

Active Directory - Gestion des rôles FSMO



Difficulté : Intermédiaire

Notions : Active Directory, LDAP, Rôle FSMO

I. Introduction

Cette procédure vise à expliquer le transfert des rôles FSMO. En effet, l'un des principes clé d'Active Directory réside dans la gestion de ces rôles.

Ces rôles sont par défaut tous portés par le contrôleur de domaine principal mais peuvent être répartis pour plus de souplesse. Il peut également être nécessaire de les transférer dans le cadre de l'arrêt définitif d'un serveur qui les portait auparavant.

Il est également possible de forcer leur réattribution à un nouveau DC si celui qui les portait avant n'est plus disponible suite à un incident ayant entraîné sa perte ou sa destruction.

II. Transférer les rôles FSMO

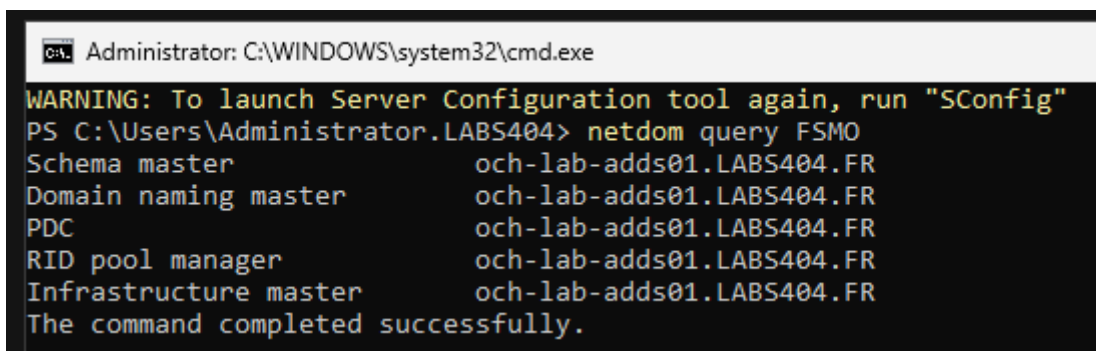
Conseil : Bien qu'une méthode pour transférer ces rôles existe en GUI, elle est relativement fastidieuse car il faut en effet aller chercher à plusieurs endroits dans les outils d'administration. Aussi le plus rapide et pratique est de procéder en CLI.

En batch (méthode legacy)

Ouvrir une CMD sur le serveur Active Directory qui va reprendre les rôles.

Vérifier qui porte les rôles actuellement avec la commande :

```
netdom query FSMO
```



```
Administrator: C:\WINDOWS\system32\cmd.exe
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\Users\Administrator.LABS404> netdom query FSMO
Schema master                och-lab-adds01.LABS404.FR
Domain naming master         och-lab-adds01.LABS404.FR
PDC                          och-lab-adds01.LABS404.FR
RID pool manager             och-lab-adds01.LABS404.FR
Infrastructure master         och-lab-adds01.LABS404.FR
The command completed successfully.
```

Ici c'est le DC principal qui porte tous les rôles.

Ouvrir la console NTDS Utils.

ntdsutil

Entrer en mode de maintenance du shema.

role

Se connecter au serveur de destination des rôles

connection
connect to server <FQDN>
q

Administrator: C:\WINDOWS\system32\cmd.exe

```
PS C:\Users\Administrator.LABS404> ntdsutil
C:\WINDOWS\system32\ntdsutil.exe: role
fsmo maintenance: connection
server connections: connect to server och-lab-adds02.labs404.fr
Binding to och-lab-adds02.labs404.fr ...
Connected to och-lab-adds02.labs404.fr using credentials of locally logged on user.
server connections: q
fsmo maintenance: _
```

Pour transférer les rôles, utiliser la commande suivante

transfer <NomDuRôle>

Attention : En cas de transfert forcé, la commande est `seize`. Mais cela ne doit être utilisé que si l'ancien DC n'est plus disponible. La procédure par défaut est celle donnée ci-dessus.

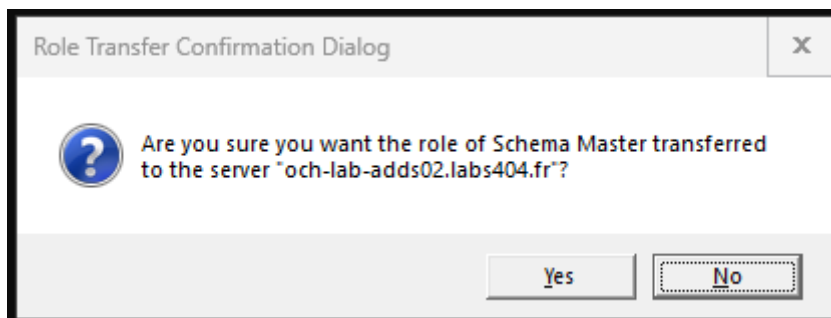
Il y a 5 rôles à transférer, dans cet ordre là :

- RID master
- schema master
- infrastructure master

- naming master
- pdc

Info : à chaque transfert, NTDSUTIL affiche le résumé des rôles, il est ainsi possible de vérifier au fur et à mesure leur bon transfert.

Pour chaque commande transfer, la fenêtre suivante apparaît, il faut cliquer sur '**Yes**' pour valider le transfert :



Après validation :

```
fsmo maintenance: transfer RID master
Server "och-lab-adds02.labs404.fr" knows about 5 roles
Schema - CN=NTDS Settings,CN=OCH-LAB-ADDS01,CN=Servers,CN=Datacenter,CN=Sites,CN=Configuration,DC=LABS404,DC=FR
Naming Master - CN=NTDS Settings,CN=OCH-LAB-ADDS01,CN=Servers,CN=Datacenter,CN=Sites,CN=Configuration,DC=LABS404,DC=FR
PDC - CN=NTDS Settings,CN=OCH-LAB-ADDS01,CN=Servers,CN=Datacenter,CN=Sites,CN=Configuration,DC=LABS404,DC=FR
RID - CN=NTDS Settings,CN=OCH-LAB-ADDS02,CN=Servers,CN=Datacenter,CN=Sites,CN=Configuration,DC=LABS404,DC=FR
Infrastructure - CN=NTDS Settings,CN=OCH-LAB-ADDS01,CN=Servers,CN=Datacenter,CN=Sites,CN=Configuration,DC=LABS404,DC=FR
```

Répéter la procédure sur chaque rôle. A la fin du processus, quitter les outils avec '**q**'.

Une nouvelle requête indique maintenant :

```
PS C:\Users\Administrator.LABS404> netdom query FSMO
Schema master          och-lab-adds02.LABS404.FR
Domain naming master   och-lab-adds02.LABS404.FR
PDC                    och-lab-adds02.LABS404.FR
RID pool manager       och-lab-adds02.LABS404.FR
Infrastructure master   och-lab-adds02.LABS404.FR
The command completed successfully.
```

En Powershell

Avec l'arrivée de Powershell, il est désormais nativement possible d'effectuer la procédure en Powershell. Cette méthode a l'avantage d'être plus rapide et de pouvoir s'exécuter depuis n'importe quel serveur AD ou du serveur d'administration.

Se connecter à la console Powershell. Vérifier qui porte les rôles :

```
netdom query FSMO
```

```
PS C:\Users\Administrator.LABS404> netdom query FSMO
Schema master           och-lab-adds02.LABS404.FR
Domain naming master    och-lab-adds02.LABS404.FR
PDC                     och-lab-adds02.LABS404.FR
RID pool manager        och-lab-adds02.LABS404.FR
Infrastructure master    och-lab-adds02.LABS404.FR
The command completed successfully.
```

Il est également possible de savoir qui porte quel rôle avec le script powershell suivant :

```
$domainControllers = Get-ADDomainController -Filter *
foreach ($dc in $domainControllers) {
    Write-Output "Name: $($dc.Name)"
    Write-Output "OperationMasterRoles:"
    foreach ($role in $dc.OperationMasterRoles) {
        Write-Output "- $role"
    }
}
```

La commande pour transférer un rôle est la suivante :

```
Move-ADDirectoryServerOperationMasterRole -Identity <NomServerDest> -OperationMasterRole
<NomDuRole>
```

Attention : En cas de transfert forcé, il faut ajouter l'opérande `-Force`. Mais cela n'aurait dû être utilisé que si l'ancien DC n'est plus disponible. La procédure par défaut est celle donnée ci-dessus.

Il y a 5 rôles à transférer, dans cet ordre là :

- RIDMaster
- SchemaMaster
- InfrastructureMaster
- DomainNamingMaster
- PDCEmulator

```
PS C:\Users\Administrator.LABS404> Move-ADDirectoryServerOperationMasterRole -Identity och-lab-ADDS01 -OperationMasterRole RIDMaster

Move Operation Master Role
Do you want to move role 'RIDMaster' to server 'och-lab-adds01.LABS404.FR' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

A la fin du transfert, il est possible d'afficher si le serveur de destination a bien hérité des rôles :

```
Get-ADDomainController -Identity <NomServeurDest> | Select-Object OperationMasterRoles -
ExpandProperty OperationMasterRoles
```

```
PS C:\Users\Administrator.LABS404> Get-ADDomainController -Identity och-lab-adds01 | select-object operationMasterRoles -ExpandProperty OperationMasterRoles | fl
SchemaMaster
DomainNamingMaster
PDCEmulator
RIDMaster
InfrastructureMaster
```

Revision #2

Created 2026-07-30 08:30:07 UTC by Olivier

Updated 2026-07-30 08:32:16 UTC by Olivier