement des ressources stockés dans une zone DNS en tenant compte d'une période définie par l'administrateur.

Sélectionnez le serveur/clique droit/ Définir le vieillissement/nettoyage pour toutes les zones

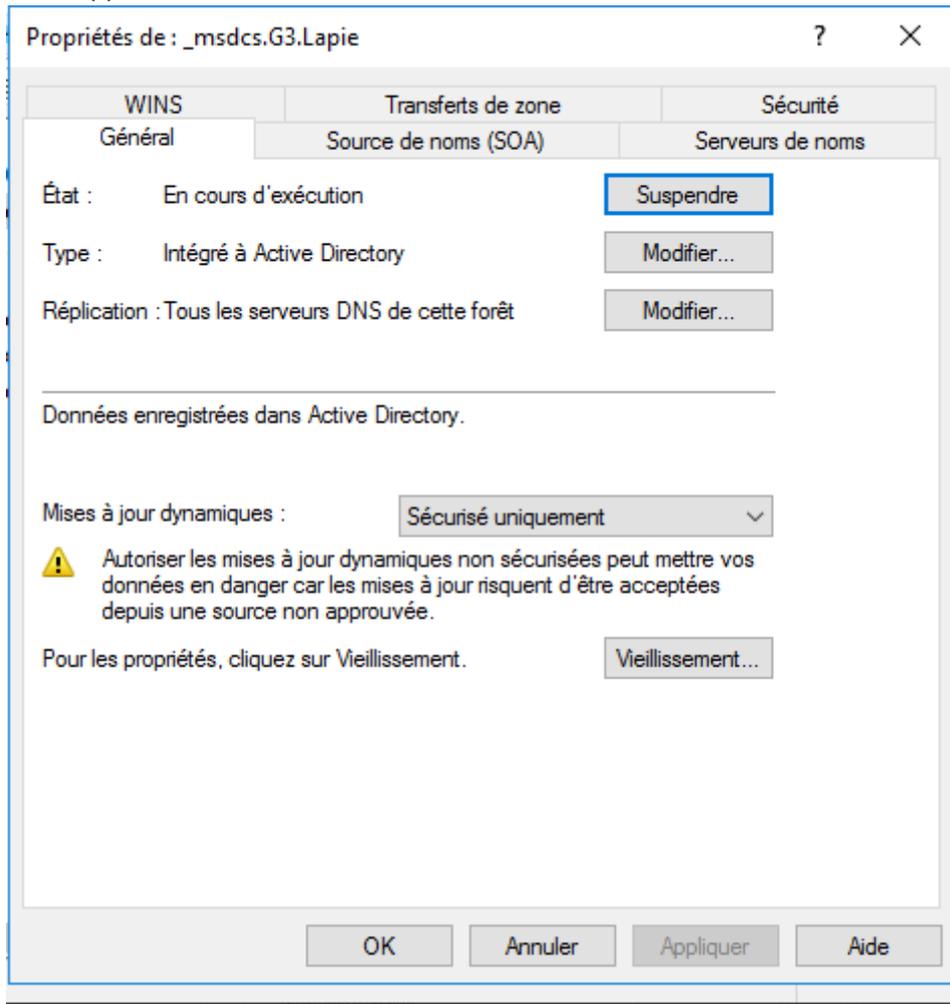
Cochez l'option : Nettoyer les enregistrements de ressources obsolètes. Laissez les valeurs proposées par défaut. Cliquez sur « OK ».



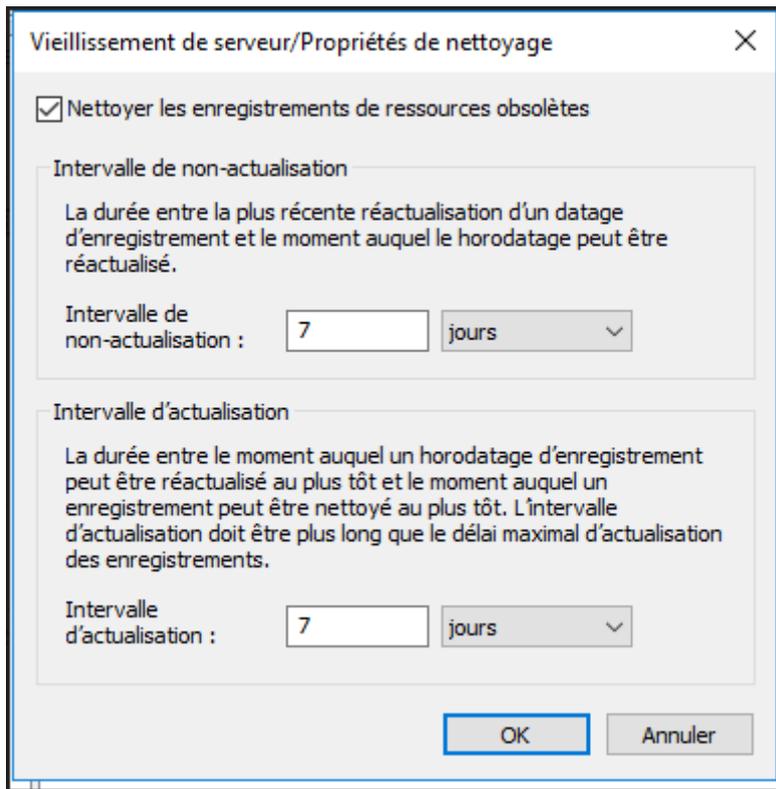
Cochez l'option Appliquez ces paramètres aux zones existantes intégrées à Active Directory. Cliquez sur OK.



Développez les « Zones de recherches directes ».



Cliquez sur le bouton « Vieillessement... ». Vérifiez que l'option « Nettoyer les enregistrements de ressources obsolètes » est bien cochée. Validez l'ensemble.



Vieillessement de serveur/Propriétés de nettoyage

Nettoyer les enregistrements de ressources obsolètes

Intervalle de non-actualisation
La durée entre la plus récente réactualisation d'un datage d'enregistrement et le moment auquel le horodatage peut être réactualisé.

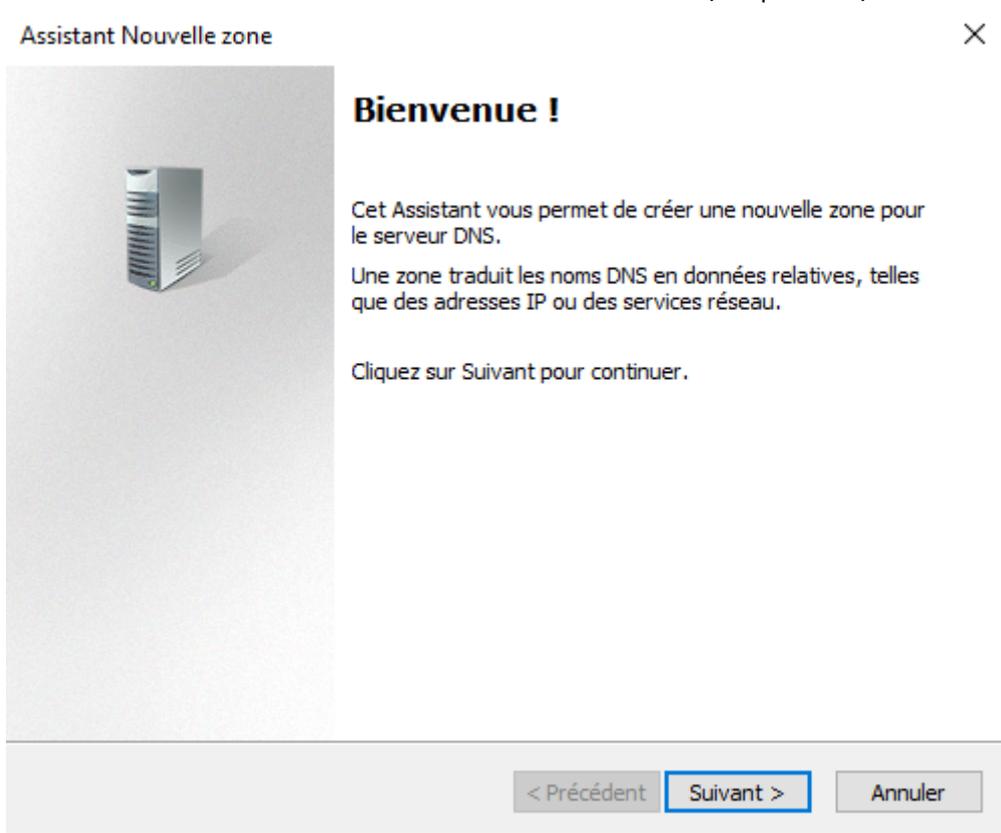
Intervalle de non-actualisation : jours

Intervalle d'actualisation
La durée entre le moment auquel un horodatage d'enregistrement peut être réactualisé au plus tôt et le moment auquel un enregistrement peut être nettoyé au plus tôt. L'intervalle d'actualisation doit être plus long que le délai maximal d'actualisation des enregistrements.

Intervalle d'actualisation : jours

OK Annuler

La zone de recherche inversée n'a pas été déclarée par l'assistant AD DS . Vous devez le faire manuellement. Sélectionner : Zone de recherche inversées/Clique droit/Nouvelle Zone



Assistant Nouvelle zone

Bienvenue !

Cet Assistant vous permet de créer une nouvelle zone pour le serveur DNS.

Une zone traduit les noms DNS en données relatives, telles que des adresses IP ou des services réseau.

Cliquez sur Suivant pour continuer.

< Précédent **Suivant >** Annuler

Cliquez sur suivant. Cochez les options « Zone principale » et « Enregistrer la zone dans Active Directory ». Cliquez sur « Suivant »

Assistant Nouvelle zone

Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.

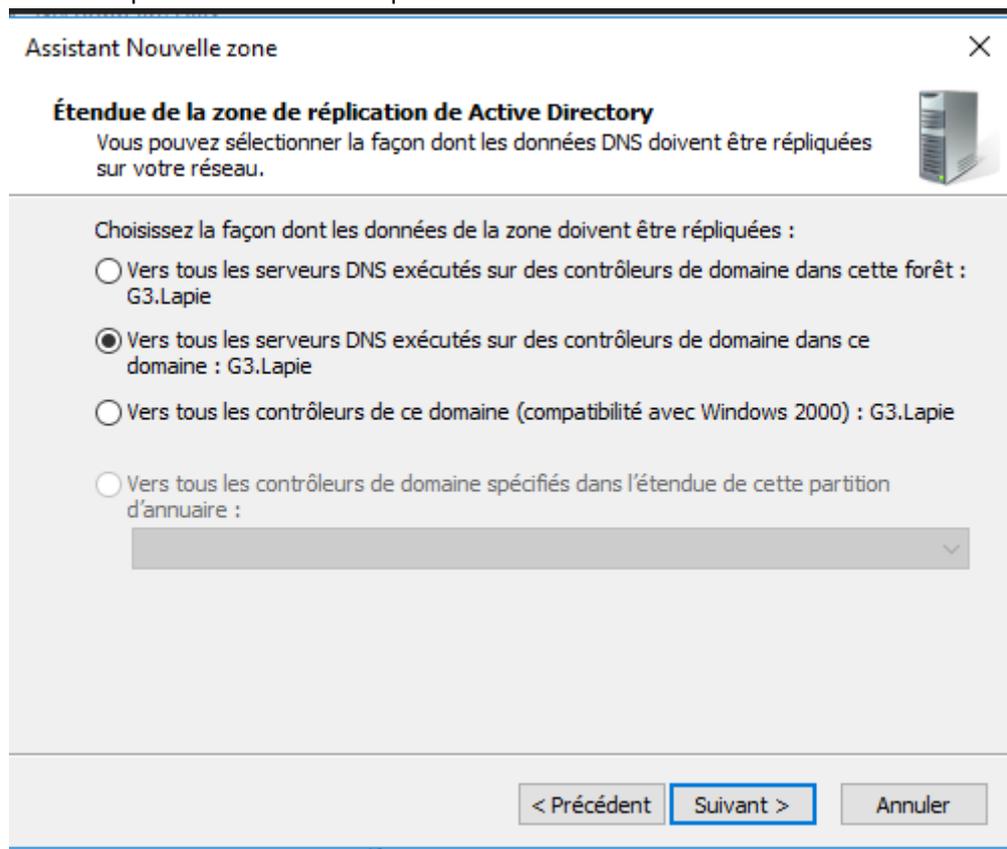
Sélectionnez le type de zone que vous voulez créer :

- Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- Zone secondaire
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- Zone de stub
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent Suivant > Annuler

Cochez l'option : « Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine :prevert-xx.local ». Cliquez sur « Suivant ».



Assistant Nouvelle zone

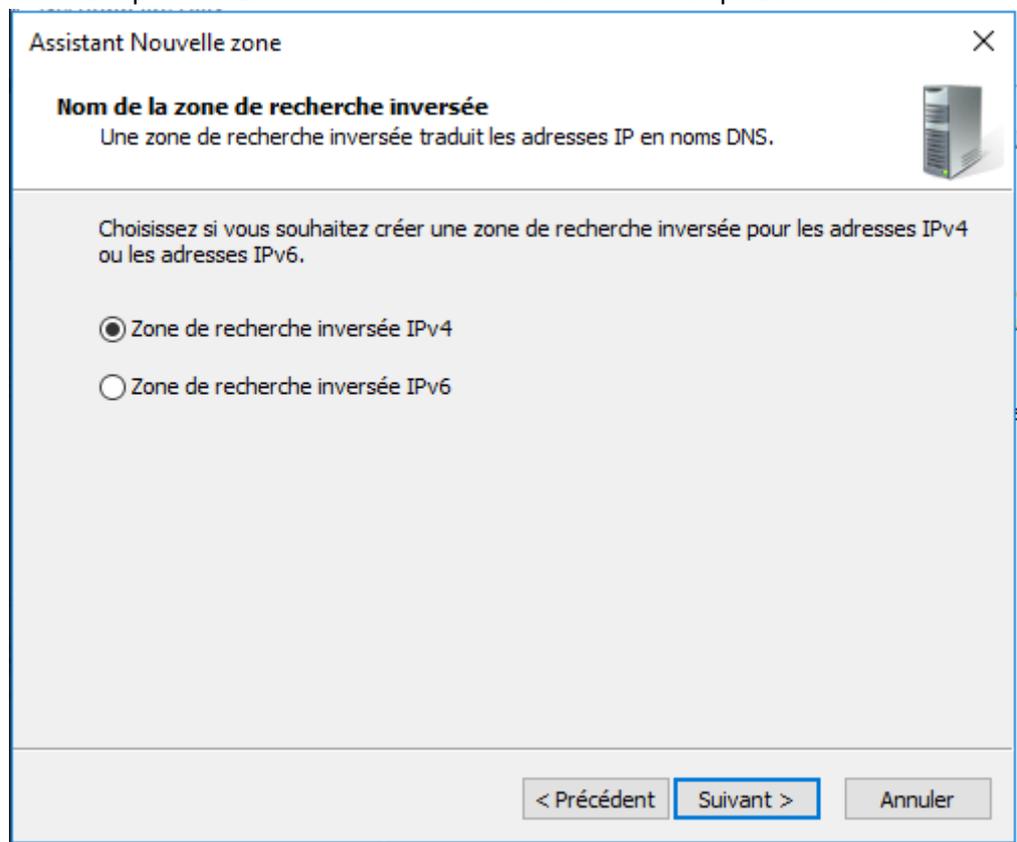
Étendue de la zone de réplication de Active Directory
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

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 : G3.Lapie
- Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : G3.Lapie
- Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : G3.Lapie
- Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

< Précédent Suivant > Annuler

Cochez l'option : « Zone de recherche inversées IPv4 ». Cliquez sur « Suivant »



Assistant Nouvelle zone

Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

- Zone de recherche inversée IPv4
- Zone de recherche inversée IPv6

< Précédent Suivant > Annuler

Tapez l'ID de votre réseau : 192.168.1 / Cliquez sur « Suivant »

Assistant Nouvelle zone

Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :

< Précédent Suivant > Annuler

Cochez l'option : « n'autorisez que les mises à jour dynamiques sécurisées »/ Cliquez sur « Suivant ».

Assistant Nouvelle zone

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.

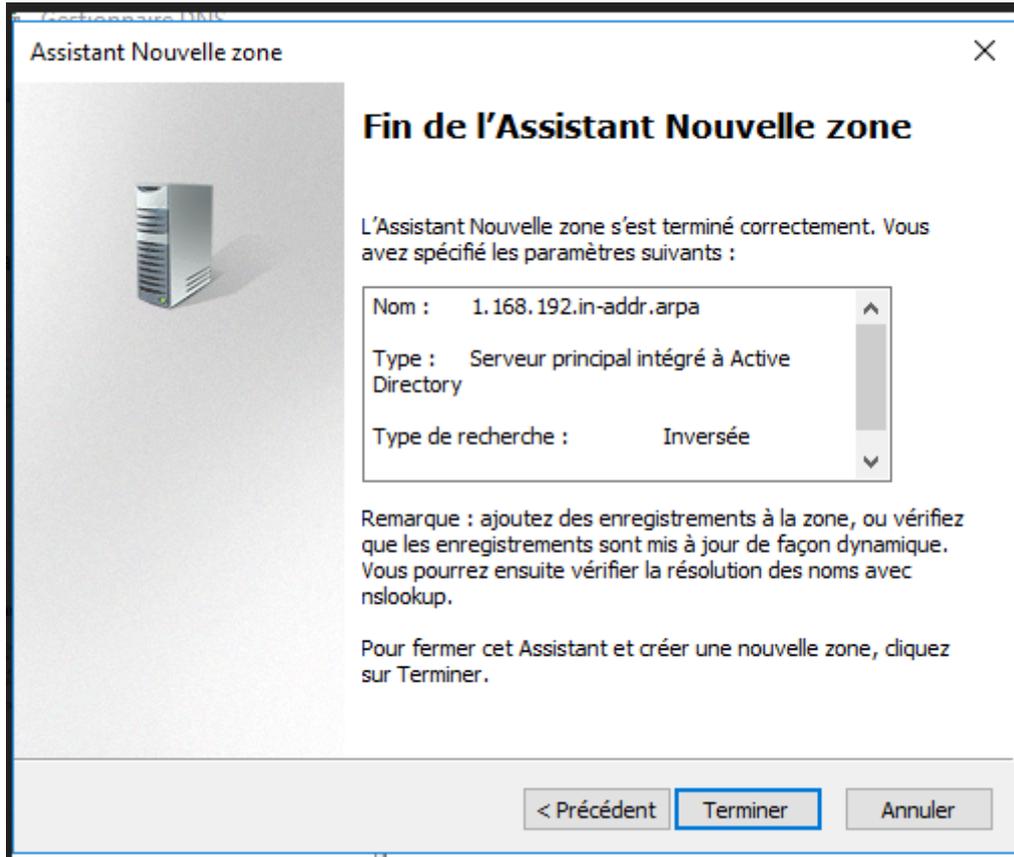
Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.

 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.

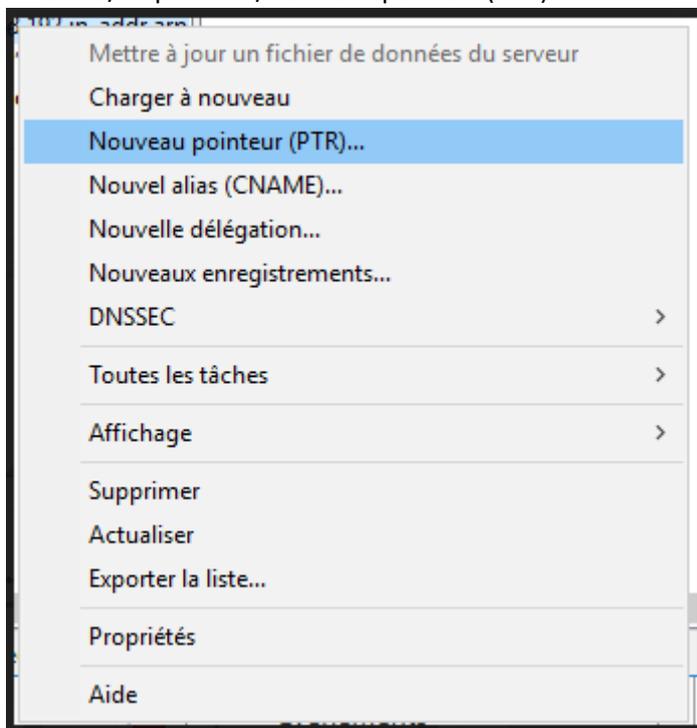
Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent Suivant > Annuler

Cliquez sur terminez



Nous allons définir le premier enregistrement de type PTR(PoinTeR)/Sélectionner la zone inversée/clique droit/Nouveau pointeur(PTR)



Tapez : l'adresse IP du serveur AD et son nom de domaine complet(FQDN)/Cliquez sur « OK »./Fermez le « Gestionnaire DNS »

Nouvel enregistrement de ressource

Pointeur (PTR)

Adresse IP de l'hôte :
192.168.1.13

Nom de domaine pleinement qualifié (FQDN) :
13.1.168.192.in-addr.arpa

Nom de l'hôte :
Parcourir...

Autoriser tout utilisateur identifié à mettre à jour tous les enregistrements DNS avec le même nom. Ce paramètre s'applique uniquement aux enregistrements DNS pour un nouveau nom.

OK Annuler

Vous devez tester manuellement avec la commande « nslookup ».le fonctionnement des zones de recherche directes et inversées. /Lancez l'invite de l'invite de commandes.

```
C:\Users\Administrateur>nslookup 192.168.1.13
Serveur : UnKnown
Address: ::1

Nom : DomainDnsZones.G3.Lapie
Address: 192.168.1.13

C:\Users\Administrateur>nslookup DomainDnsZones.G3.Lapie
Serveur : UnKnown
Address: ::1

Nom : DomainDnsZones.G3.Lapie
Addresses: 2a01:cb00:b6d:af00:d4d4:3c6:fae:4d57
           192.168.1.13

C:\Users\Administrateur>
```

Testez également la commande ipconfig/registerdns

```
>
C:\Users\Administrateur>ipconfig/registerdns

Configuration IP de Windows

L'inscription des enregistrements de ressource DNS pour toutes les cartes de
cet ordinateur a été initiée. Toute erreur sera signalée dans l'Observateur
d'événements dans 15 minutes.

C:\Users\Administrateur>
```