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 sous Wondows

ADDS : Gestion FSMO

Formatrice : ZITI Ilham

Sommaire

1. Introduction

Lorsque l'on met en place un environnement Active Directory, il y a de très fortes chances que l'on ait plusieurs contrôleurs de domaine. De ce fait, tous les contrôleurs de domaine « normaux » disposent d'un accès en écriture sur l'annuaire.

Cependant, certaines tâches sont plus sensibles que d'autres, et il serait dangereux d'autoriser la modification de certaines données sur deux contrôleurs de domaine différents, en même temps. De ce fait et pour minimiser les risques de conflits, Microsoft a décidé d'implémenter les rôles FSMO qui permettent de limiter la modification de certaines données internes à l'annuaire Active Directory.

Au sein d'un environnement, on attribuera la notion de **rôle FSMO** à **maître d'opération** . En fait, le **maitre d'opération** est le contrôleur de domaine qui détient un ou plusieurs rôles FSMO. **Détenir un rôle signifie pour un contrôleur de domaine qu'il est capable de réaliser une action particulière au sein de l'annuaire .**

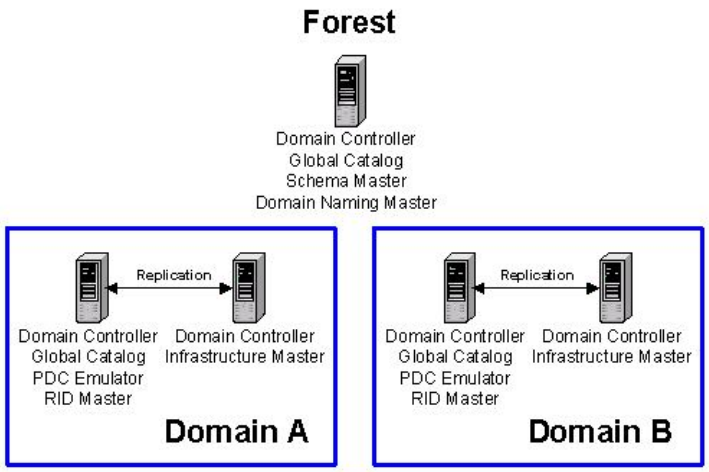
Il existe deux types :

Les rôles situés à la racine de la forêt :

- Maître de schéma (SM)
- Maître d'attribution de noms de domaines (DNM)

Les rôles situés à la racine de chaque domaine :

- Maître d'infrastructure (IM)
- Maître des ID relatifs (RID)
- Emulateur du contrôleur principal de domaine (PDC)



2. Maître de schéma (Schema Master)

Appelé également Maître d'opération, il gère l'ensemble des mises à jour et modifications du schéma.

Il assure également les réplications sur l'ensemble des contrôleurs de domaines.

Au niveau du domaine racine de la forêt, il doit être placé avec le Maître d'attribution des noms de domaine et également avec le PDC.

S'il n'est pas disponible, aucune modification sur le schéma ne pourra être appliquée ultérieurement.

En résumé, il est unique au sein d'une forêt et gère la structure du schéma.

3. Maître d'attribution des noms domaine (Domain Naming Master)

Il contrôle les ajouts et suppressions de domaines dans la forêt.

Il est également en charge de la création et/ou suppression de relations avec les domaines externes.

Enfin, il gère aussi les objets qui servent à établir le lien entre les différentes partitions et le domaine.

Ces derniers sont stockés dans la partition de Configuration.

Le rôle doit être placé avec le Maître de schéma et avec le PDC.

En cas d'utilisation sous Windows Server 2003 ou ultérieur, il ne devra en aucun cas être GC (Global Catalog).

S'il n'est pas disponible, aucun ajout ou suppression de domaine ne sera possible.

En conséquence, un serveur de secours avec une réplication directe de maître à partenaire est nécessaire.

En résumé, il est unique au sein d'une forêt et attribue les noms de domaine.

4. Maitre RID (RID Master)

Les objets créés au sein de l'annuaire Active Directory dispose de plusieurs identifiants uniques. Parmi eux, il y a notamment le GUID et le DistinguishedName mais aussi l'identifiant de sécurité « SID », c'est ce dernier qui nous intéresse dans le cadre du maître RID.

Le RID est un identifiant relatif qui est unique au sein de chaque SID, afin d'être sûr d'avoir un SID unique pour chaque objet de l'annuaire. Le SID étant constitué d'une partie commune

qui correspond au domaine, le RID est essentiel pour rendre unique chaque SID. C'est là que le maître RID intervient...

Unique au sein d'un domaine, ce maître d'opération devra allouer des blocs d'identificateurs relatifs à chaque contrôleur de domaine du domaine. Ainsi, chaque contrôleur de domaine aura un bloc (pool) de RID unique qu'il pourra attribuer aux futurs objets créés dans l'annuaire.

En résumé, il est unique au sein d'un domaine et attribue des blocs de RID aux contrôleurs de domaine pour assurer que les SID des objets soient unique.

5. Le PDC Emulator

L'émulateur PDC (*Primary Domain Controller*) est unique au sein d'un domaine et se doit d'assurer cinq missions principales :

- Modification des stratégies de groupe du domaine (éviter les conflits et les écrasements)
- Synchroniser les horloges sur tous les contrôleurs de domaine (heure et date)
- Gérer le verrouillage des comptes
- Changer les mots de passe
- Assure la compatibilité avec les contrôleurs de domaine Windows NT

En résumé, il est unique au sein d'un domaine et assure diverses missions liées à la sécurité et par défaut il joue le rôle de serveur de temps pour l'ensemble du domaine.

6. Localiser les rôles FSMO

Pour savoir sur quels serveurs sont présents les rôles FSMO, la commande **netom query fsmo** permet de lister les rôles et les serveurs qui possèdent chaque rôle.

```
C:\Windows\system32>netdom query fsmo
Contrôleur de schéma         AD1.ntic.ma
Maître des noms de domaine   AD1.ntic.ma
Contrôleur domaine princip.  AD1.ntic.ma
Gestionnaire du pool RID     AD1.ntic.ma
Maître d'infrastructure      AD1.ntic.ma
L'opération s'est bien déroulée.
```

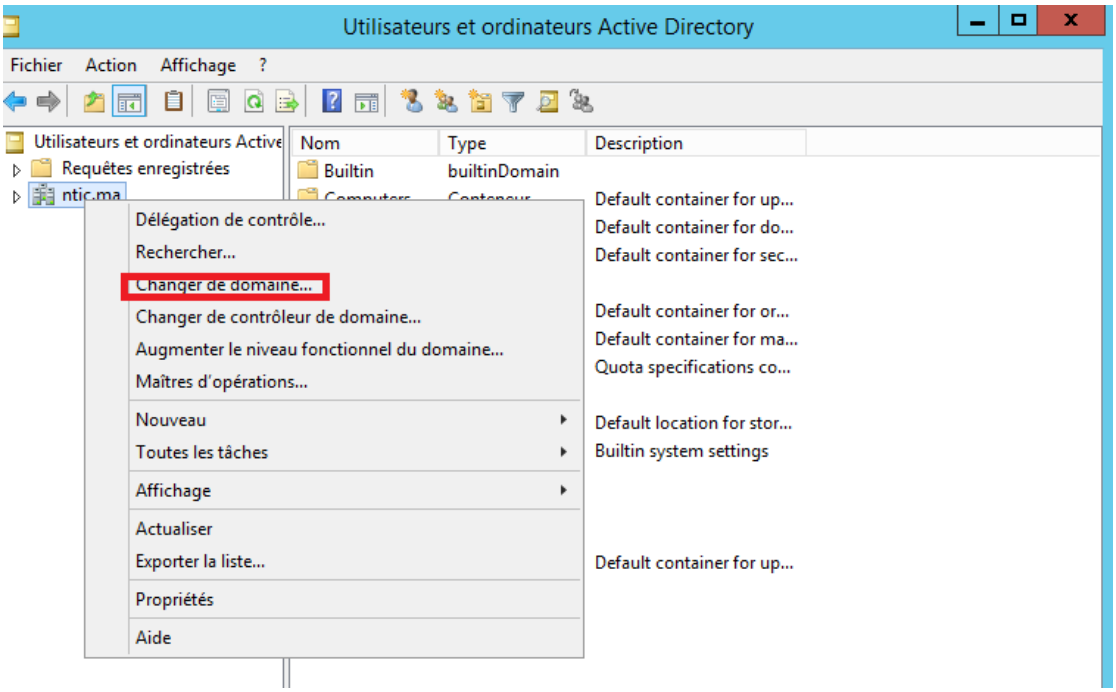
7. Déplacement des rôles FSMO

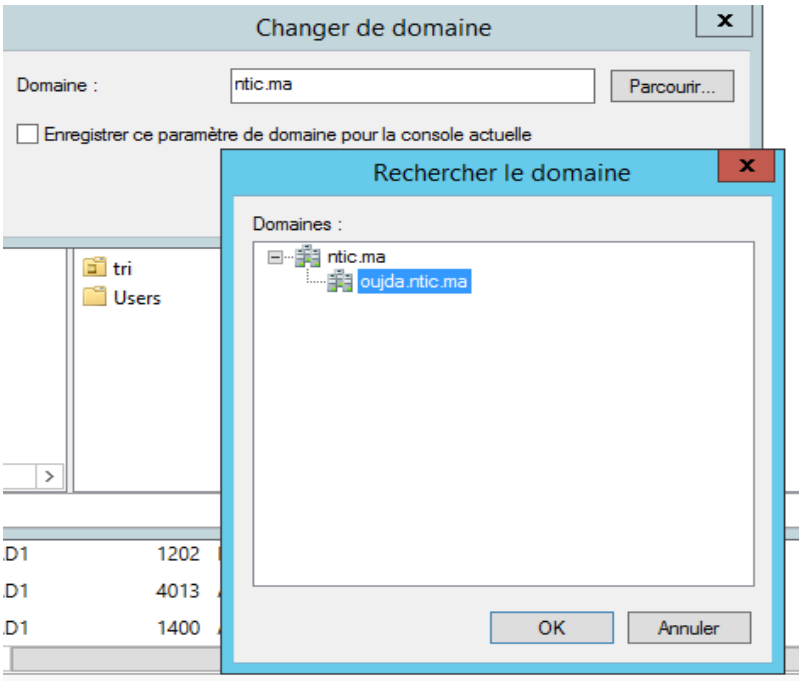
Par défaut, le premier contrôleur de domaine du domaine détient les cinq rôles FSMO, par faute de choix. Pour éviter de donner à un maitre d'opération la totalité des droits sur l'annuaire, il est possible de transférer les rôles les répartir entre plusieurs contrôleurs de domaine.

7.1 Graphiquement

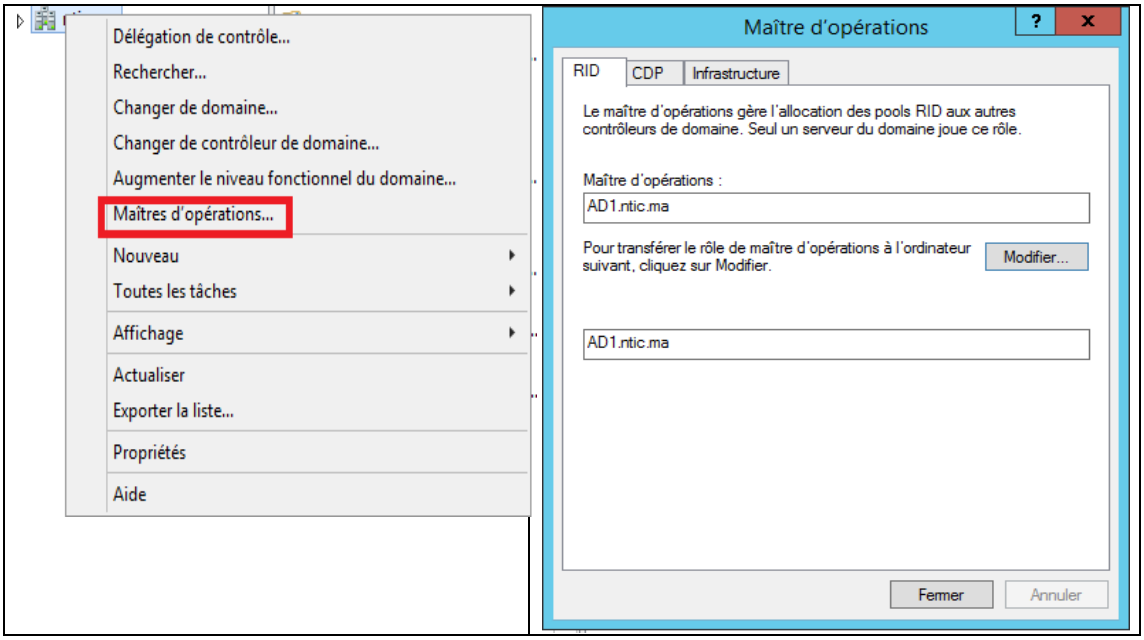
Lors d'une migration et pour les rôles de domaine, l'opération est a effectué sur chaque domaine concerné.

Dans la console "Utilisateur et Ordinateur Active Directory", sélectionner le contrôleur de domaine qui doit prendre les rôles. Ensuite, il suffit d'aller dans les rôles FSMO, puis de cliquer sur transférer pour chacun des 3 rôles.



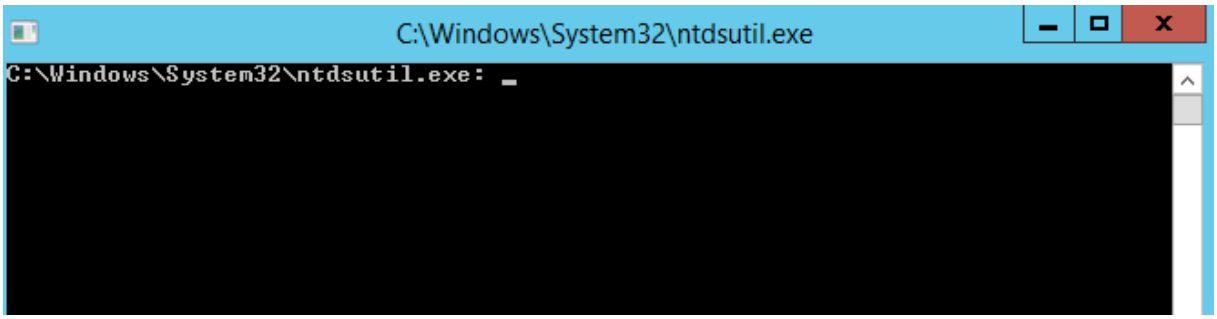


Après avoir sélectionné le DC qui doit prendre en charge les rôles, faites un clic droit sur le nom du domaine et sélectionner « Maîtres d'opérations… »



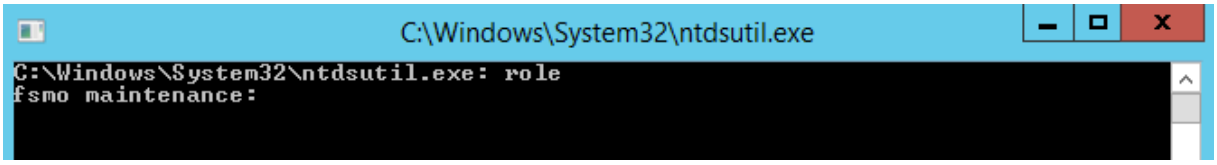
7.2 L'utilitaire NTDSUTILS

Aller dans Démarrer, Exécuter puis de saisir "**ntdsutil.exe**"



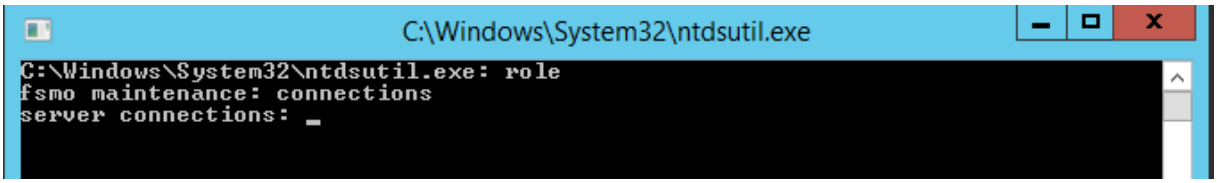
Pour passer en mode FSMO il faut saisir la commande suivante :

```
role
```



Il faut établir une connexion avec le serveur auquel on veut transférer un ou des rôles. Pour cela, dans le mode « **fsmo maintenance** », taper la commande :

```
connections
```



Pour établir la connexion avec le serveur, taper la commande :

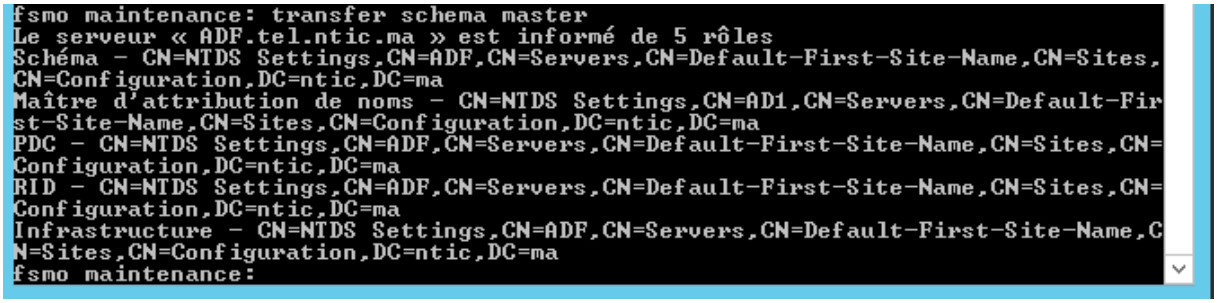
```
connect to server nom_serveur
```

Maintenant il faut retourner au mode fsmo maintenance, taper la commande "q"

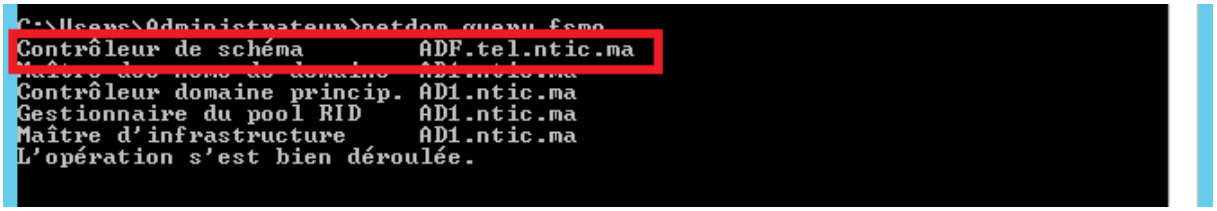
Chaque rôle dispose d'une commande pour le transfère

Nom du Maître	Commande
RID	transfer RID master
Schema	transfer schema master
Maître d'infrastructure	transfer infrastructure master
Attribution des noms de domaine	transfer domain naming master
Émulateur PDC	transfer pdc

Pour transférer par exemple le maitre Schéma



Pour vérifier si les rôles sont bien transférés utiliser la commande **netom query fsmo**



7.3 PowerShell

La commande pour déplacer les rôles FSMO est :

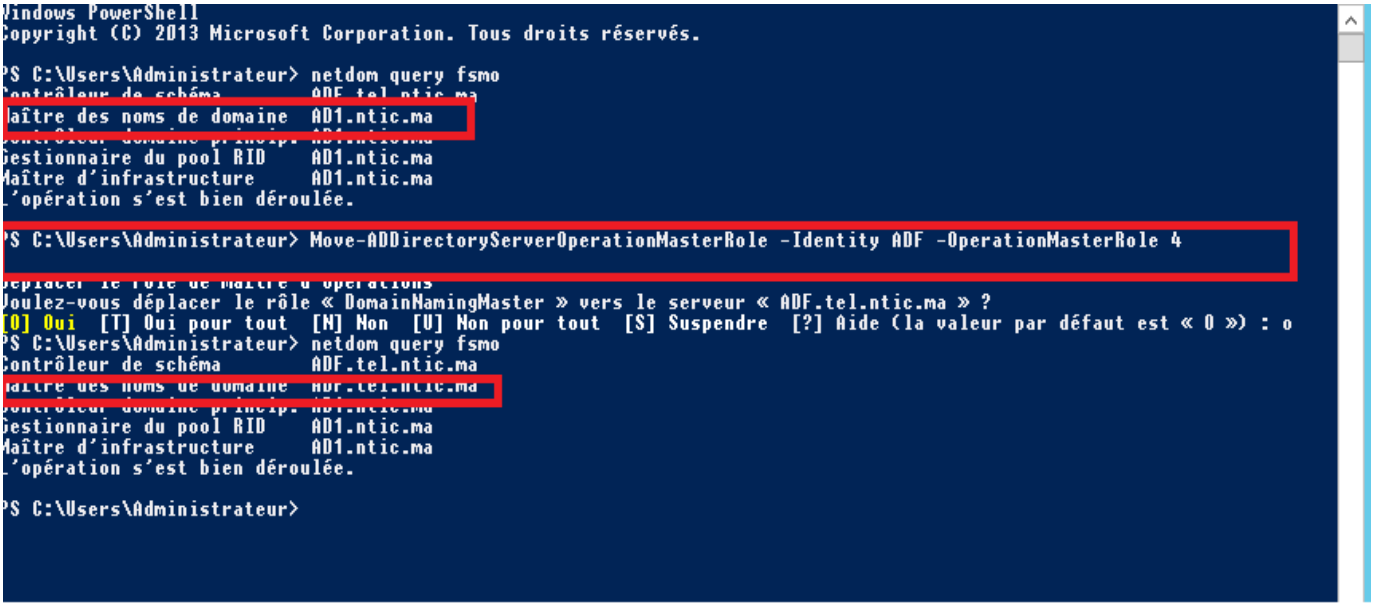
Move-ADDirectoryServerOperationMasterRole –Identity « contrôleur de domaine cible » -OperationMasterRole [rôles FSMO]

À la place de « contrôleur de domaine cible » renseigner le nom du contrôleur de domaine qui va recevoir les rôles FSMO.

À la place de [rôles FSMO] renseigner soit le nom du rôle sans espace entre les mots, par exemple « SchemaMaster » et non « Schema master », ou renseigner le chiffre qui correspond au rôle FSMO, ci-après un tableau associatif des rôles FSMO avec leurs chiffres attribués.

Nom du rôle	Numéro
PDCEmulator	0
RIDMaster	1
InfrastructureMaster	2
ShemaMaster	3
DoaminNamingMaster	4

Par exemple pour Transfer le maitre Attribution des noms de domaine



8. Reference

https://www.it-connect.fr/chapitres/les-cinq-roles-fsmo/

https://www.it-connect.fr/chapitres/les-cinq-roles-fsmo/

https://www.supinfo.com/articles/single/5126-windows-serveur-2016-deplacer-roles-fsmo

https://www.supinfo.com/articles/single/3378-deplacement-roles-fsmo-active-directory

https://www.it-connect.fr/transfert-des-roles-fsmo-avec-ntdsutil/