Information sur les rôles FSMO et migration de ces derniers

Cette petite fiche concerne les rôles FSMO d'active Directory et leurs utilités.

Cette documentation est réalisée dans le cadre d'un TP guidé, il peut donc y avoir d'autre méthode plus ou moins simple pour y parvenir. Pour mieux s'y retrouver cette documentation disposera de plusieurs screenshots illustrant les consignes.

Les rôles FSMO (Flexible Single Master Operation)

● Dans AD, il existe 5 maîtres d’opération.
● Les contrôleurs FSMO endossent une fonction particulière
● Certaines tâches doivent être centralisées.
● Il peut exister un FSMO par domaine ou par forêt.
● Par défaut, AD attribue les rôles FSMO au premier contrôleur de domaine
● Il est fortement conseillé de rétrograder un CD avant de le supprimer du domaine surtout si c’est le premier installé (le transfert des rôles FSMO se fait alors automatiquement)

5 types de rôles dans AD

1. Maître de schéma (Schema Master)
2. Maître d’attribution de noms de domaine (Domain Naming Master)
3. Maître RID (RID Master)
4. Émulateur PDC (PDC Emulator)
5. Maître d’infrastructure (Infrastructure Master)

Maître de schéma (Schema Master)

1. Unique dans une forêt
2. Gère la structure AD (le schéma)

3. Le Schéma ne peut être modifier que sur le serveur qui a ce rôle
4. Il est ensuite répliqué sur les autres DC
5. Exemple : Exchange modifie le schéma AD
6. En cas d'indisponibilité : Impossible de modifier le schéma

Maître d'attribution de noms de domaine (Domain Naming Master)

1. Unique dans une forêt
2. Gère l'attribution de noms de domaines
3. Le maître d'opération de nom de domaine est en charge d'attribuer les nouveaux noms de domaines aux contrôleurs de domaine.
4. Dès que vous lancez DCPROMO pour créer un nouveau domaine, DCPROMO s'arrête et localise le FSMO attribution de nom de domaine afin de vérifier que le nouveau domaine n'existe pas
5. Si le nouveau contrôleur ne joint pas le maitre d'opération de nom de domaine, il refuse de continuer l'installation
6. En cas d'indisponibilité : Impossible d'ajouter ou de modifier un nom de domaine

Maître RID (RID Master)

1. 1 par domaine
2. Chaque objet possède un SID sous la forme :
    1. S-1-5-21-D1-D2-D3-RID
3. D1-D2-D3 sont 3 nombres de 32 bits gérés aléatoirement à l'installation du domaines et ne bougent pas, tous les SID dans un domaine sont identiques à l'exception des derniers 32 bits appelés RID
4. Si un DC a besoin de générer un nouveau SID, il connaît d'avance la première partie et n'a besoin que d'un RID.
5. Par défaut le maître du pool des ID relatifs délivre 500 RID à chaque DC
6. Les CD rechargent leur pool dès qu'ils ont utilisé 250 RID
7. En cas d'indisponibilité : Pas d'effet immédiat, puis quand le pool est vide, impossible de créer de nouveaux objets

Émulateur PDC (PDC Emulator)

1. 1 par domaine
2. Gère globalement la sécurité :
    1. Synchronise les modifications des stratégies de groupe du domaine (éviter les conflits et les écrasements)
    2. Synchroniser les horloges sur les DC (les jetons d'authentifications utilise un horodatage)
    3. Synchronise les verrouillages des comptes
    4. Synchronise les mots de passe
3. En cas d'indisponibilité : pas de changement de mot de passe, pas de verrouillage de compte, pas de modifications de GPO

Maître d'infrastructure (Infrastructure Master)

1. 1 par domaine
2. Dans un réseau multi-domaine, il est difficile de répercuter rapidement les modifications de comptes utilisateurs ou de groupes sur les différents domaines.
3. Vous pouvez placer un utilisateur dans un groupe d'un autre domaine mais cette modification

peut prendre un certain temps.
4. Le maître d'infrastructure accélère ce processus : il maintient une sorte de table de référence : Utilisateur du domaine formation.test fait parti d'un groupe du domaine production.test
5. En cas d'indisponibilité : lenteurs de réplication inter-domaine, impossibilité de faire des corrélations inter-domaine

Savoir ou sont les rôles FSMO

```
netdom query fsmo
```

Transfert en Powershell des rôles d'un serveur à un autre

```
Move-ADDirectoryServerOperationMasterRole -Identity "SRVAD02" -
OperationMasterRole
SchemaMaster,DomainNamingMaster,PDCEmulator,RIDMaster,InfrastructureMaster
```