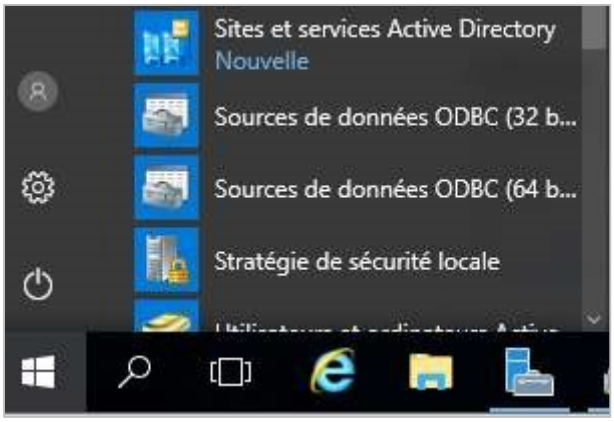
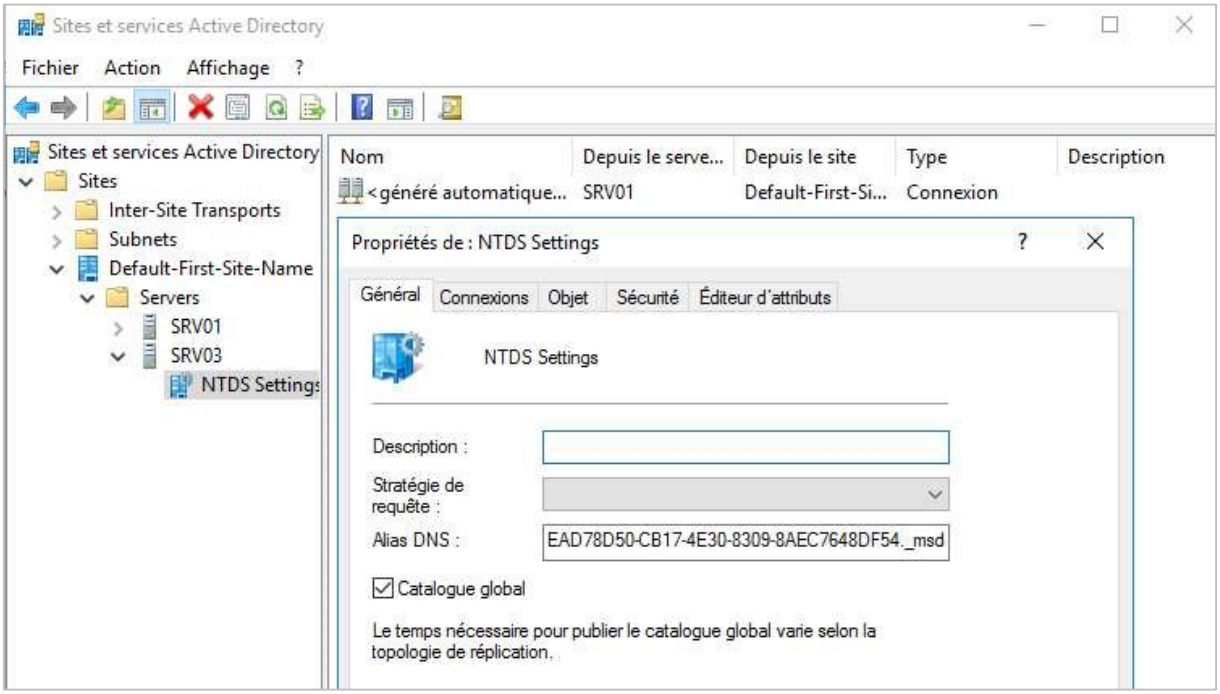
Vérification :

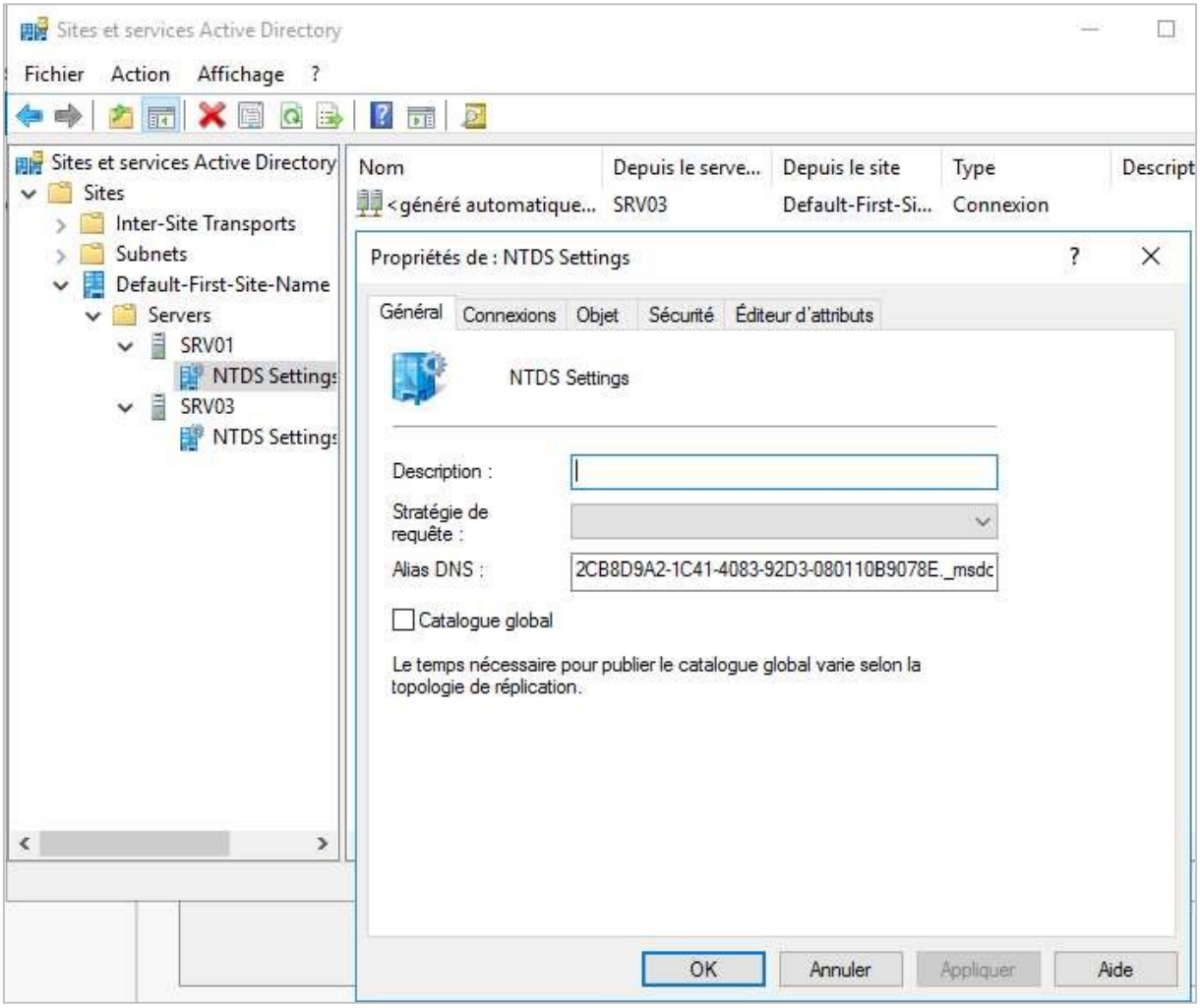
1. Ouvrir le console « Sites et services Active Directory » sur le nouveau serveur 2016.



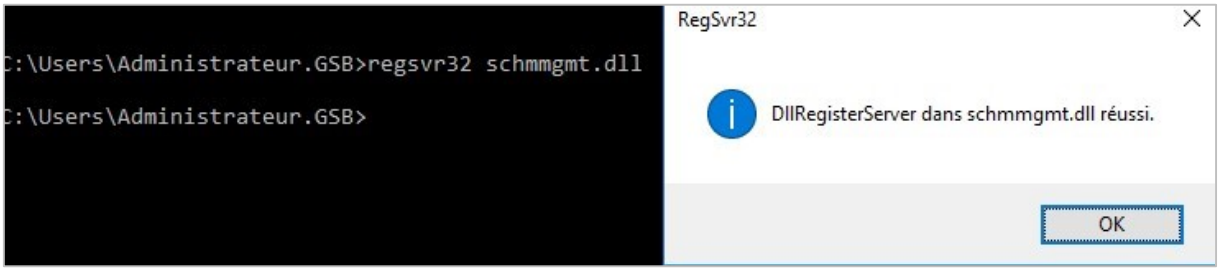
2. Déployez l'arborescence comme ci-dessous, ouvrir les propriétés de « NTDS Settings ». Et cochez la case « Catalogue global ».



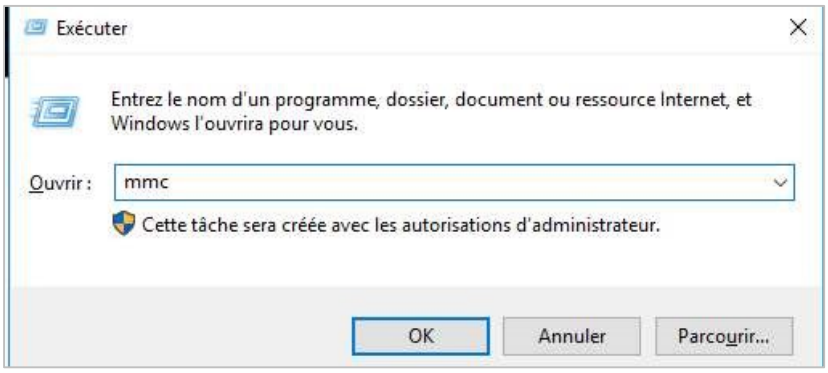
3. Sur l'ancien annuaire d'active directory, faites de même et décocher « Catalogue global ».



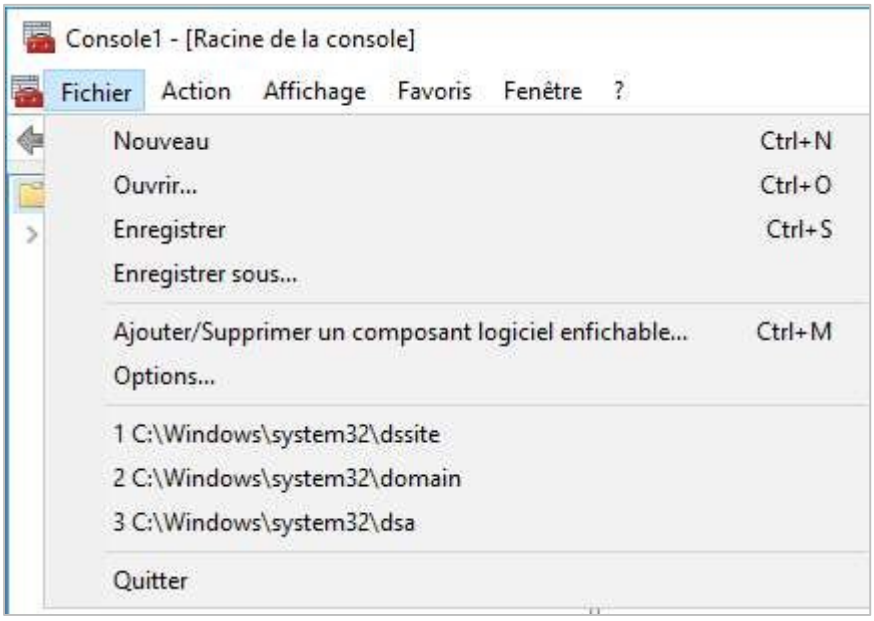
4. Ouvrir le cmd, et lancer la commande « regsvr32 schmmgmt.dll » sur le nouveau serveur.



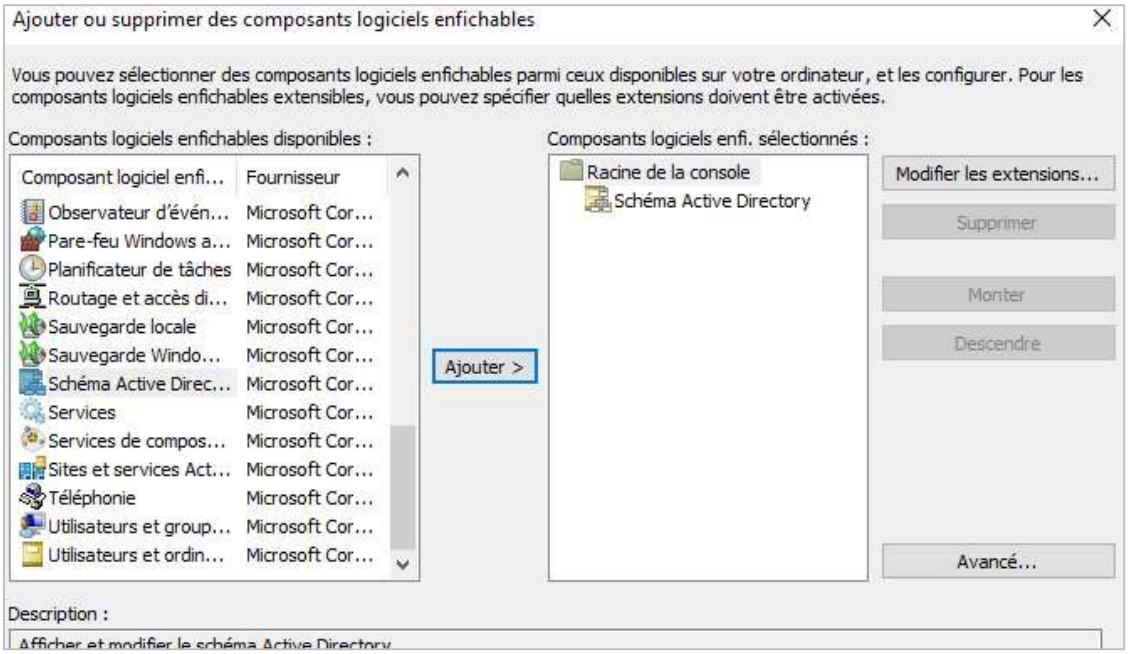
5. Appuyez simultanément sur la touche Windows + R. Renseignez « mmc ».



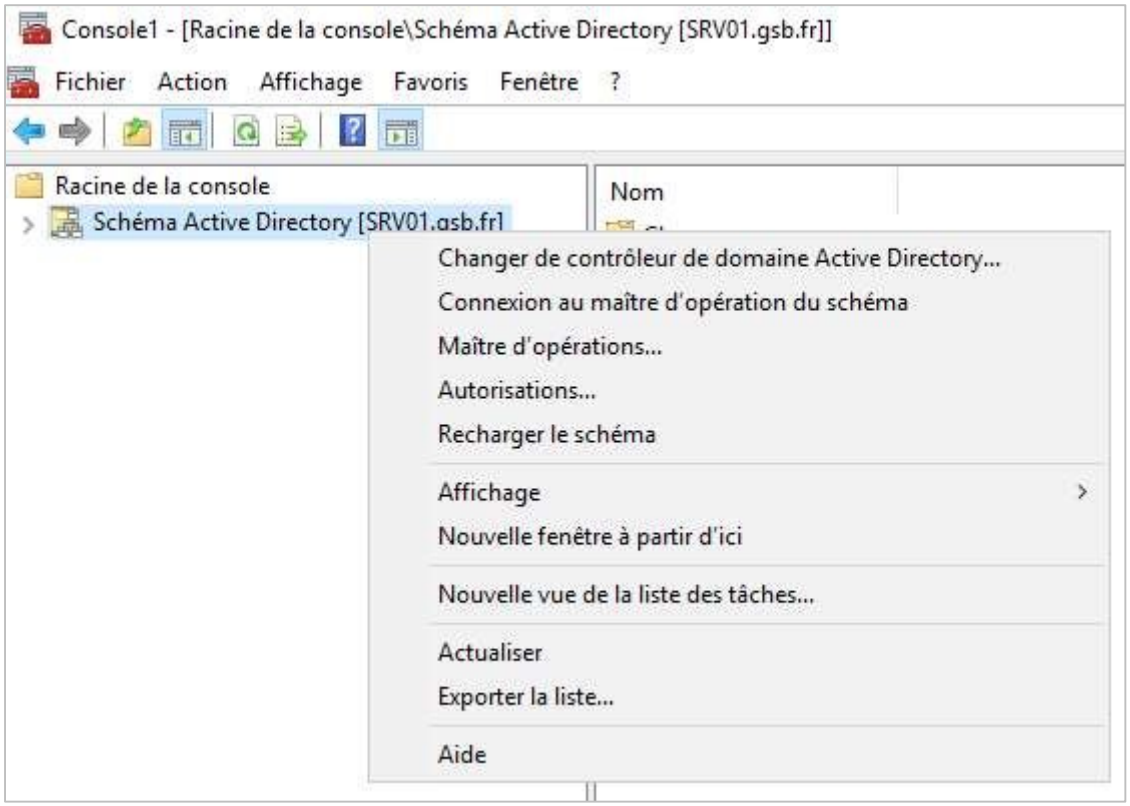
6. Faire « Fichier » puis cliquez sur « Ajouter/Supprimer un composant logiciel enfichable... »



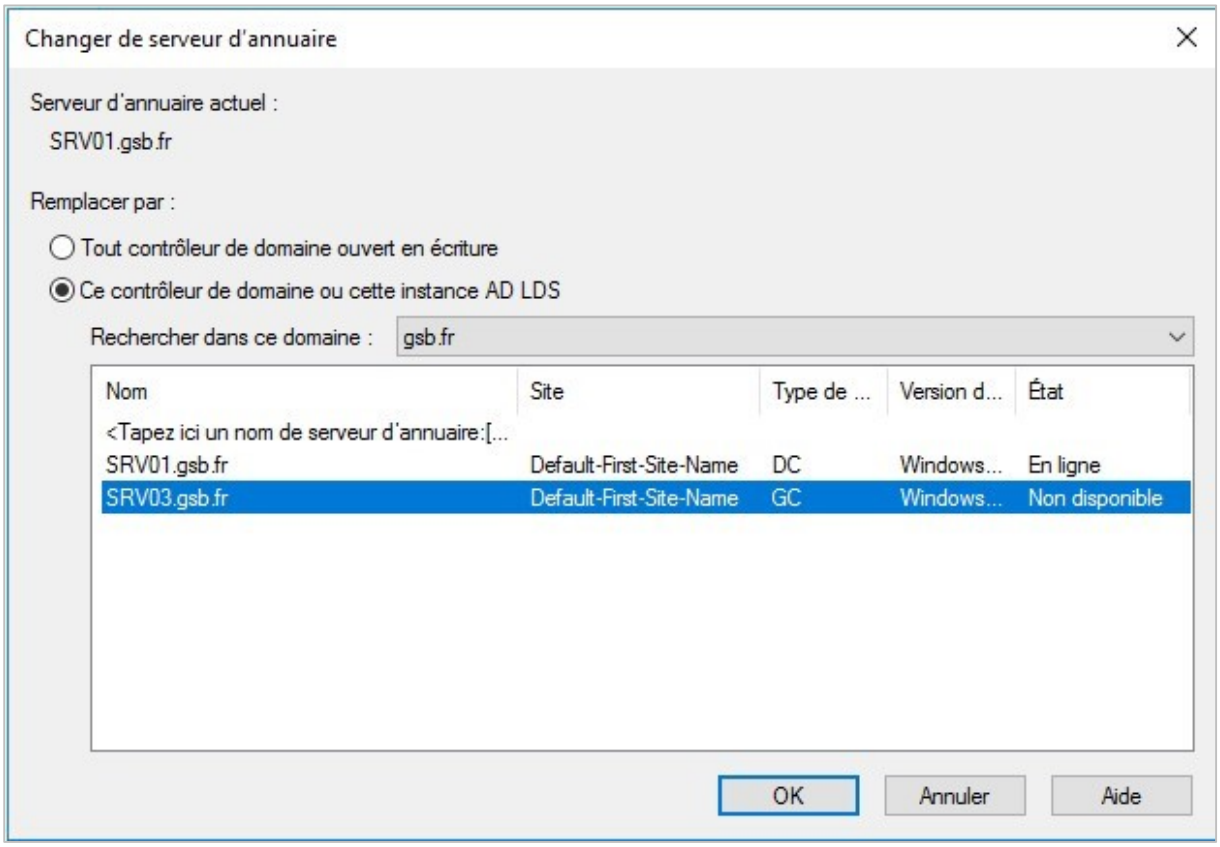
7. Ajoutez la console « Schéma Active Directory ».



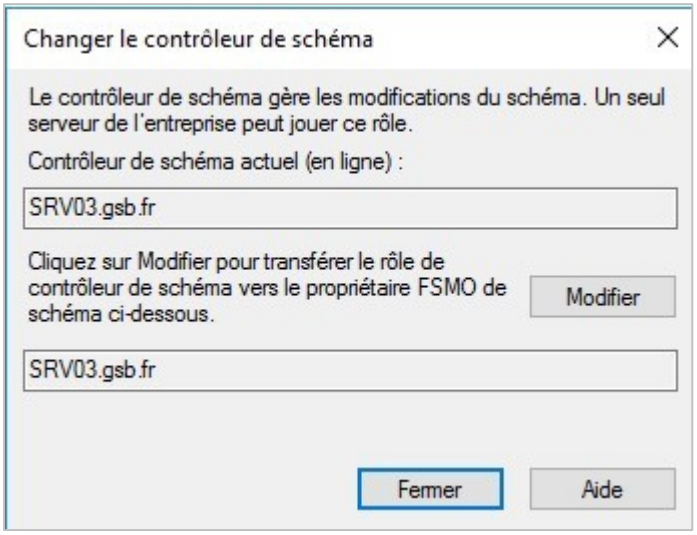
8. Faire un clic droit, puis cliquez sur « Changer de contrôleur de domaine Active Directory »



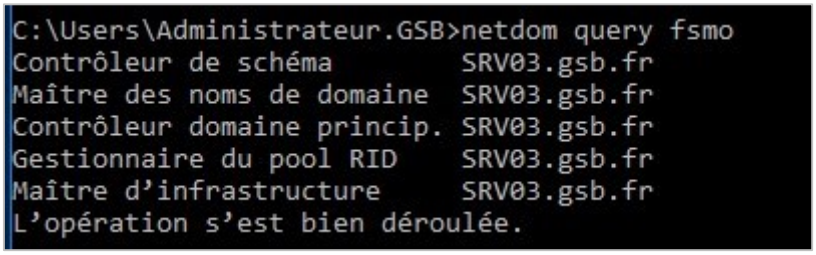
9. Cochez « Ce contrôleur de domaine ou cette instance AD LDS », puis sélectionner le nouveau serveur d'annuaire. Et cliquez sur « OK ».



10. Cliquez sur « Modifier ».



11. Dernière vérification pour voir si notre nouveau serveur a bien récupéré tout le fsmo.



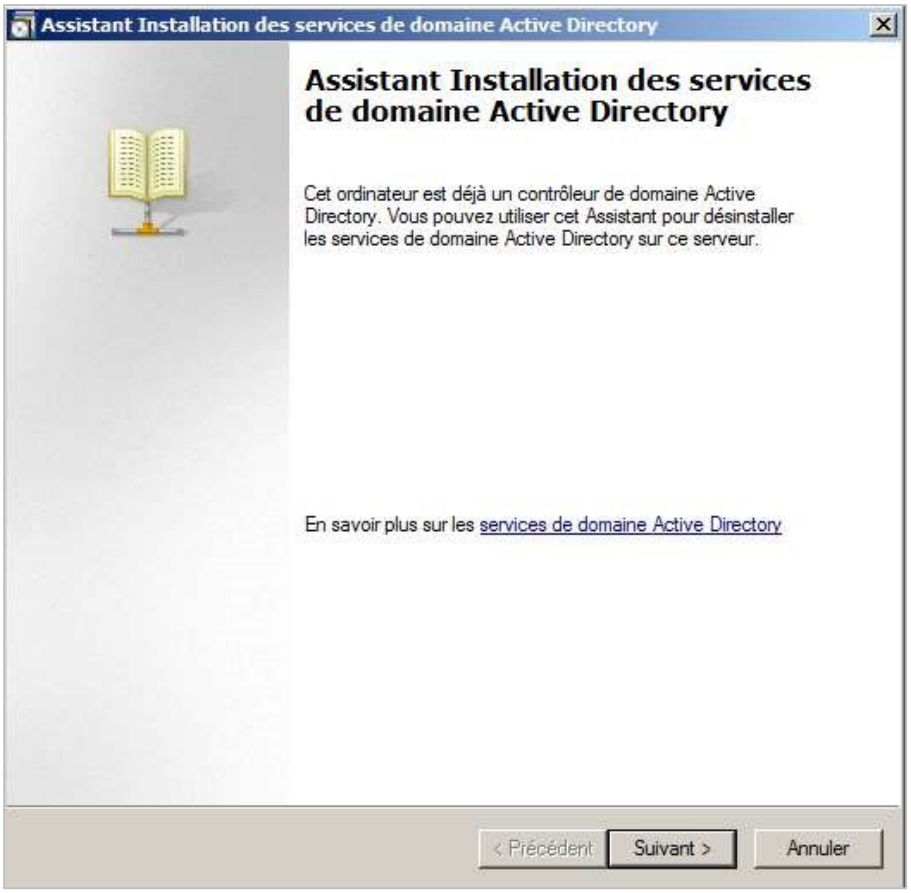
Suppression serveur d'origine :

1. Dans l'invite de commande, tapez les commandes suivantes : « dcdiag » et « dcpromo ».

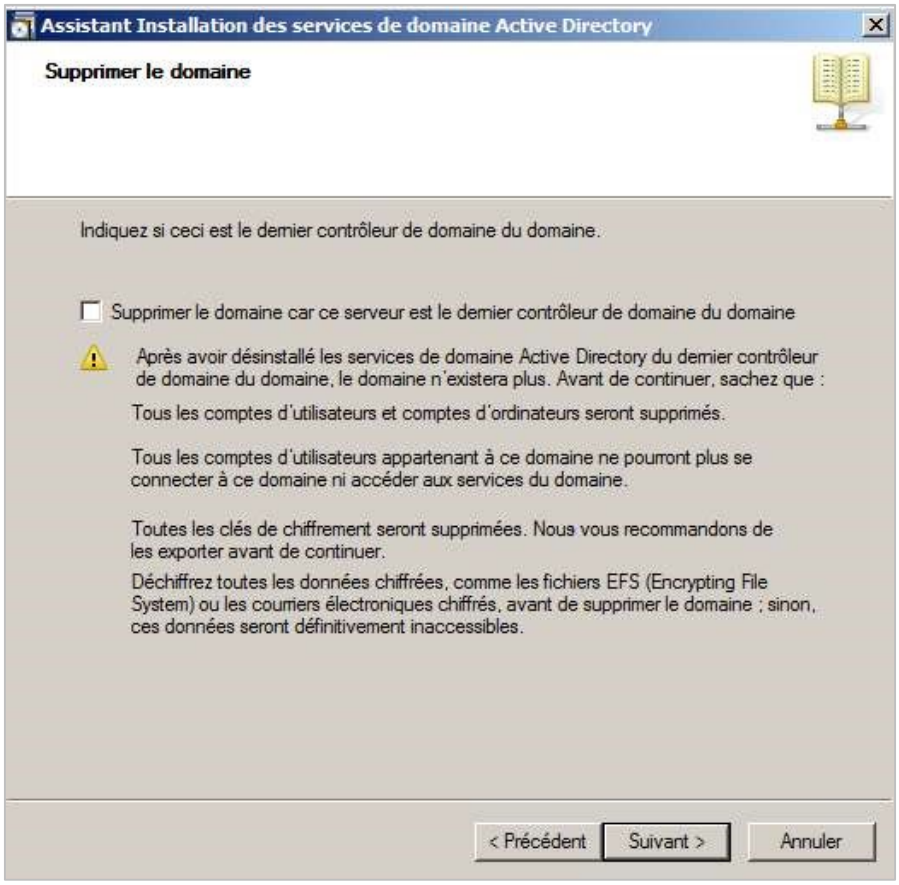
```
C:\Users\Administrateur>dcdiag_
```

```
C:\Users\Administrateur>dcpromo
```

2. Cliquez sur « Suivant ».

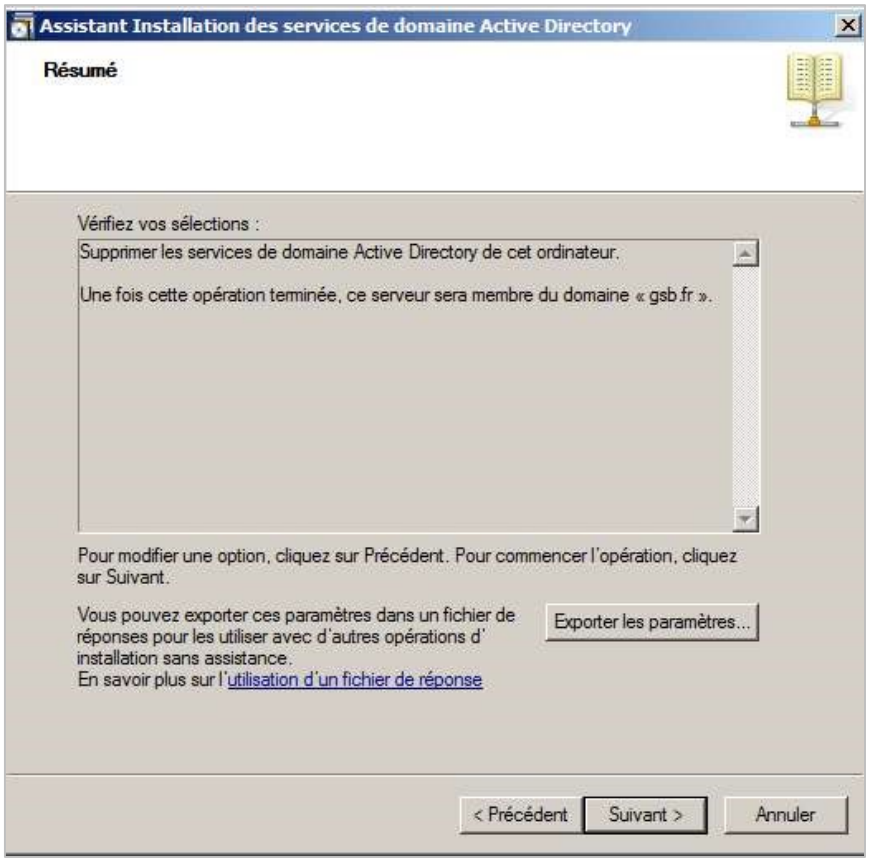


3. Ne pas cocher la case ! Cliquez sur « Suivant ».



4. Renseignez le mot de passe Administrateur.

5. Cliquez sur « Suivant ».



6. Cochez la case « Redémarrer à la fin de l'opération » et attendre le redémarrage.

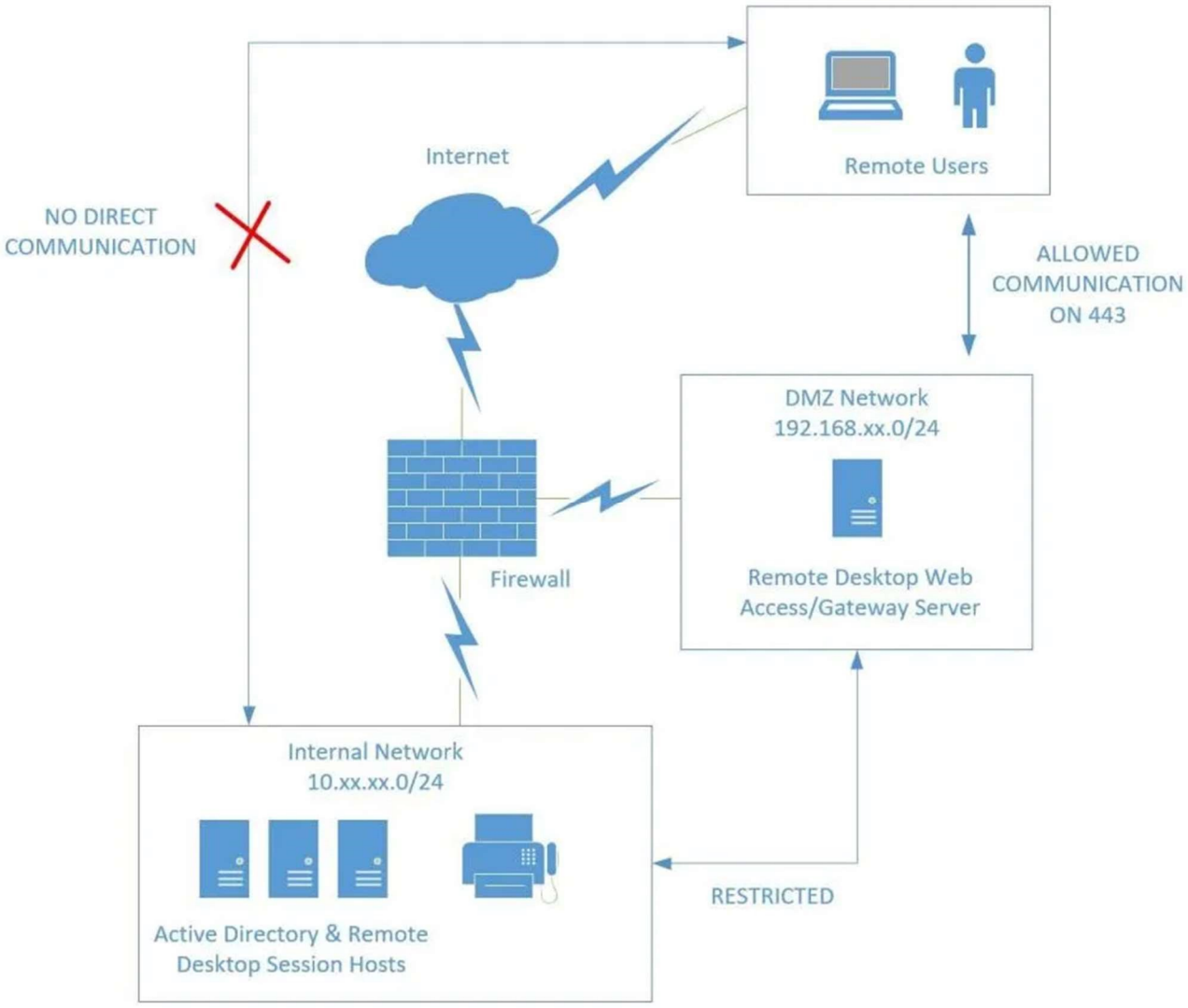
Le serveur n'est plus configuré pour fonctionner sur le domaine. Il peut être éteint.

Attention, les rôles Active directory et DNS sont toujours présents. Il est donc préférable de supprimer les rôles.

Axes d’améliorations

En effet, afin de procéder de façon préventive. Il est préférable de mettre en place la ferme dans une DMZ. Cela permet de continuer l’activité malgré l’impossibilité de se connecter de façon directe à l’infrastructure. Dans ce cas, l’activité fonctionne mais en dégradé.

L’installation de la ferme dans une DMZ privée permet de se connecter au serveur en étant présent sur le réseau de l’entreprise. Or, il est possible de rajouter l’installation dans une DMZ publique afin d’y accéder par internet. Voir Schéma ci-dessous.



Grace a la DMZ, il sera impossible d'attaquer les machines du réseau interne depuis le serveur RDS.
A l’inverse, sans DMZ, dès que le serveur web est piraté, le pirate peut s'attaquer aux machines du réseau interne.

La DMZ permet aussi d’empêcher des employés mal intentionnés d'aller bidouiller les serveurs.