

Projet 4.5 : Mise en place d'un AD secondaire ADSecL

Table des matières

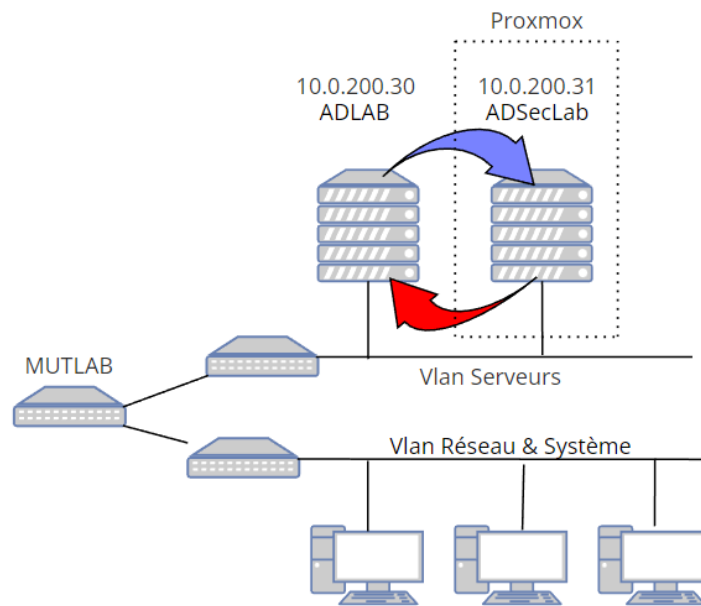
RODC présentation :	3
Schéma RODC GSB.fr :	3
Configuration ADSecLab en mode RODC :	4
Prérequis :	4
Installation du service ADDS en mode RODC :	4
Synchronisation service DHCP :	7
Configuration du DHCP « ADLAB »	8
Type de basculement :	9
Réplication service DNS.....	10
Type de Réplication :	10
Connexion au Serveur DNS ADLAB.....	11
Vérification de la réplication DNS :	12
Important :	12

RODC présentation :

Le mode RODC (Read-Only Domain Controller) est un type de serveur dans un réseau Windows Server qui permet de fournir une redondance si un serveur principal tombe en panne. Il stocke une copie en lecture seule de la base de données Active Directory, ce qui signifie qu'il ne peut pas être modifié directement. Cela permet de limiter les risques de sécurité en cas de vol ou d'attaque, car les informations stockées sur le RODC sont en lecture seule. Si le serveur principal tombe en panne, le RODC peut être utilisé pour authentifier les utilisateurs et fournir des services de base, ce qui permet de maintenir la continuité des opérations jusqu'à ce que le serveur principal soit rétabli.

<u>Avantages</u>	<u>Inconvénients</u>
Réduction des risques de sécurité	Limitation fonctionnelles
Utilisation dans des sites distants	Configuration initiale complexe
Authentification local des utilisateurs	Maintenance et support technique plus complexe
Possibilité de limiter l'exposition des informations	Besoin de mettre à jours les RODC avec les DCs en amont
Possibilité d'utiliser des comptes de service sans risques	Possibilité de perte de données en cas de panne du DC maître

Schéma RODC GSB.fr :

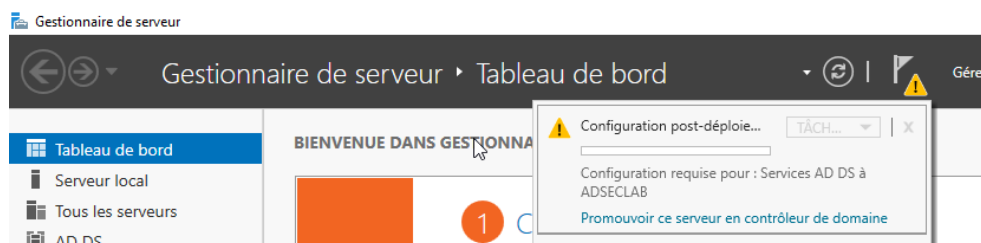


Configuration ADSecLab en mode RODC :

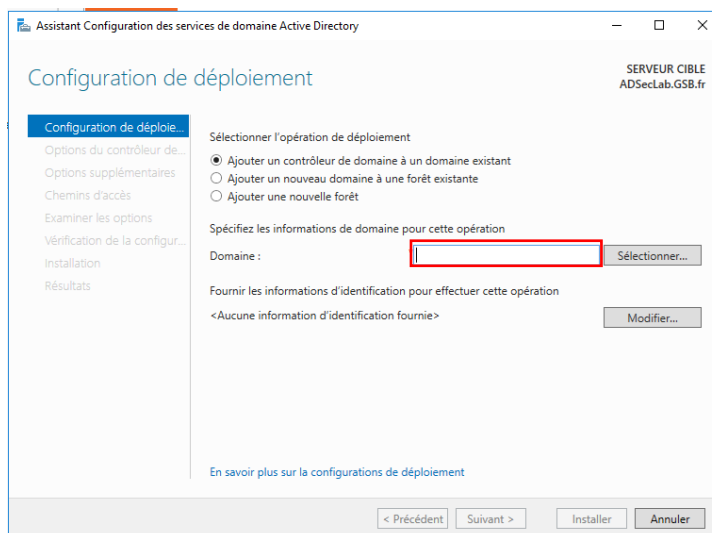
Prérequis :

- Avoir le même système d'exploitation « Windows Serveur 2016 ».
- Mettre une adresse IPv4 statique et configuré le DNS « 10.0.200.30 » & « 10.0.200.31 ».
- Configuré le nom du Windows Serveur « ADSecLab ».
- Redémarrer le serveur pour l'application du changement de nom.

Installation du service ADDS en mode RODC :

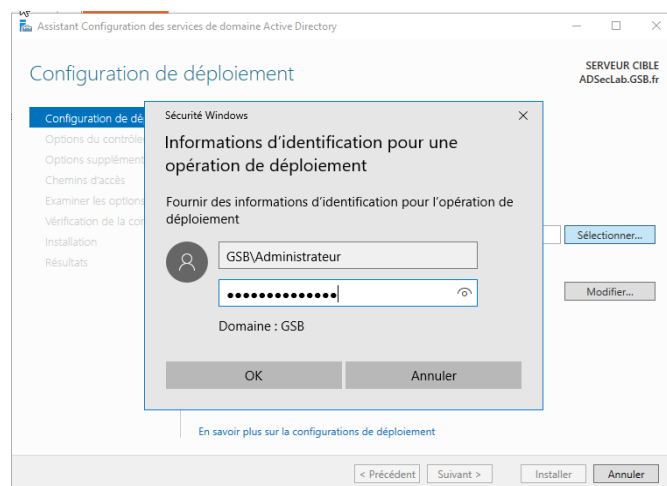


Une le service ADDS installer veuillez à promouvoir ce contrôleur de domaine.

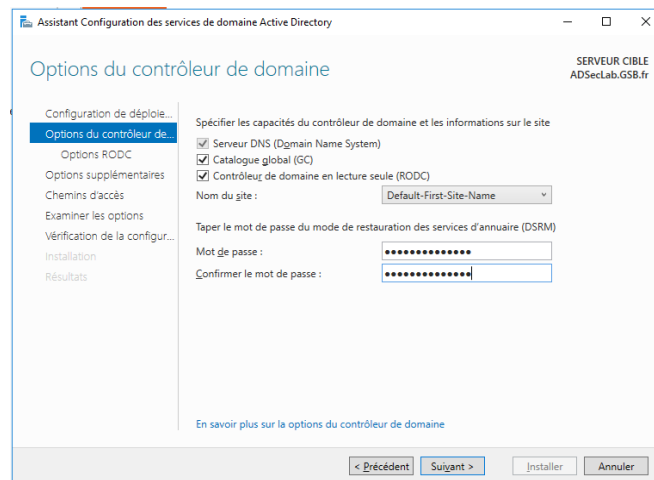


Veillez cocher la case « Ajouter un contrôleur de domaine déjà existant » et renseigner le nom de domaine dans case « Domaine » qui **GSB.fr**.

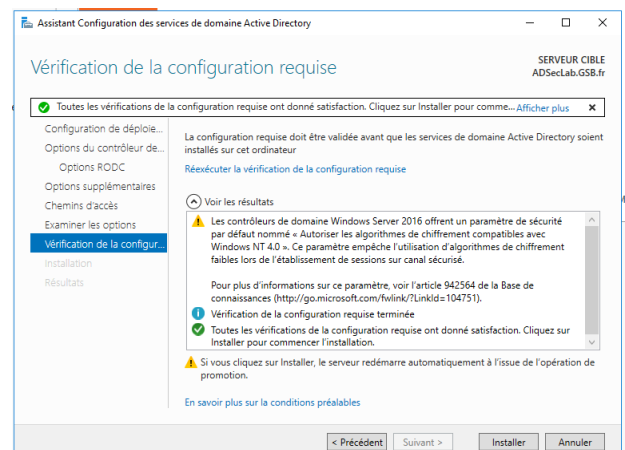
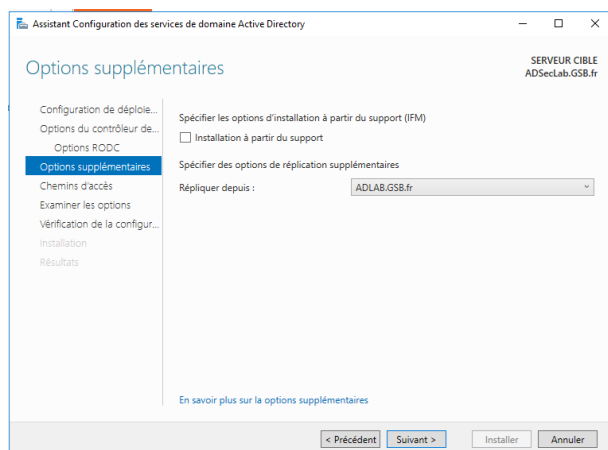
Une demande de vérification sera demandée pour rejoindre le domaine existant « compte administrateur » à renseigner :



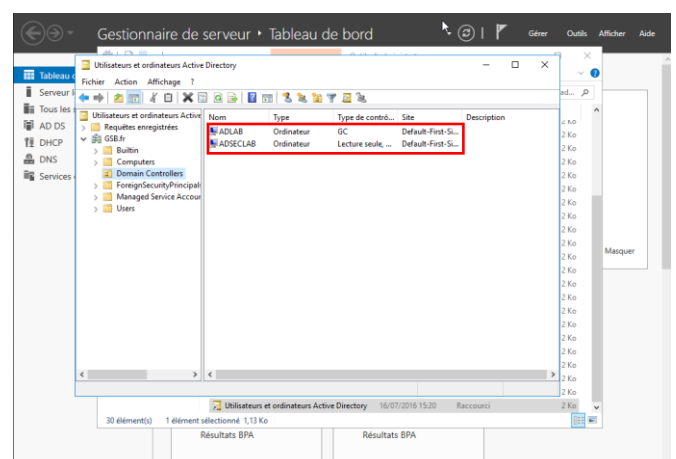
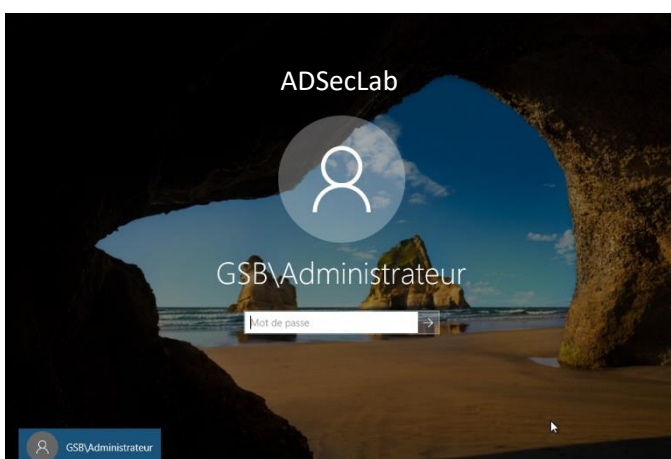
Cocher bien la case « Contrôleur de domaine en lecture seule (RODC) » et renseigner un mot passe propre pour ce Windows Serveur 2016.

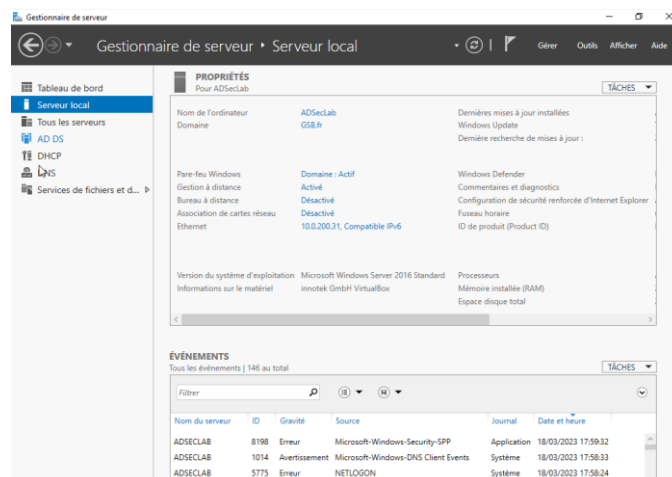


Veillez bien sélectionner le nom la machine « ADLAB.GSB.fr » et puis continuer jusqu'à installer.



Une fois installer le Windows Serveur va redémarrer et il sera joint au domaine.



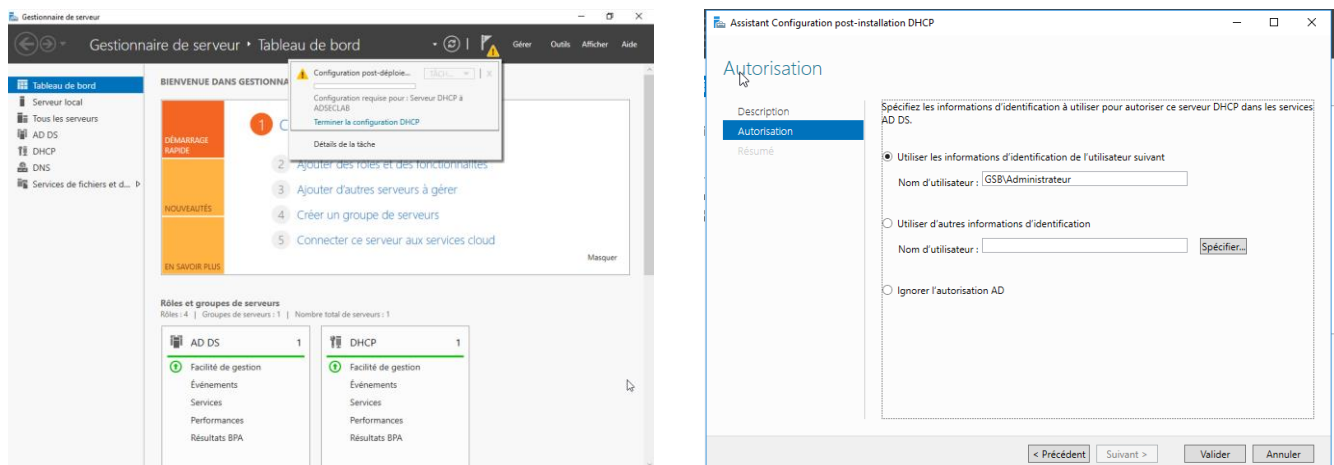


Maintenant le Windows serveur « ADSecLab » et désormais en mode RODC.

Les informations relatives aux comptes d'utilisateurs, aux groupes et aux mots de passe sont stockées dans une partition appelée "Partition de compte" qui est répliquée vers le RODC. Les informations relatives de la stratégie du groupe ne sont pas stockées dans la partition de compte, mais sont plutôt stockées dans une partition appelée "Partition des stratégies de groupe" qui est également répliquée vers le RODC.

Synchronisation service DHCP :

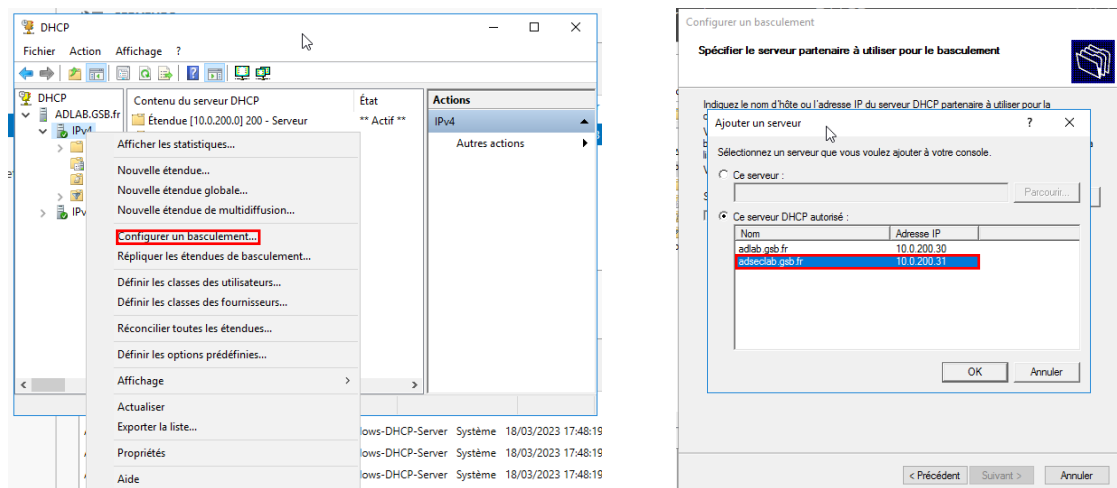
Installer le service DHCP sur « ADSecLab » et cliquez sur « Terminer la configuration DHCP » :



La configuration sur « ADSecLab » est désormais terminée la synchronisation vas se faire sur « ADLAB ».

Configuration du DHCP « ADLAB »

Entrer le gestionnaire du service DHCP et cliquer sur « configurer un basculement... » et sélectionner « adseclab.gsb.fr » en cochant la case « ce serveur DHCP autorisé : »



Type de basculement :

Configurer un basculement

Créer une relation de basculement

Créer une relation de basculement avec le partenaire adseclab

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode :

Configuration du serveur de secours

Rôle du serveur partenaire :

Adresses réservées pour le serveur de secours : %

☐ Intervalle de basculement d'état : minutes

☒ Activer l'authentification du message

Secret partagé :

< Précédent **Suivant >** Annuler

Configurer un basculement

Un basculement va être configuré entre adlab.gsb.fr et adseclab avec les paramètres suivants.

Étendues :

Configurer un basculement ?

Progression de la configuration du basculement.

Le journal ci-dessous montre la progression des diverses tâches de configuration du basculement, ainsi que les erreurs rencontrées.

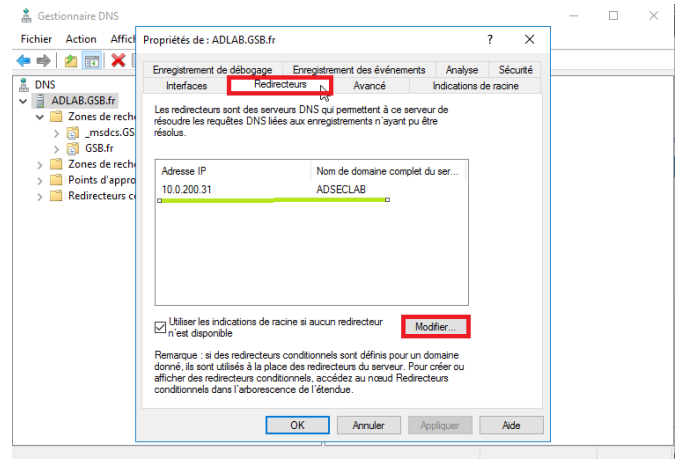
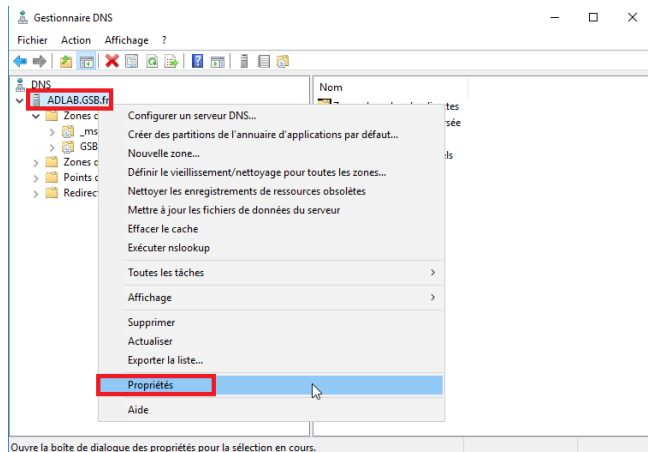
Ajouter des étendues sur le serveur partenaireRéussite
Désactiver des étendues sur le serveur partenaireRéussite
Création de la config. du basculement sur le serveur partenaireRéussit
Création de la configuration du basculement sur le serveur hôteRéussi
Activer des étendues sur le serveur partenaireRéussite
Réussite de la configuration du basculement.

Fermer

< Précédent Terminer Annuler

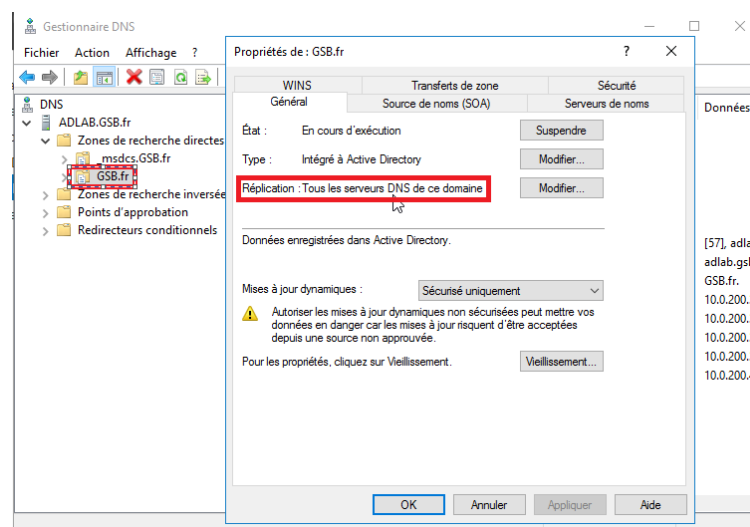
Réplication service DNS

Sur « ADLAB.GSB.fr » aller dans le gestionnaire DNS et faire propriétés sur « ADLAB.GSB.fr » puis se rendre sur « Redirecteurs » et ajouter « ADSecLab.GSB.fr » via son IP :

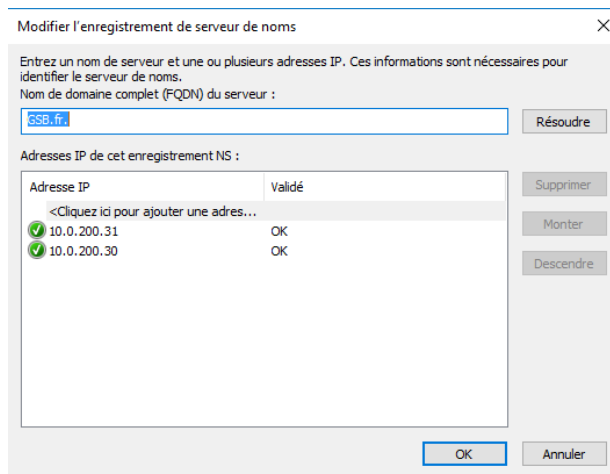
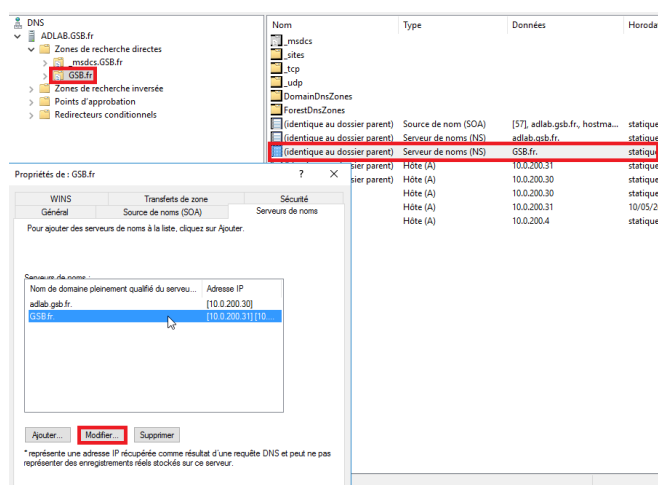


Type de Réplication :

Dans la zone de recherches directes faire un clic droit sur « GSB.fr » et propriétés, coché la case « Tous les serveurs DNS de ce domaine » :



Dans le dossier GSB.fr recherchait la ligne « serveur de noms (NS) GSB.fr » et effectuait un double clique puis rajouter l'adresse IP de « ADSecLab » :

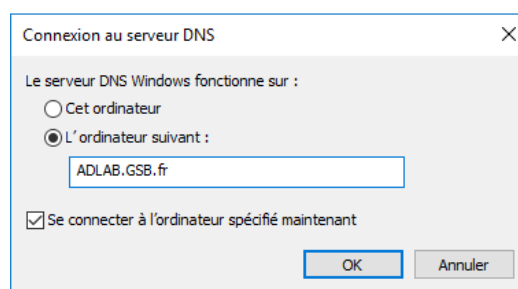
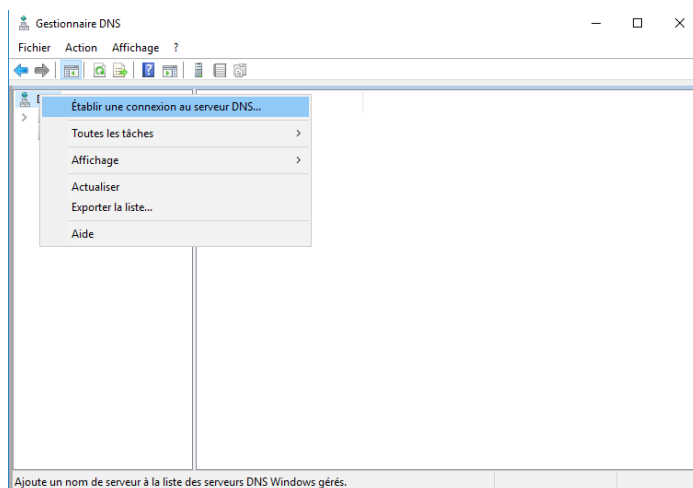


La configuration coté ADLAB est maintenant terminé

Connexion au Serveur DNS ADLAB

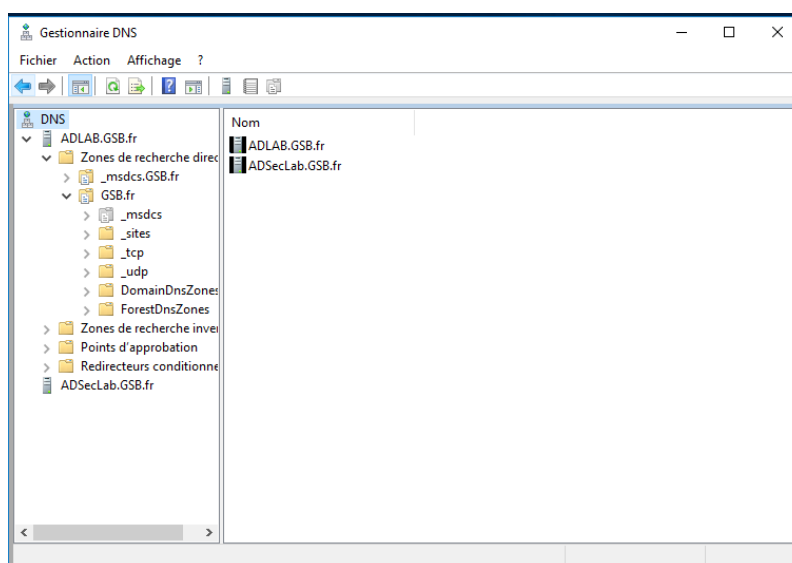
Sur « ADSecLab.GSB.fr » rendez-vous sur le gestionnaire DNS et faire un clic droit sur « DNS ».

Ajouter le serveur DNS maître à atteindre puis « Ok ».



Vérification de la réplication DNS :

Sur ADSecLab.GSB.fr il a réussi à joindre le serveur « ADLAB.GSB.fr » :



Vérification avec la commande « nslookup »

```
C:\Users\Administrateur.GSB>nslookup GSB.fr
DNS request timed out.
    timeout was 2 seconds.
Serveur : UnKnown
Address: ::1

Nom :      GSB.fr
Addresses: 10.0.200.30
           10.0.200.31
```

Important :

Après modification du gestionnaire DNS sur ADLAB.fr, actualisé sur ADSecLab.GSB.fr pour qu'il puisse bien prendre en considération la modification.