Migration Active Directory

Windows Server 2012 à 2022

# Prérequis :

Windows Server 2012 :

* Niveau fonctionnel du domaine et de la forêt 2008 minimum (voir Annexe au besoin)

Windows Server 2022 :

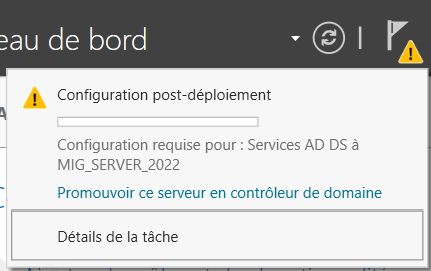
* Joint au domaine avec un nom différent
* Connecté au compte Administrateur du domaine
* Services ADDS installés

Dans cet exemple, on migre le domaine test.lan depuis Mig\_Server\_2012 vers Mig\_Server\_2022

# Migration du domaine :

## Server 2022 comme contrôleur secondaire

Promouvoir le nouveau serveur comme contrôleur du domaine déjà existant.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

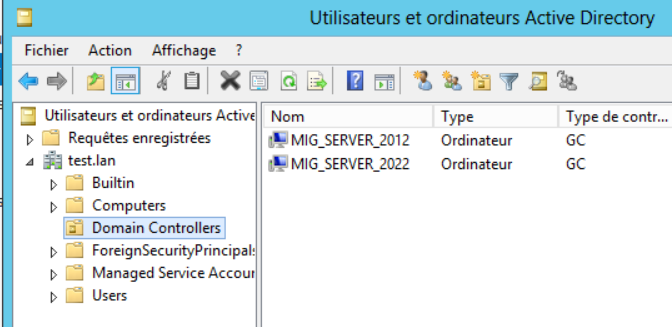
Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

Si une erreur de type « Incompatibilité avec FRS » apparaît, se référer à l’annexe. Si tout est prêt pour la configuration, ce message est visible avant le début de l’installation :



Après redémarrage du serveur, on peut repérer le nouveau contrôleur de domaine dans la console de gestion des utilisateurs et ordinateurs Active Directory :



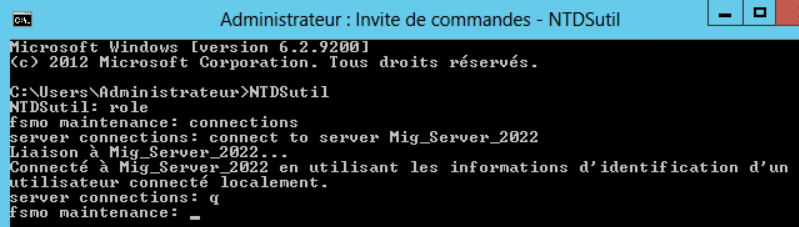
## Transfert des rôles FSMO

Le contrôleur de domaine utilise 5 rôles dits FSMO, qu’il faut déplacer, sinon il sera impossible de rétrograder l’ancien serveur.

Les 5 rôles sont :

* **Contrôleur de schéma** : le contrôleur qui a ce rôle a la charge de la gestion et de la modification du schéma du domaine
* **Maitre d’attribution des noms de domaines** : le contrôleur qui a ce rôle a la charge de l’attribution des noms de domaines, ses le serveur DNS référant dans la forêt.
* **Maitre RID** : le contrôleur qui a ce rôle est en charge de la distribution des RID qui composent les SID (identifiant unique pour les objets). Le maitre RID est en charge de la distribution de pool de RID aux différents contrôleurs de domaine.
* **Maître d’infrastructure** : le contrôleur qui a ce rôle a la charge de la réplication et des liens entre plusieurs domaines.
* **Emulateur PDC** : le contrôleur qui a ce rôle est en charge de plusieurs missions, notamment : modification des stratégies de groupes, synchronisation des horloges entre les tous les contrôleurs de domaine, gestion des verrouillages des comptes, changements des mots de passe, assurer les compatibilités entre les différents contrôleurs de domaines.

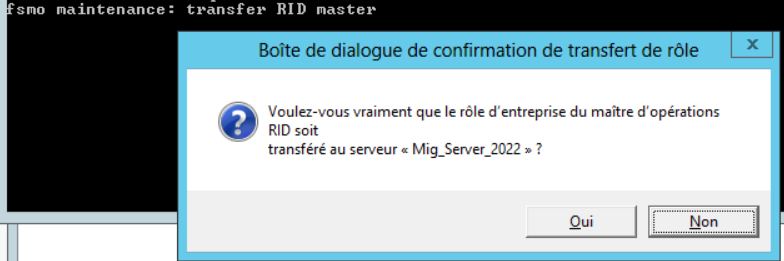
La passation des rôles se fait avec l’utilitaire DOS ntdsutil, **depuis le serveur initial** en administrateur :



Remplacer Mig\_Server\_2022 par le nom du serveur de destination

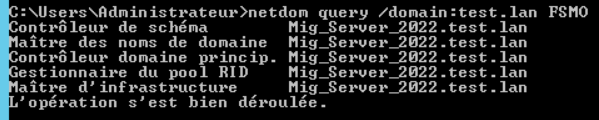
Transférer les 5 rôles explicités précédemment :

* transfer RID master
* transfer infrastructure master
* transfer schema master
* transfer naming master
* transfer pdc



Enfin, quitter l’outil en entrant 2 fois **q**.

On peut vérifier que tous les rôles ont bien été transférés :



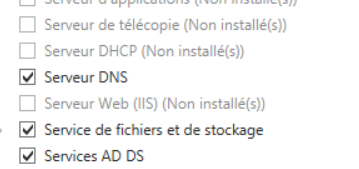
## Retirer l’ancien contrôleur

À cette étape, il faut bien migrer les autres rôles de l’ancien contrôleur de domaine, en particulier les DNS :

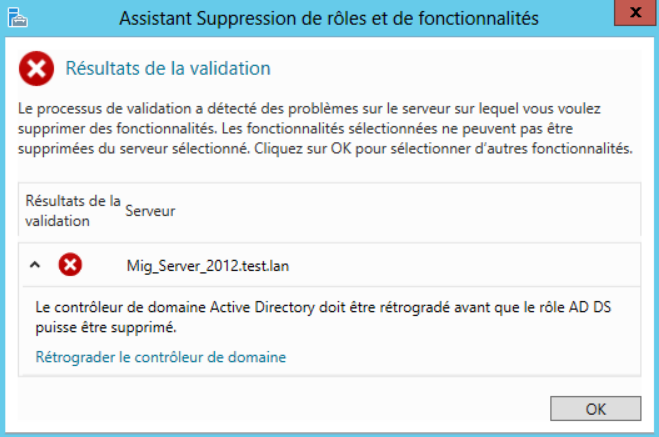
* Modifier les paramètres DHCP pour pointer vers le nouveau serveur
* Modifier les DNS du nouveau serveur en 127.0.0.1
* Modifier les DNS de l’ancien serveur vers l’IP du nouveau serveur
* Modifier toutes les éventuelles configurations statiques

Et vérifier que tous les services fonctionnent toujours comme d’habitude. La dernière étape est irréversible, corriger toute erreur avant de passer à la suite.

Depuis le Gestionnaire de Serveur, retirer la fonctionnalité AD DS de l’ancien serveur :

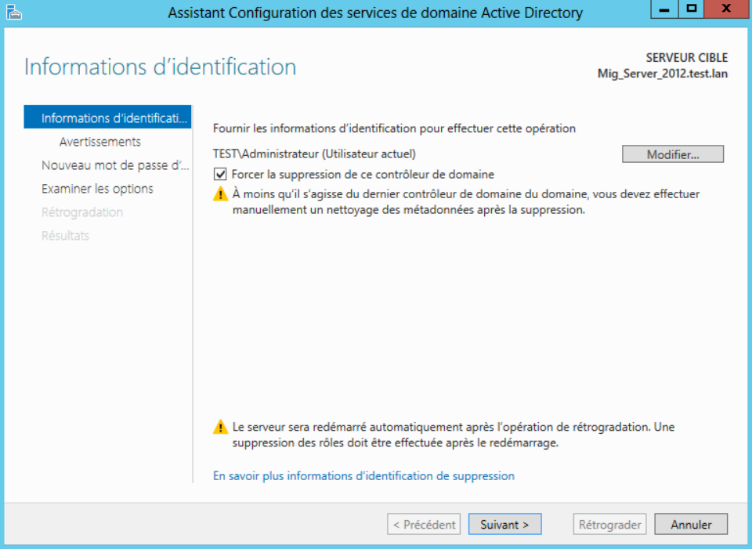
Gérer > Supprimer des rôles ou fonctionnalités… 

L’assistant invite automatiquement à rétrograder le contrôleur de domaine avant de poursuivre.

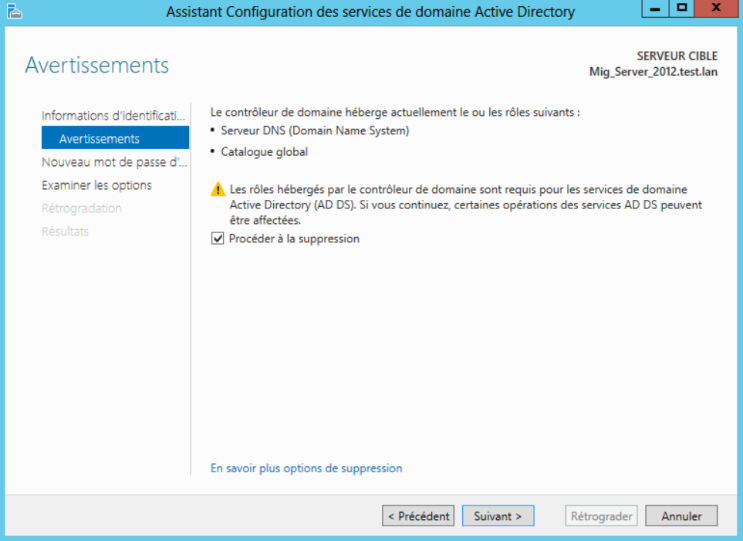


Suivez les indications, en cochant les cases nécessaires :

Forcer la suppression de ce contrôleur de domaine



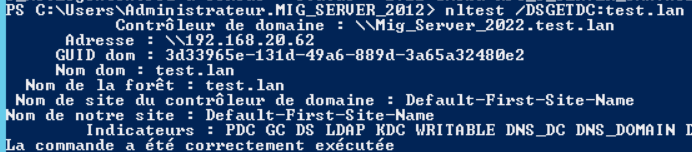
Procéder à la suppression (avec un rappel sur les services interrompus, à vérifier)



Et indiquer le mot de passe d’Administrateur local qui sera affecté au serveur à la suite de sa rétrogradation.

Une fois le serveur redémarré, on peut vérifier que le nouveau serveur est bien le contrôleur de domaine actif :

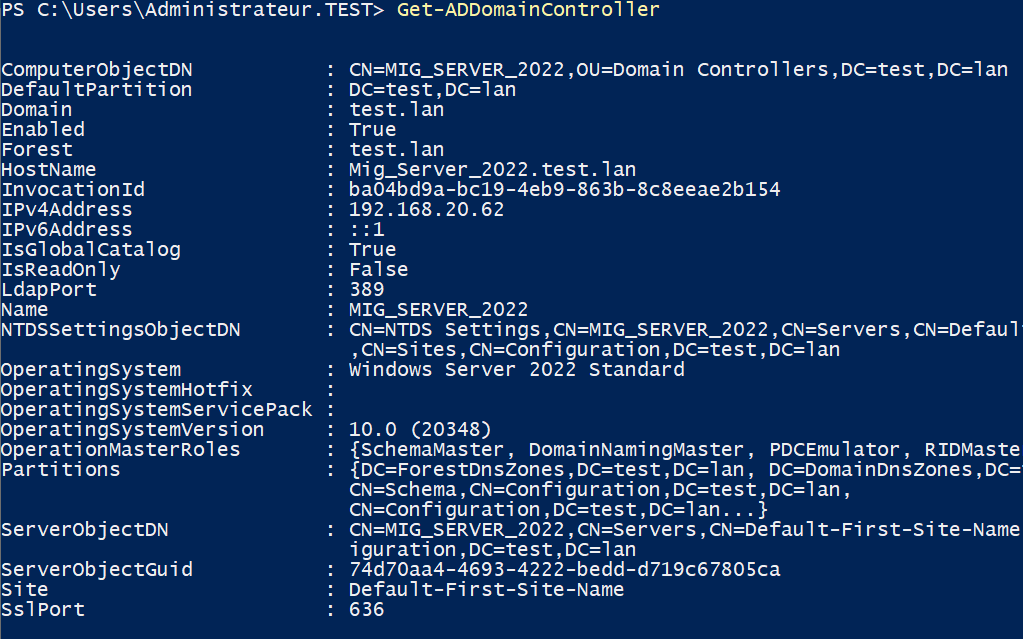
Sur l’ancien serveur



Une image contenant texte, capture d’écran, Police, information

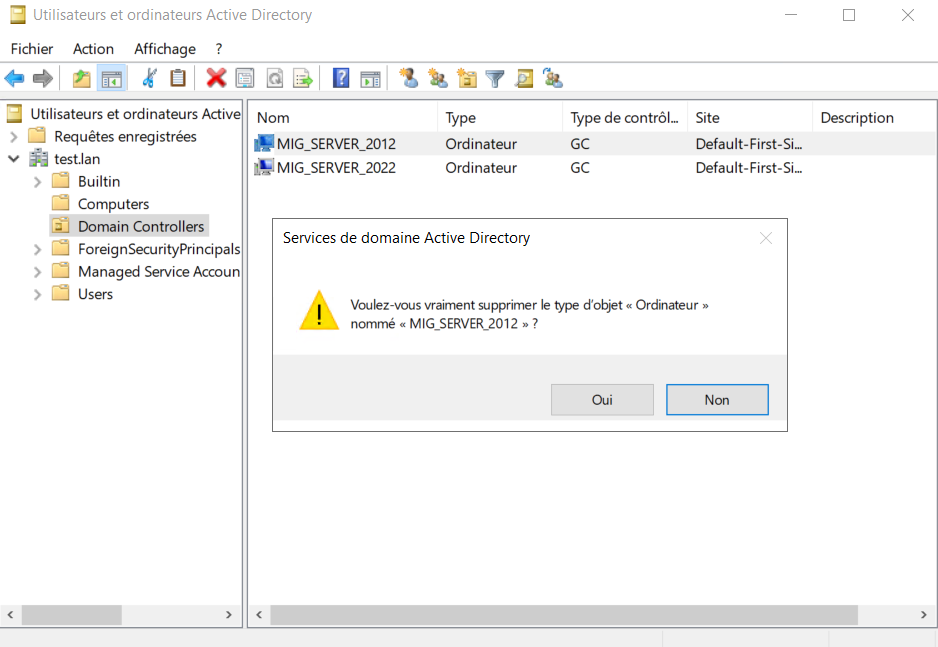
Description générée automatiquement

Sur le nouveau serveur

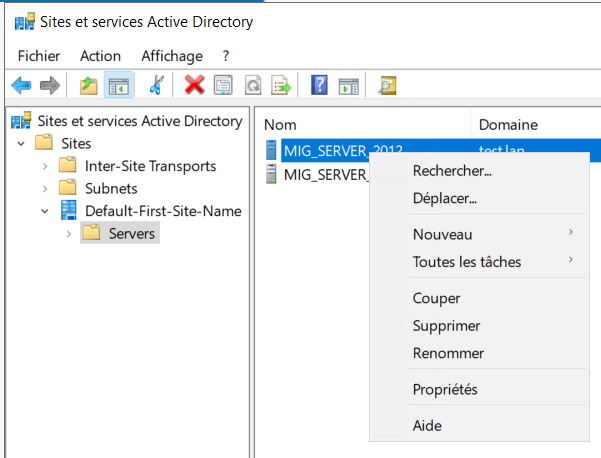


Pour finir, on peut supprimer toute trace de l’ancien serveur :

Supprimer le serveur depuis la console Utilisateurs et ordinateurs Active Directory



Puis depuis la console Sites et services Active Directory



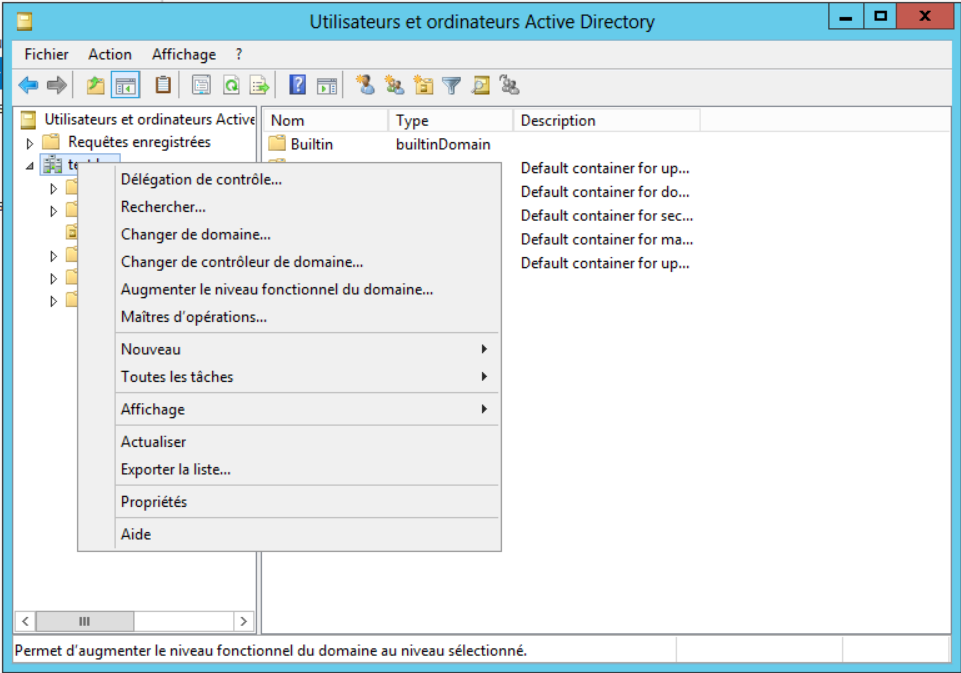
Finalement, on peut promouvoir le niveau fonctionnel du domaine et de la forêt si besoin (voir annexe)

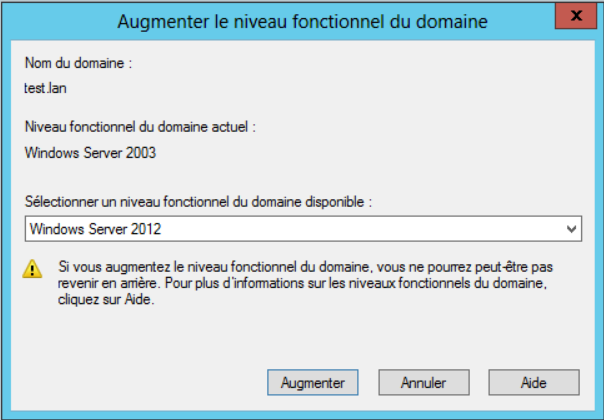
# Annexes

## Promouvoir le niveau fonctionnel du domaine et de la forêt

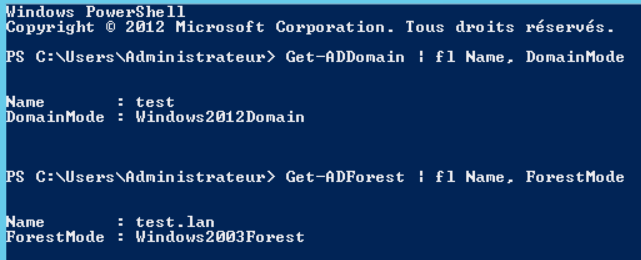
Le niveau fonctionnel de la forêt ne peut pas être supérieur à celui du domaine. Il faut donc commencer par augmenter le domaine, puis la forêt.

Depuis la console Utilisateurs et ordinateurs Active Directory, initier l’augmentation du niveau fonctionnel du domaine :

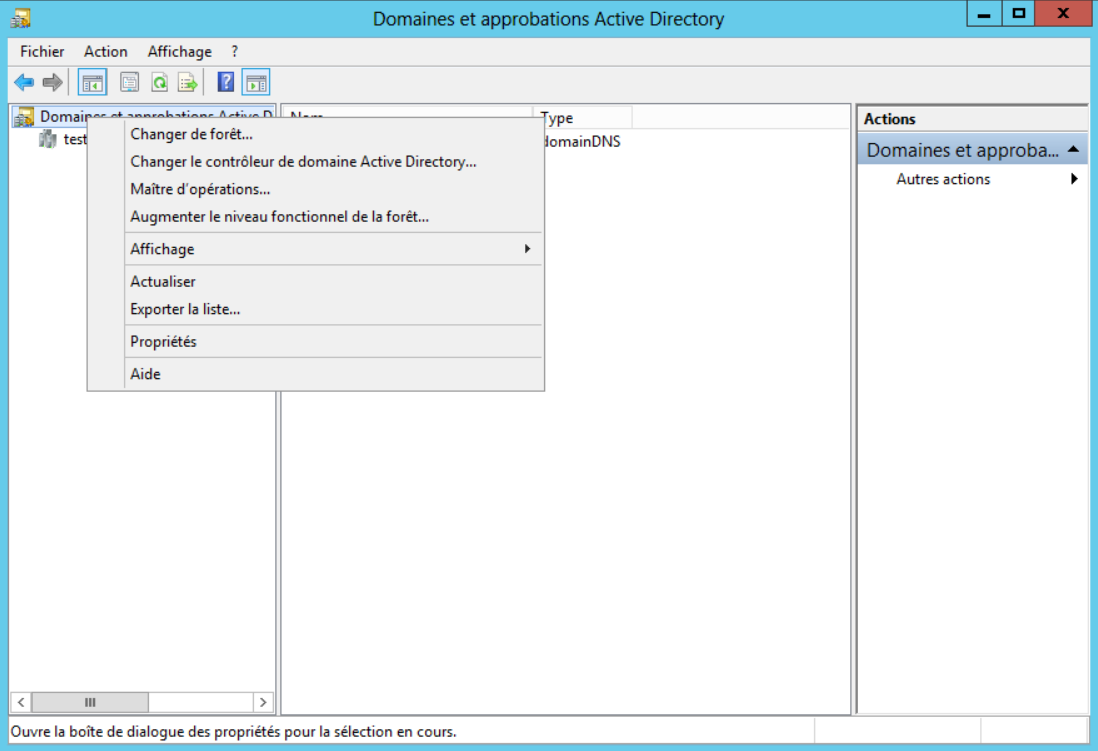




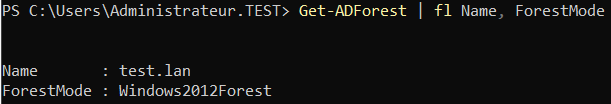
Vérifier que le niveau souhaité est atteint :



Depuis la console Domaines et approbations Active Directory, initier l’augmentation du niveau fonctionnel de la forêt :



Vérifier que le niveau souhaité est atteint :



Lorsque le niveau fonctionnel du domaine est mis à niveau, le mot de passe du compte système **krbtgt** est automatiquement modifié. Si vous avez un serveur Exchange sur site dans votre domaine, il peut s'arrêter en raison de problèmes d'authentification. Après avoir mis à jour le DFL, il faut redémarrer le service Kerberos Key Distribution Center (KDC) sur tous les contrôleurs de domaine :



## Migrer Sysvol de FRS à DFSR

<https://www.it-connect.fr/active-directory-migrer-sysvol-de-frs-a-dfsr/>