MENU PRINCIPAL

- Page d'accueil
- **Articles et tutoriaux**
  - Windows Azure
  - Windows 2012
  - Windows 2008 / R2
  - Windows 2003 / R2
  - Windows SBS
  - PowerShell
  - Divers
- Tips
- Téléchargements
- Contact

recherche...

Localiser et déplacer les maîtres d'opérations Active Directory

Lundi, 04 Octobre 2010 00:00 Augagneur

Sommaire

Introduction

Les maîtres d'opérations peuvent être déplacés d'un contrôleur à un autre pour des raisons de performances ou de bonnes pratiques. Les cas les plus fréquents sont cependant une migration ou pire un crash d'un contrôleur. Nous allons donc voir dans un premier temps comment localiser les maîtres d'opérations dans votre infrastructure et ensuite comment les déplacer celons les différents cas de figure.

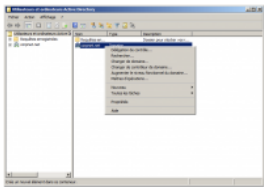
Si vous désirez plus d'information sur les maîtres d'opérations, nous vous engageons à lire notre article **Les maitres d'opérations Active Directory**.

Microsoft a également réalisé un KB très complet sur la localisation des rôles que vous pouvez consulter **ici**.

Localiser et déplacer les maîtres d'opérations par l'interface graphique

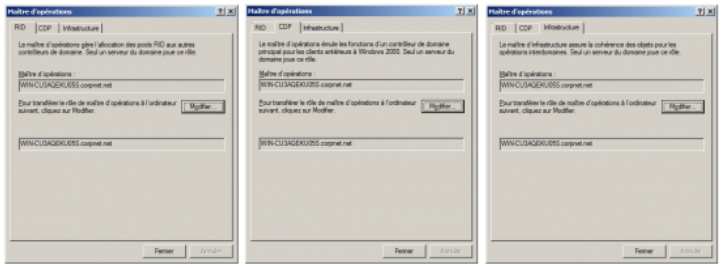
Nous allons débuter par l'utilisation de l'interface graphique pour localiser et déplacer les 5 rôles. En effet, l'interface graphique permet de réaliser les deux opérations de façon similaire. Bien entendu, les deux possibilités n'ont pas les mêmes implications cependant nous avons trouvé plus pertinent de les regrouper.

Localisons dans un premier temps les maîtres d'opérations de niveau domaine (*Maître RID*, *Maître d'infrastructure* et *émulateur PDC*) en ouvrant la mmc « **Ordinateurs et utilisateurs Active Directory** » depuis « **Démarrer** » | « **Outils d'administration** ». Réalisons ensuite un clic droit sur la racine « **[MONDOMAINE]** » et sélectionner « **Maîtres d'opérations…** ».



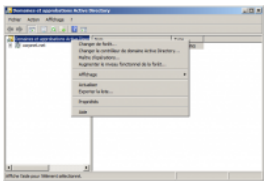
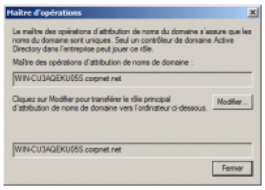
Nous avons dès lors accès à trois onglets pour chacun des rôles « **RID** », « **CPD** » et « **Infrastructure** ». Le champ « **Maître d'opérations** » indique quel est le contrôleur détenteur du rôle. Le deuxième champ indique tout simplement quel est le serveur sur lequel la console est connectée.

Nous pouvons voir également le bouton « **Modifier…** » qui permet justement de déplacer le rôle. Il faudra cependant réaliser cette action depuis le serveur devant accueillir le rôle car vous n'avez pas la possibilité de choisir un contrôleur spécifique à partir d'une liste. Le deuxième champ sert justement à identifier clairement vers quel serveur vous vous apprêtez à transférer le rôle.

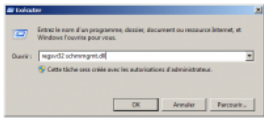


Concernant les deux autres maîtres d'opérations, de niveau forêt, il faudra accéder à deux interfaces graphiques différentes.

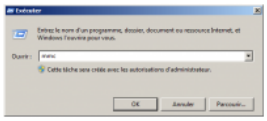
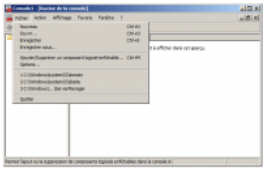
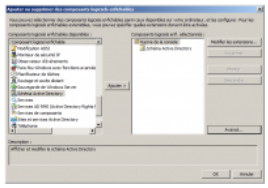
Pour localiser le *maître d'attribution de noms de domaine*, ouvrez la mmc « **Domaines et approbations Active Directory** » et sélectionnez « **Maître d'opérations…** » à l'aide d'un clic droit directement sur la racine « **Domaine et approbations Active Directory** ». La fenêtre « **Maître d'opérations** » se présente exactement sous la même forme que précédemment et « **Modifier…** » s'utilise dans les mêmes conditions.

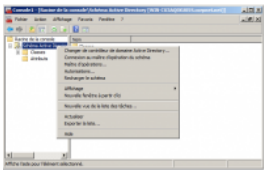
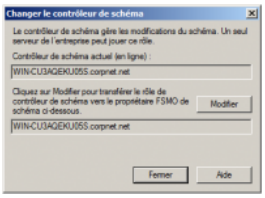
Pour le dernier maître d'opérations *Maître de schéma*, nous allons passer par la mmc « **Schéma Active Directory** », toutefois la console n'est pas disponible par défaut et il faut inscrire au préalable sa DLL. Depuis « **Executer** », lancer la commande « **regsvr32 schmmgmt.dll** ».



Une fois la commande exécutée, lançons « **mmc** » toujours à partir de « **Executer** ». Depuis *mmc*, aller dans « **Fichier** » | « **Ajouter/Supprimer un composant logiciel enfichable…** », sélectionner le composant logiciel enfichable « **Schéma Active Directory** » et cliquer sur « **Ajouter** ».

Désormais, nous avons le logiciel composant enfichable « **Schéma Active Directory** » à notre disposition. Double-cliquons sur la racine pour nous connecter sur le serveur local et accéder aux différentes propriétés. Sélectionnons « **Maître d'opérations…** » à l'aide d'un clic droit pour enfin afficher le nom du contrôleur désigné comme maître de schéma et pour en changer le cas échéant et si nécessaire.

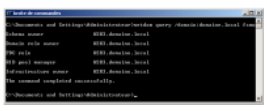



Localiser et déplacer les maîtres d'opérations par l'invite de commandes

La ligne de commande est plus efficace pour localiser rapidement les maîtres d'opérations. En effet, l'usage de l'interface graphique nécessite l'accès à trois mmc différentes et l'enregistrement d'une DLL pour obtenir ces informations alors qu'une simple commande va nous permettre d'obtenir le même résultat. Nous avons la possibilité d'utiliser par exemple l'outil *NETDOM*, *DCDIAG* ou *NTDSUTIL*.

Remarque : Les manipulations réalisées ci-dessous sont faites sur un contrôleur « W2K3 » disposant des 5 rôles pour le domaine « domaine.local ».

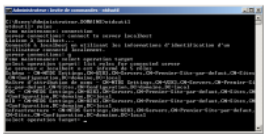
« **NETDOM** » est l'outil fournissant le résultat le plus clair. Il suffit de saisir « **netdom query /domain:[MONDOMAINE] fsmo** » à partir de l'invite de commandes pour obtenir la liste des maîtres d'opérations et les serveurs associés.



Pour « **DCDIAG** » il suffira de lancer depuis l'invite de commandes « **dcdiag /test:KnowsOfRoleHolders /v** » et d'analyser le résultat au niveau de *Démarrage du test : KnowsOfRoleHolders*. Pour chaque rôle vous avez le *CN* du serveur détenant les rôles après *CN=NTDS Settings*.

« **NTDSUTIL** » est un peu plus complexe étant l'outil de maintenance Active Directory alors que *DCDIAG* n'est, quant à lui, qu'un outil d'analyse. Nous allons commencer par lancer la commande « **ntdsutil** » depuis l'invite de commandes. Ensuite il faudra saisir séquentiellement les commandes suivantes :

roles
connection
connect to server [MONSERVEUR]
quit
select operation target
list roles for connected server

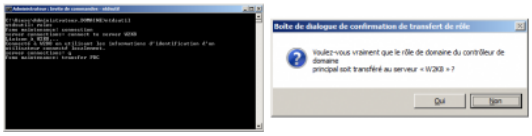


Nous obtenons donc un résultat similaire à celui fourni par *DCDIAG* grâce à la commande « **list roles for connected server** ».

Remarque : Les manipulations réalisées ci-dessous sont faites sur un contrôleur « W2K8 » en liaison avec un contrôleur « W2K3 » disposant des 5 rôles pour le domaine « domaine.local ».

Pour déplacer les maîtres d'opérations depuis l'invite de commande, nous n'aurons pas d'autres choix que d'utiliser « **NTDSUTIL** ». Pour transférer un rôle, il faudra, comme à travers la mmc, se connecter sur le serveur qui l'accueillera et saisir les commandes suivantes :

roles
connection
connect to server [MONSERVEUR]
quit
transfer PDC
transfer RID master
transfer infrastructure master
transfer naming master
transfer schema master



A chaque transfert, une demande de confirmation apparaîtra sous la forme d'un popup.

Forcer le déplacement des maîtres d'opérations

On parle en général de *saisir* les maîtres d'opérations ou encore plus communément on utilise le terme de *seize*. Cela correspond à forcer le transfert des rôles sans prévenir le contrôleur détenteur parce qu'il n'est pas possible de le faire autrement. En effet, quand un transfert des maîtres d'opérations est réalisé entre deux contrôleurs, le nouveau contrôleur prévient l'ancien contrôleur qu'il est désormais le maître d'opérations. Lorsqu'on réalise une opération de saisie des rôles, le nouveau contrôleur maître ne préviendra pas son homologue. Ce genre de manipulation est réalisé dans le cadre d'une avarie grave et irréparable d'un maître d'opération, qui n'étant plus joignable, ne peut réaliser le transfert des rôles dans un cadre normal.

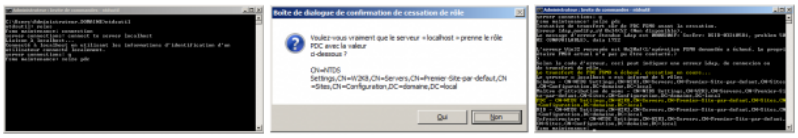
ATTENTION !!! Lorsque les maîtres d'opérations sont saisis, il ne faut en aucun cas que le l'ancien contrôleur maître ressurgisse sur le domaine. En effet, n'étant pas au courant de cette saisie de rôles, ceci pourrait entraîner de lourdes conséquences.

Remarque : Les manipulations réalisées ci-dessous sont faites sur un contrôleur « W2K3 » disposant des 5 rôles et un contrôleur « W2K8 » qui va en prendre possession. Le domaine est « domaine.local ».

La saisie est réalisée par le biais de la commande « **NTDSUTIL** ». Lançons donc la commande « **ntdsutil** » depuis l'invite de commandes et exécutons les commandes suivantes :

roles
connection
connect to server [MONSERVEUR]
quit
seize PDC
seize RID master
seize infrastructure master
seize naming master
seize schema master

A chaque demande de saisie, « **NTDSUTIL** » essayera toujours dans un premier temps de transférer si possible chaque rôle. En toute logique, cela échoue est génère une erreur car la prise de rôles forcée est liée à l'impossibilité de les transférer simplement donc ne tenez pas compte de l'erreur du type *problem 502*. Vous aurez également un popup qui apparaîtra pour valider la prise de rôle. Enfin, réalisez une vérification sur la saisie des rôles à l'aide de la commande « **list roles for connected server** ».



Une saisie des rôles induit donc qu'un contrôleur n'a pu être rétrogradé. Malgré son absence physique au sein de votre infrastructure, il est cependant toujours présent dans la base Active Directory. Nous aurons donc besoin de le supprimer manuellement de la base Active Directory une fois les rôles transférés. Cette opération s'appelle *metadata cleanup* et est détaillé dans un article Microsoft à votre disposition **ici**.

Conclusion

Nous avons donc vu dans cet article comme localiser et déplacer les maîtres d'opérations qui servira de point de départ à un prochain article sur les règles de placement pour assurer un fonctionnement optimal de votre annuaire Active Directory.

Mise à jour le Dimanche, 15 Mai 2011 17:31

COMMENTAIRES

#1 16-03-2011 09:00 **+ 1**

Bonjour,

Un grand merci pour l'ensemble des vos articles, très claires.
Il ne maque plus qu'un exemple de répartition des rôles.

Les maîtres d'opérations peuvent être déplacés d'un contrôleur à un autre pour des raisons de performances ou de bonnes pratiques :

Pour 2 DC (2008-2003) dans 1 seule domaine, quelle sont les bonnes pratiques pour la répartition des rôles, en plus que les 2 DC seront catalogue global ?.

Cordialement.

#2 26-05-2011 14:21 **+ 2**

Merci pour cet article très clair (ainsi que tous les autres de votre site...)
Peut-être une amélioration possible : lorsqu'il s'agit de lancer la commande
regsvr32 schmmgmt.dll
il faut le faire dans un cmd avec droits d'administration, au risque de recevoir un message d'erreur...

Merci encore ! Michel

#3 29-02-2012 02:06 **0**

Article élaboré avec un grand professionnalisme et une limpidité d'informaticiens perspicaces et talentueux.

Grand merci pour ce travail précieux et intéressant.

#4 26-10-2012 08:11 **0**

Bonjour,
Suite à l'installation d'un active directory "secondaire" sur un windows 2008 R2, je me demandais si ce tutoriel permettait bien de switcher et donc de mettre mon 2008 en "maitre", et donc a terme de se séparé de mon 2003 actuellement "maitre".
d'autre réalisation sont elles a effectué ? si oui lesquelles ?

Merci de votre futur réponse et du travail réalisé sur vos tutoriel.

Rafraîchir la liste des commentaires

AJOUTER UN COMMENTAIRE

Nom (obligatoire)

Adresse email (obligatoire)

Rafraîchir

Enregistrer

JComments