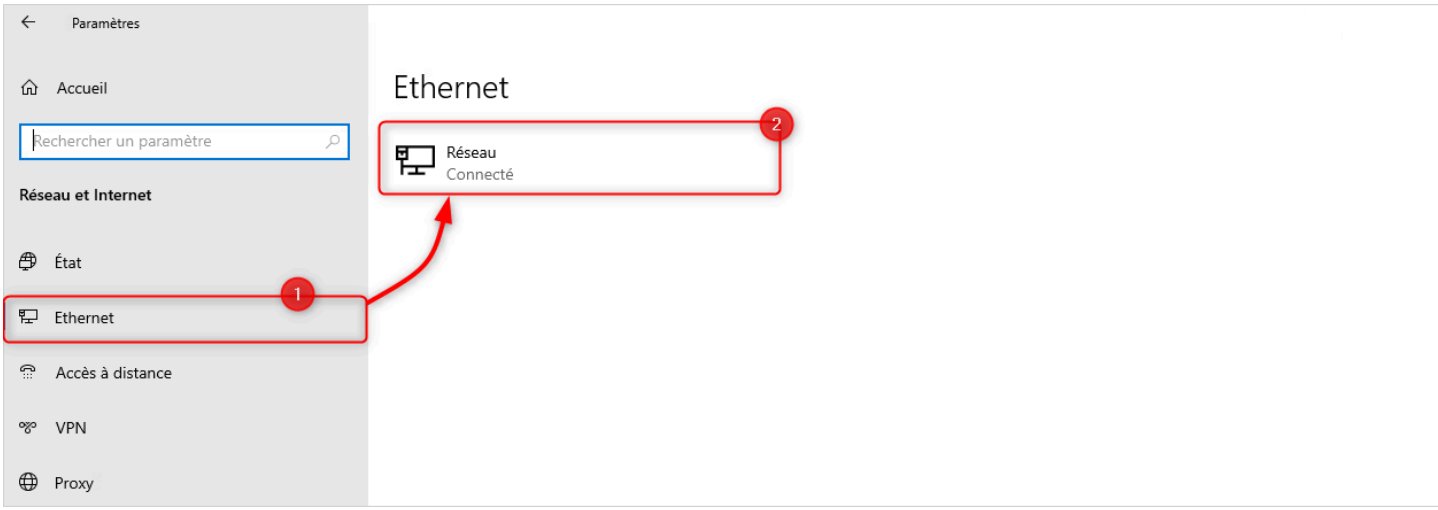
Mairie de Bidart

Documentation AD / DNS

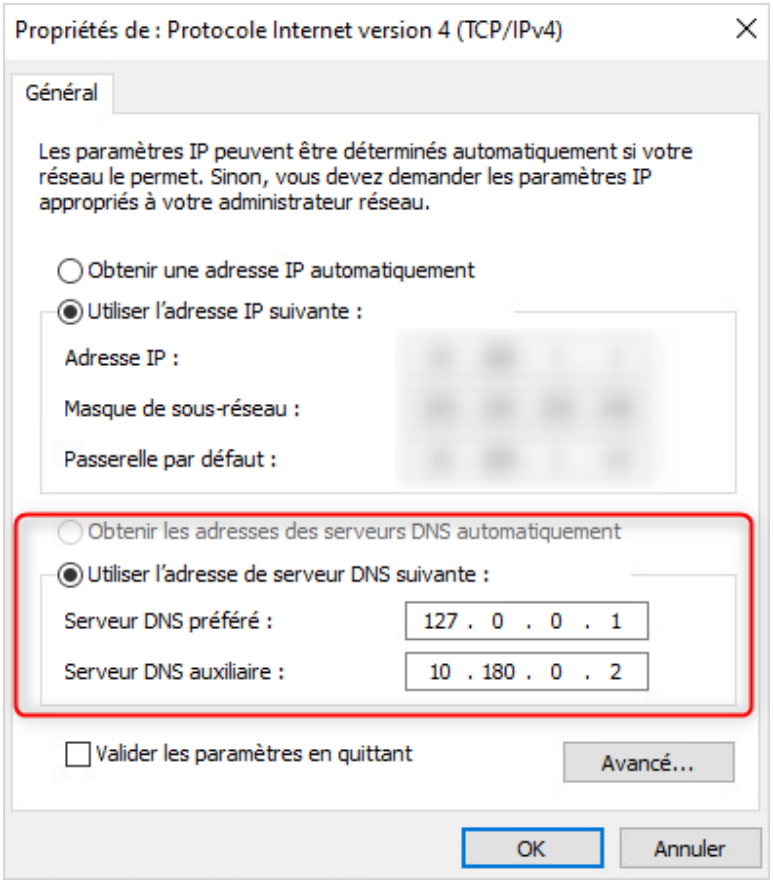


Réseau : Configuration requise

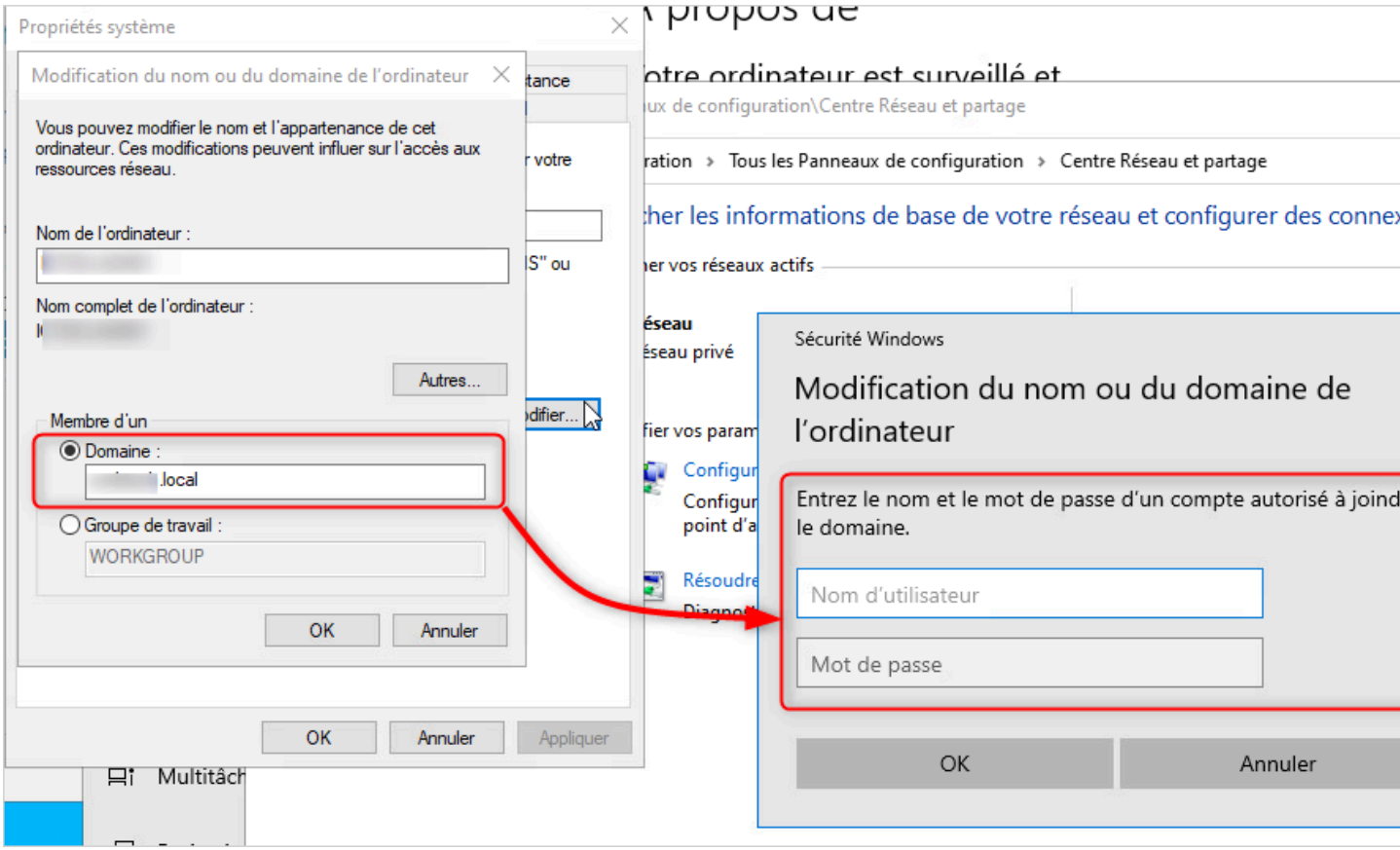
Afin de communiquer avec les contrôleurs de domaines existants, il est nécessaire de spécifier l'adresse d'un des contrôleur de domaine dans les paramètres DNS afin de résoudre le domaine local (par exemple : vemotech.local).

Nous allons aller dans les **Paramètres Windows > Réseau et Internet > Ethernet**. Sélectionnez la carte réseau (NIC) du serveur.

Dans la section "Paramètres IP (IPv4)". Cliquez sur le bouton "Modifier" :



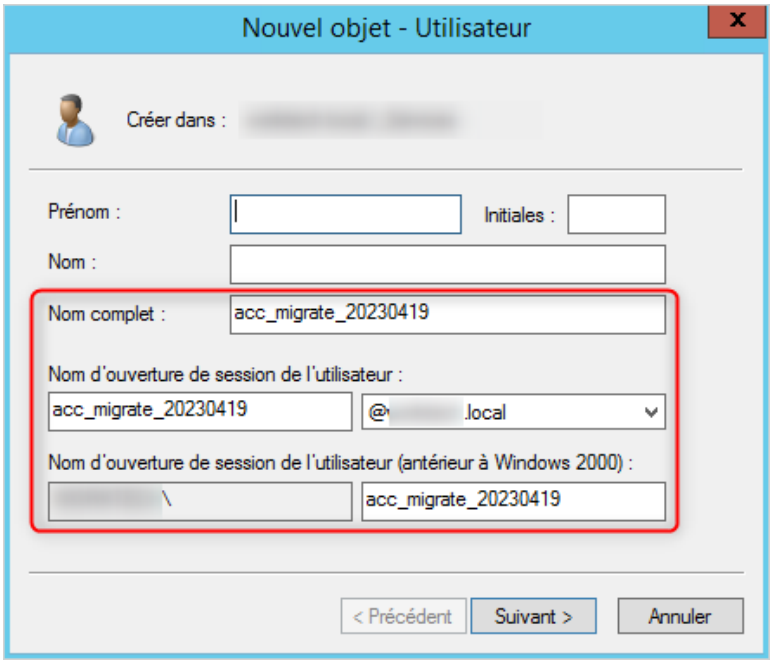
Garder comme DNS primaire 127.0.0.1 (car le Windows Server actuel sera un nouveau contrôleur de domaine se basant sur son propre serveur DNS). Spécifier comme DNS secondaire un des contrôleur de domaine dans la forêt AD.



Joindre le Windows Server à l'Active Directory

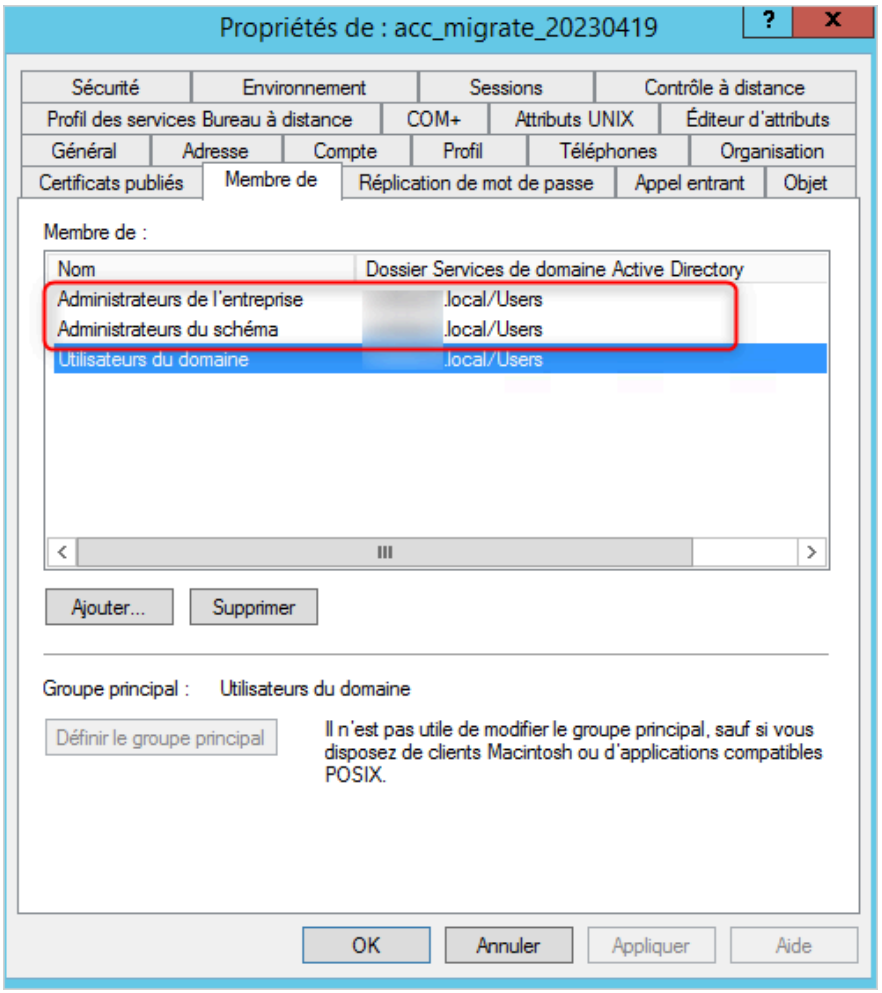
Il est nécessaire de joindre la machine à l'Active Directory existant de l'entreprise. Pour cela, aller dans **Panneau de Configurations > Système**. Dans Paramètres Avancées, renommez le PC.

Sélectionnez la case "Domaine", dans "Membre d'un" :



Le domaine doit être écrit au format **domain.local** afin d'être résolus par les contrôleurs de domaines locaux via les serveurs DNS spécifiés sur la machine.

Spécifiez le compte Administrateur du domaine au format **DOMAIN\Administrateur**.



Création d'un compte de migration dédié

Si comme dans le cadre de ce tutoriel, vous souhaitez mettre à jour la version du schéma (contrôleur de domaine existant antérieure à Windows Server 2019). Nous allons créer un compte dédié afin de réaliser cette opération (nom de compte exemple : acc_migrate_20230419).

Le compte qui a été spécifié doit faire partir des groupes suivants :

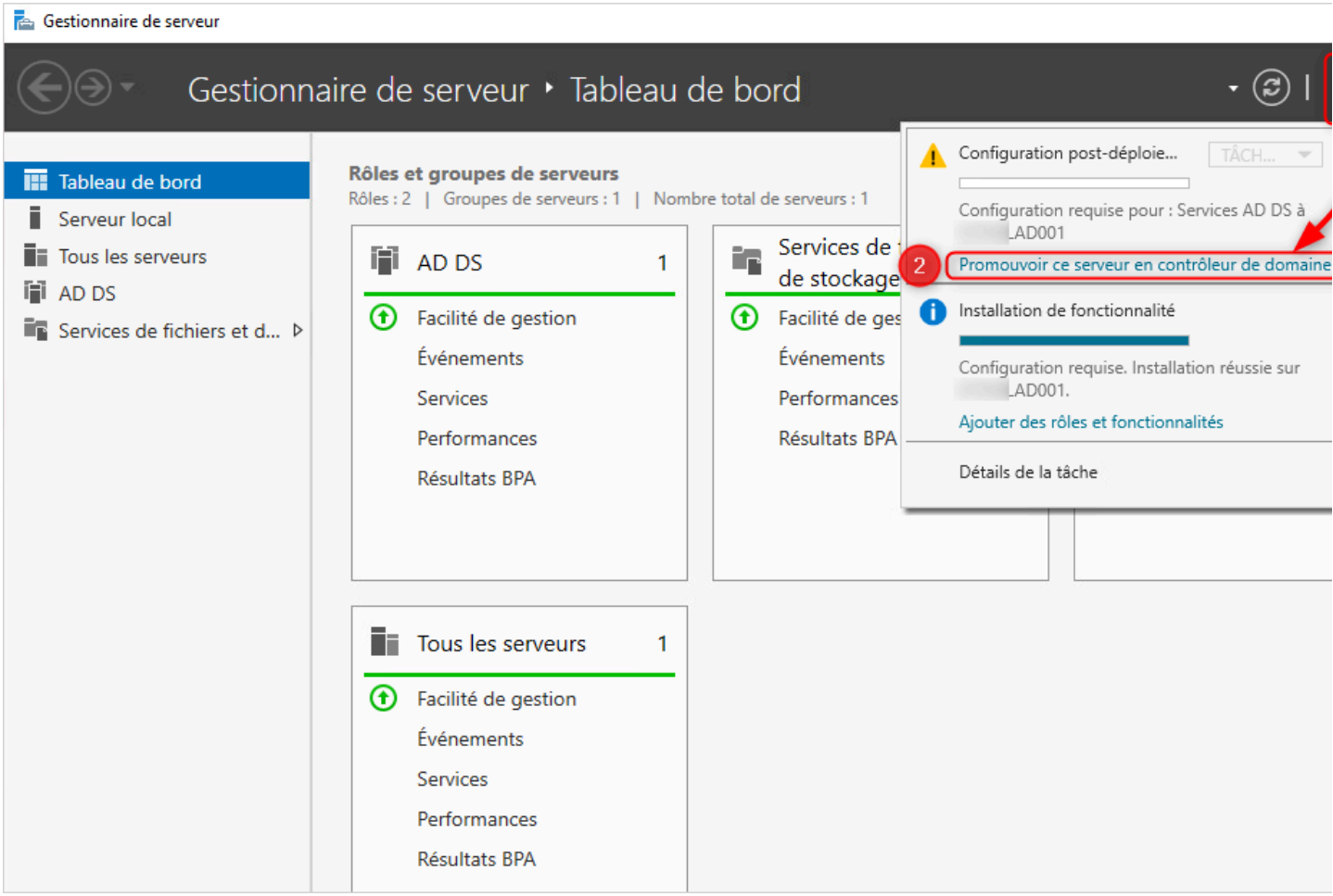
- Administrateurs de l'entreprise,
- Administrateurs du schéma.

Supprimez une fois la migration effectuée, de ce compte dédié.

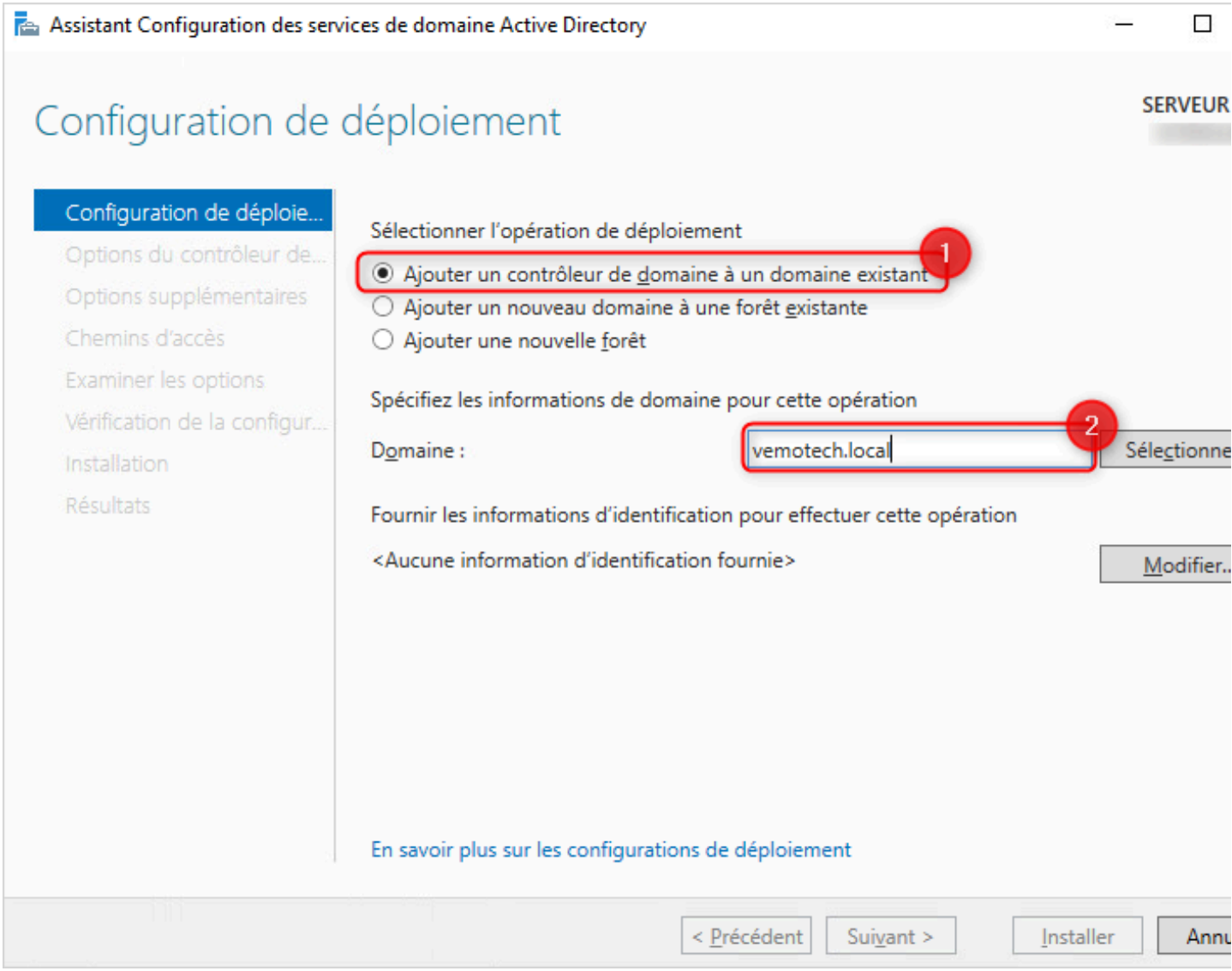
Ajouter un contrôleur de domaine à une forêt existante

Le processus de migration d'un contrôleur de domaine à une forêt existante (un domaine Active Directory) commence par l'ajout d'un nouveau serveur de domaine Active Directory.

Dans le Gestionnaire de serveur, une configuration supplémentaire est requise pour le rôle "AD DS" cliquez sur "Promouvoir de serveur en contrôleur de domaine".

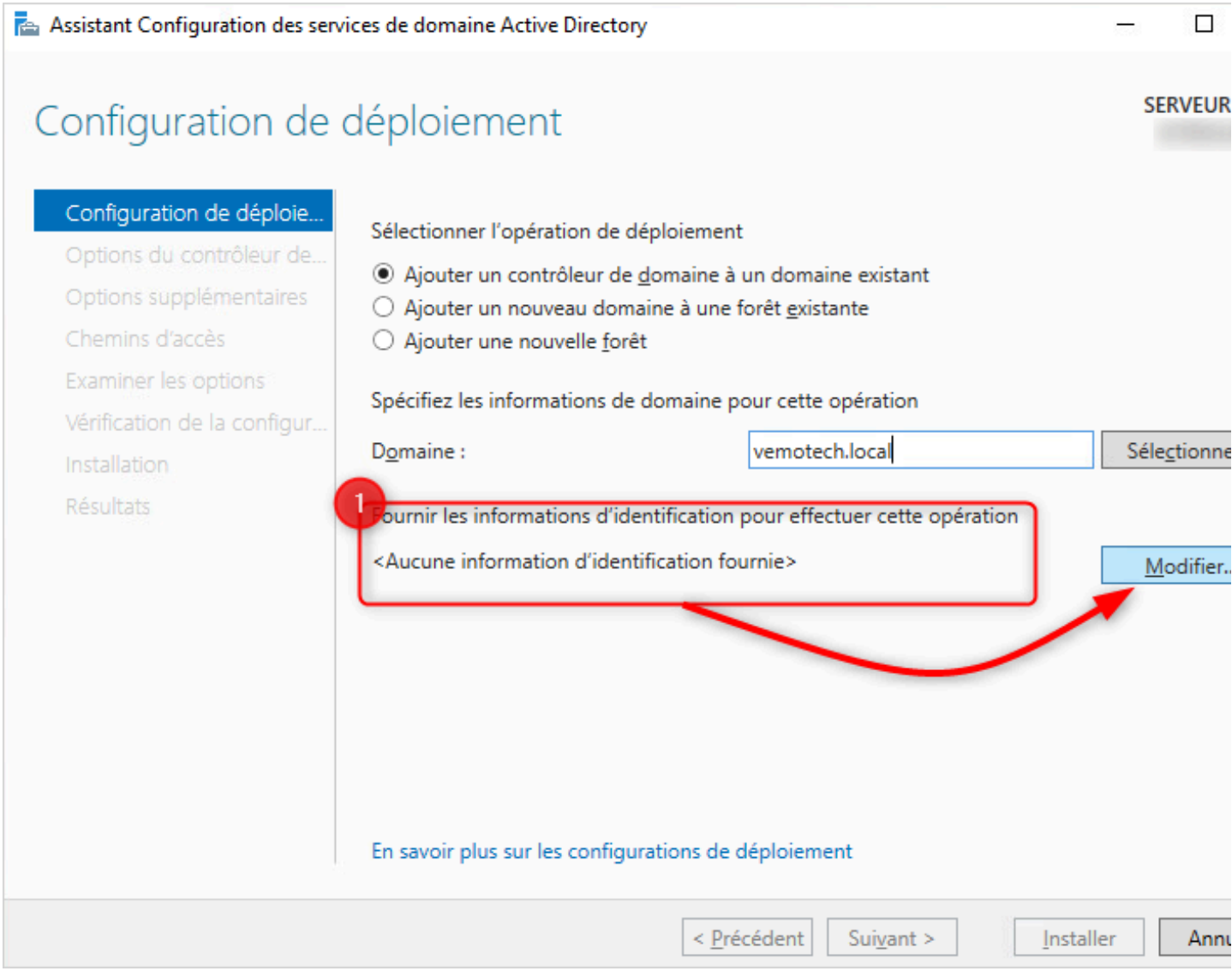


Un assistant s'ouvre. Sélectionnez "Ajouter un contrôleur de domaine à un domaine existant" afin de créer un nouveau domaine Active Directory lors des options de déploiement du contrôleur de domaine. Renseignez ensuite le domaine où le contrôleur de domaine souhaite s'y ajouter :

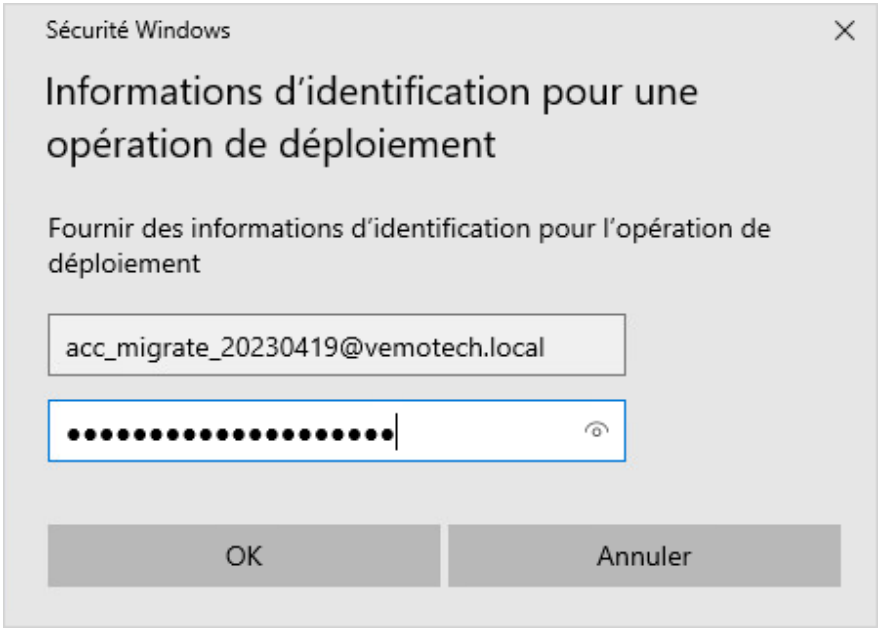


Une fois le domaine renseigné, fournir les informations d'identification destinées à se connecter au domaine Active Directory :

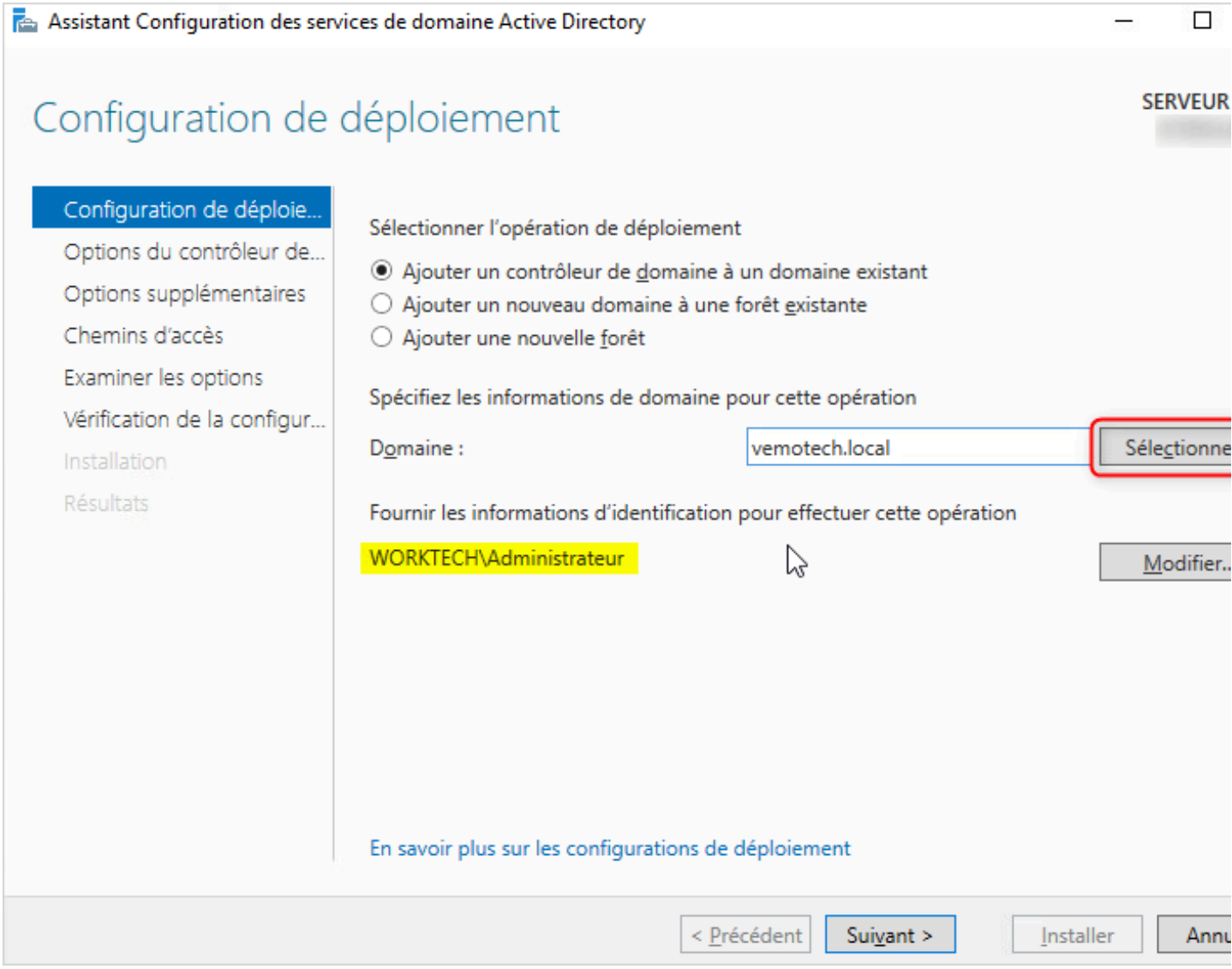
Le format de l'utilisateur doit être user@domain.local.



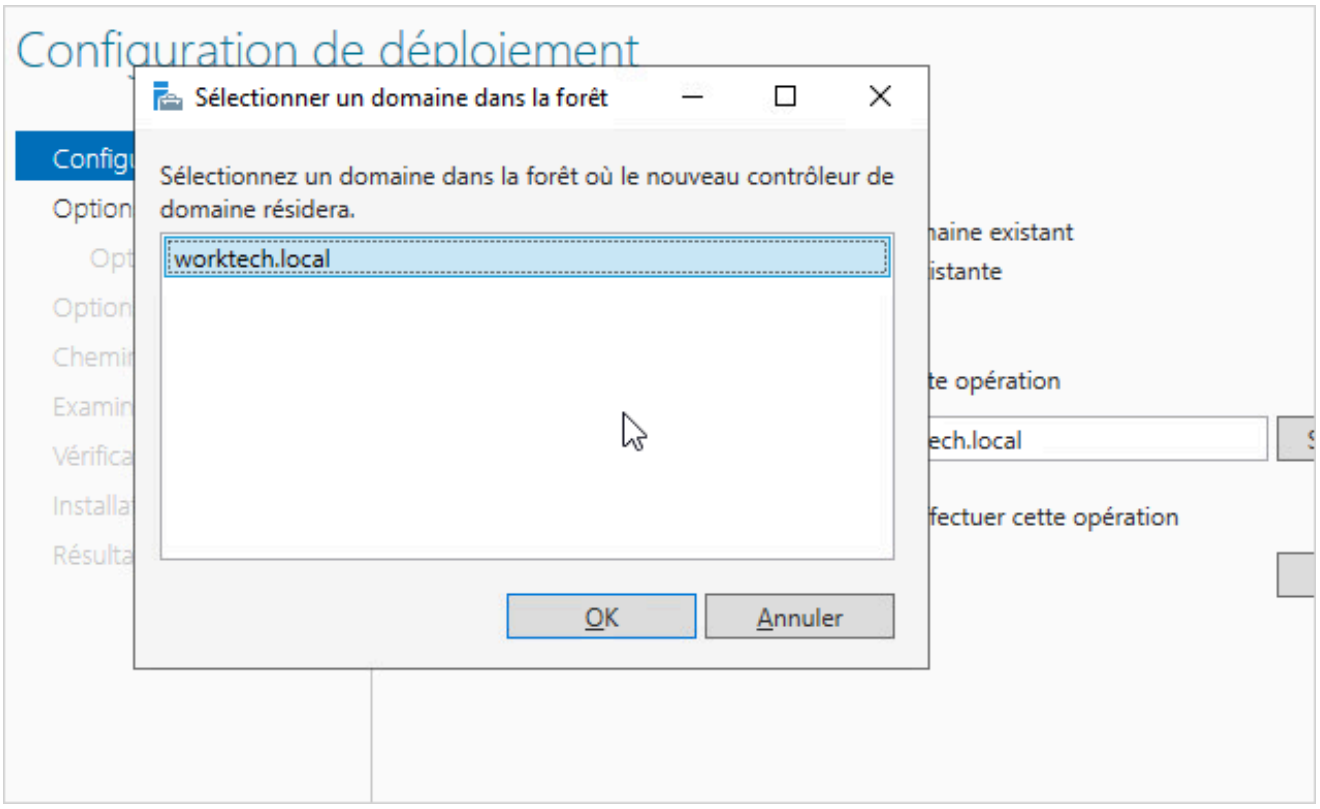
Spécifiez sous la forme compte@domain.local le compte de service avec les droits spécifiés dans les prérequis :



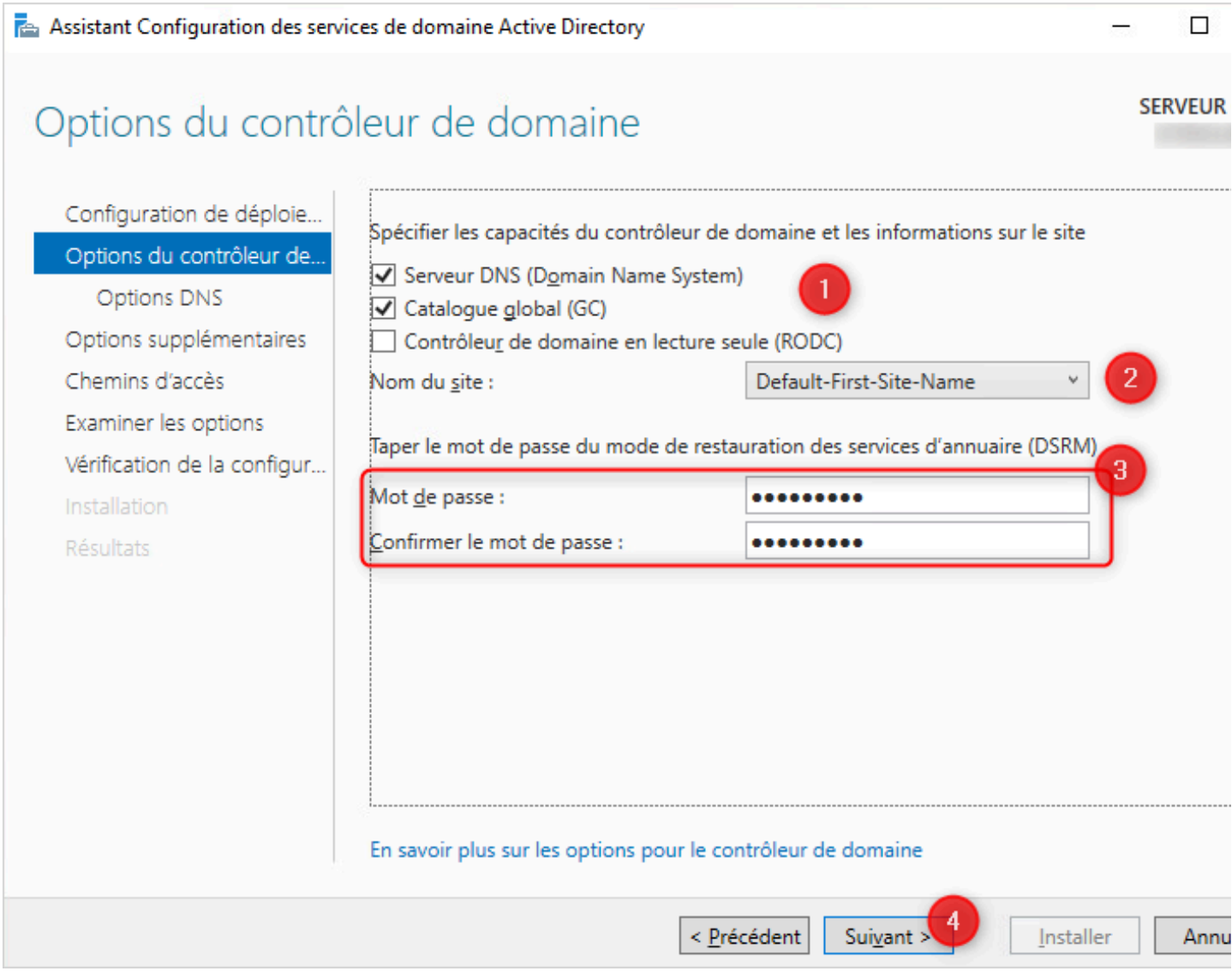
Une fois les informations spécifiées, cliquez sur le bouton "Sélectionner" pour choisir le domaine récupéré :



Sélectionnez le domaine récupéré, puis cliquez sur OK :

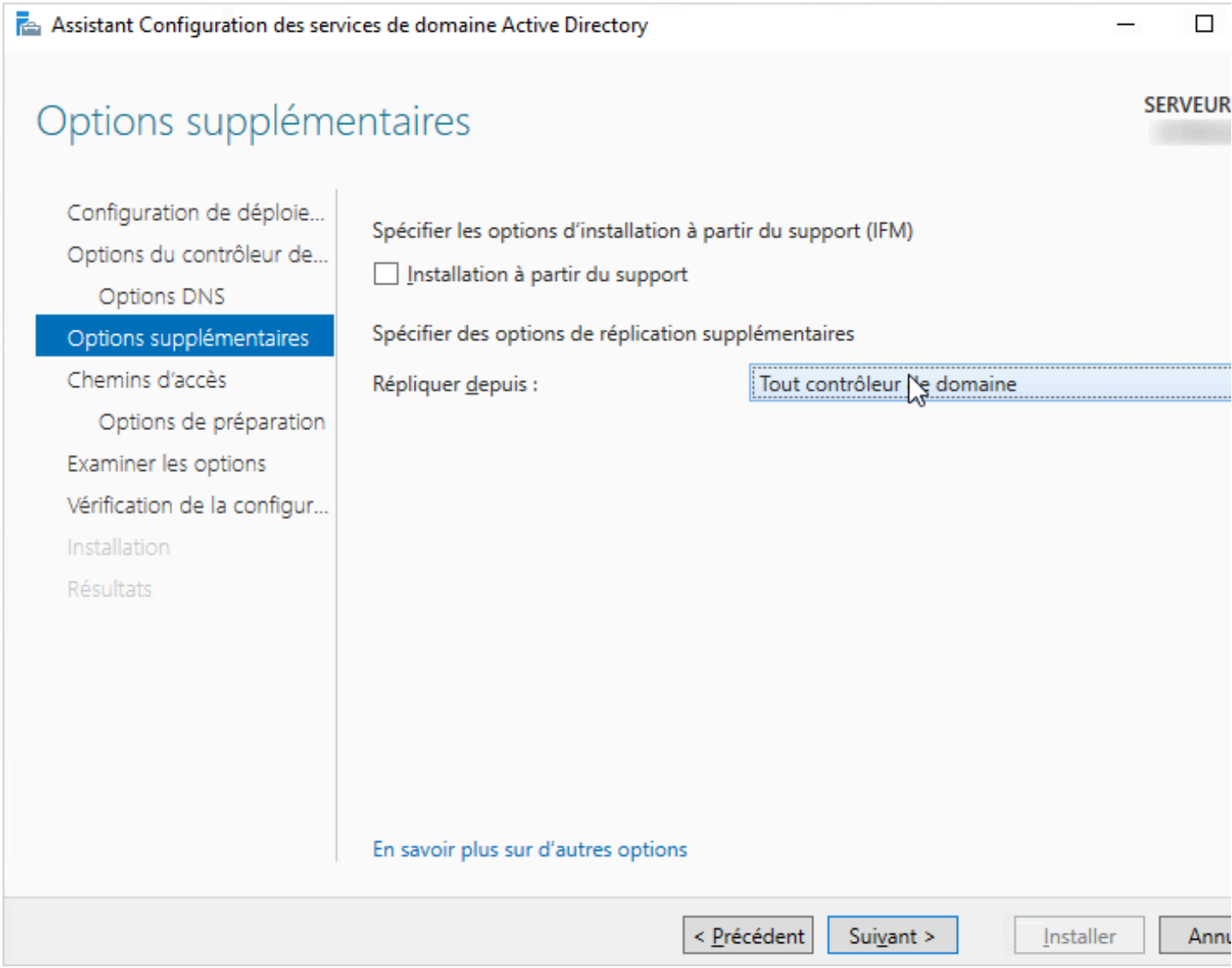


Cliquez ensuite sur "Suivant" afin de poursuivre l'assistant de configuration. Ici, vous spécifiez les capacités du nouveau contrôleur de domaine. Par défaut, il fera office de serveur DNS et catalogue global. Gardez ces options par défaut :

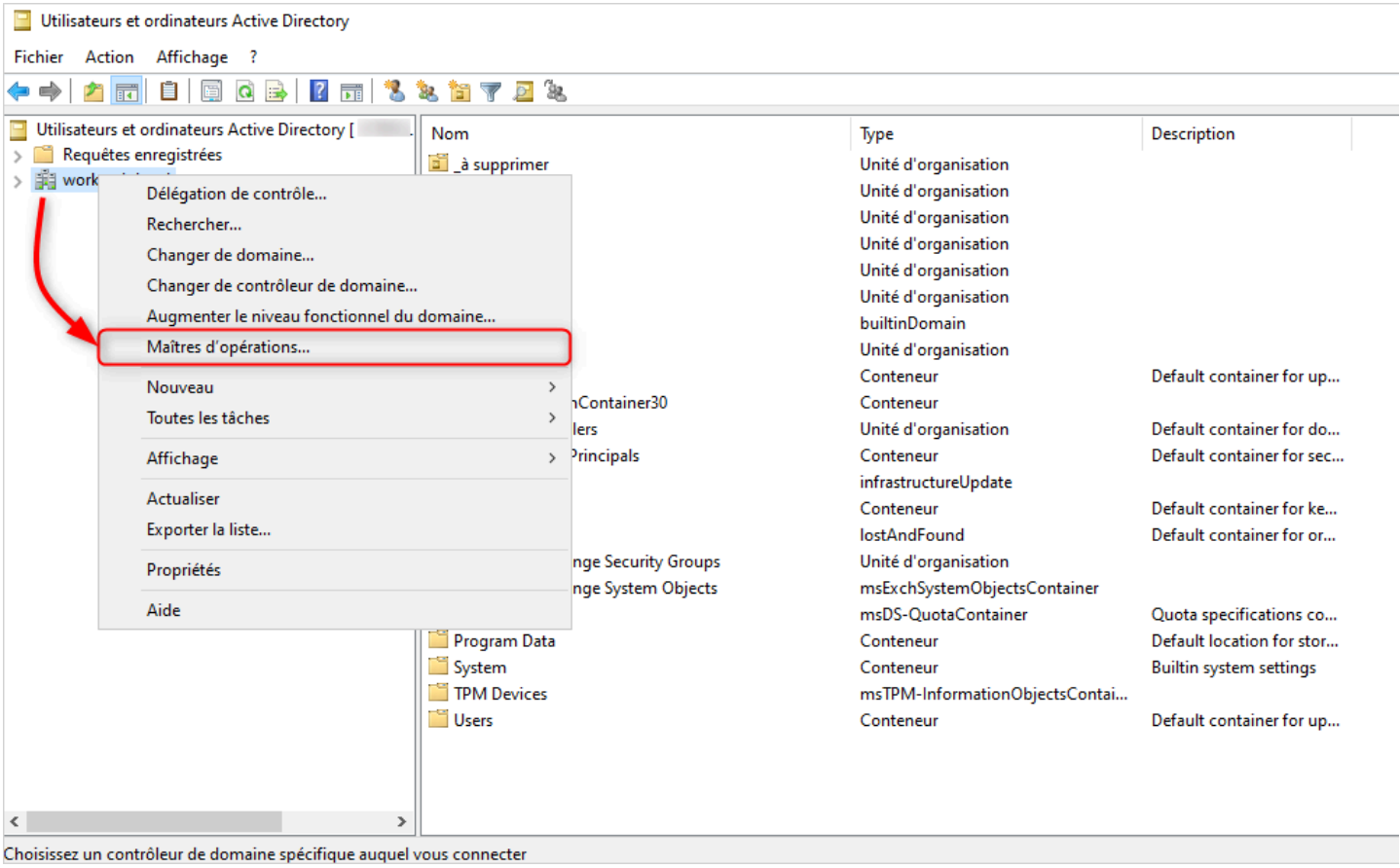


Vous pouvez, en fonction de vos besoins, garder ce nouveau contrôleur de domaine en lecture seule uniquement. Renseignez le mot de passe d'accès au service de restauration (de lecture) de l'annuaire AD.

Répliquez ensuite le nouveau DC sur les contrôleurs de domaine existants :



Valider les écrans successifs, puis confirmez l'installation en cliquant sur "Installer".

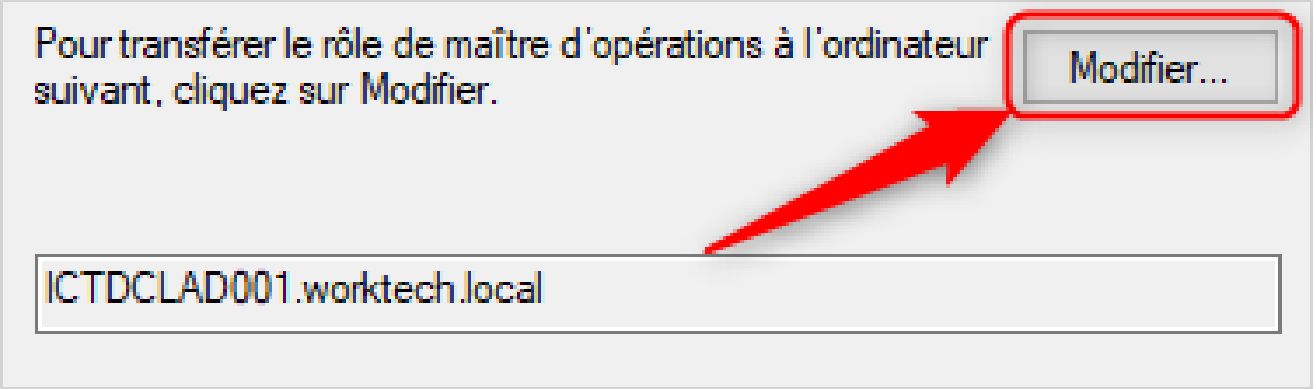

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active Directory [
Requêtes enregistrées
Délégation de contrôle...
Rechercher...
Changer de domaine...
Changer de contrôleur de domaine...
Augmenter le niveau fonctionnel du domaine...
Maîtres d'opérations...
Nouveau
Toutes les tâches
Affichage
Actualiser
Exporter la liste...
Propriétés
Aide
Nom
Type
Description
_à supprimer
Unité d'organisation
builtinDomain
Conteneur
Default container for up...
Unité d'organisation
Default container for do...
Default container for sec...
infrastructureUpdate
Default container for ke...
lostAndFound
Default container for or...
msExchSystemObjectsContainer
msDS-QuotaContainer
Quota specifications co...
Program Data
Default location for stor...
System
Builtin system settings
TPM Devices
msTPM-InformationObjectsContai...
Users
Default container for up...
Choisissez un contrôleur de domaine spécifique auquel vous connecter

Maîtres d'opérations (FSMO)

Notre nouveau contrôleur de domaine a été intégré dans notre domaine et est un contrôleur de domaine Active Directory. Cependant, étant donné que notre migration s'étend sur une version du contrôleur de domaine assez vielle (Windows Server 2012 R2), il ne sera pas possible d'augmenter directement le niveau fonctionnel du domaine.

Constat du problème

À l'aide d'un Invite de commande ou PowerShell, on souhaite récupérer le contrôleur de domaine primaire :




```
PS C:\Users\antoine> netdom query fsmoSchema master
DC-WS2K12.vemotech.localDomain naming master   DC-WS2K12.vemotech.localPDC
DC-WS2K12.vemotech.localRID pool manager       DC-WS2K12.vemotech.localInfrastructure
master  DC-WS2K12.vemotech.localThe command completed successfully.
```

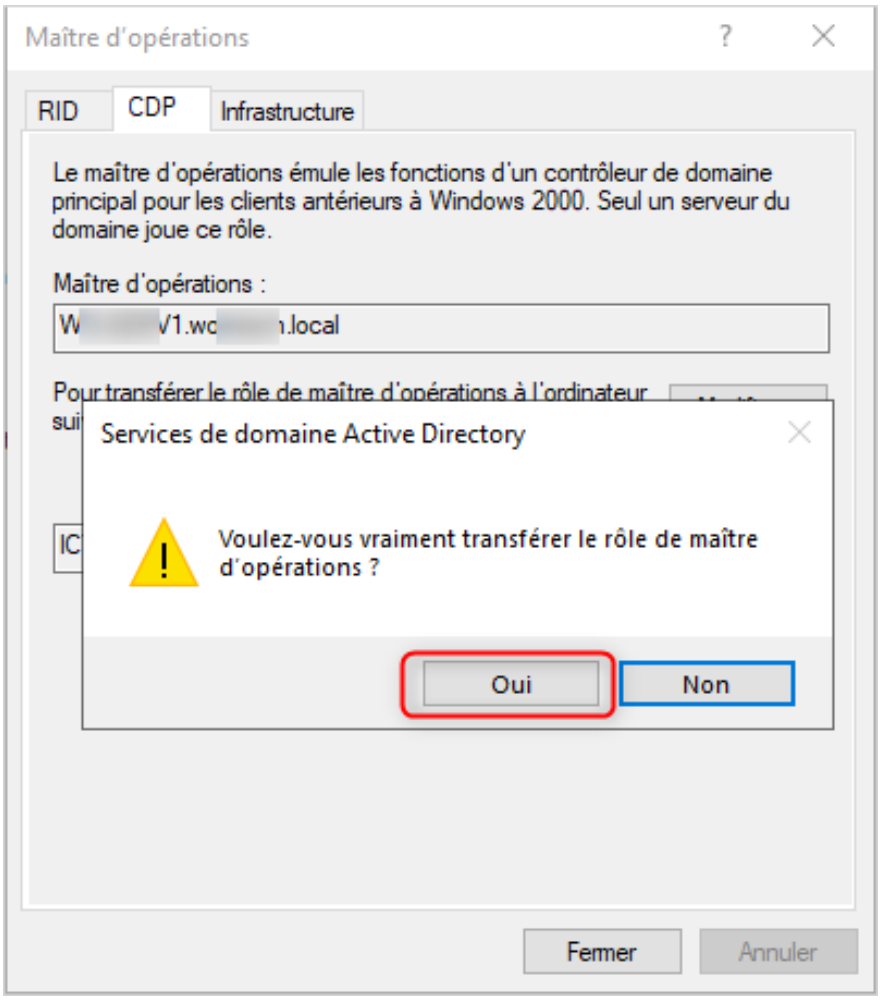
La commande netdom query fsmo décrit le contrôleur de domaine primaire au domaine Active Directory et nous remarquons ainsi que notre "ancien" contrôleur de domaine occupe tous les rôles essentiels (ici : DC-WS2K12.vemotech.local).

Remédiation

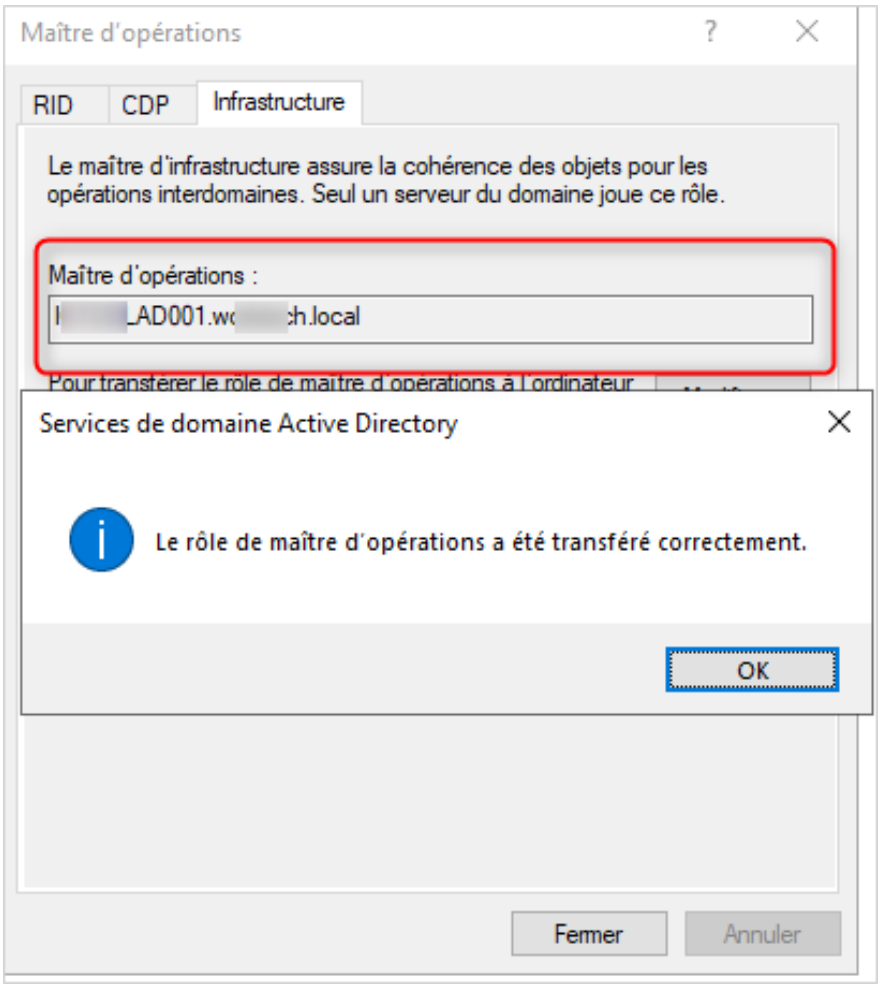
Il est ici question de modifier les maîtres d'opération. C'est une action qui définit le contrôleur primaire du domaine. Actuellement, sans notre cas, il s'agit du Windows Server 2012 R2.

Utilisateurs et ordinateurs Active Directory

Dans un premier temps, sur le nouveau contrôleur de domaine (Windows Server 2022), veuillez ouvrir la console "Utilisateurs et ordinateurs Active Directory" ou actionnez les touches Windows + R (Exécuter), puis saisir : dsa.msc. Vous obtenez une vue complète de votre annuaire LDAP Active Directory :



Sélectionnez le domaine (XXX.local) dans la colonne de gauche, puis effectuez un clic droit > "Maîtres d'opérations".

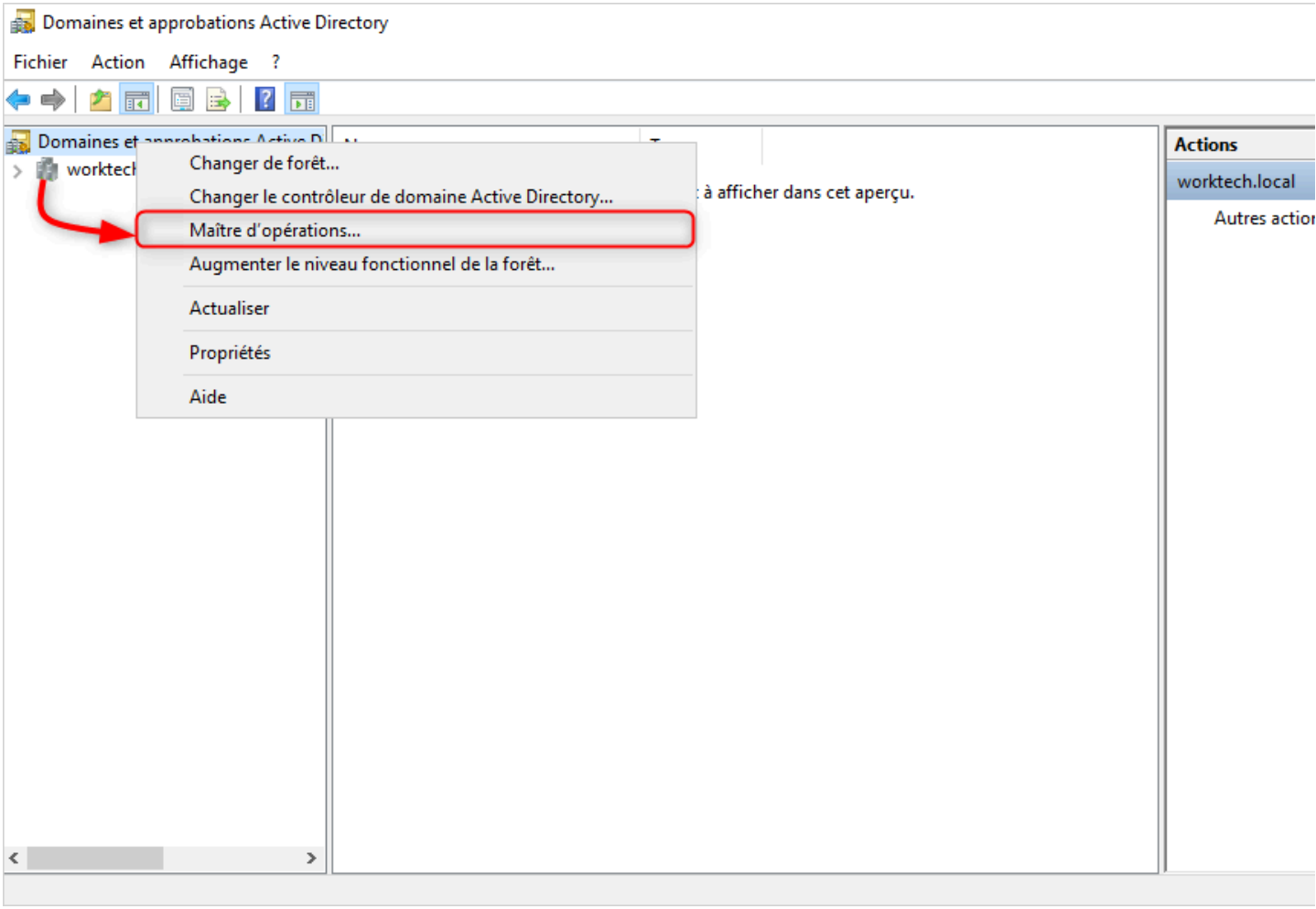


Il est question ici de réaliser un transfert des trois niveaux suivants :

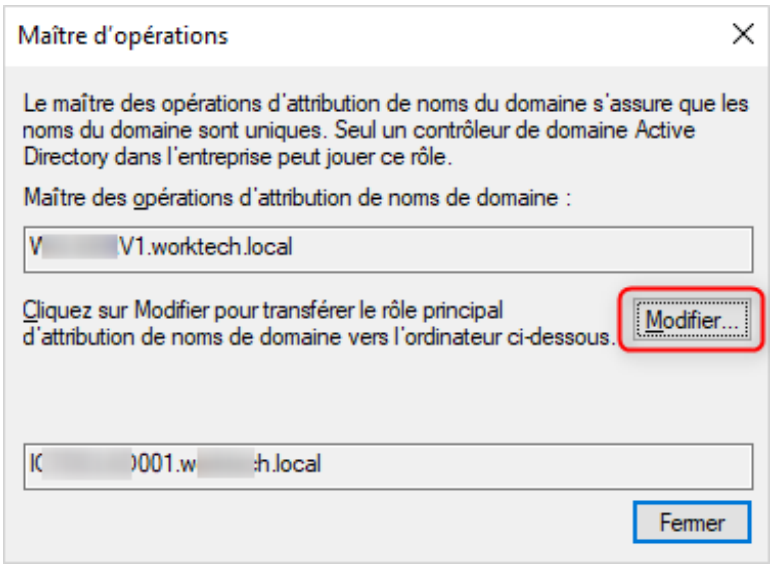
- RID : gère l'allocation des pools RID aux autres contrôleurs de domaine. Le maître RID est responsable du traitement des demandes de pool RID provenant de tous les contrôleurs de domaine d'un domaine particulier.
- CDP : gère la compatibilité des contrôleurs de domaines pour les clients antérieurs à Windows 2000.
- Infrastructure : gère la cohérence des objets créés sur un AD pour les répliquer sur les AD membres (secondaires).

À noter que le maître d'opérations est exclusivement réservé au serveur primaire choisi.

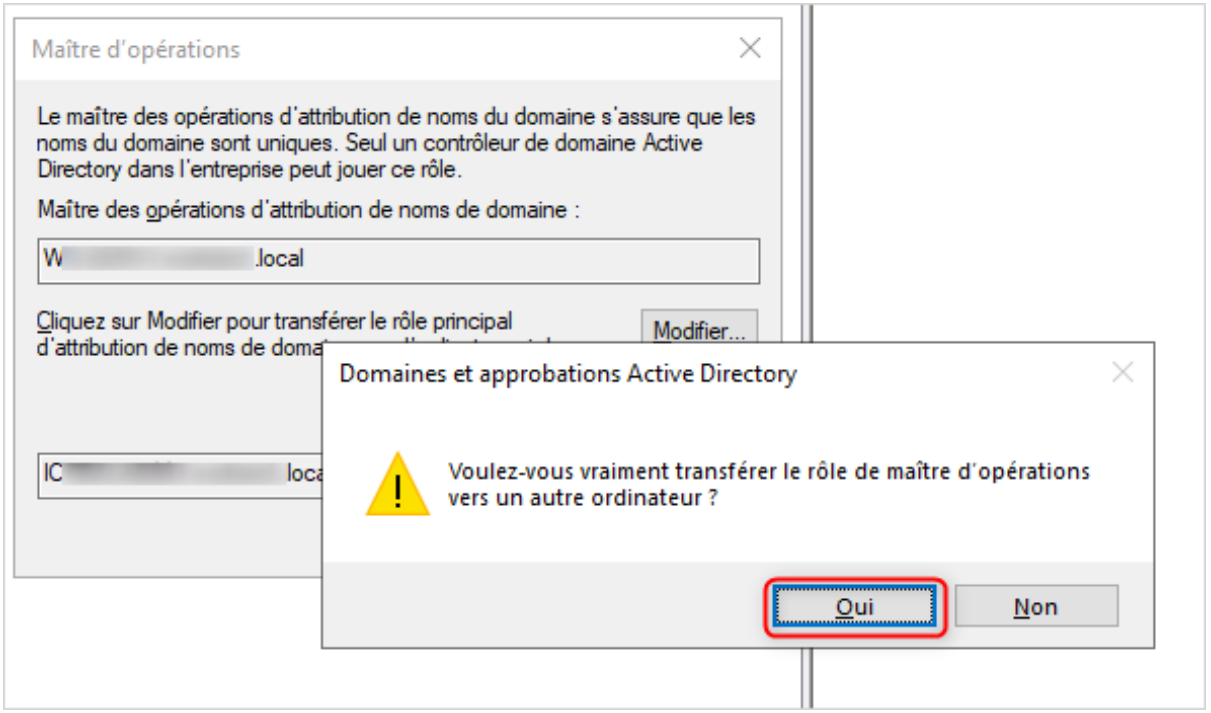
Afin d'effectuer ce changement, dans "Maîtres d'opérations", effectuez le transfert du rôle sur le nouveau contrôleur de domaine en cliquant sur le bouton "Modifier" :

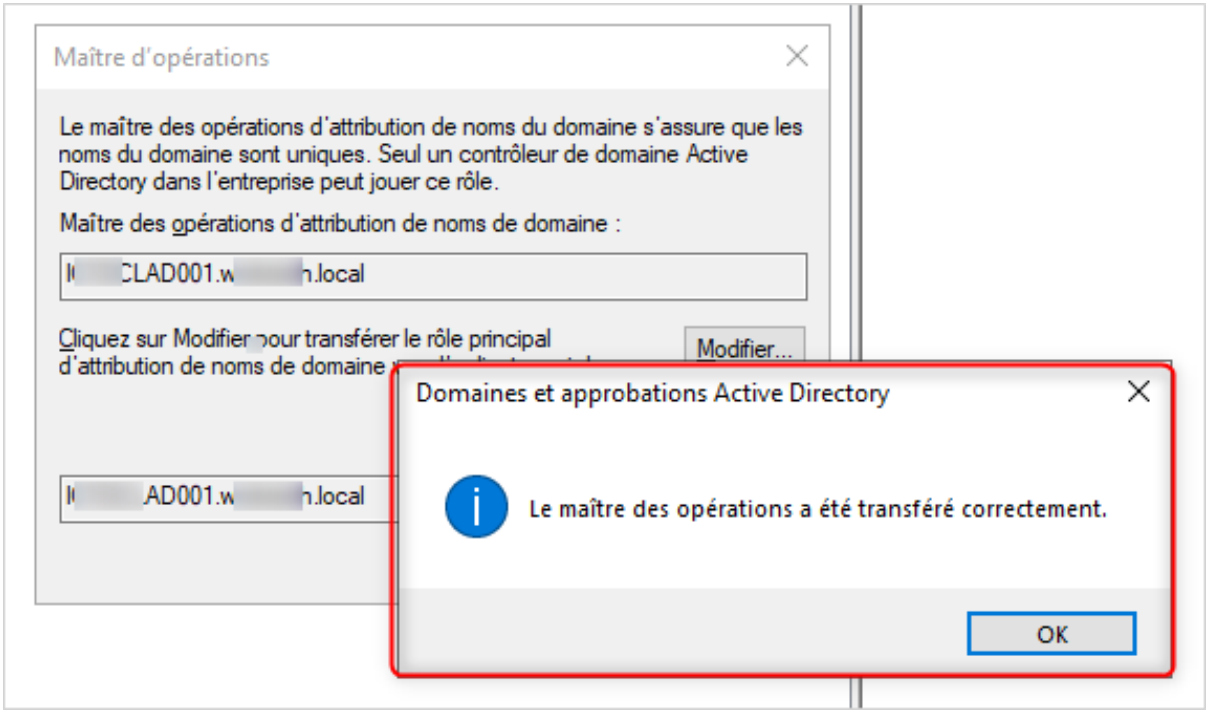


Confirmez le transfert, et un message de succès sera affiché si tout est OK :



Réalisez la même opération pour les trois rôles. Le maître d'opération doit être attribué au nouveau contrôleur de domaine :

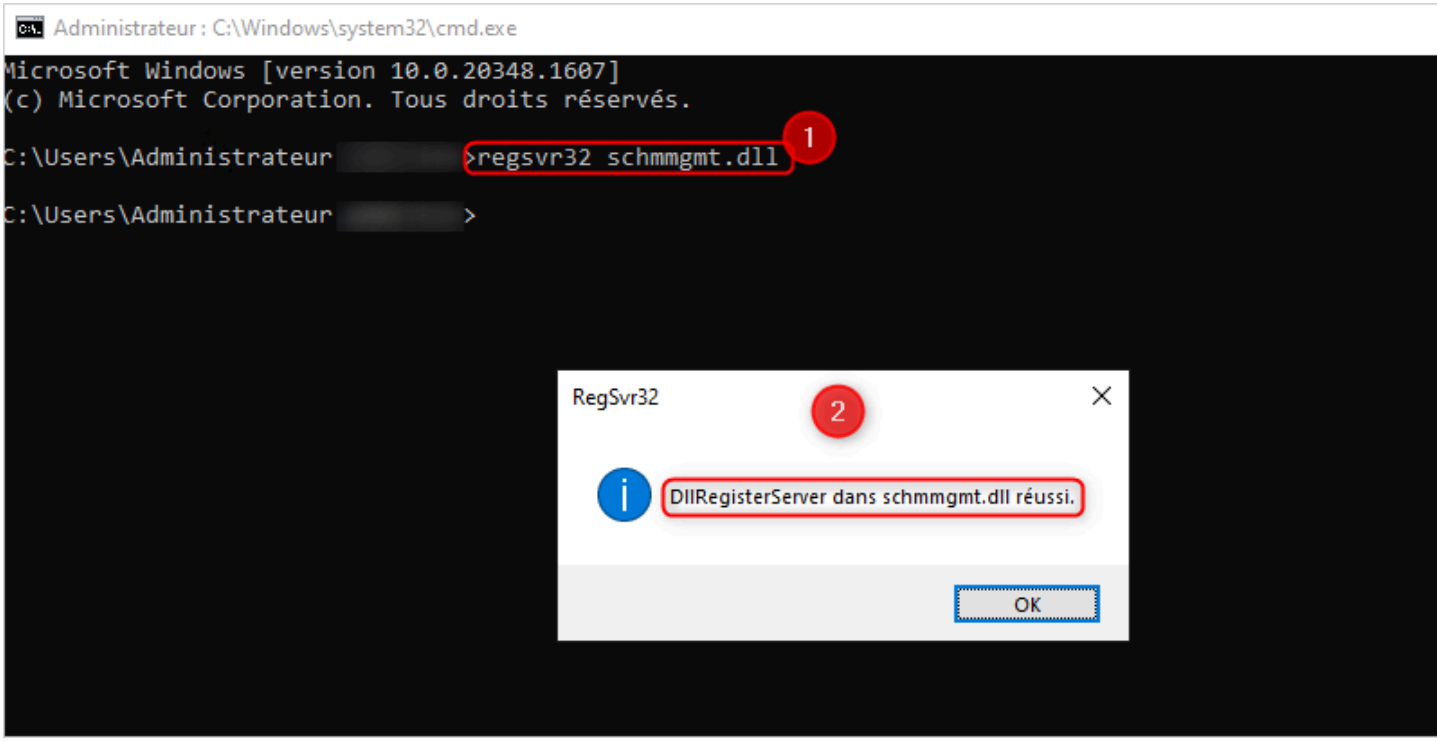




Domaines et approbations Active Directory

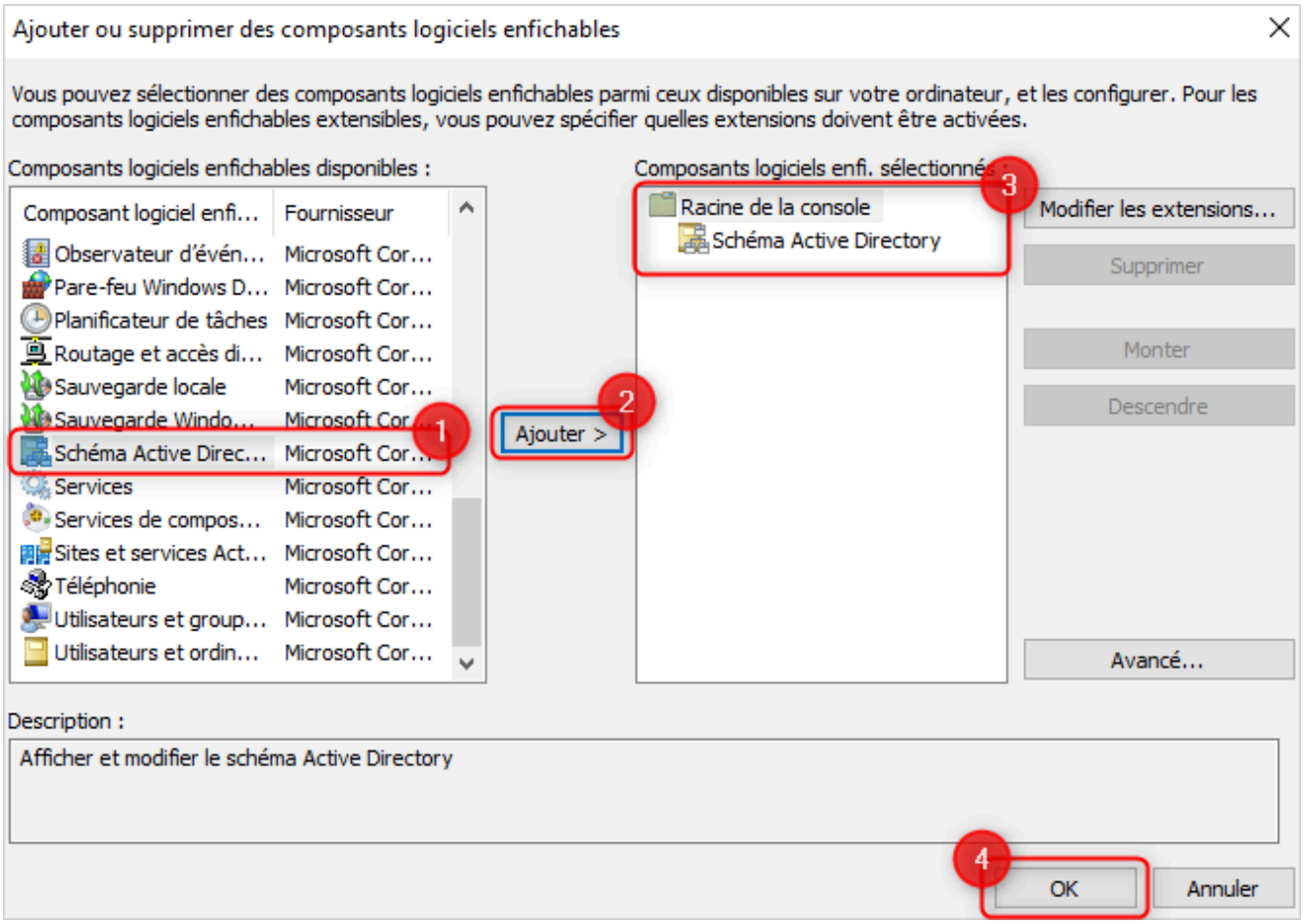
Ensuite, veuillez ouvrir la console "Domaines et approbations Active Directory" ou actionnez les touches Windows + R (Exécuter), puis saisir : domain.msc. Comme pour le passage précédent, il est nécessaire de migrer l'ancien DC vers le nouveau.

Sélectionnez le domaine (XXX.local) dans la colonne de gauche, puis effectuez un clic droit > "Maîtres d'opérations" :

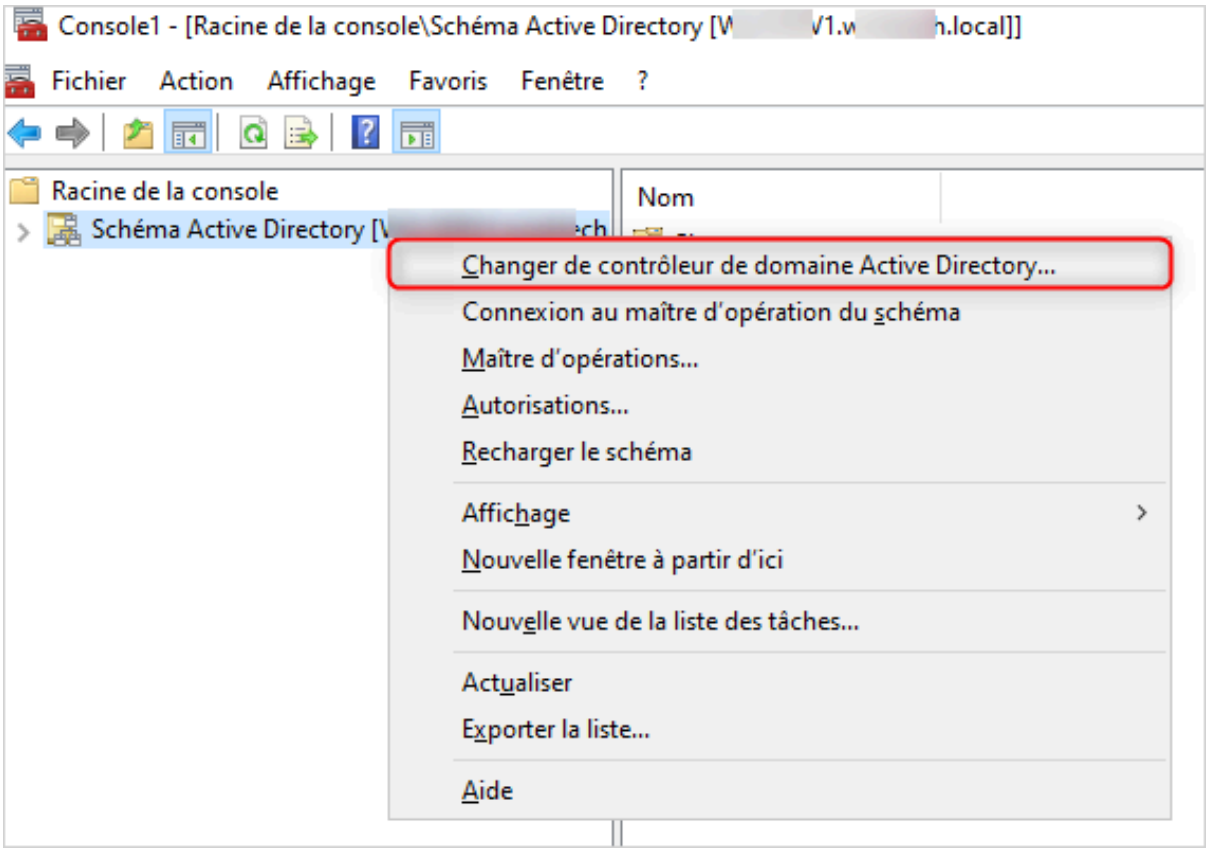


Il est question ici de réaliser un transfert du rôle d'attribution de noms du domaine et gère la cohérence de ces derniers.

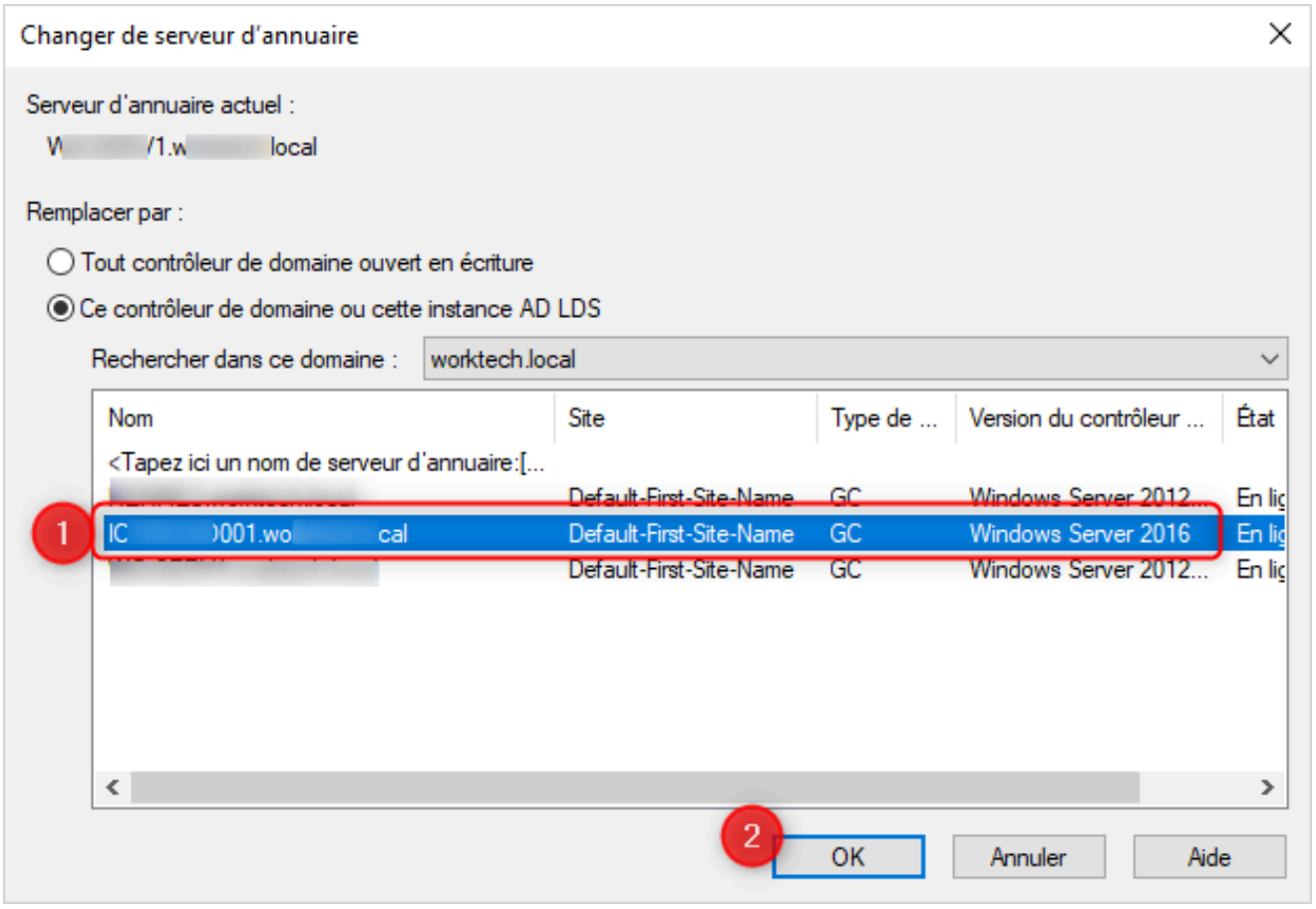
Actuellement, le maitre des opération d'attribution de noms de domaine est le serveur sous Windows Server 2012 R2 (à migrer). Cliquer sur modifier afin de réaliser le transfert :



Confirmez le transfert vers le domaine actuel :



La modification a bien été effectuée :

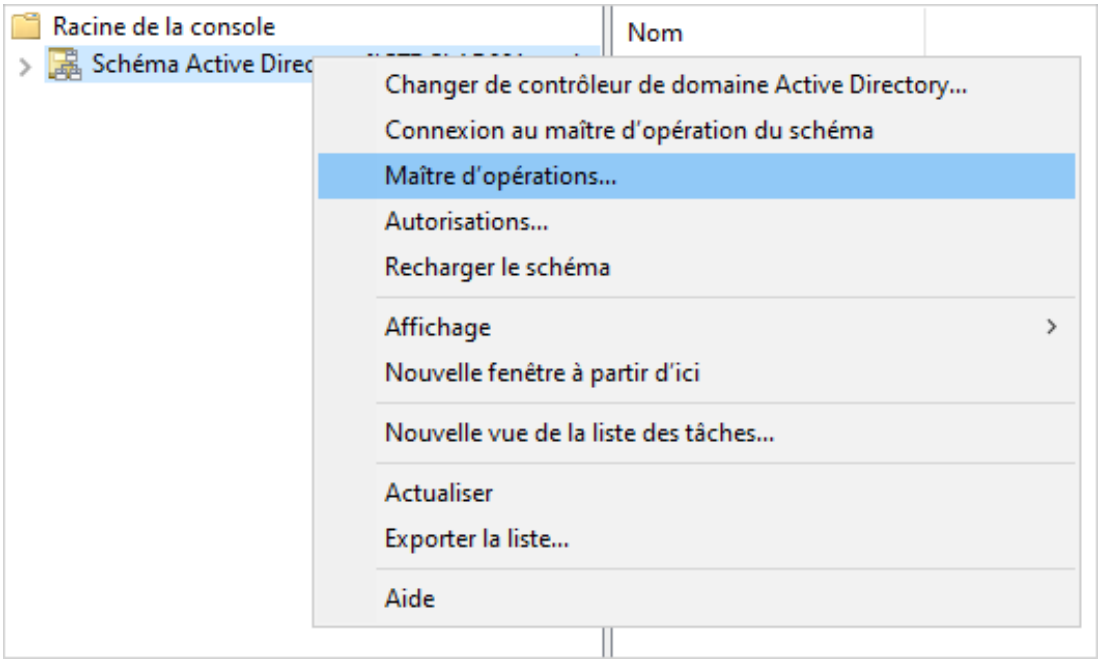


Accès à la console "Schéma Active Directory"

Par défaut, la console "Schéma Active Directory" n'est pas disponible par défaut. On enregistre ainsi la DLL correspondante avec l'instruction regsvr32 schmmgmt.dll. Dans notre cas, il est nécessaire de charger la DLL, correspondante à la console "Schéma Active Directory".

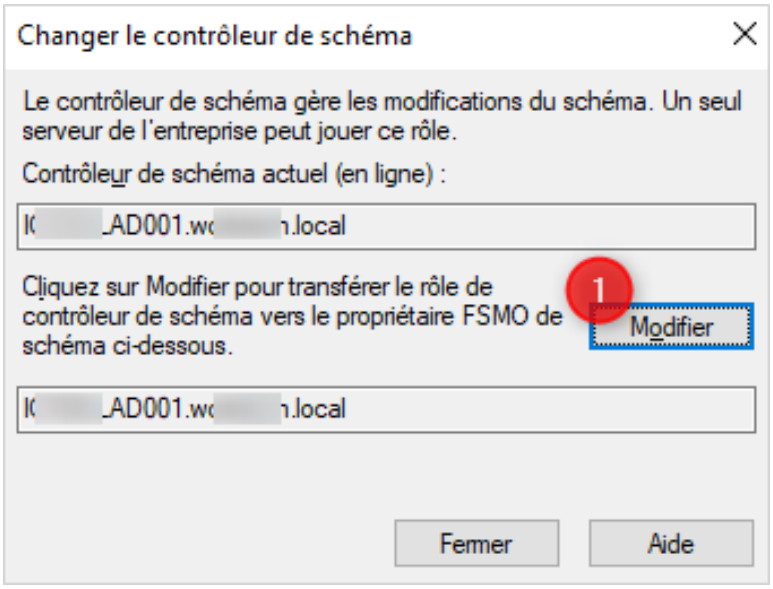
```
C:\Users\Administrateur.DOMAIN>regsvr32 schmmgmt.dll
```

Le résultat est le suivant :



Ouvrez la console "MMC" ou actionnez les touches Windows + R (Exécuter), puis saisir : mmc. On aura la possibilité d'ajouter le composent enfichable.

Sélectionner la console "Schéma Active Directory", cliquer sur Ajouter, puis OK afin de valider l'ouverture de la console.



Changer de contrôleur de domaine

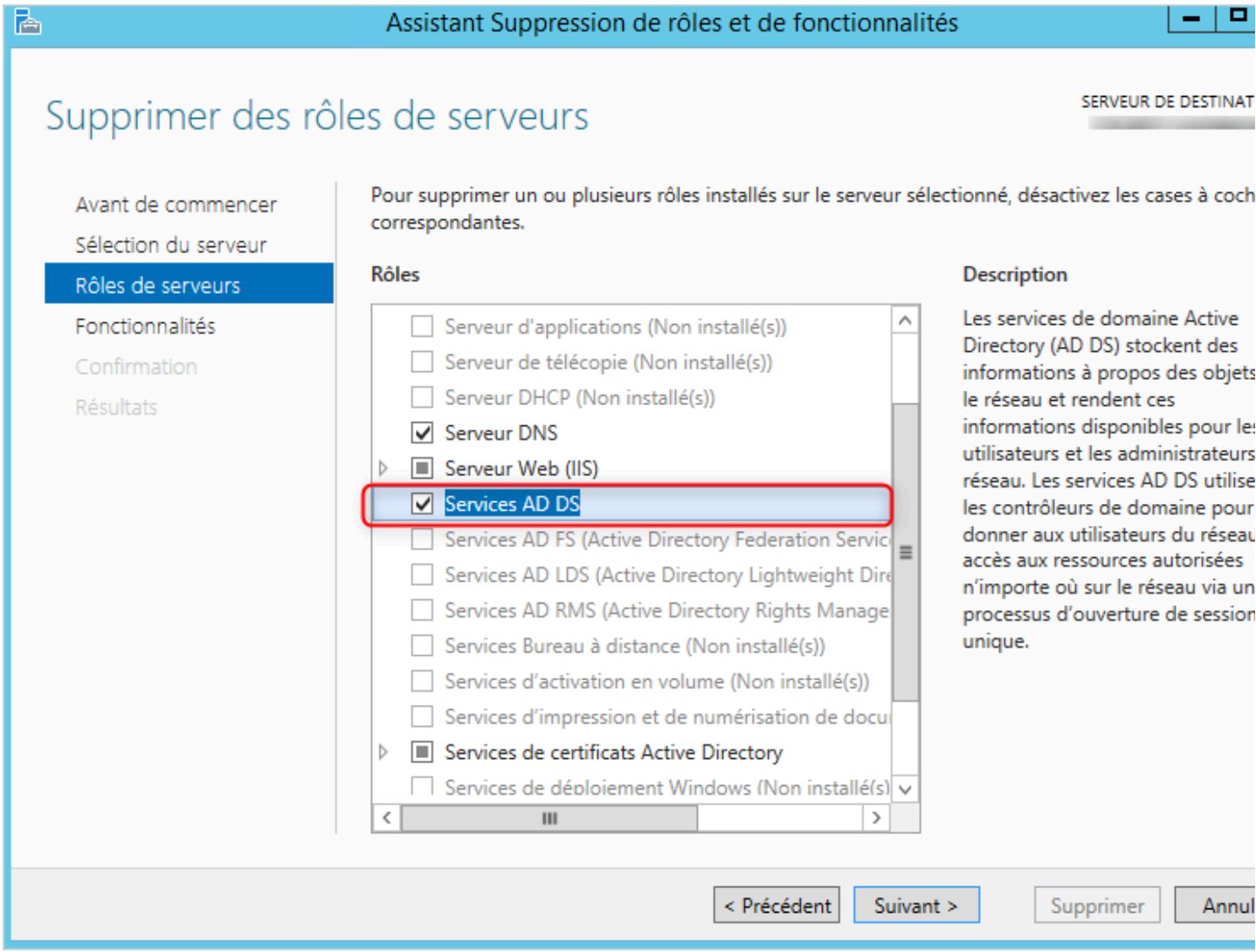
En effectuant un clic-droit, changez de contrôleur de domaine en sélectionnant le domaine (XXX.local) dans la colonne de gauche, puis effectuez un clic droit > "Changer de contrôleur de domaine Active Directory..." :

```
PS C:\Users\[redacted]> netdom query fsmo
Paramètre incorrect.

Try "NETDOM HELP" for more information.

PS C:\Users\[redacted]> _
```

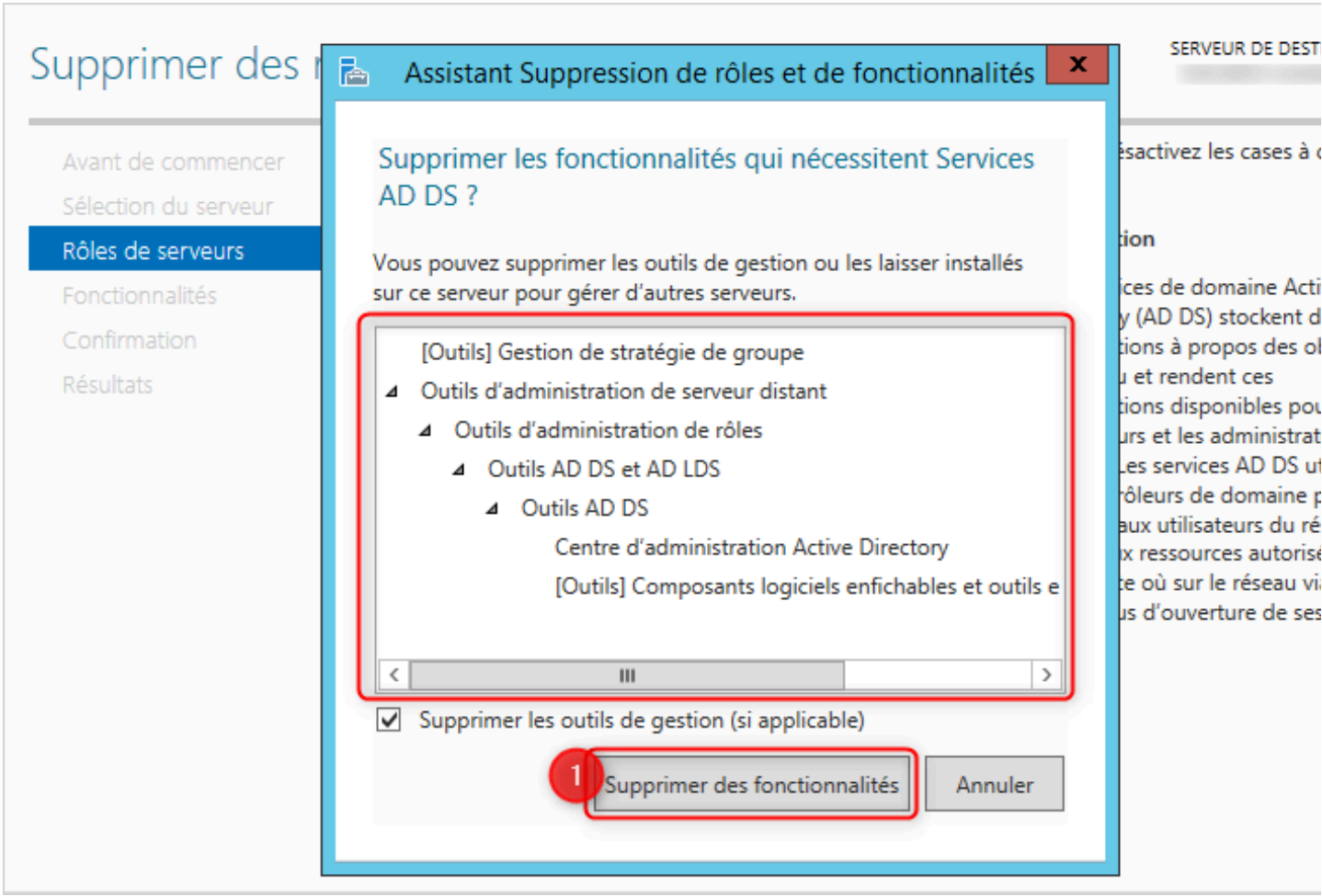
Sélectionnez le nouveau contrôleur de domaine :

Maîtres d'opérations

Comme pour le passage précédent, il est nécessaire de migrer l'ancien DC vers le nouveau. Sélectionnez le domaine (XXX.local) dans la colonne de gauche, puis effectuez un clic droit > "Maîtres d'opérations" :



Changez ensuite le contrôleur de schéma sur le nouvel AD en cliquant sur modifier, puis confirmer le message :

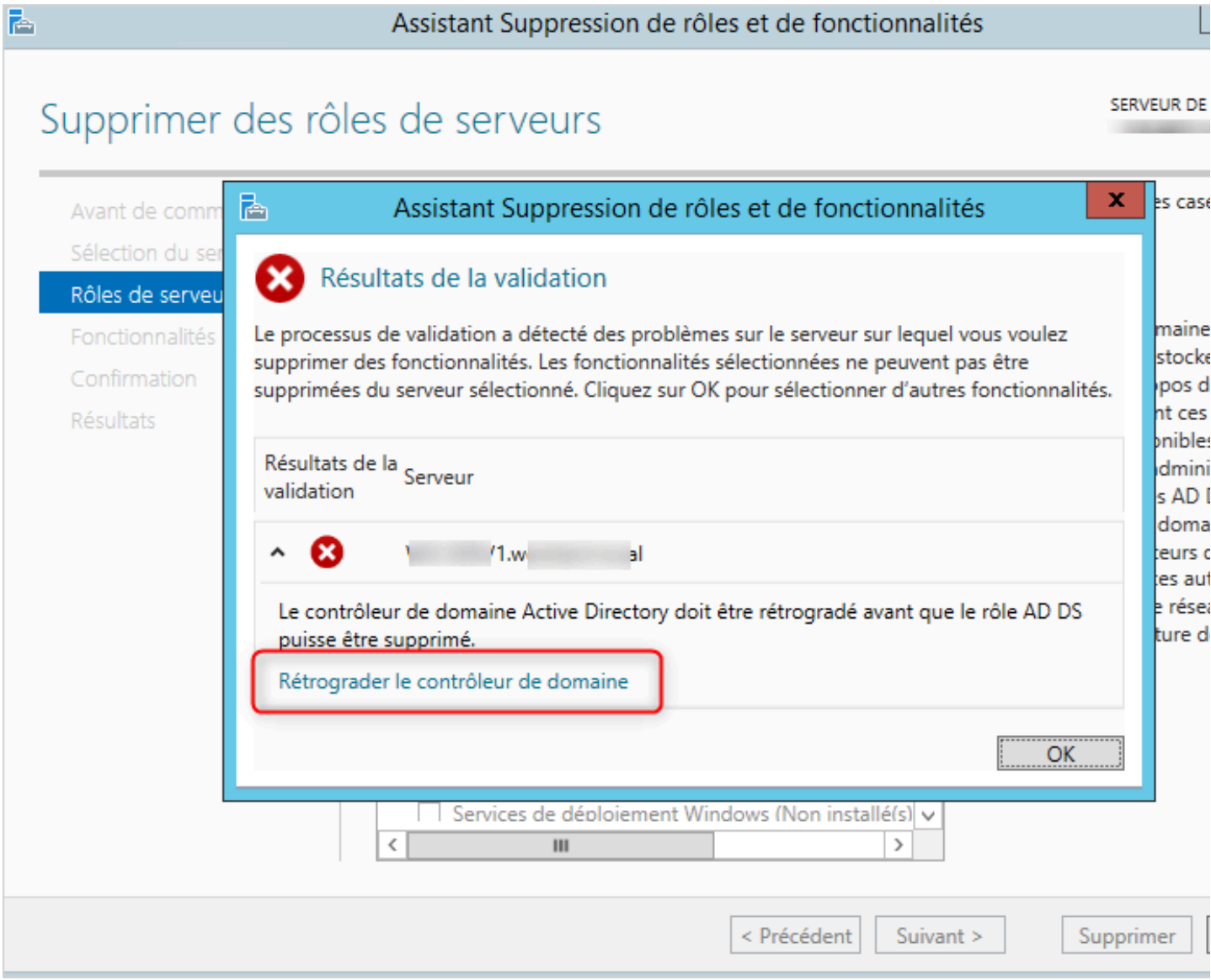


Vous pouvez réaliser toutes ses actions à l'aide d'une seule ligne PowerShell :

```
PS1 $> Move-ADDirectoryServerOperationMasterRole -Identity ICTDCLAD001
-OperationMasterRole SchemaMaster, RIDMaster, DomainNamingMaster, PDCEmulator,
InfrastructureMaster -Confirm:$False
```

Vérification des rôles FSMO

La procédure est terminée. Sur le contrôleur de domaine récent, réalisez la même commande afin de récupérer le FSMO du domaine avec netdom query fsmo :




```
C:\Users\Administrateur.DOMAIN>netdom query fsmoContrôleur de schéma
DC-WS2K22.vemotech.localMaître des noms de domaine
DC-WS2K22.vemotech.localContrôleur domaine princip.
DC-WS2K22.vemotech.localGestionnaire du pool RID    DC-WS2K22.vemotech.localMaître
d'infrastructure     DC-WS2K22.vemotech.localL'opération s'est bien déroulée.
```

Si vous obtenez une erreur en tentant de réaliser cette opération sur un poste du domaine, c'est normal car l'ordinateur est déconnecté de l'ancien contrôleur de domaine et n'est pas encore connecté au nouveau. Il est alors nécessaire de remplacer les serveurs DNS par le nouveau contrôleur de domaine (sinon la résolution ne se fait pas).

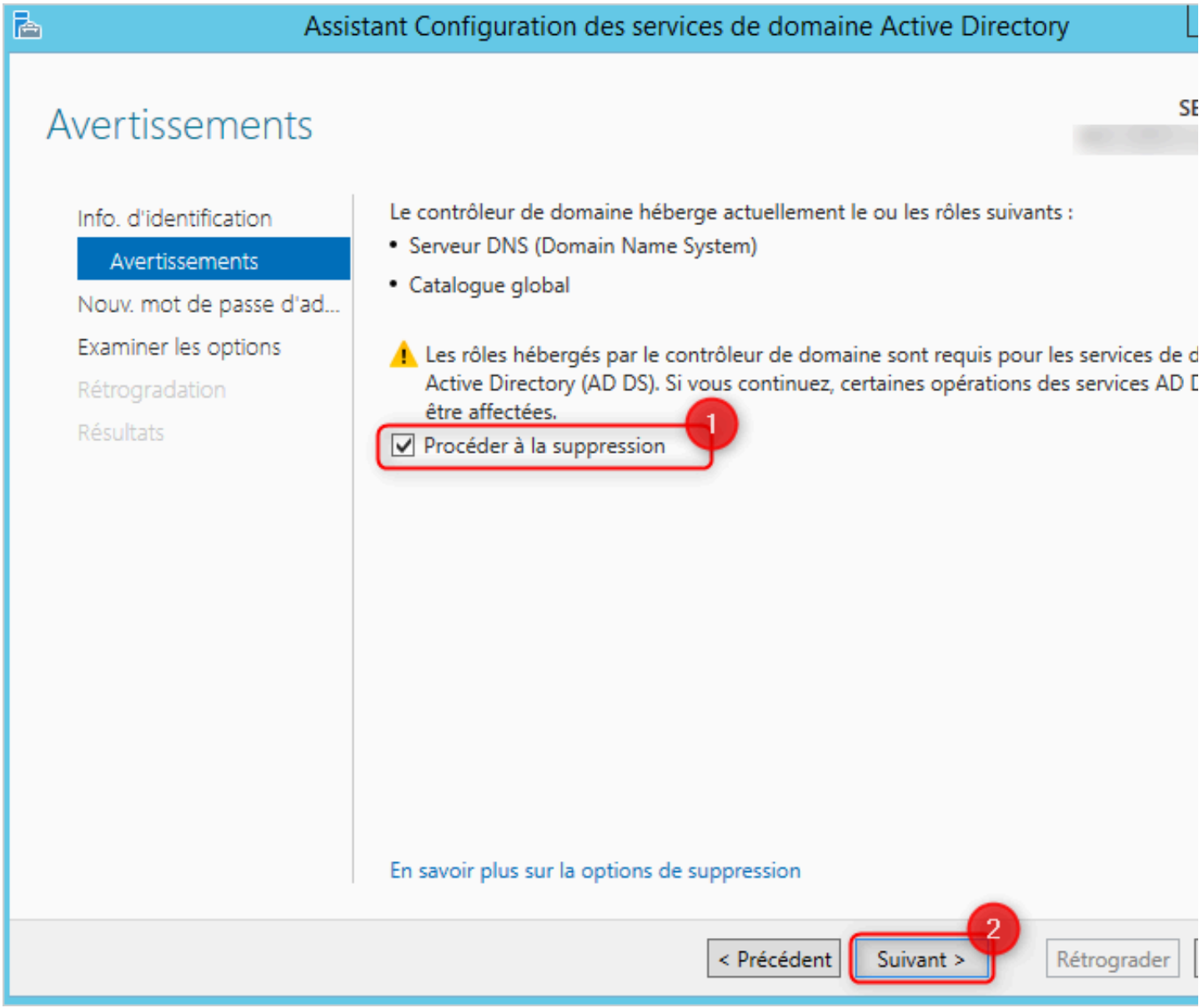
Désinstallation du contrôleur de domaine obsolète

Notre domaine est maintenant migré sur des contrôleurs de domaines récents à ce jours sous Windows Server 2022. Maintenant, il est nécessaire de supprimer le contrôleur de domaine sous Windows Server 2012 R2 afin d'augmenter le niveau fonctionnel du domaine. Plus précisément, il est question de supprimer le rôle serveur "ADDS" (Active Directory Domain Services).

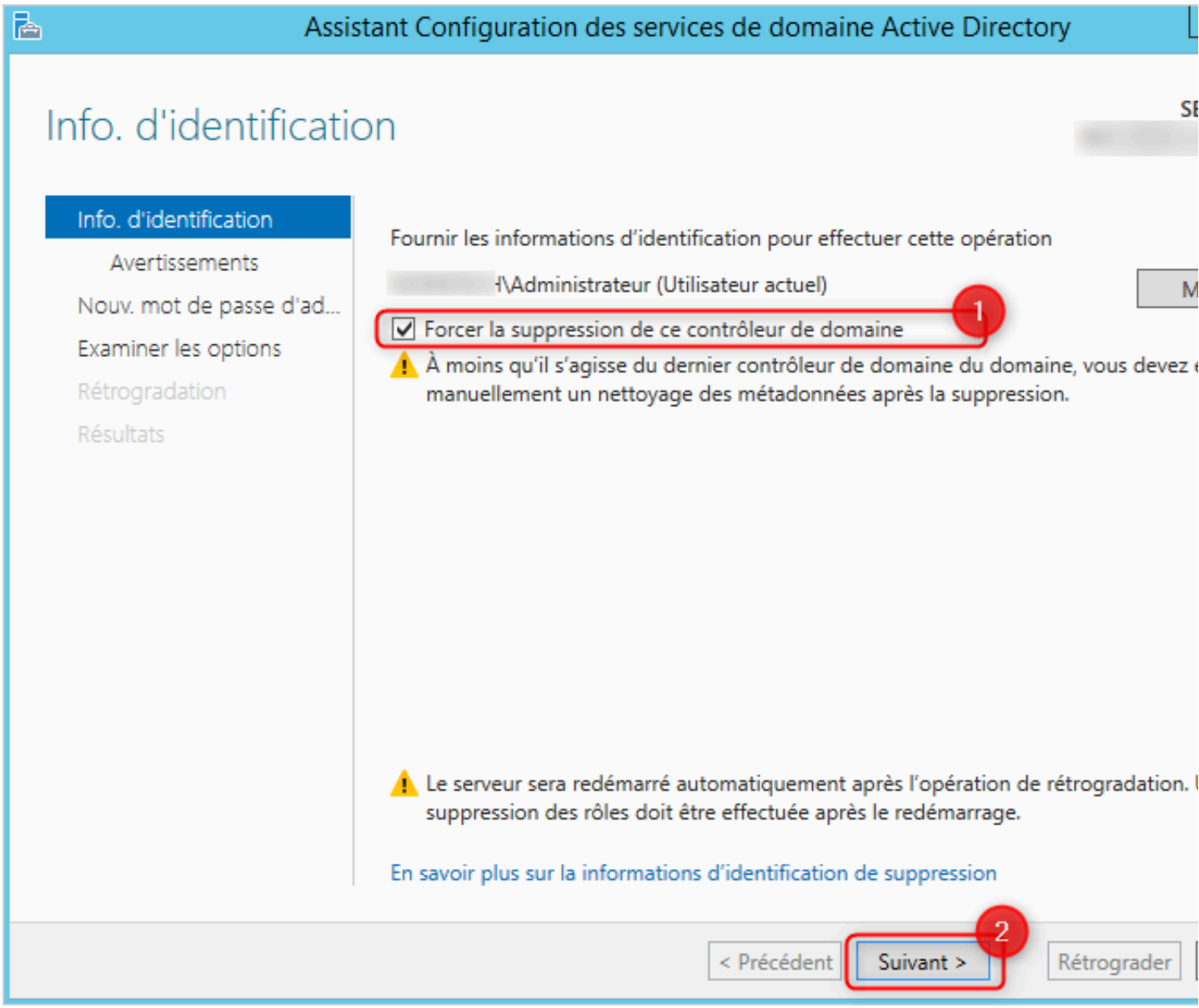
Connectez-vous au serveur Windows Server 2012 R2 (ancien DC) en tant qu'administrateur. Ouvrez ensuite le **Gestionnaire de serveur** à partir du menu Démarrer ou dans la barre des tâche Windows.

Cliquez sur "Supprimer des rôles et fonctionnalités", dans le menu "Gérer" de la barre de navigation.

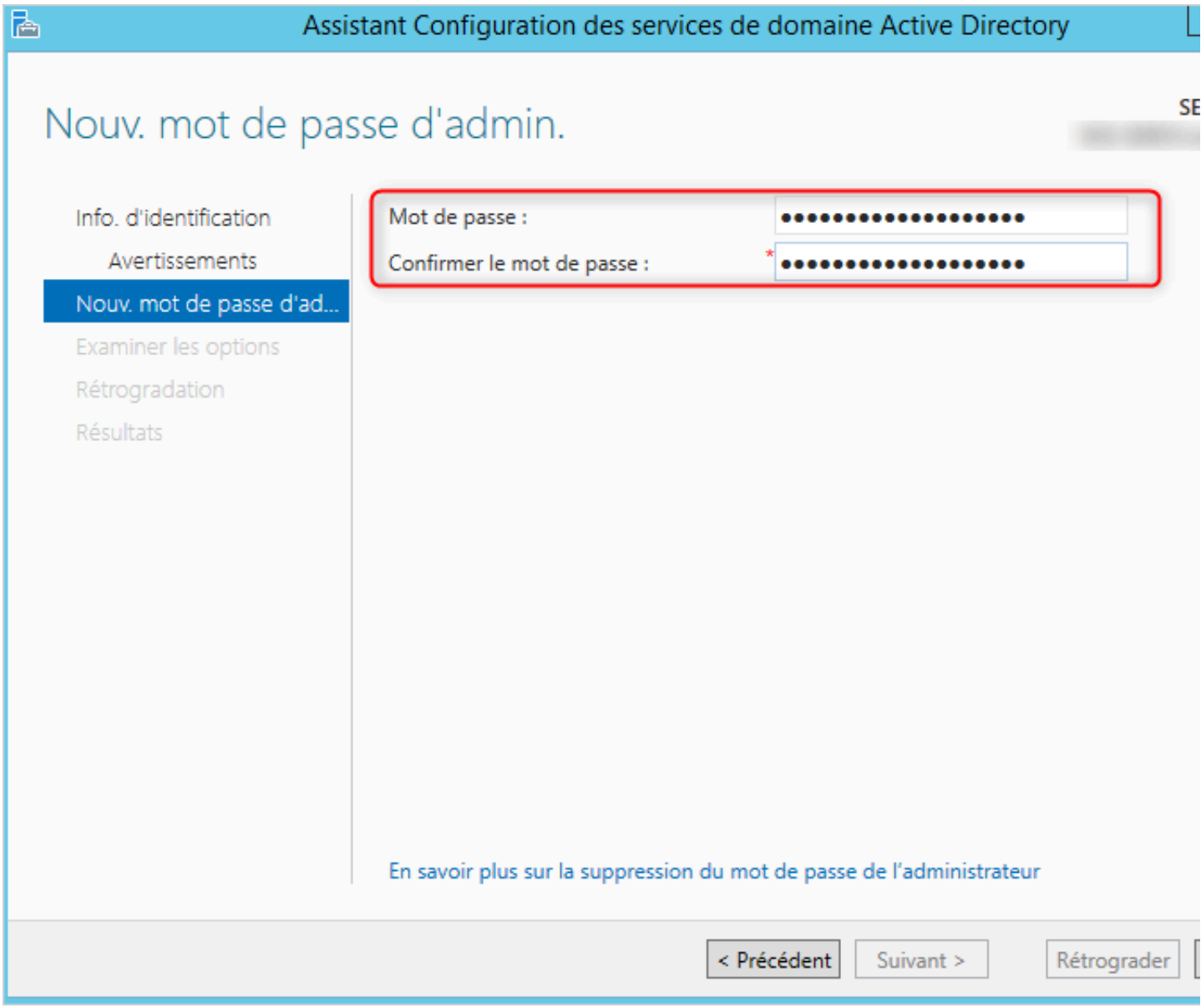
Cliquez sur Suivant jusqu'à atteindre la page "Supprimer des rôles". Sélectionnez le rôle Services AD DS (Active Directory Domain Services) dans la liste des rôles disponibles :



Supprimez également les fonctionnalités dépendantes du rôle ADDS :

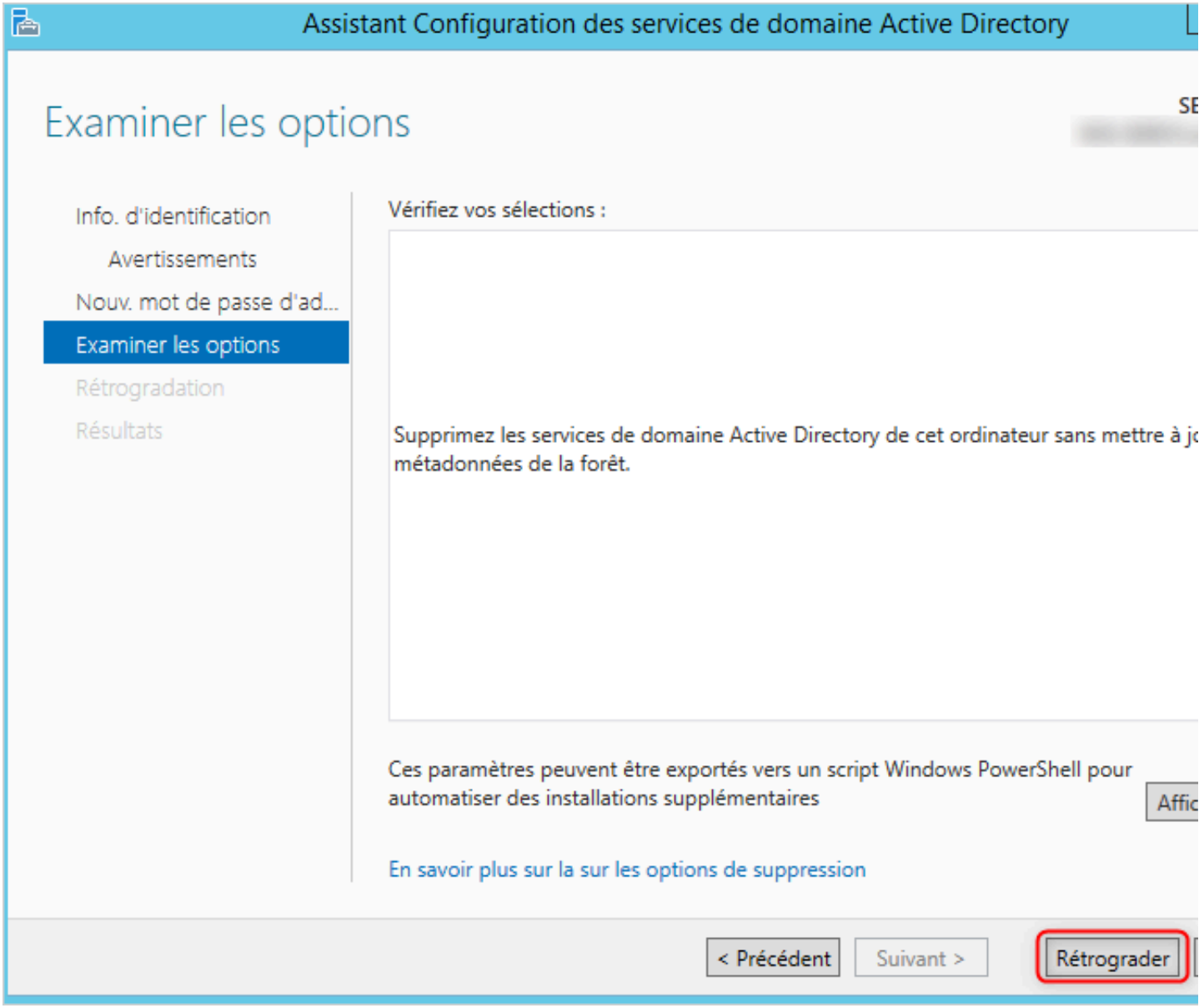


Une erreur tout à fait normale survient : "Le contrôleur de domaine Active Directory doit être rétrogradé avant que le rôle AD DS puisse être supprimé". Cliquez sur le lien "Rétrograder le contrôleur de domaine" afin d'ouvrir l'assistant de suppression :



Il est question ici d'effectuer la suppression des services hébergés sur l'ancien contrôleur de domaine sous Windows Server 2012 R2. Cochez la case "Procéder à la suppression", puis suivant :

Cochez également la case : "Forcer la suppression de ce contrôleur de domaine", puis suivant :



Quand la rétrogradation est terminée et que l'ordinateur devient un serveur membre de domaine ou un ordinateur de groupe de travail, la page "Nouveau mot de passe d'administrateur" demande de fournir un mot de passe pour le compte Administrateur de l'ordinateur local intégré.

On termine ainsi par l'action "Rétrograder".