http://WWW.CABARE.NET ©

Migration AD Windows 2008r2 (ou 2003R2) vers 2012r2 – sys 24 – Cours -

Migration AD windows 2003R2 vers 2012r2

Michel Cabaré – Ver 1.3 – Avril 2016-

Migration 2008r2 (ou 2003) vers 2012r2
planification

Michel Cabaré – Ver 1.3 – Avril 2016

www.cabare.net ©

TABLE DES MATIÈRES

INTEGRATION DC 2012R2 DANS 1 DOMAINE 2008R2

Avant de pouvoir ajouter un contrôleur de domaine doté de Windows Server 2012R2 dans un environnement Active Directory fonctionnant sous Windows 2008R2 Server vous devez mettre à jour le schéma Active Directory, et de manière générale suivre le mode opératoire suivant :

Planification de la migration

Exemple, migration d'un serveur 2008r2 sur un serveur en 2012r2

- Vérification Domaine et Réplication (**dcdiag replmon repadmin**) et **niveau fonctionnel** minimal **2003**
- Sauvegarde du **DC** intégrant le rôle **FSMO** de **Maître de schéma** + **AD**
- **Blocage réplication** (si plus d'un DC)
- Exécuter **adprep** pour le **schéma** (réplication de forêt)
- Vérification **adsiedit.msc**
- **Autorisation réplication** (si plus d'un DC)
- Exécuter **adprep** pour le **domaine** (réplication de domaine)
- Intégration nouveau serveur 2012r2 dans le domaine
- Installer les rôles **Directory Service**, **Dns** et **catalogue global** puis exécuter l'assistant de **configuration Active Directory** sur le nouveau serveur 2012r2
- Tester la **réplication** sur ce nouveau serveur
- Paramétrage **TCP-Ip** pour les **DNS** et sur le domaine
- **Migrer les rôles FSMO** sur le nouveau serveur
- Supprimer le **catalogue global** sur l'ancien serveur 2008r2
- Supprimer le **DNS** sur l'ancien serveur 2008r2
- Démonter l'ancien **DC** en 2008r2 (pas d'urgence)
- Gestion synchronisation base de temps **entre DC** et sur **Ntp**
- Augmentation si besoin du **Niveau fonctionnel (forêt** et **domaine**)

Il ne reste plus qu'à utiliser les nouvelles fonctionnalités :

Migrer la réplication SYSVOL de FRS vers DFSR, gérer une authentification plus forte (Authentication Mechanism Assurance), ADMX à la place des ADM.

Vérification Domaine

On va utiliser l'utilitaire **dcdiag** depuis une invite de commande sur un des **Cd** actuel en 2008R2. Option **/e** pour tester tous les CD et **/v** pour verbose

Dcdiag /e /v

```
C:\Users\Administrateur.CABARE-INTRA>dcdiag /e /v >c:\result-dcdiag.txt_
```

Et si tout va bien on peut aussi tester les DNS avec l'option **/test:dns**

Dcdiag /test :dns /e /v

```
C:\Users\Administrateur.CABARE-INTRA>dcdiag /test:dns /e /v >c:\result-dcdiagdns.txt
```

On peut aussi tester de manière plus approfondie la réplication sur chaque DC avec la commande et

Repadmin /showrepl **Repadmin /replsummary**

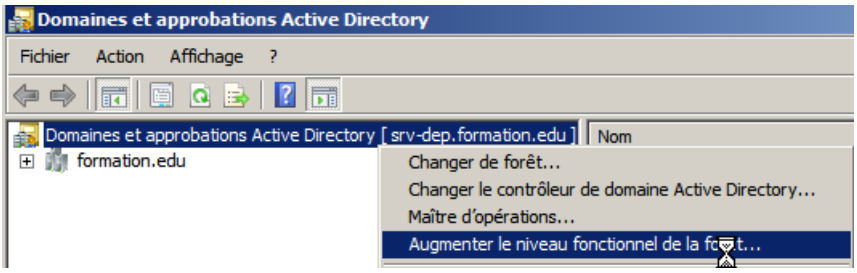
On note ou se trouvent les rôles FSMO par la commande

Netdom query fsmo

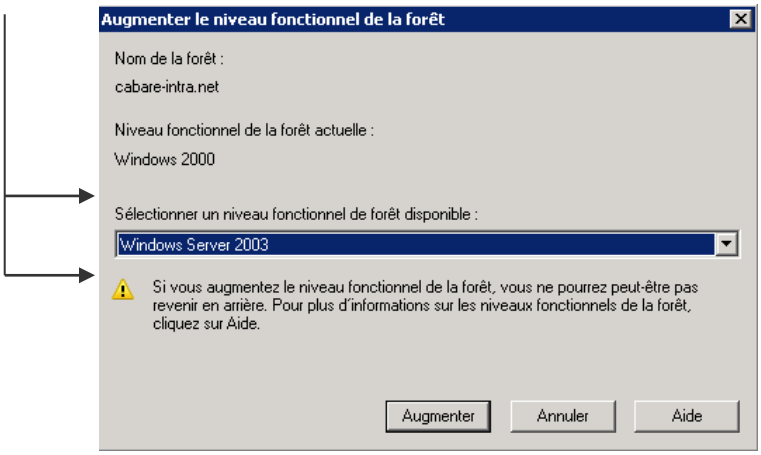
```
C:\Users\Administrateur.CABARE-INTRA>netdom query fsmo
Contrôleur de schéma         srv-dc.cabare-intra.net
Maître des noms de domaine   srv-dc.cabare-intra.net
Contrôleur domaine princip.  srv-dc.cabare-intra.net
Gestionnaire du pool RID     srv-dc.cabare-intra.net
Maître d'infrastructure      srv-dc.cabare-intra.net
L'opération s'est bien déroulée.
```

La Vérification du niveau fonctionnel en cours (2003 minimum) se fait dans **Domaines et approbations Active Directory**

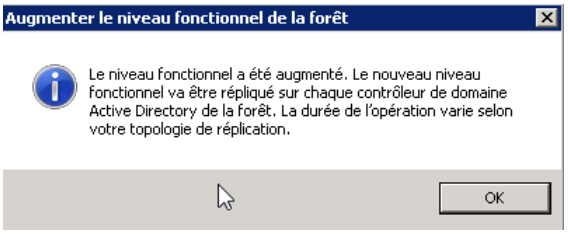
il faut se placer sur la forêt, puis clic droit **Augmenter le niveau fonctionnel de la forêt...**



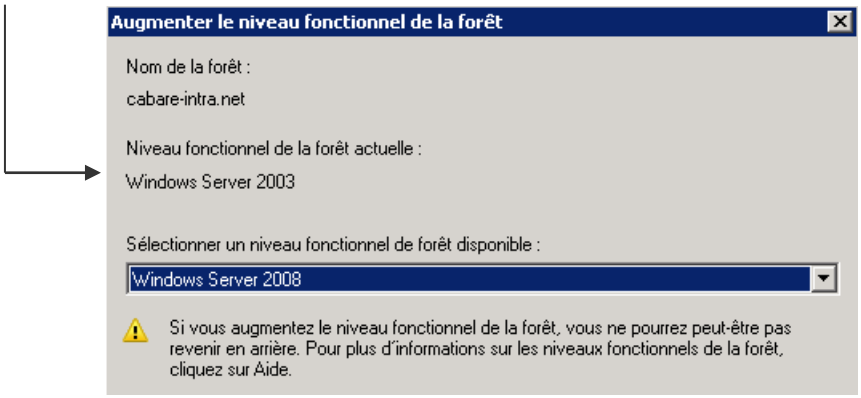
Le niveau actuel est précisé... ici dans l'exemple 2000, il faut être en 2003 minimum pour



Si on doit augmenter le niveau fonctionnel, il faut attendre la réplication dans toute la forêt !

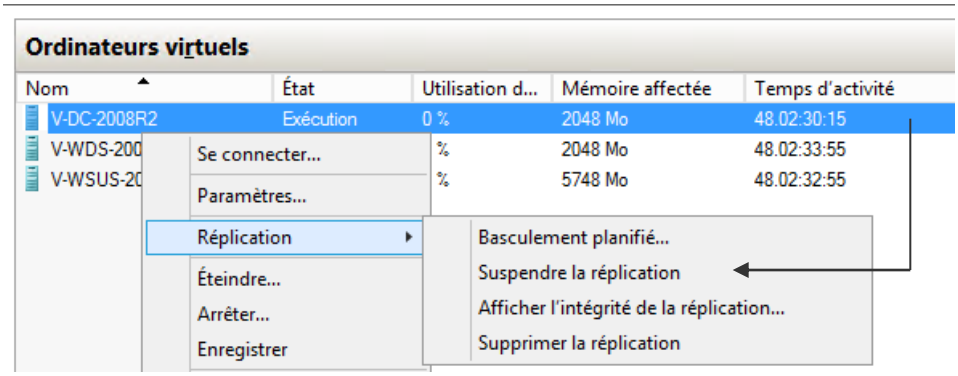


et vérifier sur tous les DC que l'on ait bien un niveau 2003



Sauvegarde du DC

Pour un ordinateur virtuel, on peut suspendre une éventuelle réplication, de manière à avoir un duplicata de la machine avant migration du schéma



Pour une machine normale on prévoit une sauvegarde complète

N.B : en cas de problème de migration du schéma, la seule solution sera repartir du CD sauvegardé et de reconstruire la forêt !!!

Blocage de la réplication

Il est possible de bloquer la réplication sortante sur un contrôleur de domaine, ceci dans le but d'effectuer des opérations de migration dessus sans affecter les autres contrôleurs de domaine.

Pour cela:

repadmin /options *nom-serveur* **+disable_outbound_repl**

```
C:\Users\Administrateur.CABARE-INTRA>repadmin /options srv-dc.cabare-intra.net +DISABLE_OUTBOUND_REPL
Actuel : Options DSA : IS_GC
Nouveau : Options DSA : IS_GC DISABLE_OUTBOUND_REPL
```

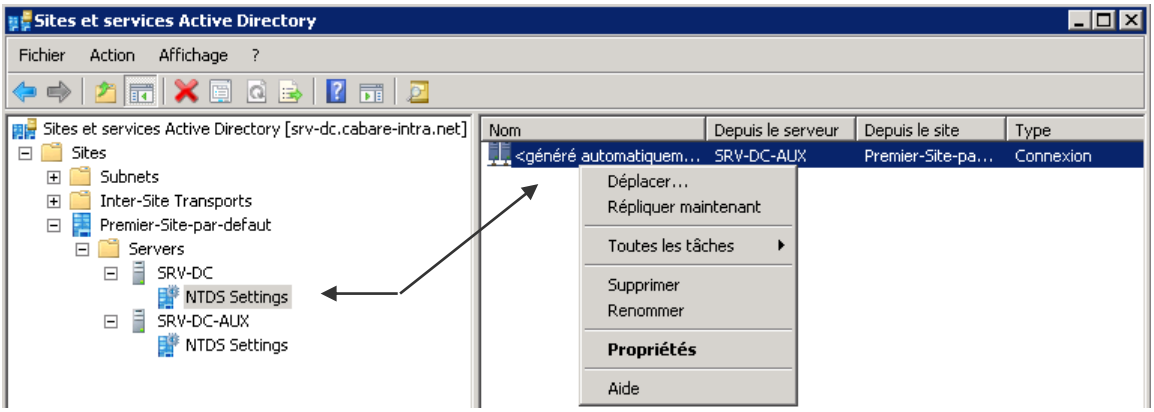
On peut vérifier avec la commande suivante (à exécuter sur le serveur qui essaye de se répliquer depuis le serveur que l'on a dévalidé):

repadmin /showrepl

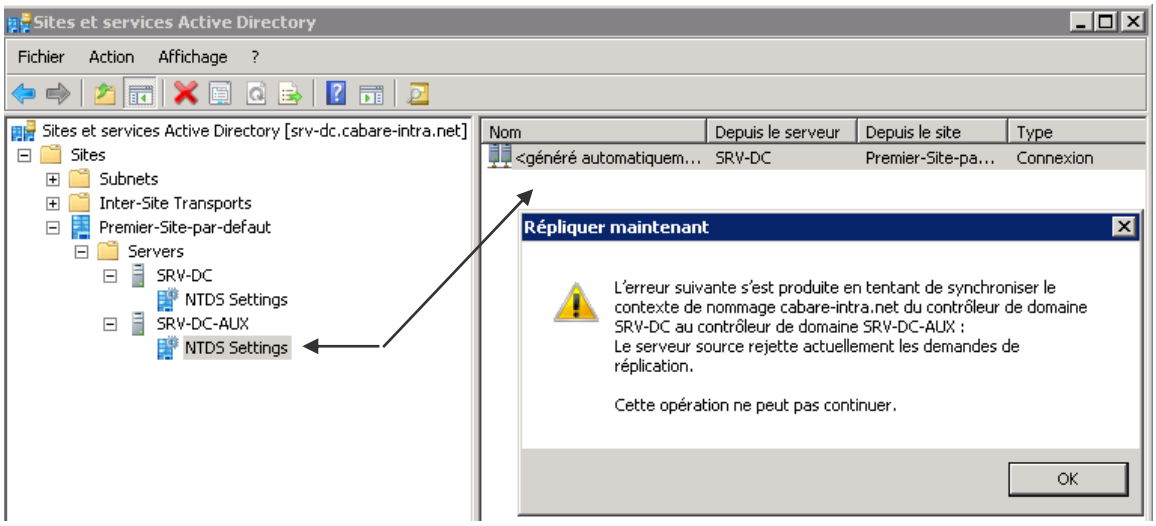
```
C:\Users\Administrateur.CABARE-INTRA>repadmin /showrepl

Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
Premier-Site-par-defaut\SRV-DC-AUX
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
ID de l'invocation DSA : 55375af3-af02-4366-9677-042f4838285a

=== INSTANCES VOISINES ENTRANTES ==================================

DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC via RPC
        GUID de l'objet DSA : dfcd6f8c-1645-4c32-b408-23ad5d96dac9
        La dernière tentative, le 2016-04-26 09:19:43, a échoué, résultat 8456 (0x2108):
            Le serveur source rejette actuellement les demandes de réplication.
        16 échecs consécutifs.
        Dernière réussite le 2016-04-26 09:04:42.
```

ou plus facilement depuis la console **Site et service Active Directory**

Il ne faut pas tester si SRV-DC se réplique depuis SRV-DC-AUX



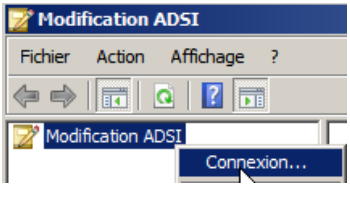
Mais plutôt si SRV-DC-AUX ne peut plus se répliquer depuis SRV-DC !



Dans le cas d'un environnement plus conséquent procéder de même pour tous les CD supplémentaires

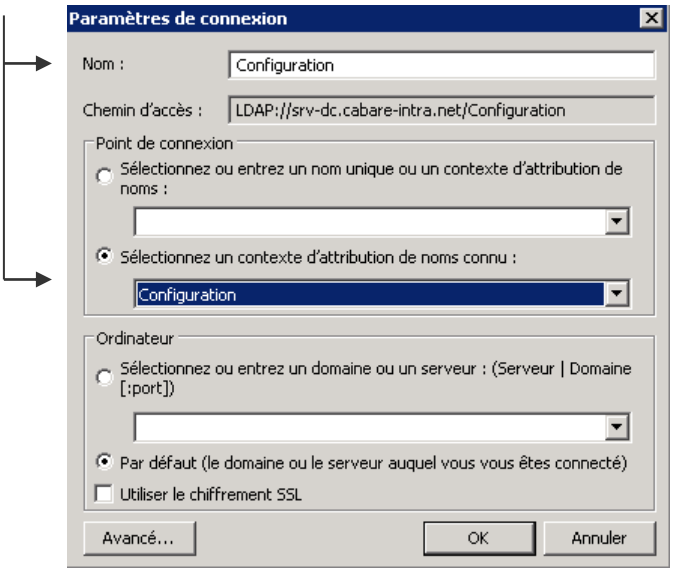
Vérification version schéma forêt et domaine

On sait que notre mode fonctionnel est 2003, on a bloqué notre CD avec le maitre de schéma, on va vérifier la version actuelle du schéma… via l'utilitaire **adsiedit.msc**

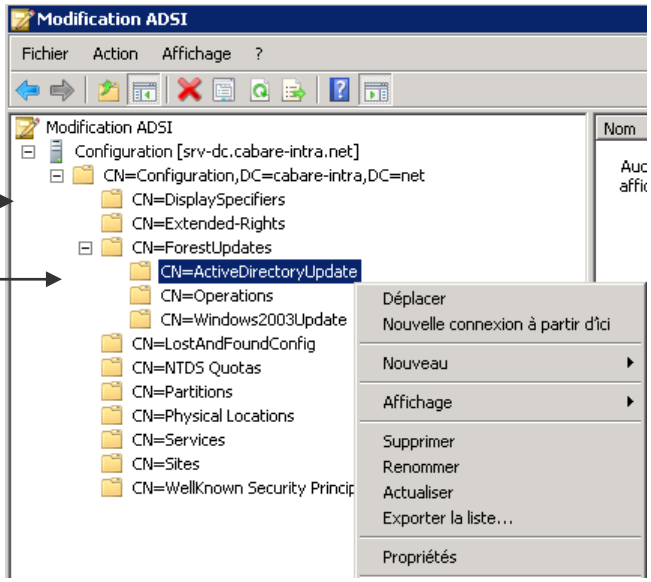


via la console **adsiedit.msc** puis clic droit / **connexion**.

demander **Sélectionnez un contexte d'attribution de noms connu**, puis **Configuration**



on obtient

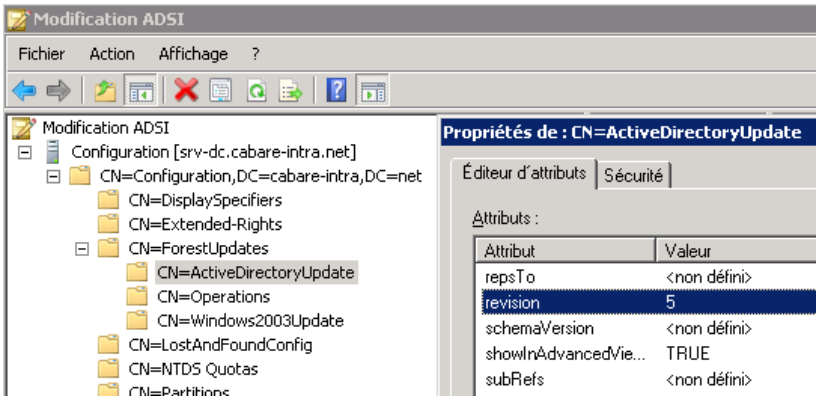


Développer **Configuration**, puis

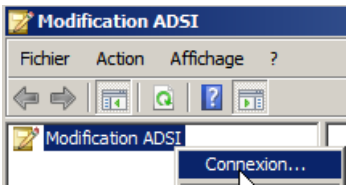
CN=Configuration, DC=domaine_racine_forêt

Développer sur **CN=ForestUpdates**. Demander les propriétés de **CN=ActiveDirectoryUpdate**,

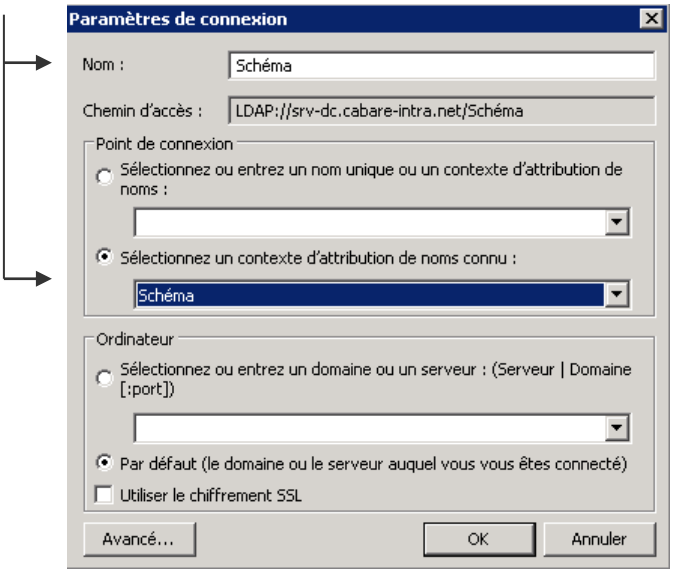
Vérifier que l'attribut **Revision** à pour valeur **4** pour 2008, ou **5** pour Windows Server 2008 R2,.



Il faut maintenant tester la version de schéma ... donc **Connexion**.

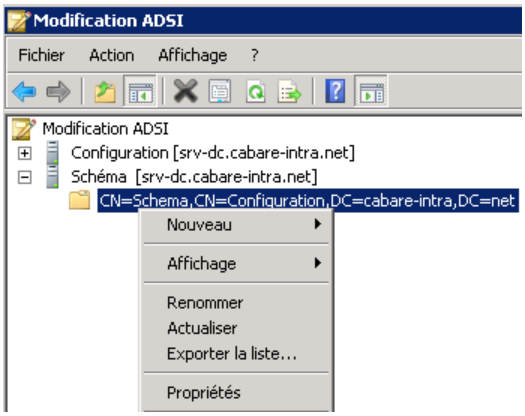


dans **Sélectionnez un contexte d'attribution de noms connu**, puis **Schéma**

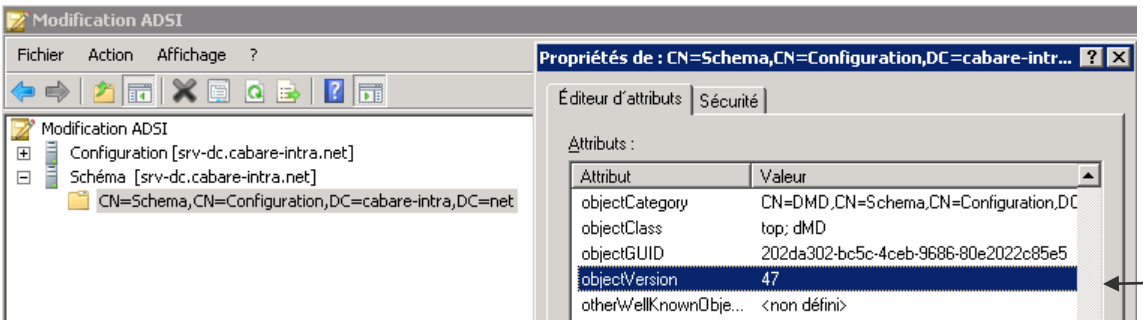


Développer **Schéma**,

puis demander les **propriétés** de **CN=Schema,CN=Configuration,DC=***domaine_racine_forêt*,



l'attribut **objectVersion** à pour valeur **46** pour 2008 ou **47** pour 2008 R2



Les principales versions de schéma existantes sont

30	Windows 2003	31	Windows 2003 R2
44	Windows Server 2008	47	Windows server 2008r2
56	Windows Server 2012	69	Windows Server 2012r2

Adprep pour la forêt

- Depuis le DVD de Windows Server 2012R2 copier le contenu du dossier **\support\adprep** dans un dossier Adprep sur le Serveur ayant le rôle de **contrôleur de schéma**.
- Taper: **Adprep.exe /forestprep**

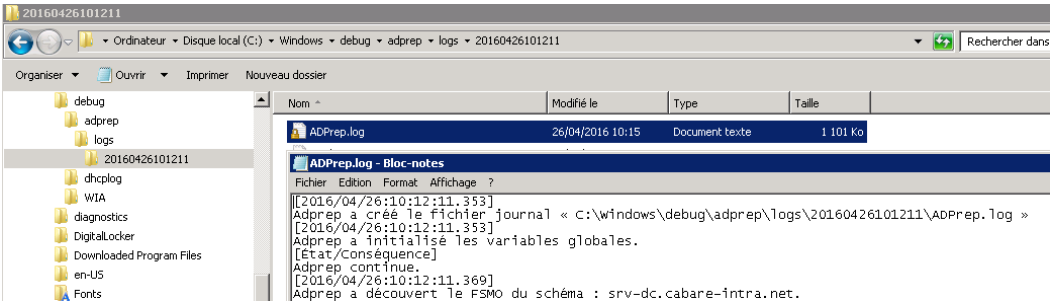
```
C:\adprep>adprep /forestprep
```

un avertissement apparaît et on confirme, c'est parti… Et ouf !

```
La version actuelle du schéma est 47

Mise à jour du schéma à la version 69

Vérification de la signature du fichier
```

```
La commande s'est terminée correctement
Connexion à « srv-dc.cabare-intra.net » en cour
Connexion en tant qu'utilisateur actuel en util
Importation de l'annuaire à partir du fichier «
Chargement des entrées.....................
351 entrées modifiées.

La commande s'est terminée correctement
.....
.....
.....
.............
.....
.....
.....
.....
Adprep a mis à jour les informations au niveau
```

Un journal existe journal de mise à jour en **c:\windows\debug\adprep**log



Vérifier que

- l'attribut **Révision** de configuration soit passé à 15
- et **ObjectVersion** de schéma à 69

Déblocage de la réplication

pour débloquer la réplication sortante on passe la commande avec – (**à la place de +**) :

Pour cela:

repadmin /options *nom-serveur* **-disable_outbound_repl**

```
C:\adprep>repadmin /options srv-dc-aux.cabare-intra.net -DISABLE_OUTBOUND_REPL
Actuel : Options DSA : IS_GC DISABLE_OUTBOUND_REPL
Nouveau : Options DSA : IS_GC
```

Il est important de na pas s'inquiéter sur les premiers messages envoyés par **repadamin / showrepl**, car il faut du temps pour que le schéma se propage…

```
=== INSTANCES VOISINES ENTRANTES ==================================

DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 10:55:31, a échoué, résultat 8418 (0x20e2):
            L'opération de réplication a échoué en raison d'une correspondance de schémas incorrecte entre les serveurs impliqués.
        64 échecs consécutifs.
        Dernière réussite le 2016-04-26 09:22:51.

CN=Configuration,DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 10:57:15, a réussi.
```

```
=== INSTANCES VOISINES ENTRANTES ================================

DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 11:03:45, a réussi.

CN=Configuration,DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 10:57:15, a réussi.
```

Pour obtenir les 5 rôles

```
Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
Premier-Site-par-defaut\SRV-DC
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : dfcd6f8c-1645-4c32-b408-23ad5d96dac9
ID de l'invocation DSA : da687c08-0afb-449c-a303-0f3809269dc0

=== INSTANCES VOISINES ENTRANTES ================================

DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 14:06:34, a réussi.

CN=Configuration,DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 13:48:53, a réussi.

CN=Schema,CN=Configuration,DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 13:48:53, a réussi.

DC=ForestDnsZones,DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 13:48:53, a réussi.

DC=DomainDnsZones,DC=cabare-intra,DC=net
    Premier-Site-par-defaut\SRV-DC-AUX via RPC
        GUID de l'objet DSA : 6d9cd951-6069-4321-84ed-f8ab28091dd3
        La dernière tentative, le 2016-04-26 13:48:53, a réussi.
```

N.B: Attendez la réplication des modifications dans toute la forêt !.

Adprep pour le domaine

Sur le contrôleur de domaine qui héberge le rôle de **maître d'infrastructure**

- Taper **adprep /domainprep**
- Si on envisage à terme d'installer un contrôleur de domaine en lecture seule (**RODC**) il faut alors aussi passer la commande:

  adprep /rodcprep

N.B: Attendez la réplication des modifications dans tout le domaine !.

Intégration nouveau serveur membre 2012

Soit un Serveur 2012r2

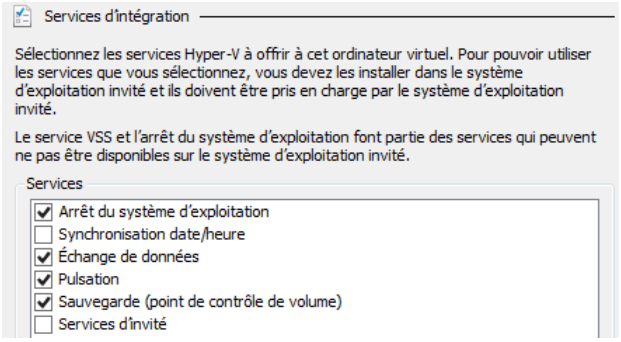
- qu'il faut renommer correctement, par exemple *srv-dc1*

- Avec un adressage Ip correct (adresse, masque, dns)
- Joint au domaine dans les règles, (compte machine dans l'AD, hôte et pointeur correspondant dans le DNS) srv-dc1

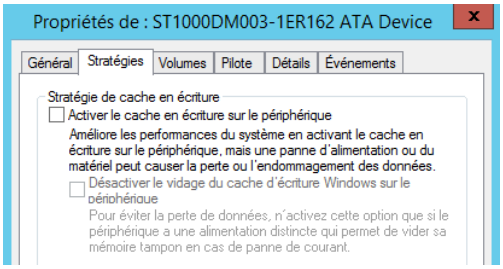
srv-dc1	Hôte (A)	192.168.1.91
192.168.1.91	Pointeur (PTR)	srv-dc1.cabare-intra.net.

- Test avec nslookup

N.B : penser à désactiver pour une VM la synchronisation date/heure dans les services d'intégration



N.B : penser à désactiver pour une VM posée sur un disque IDE le cache en écriture disque

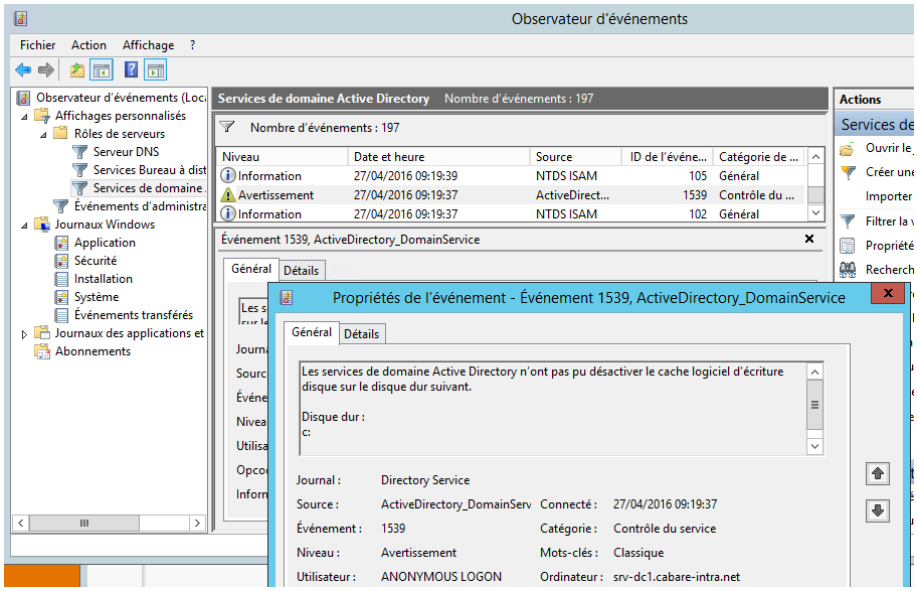


Si cela n'est pas possible,(la coche « revient » il faut soit

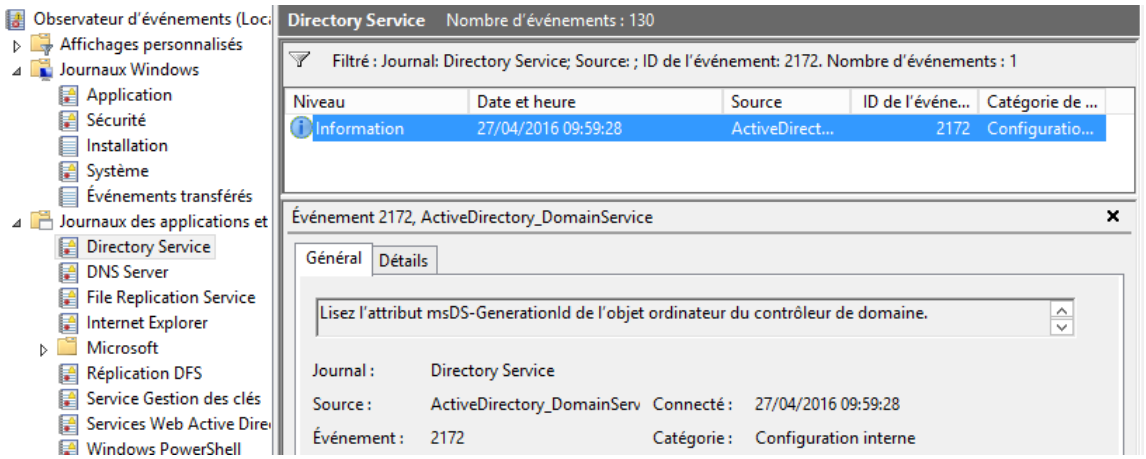
- Dévalider le cache dans le Bios
- Poser la Vm sur un disque SCSI !

En effet dans le cas d'une machine virtuelle, le cache est "émulé" et n'est pas protégé par une batterie physique. Les données qu'il contient sont donc perdues en cas de crash de votre serveur physique.

Le problème est résolu par l'installation du rollup KB2855336 Lorsque Active Directory cherche à désactiver le cache, Hyper-V répondra alors "Failure", ce qui permettra à AD de demander l'écriture directe sur le disque. La conséquence est l'apparition du warning suivant dans le journal d'évènement de votre VM. Donc sur un serveur 2012 on doit voir appraitre l'evenement 1539 sur Active directory, c'est que tout va bien !

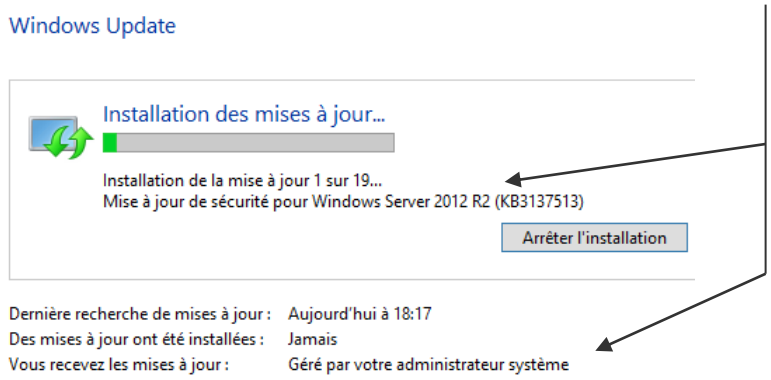


N.B : penser à ne pas faire de **snapshot** sur un **DC** sauf s'il intègre une gestion de l'évènement 2170. A partir de **Windows 2012** et si l'hyperviseur supporte le "**GenerationID**" il est possible d'utiliser des fonctionnalités supplémentaires tel que les "snapshot" ou le clonage de contrôleur de domaine. Ce dernier détectera un retour en arrière, par l'intermédiaire de cette nouvelle propriété de la machine virtuelle, il sera en mesure de rattraper le décalage de réplication.



Rôle AD DS Directory Services , DNS

Sur notre Serveur 2012r2 il faut installer les mises à jour de sécurité nécessaires

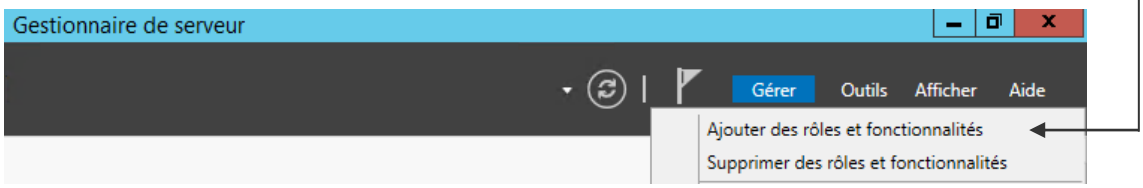


et ensuite ajouter 2 rôles qui permettront de prendre en charge le domaine

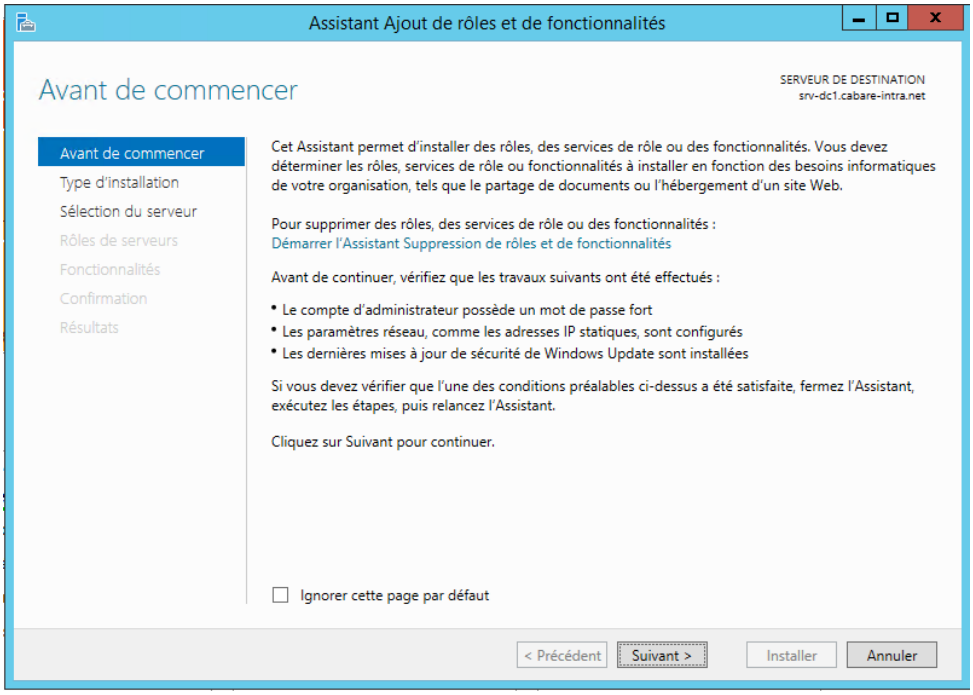
- Le rôle AD DS Directory Service
- Le rôle DNS

Soit dans le **Gestionnaire de serveur**, **Tableau de bord** puis dans **Configurer ce serveur local** on demande **Ajouter des rôles**

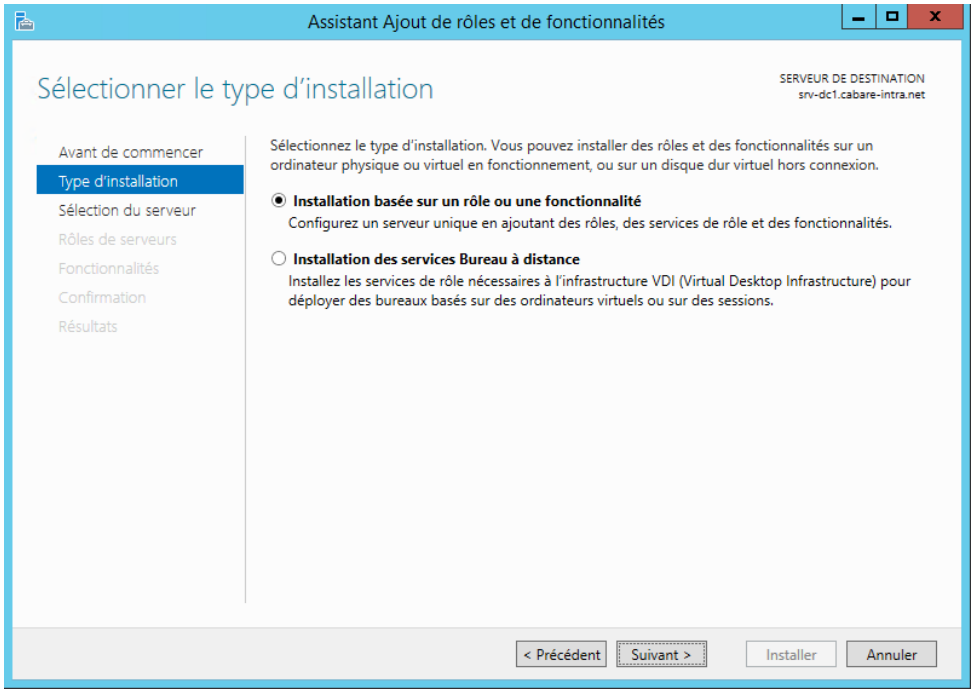
Sinon à tout moment, dans le **Gestionnaire de serveur**, en haut à droite on demande **Ajouter des rôles et des fonctionnalités**



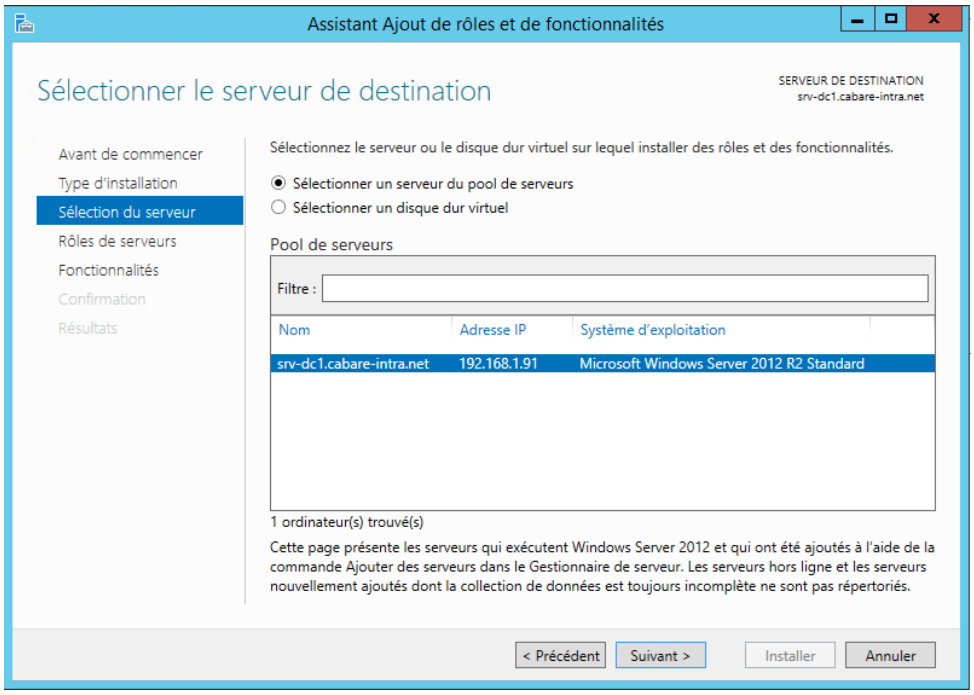
On déclanche l'assistant



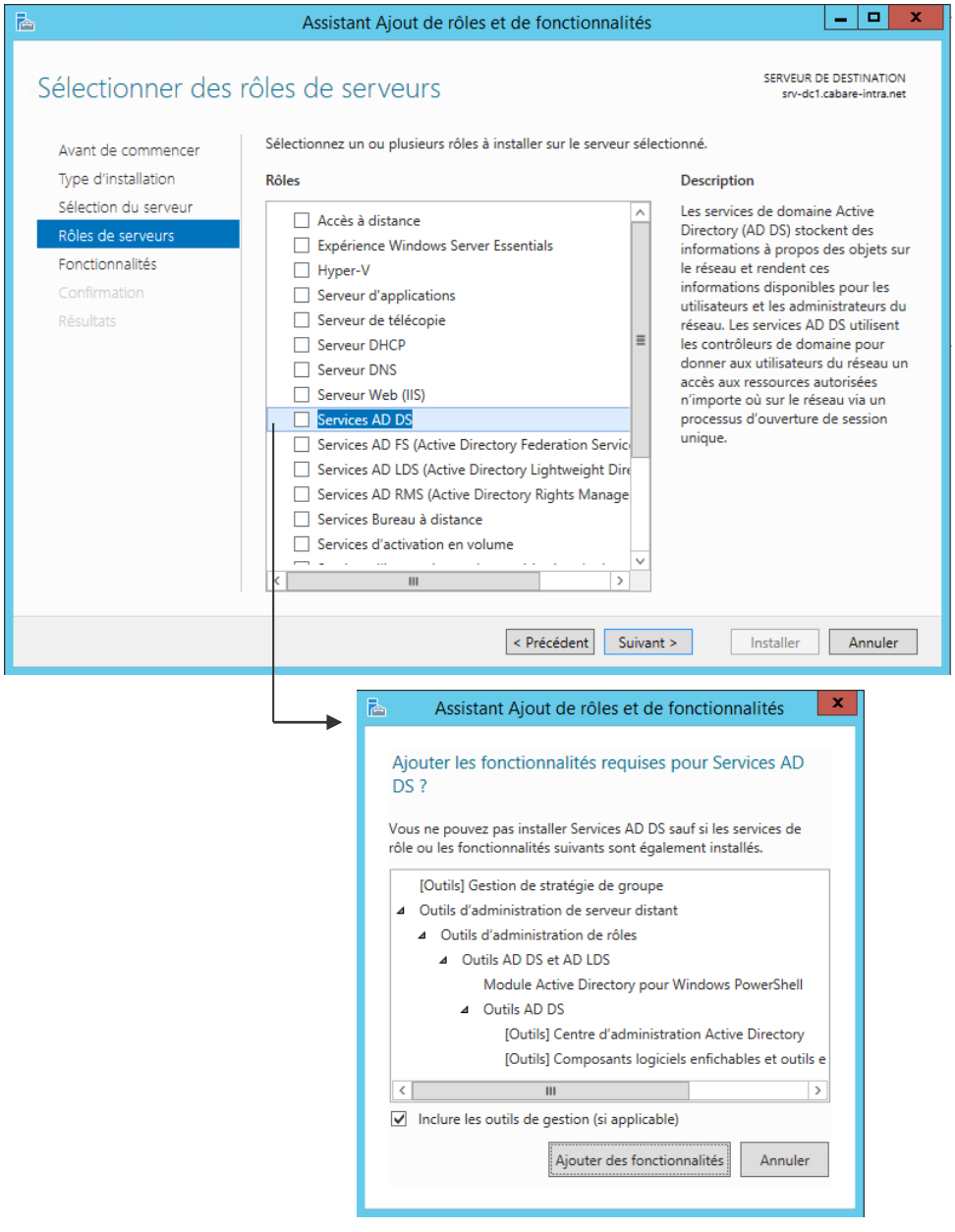
On demande d'ajouter un rôle



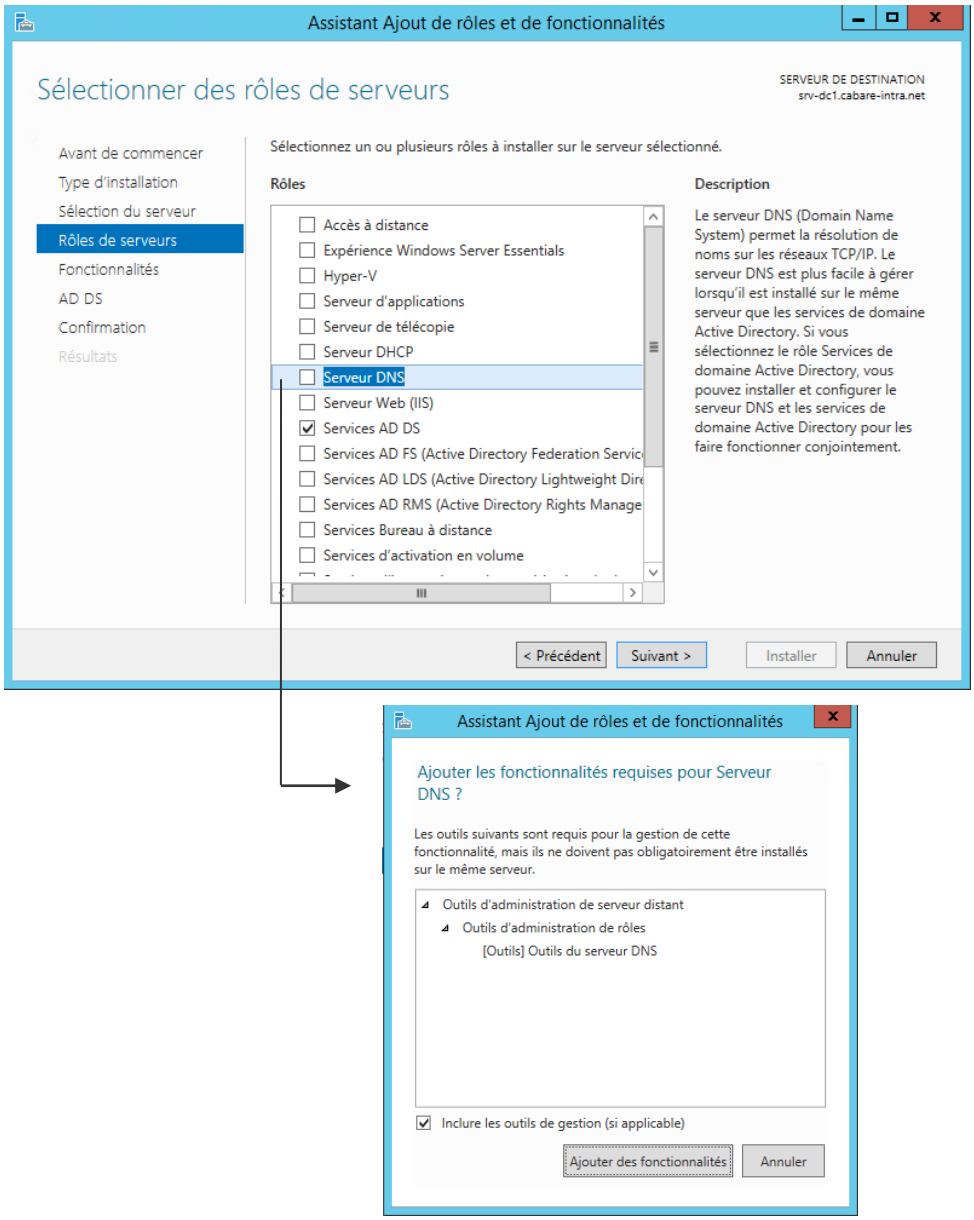
Sur notre serveur



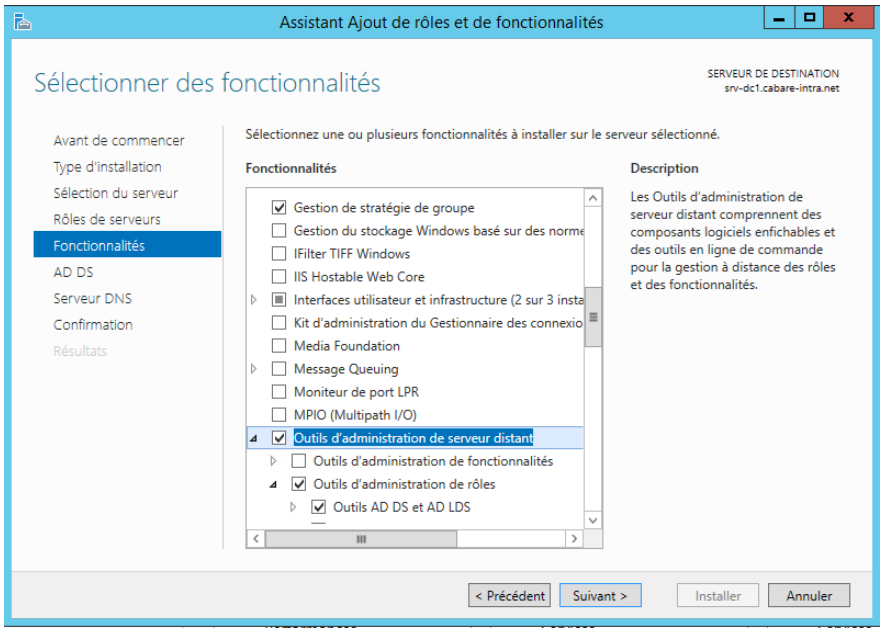
Les services **AD DS** (et les fonctionnalités associées)



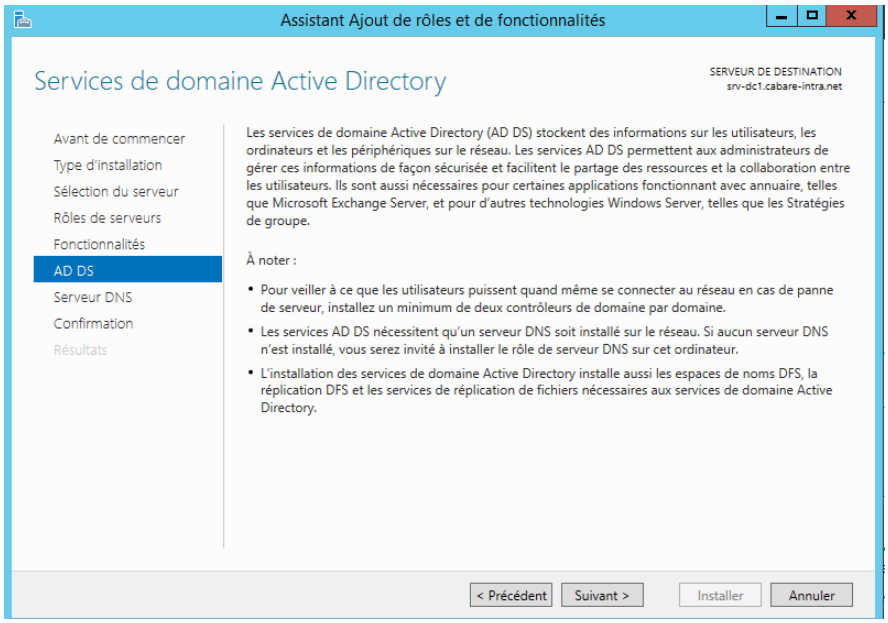
Puis le rôle **DNS** (et les fonctionnalités associées)



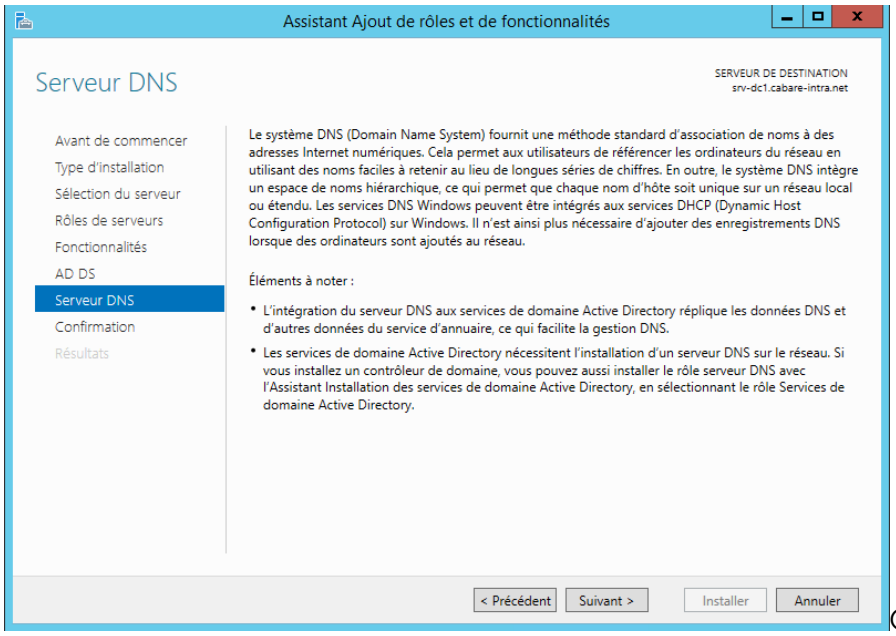
Du coup dans l'étape suivante des fonctionnalités on n'a rien à faire, ce qui doit être coché l'est déjà (cela s'est fait précédemment)



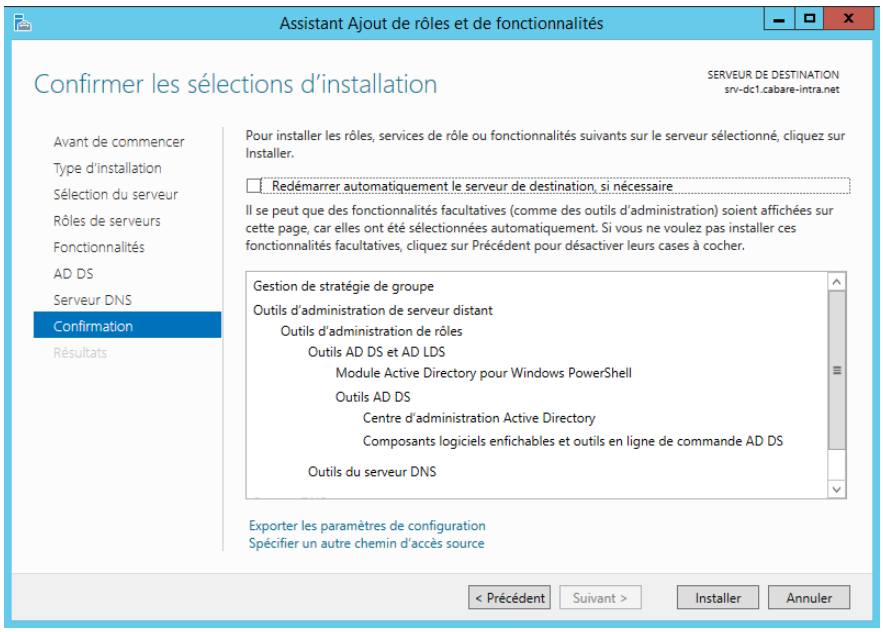
Ensuite on nous invite à penser à installer un 2° CD et un DNS au minimum…



On nous conseille de stocker la zone DNS dans Active directement…

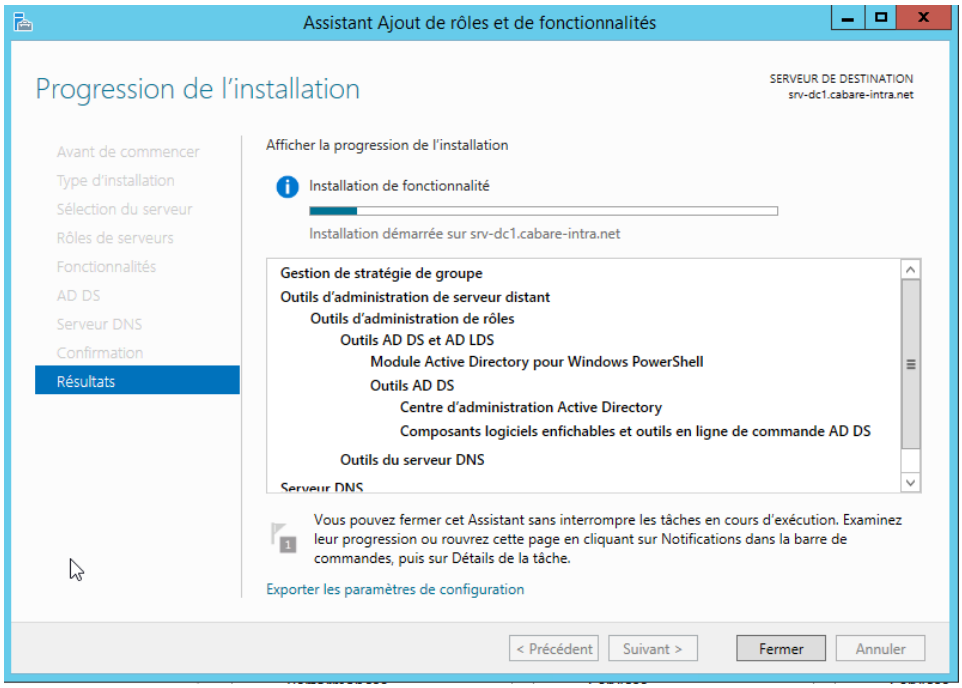


On confirme



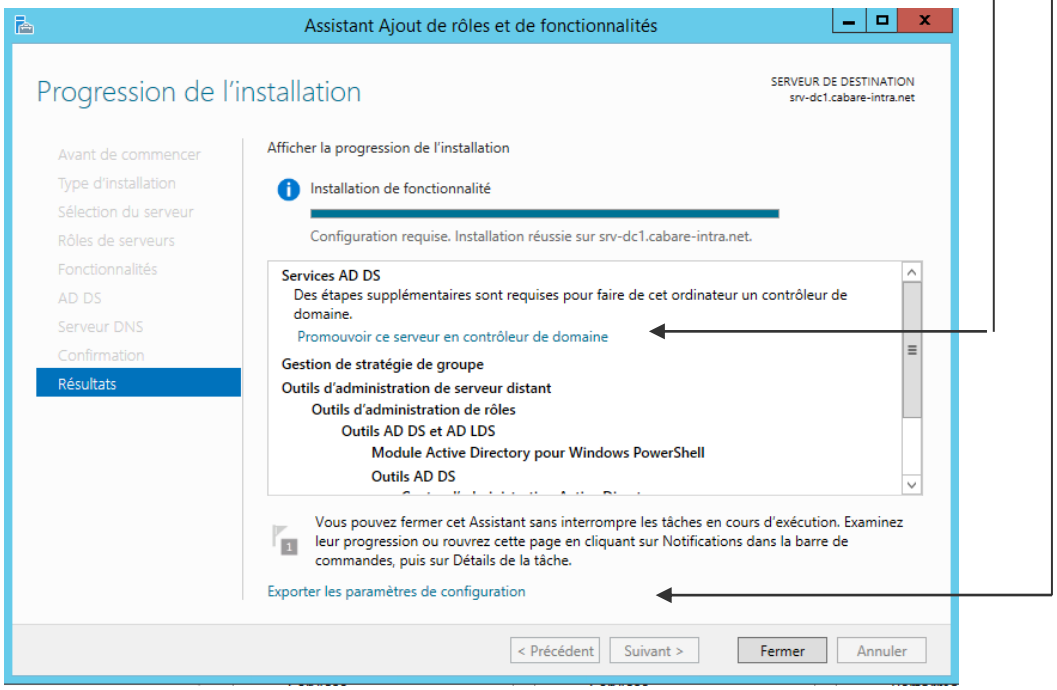
on **Installe**

Et c'est terminé



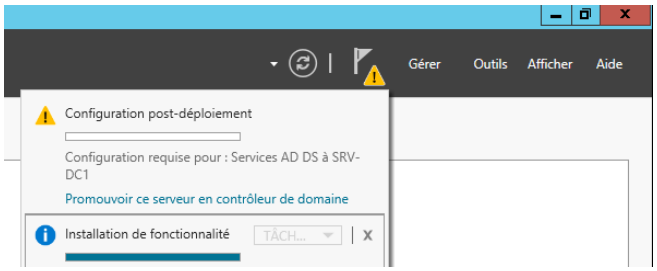
Lorsque l'on obtient la réussite de l'installation il sera possible de

- Promouvoir le serveur en CD
- Eventuellement Exporter les pramètres de configuration

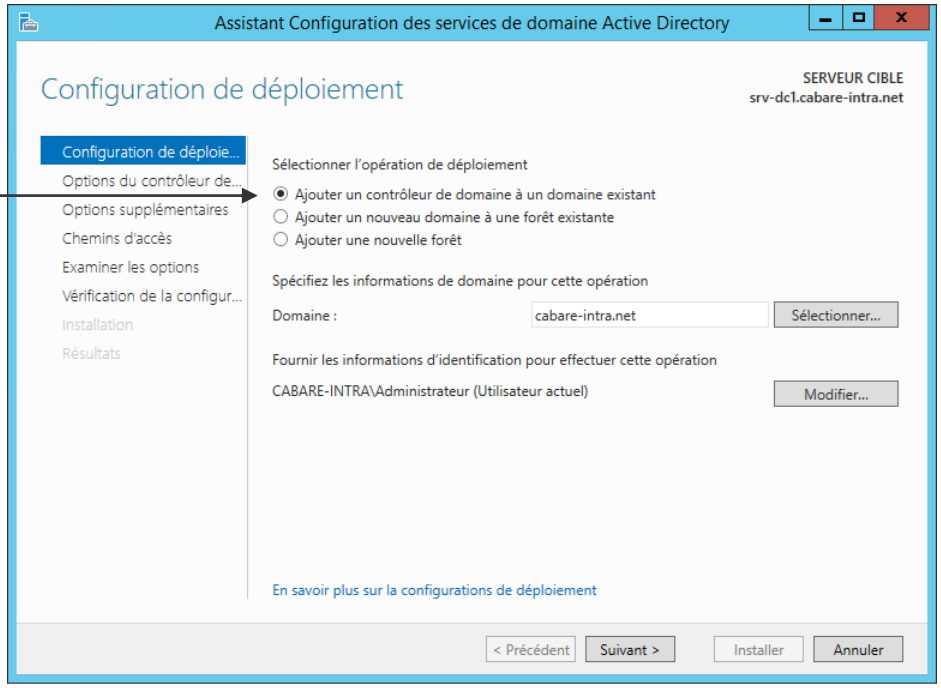


Assistant de configuration Active Directory (ex dcpromo)

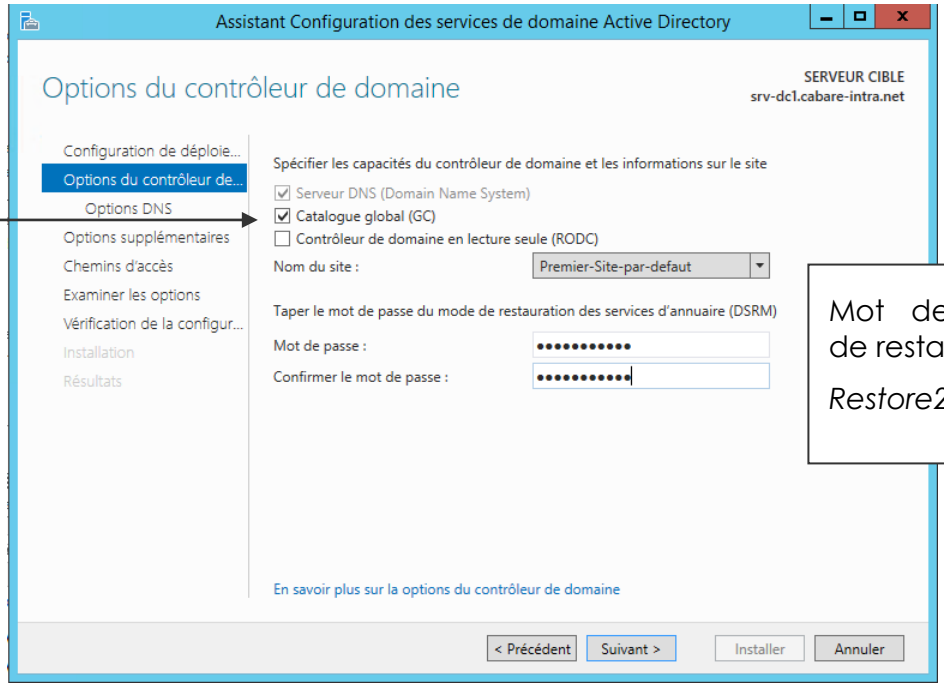
Peut importe de cliquer ou non sur le lien précédent **Promouvoir ce serveur en contôleur de domaine** car le **gestionnaire de serveur** nous le reproposera



Donc on veut ajouter un DC



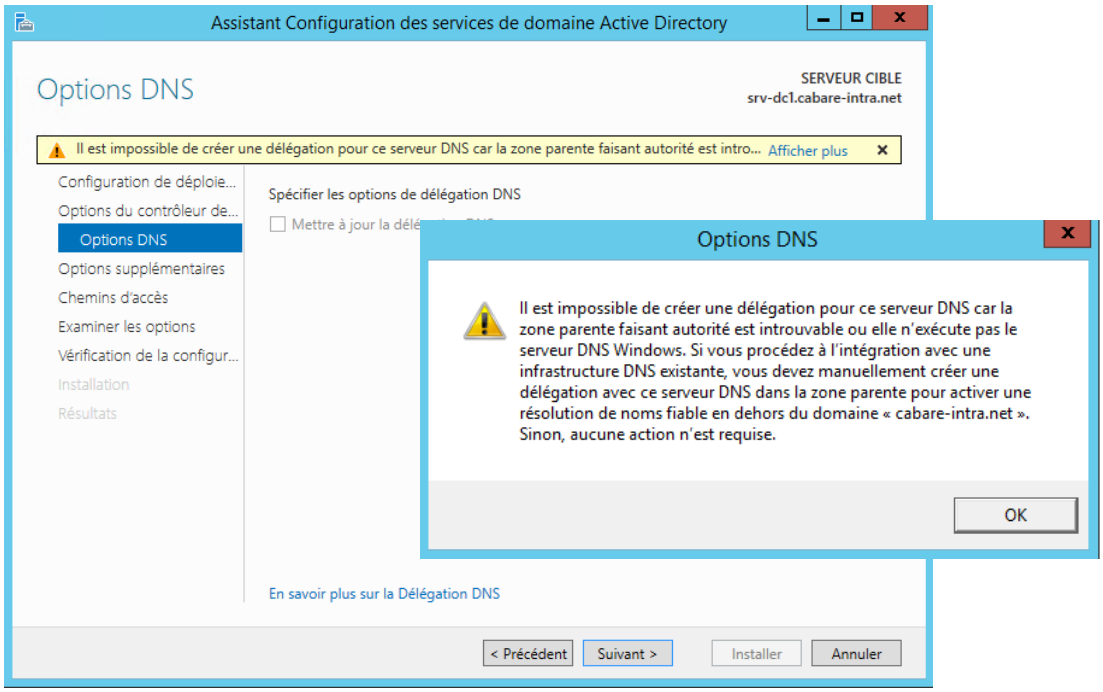
Qui sera aussi serveur DNS et Catalogue Global



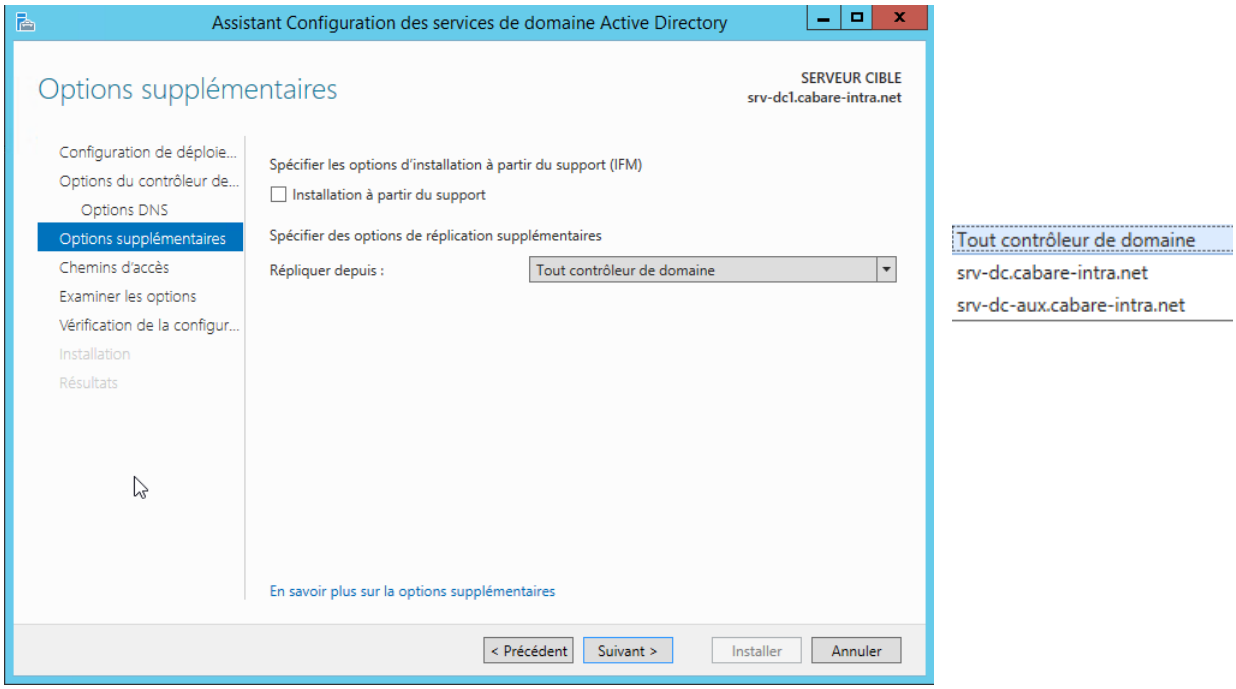
Mot de passe de restauration

Restore2012

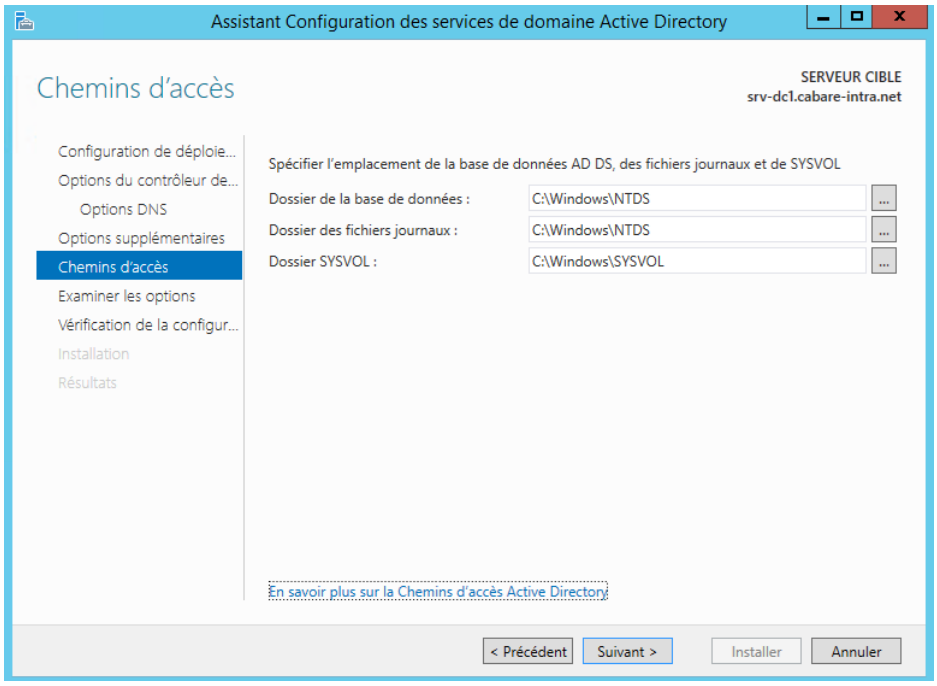
Ce message est normal car on est à la racine de la forêt



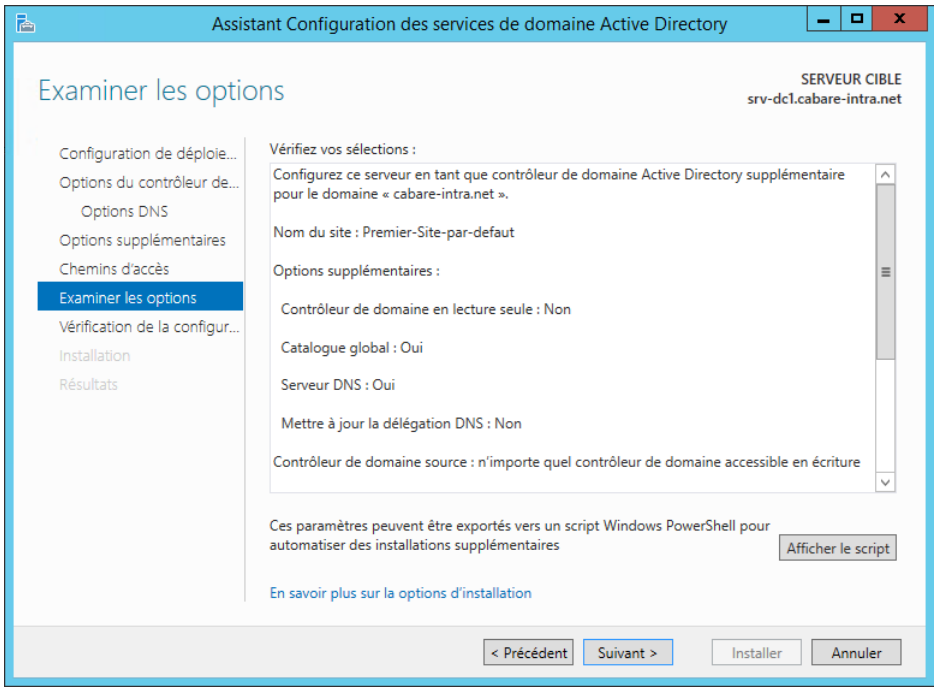
… on demande suivant



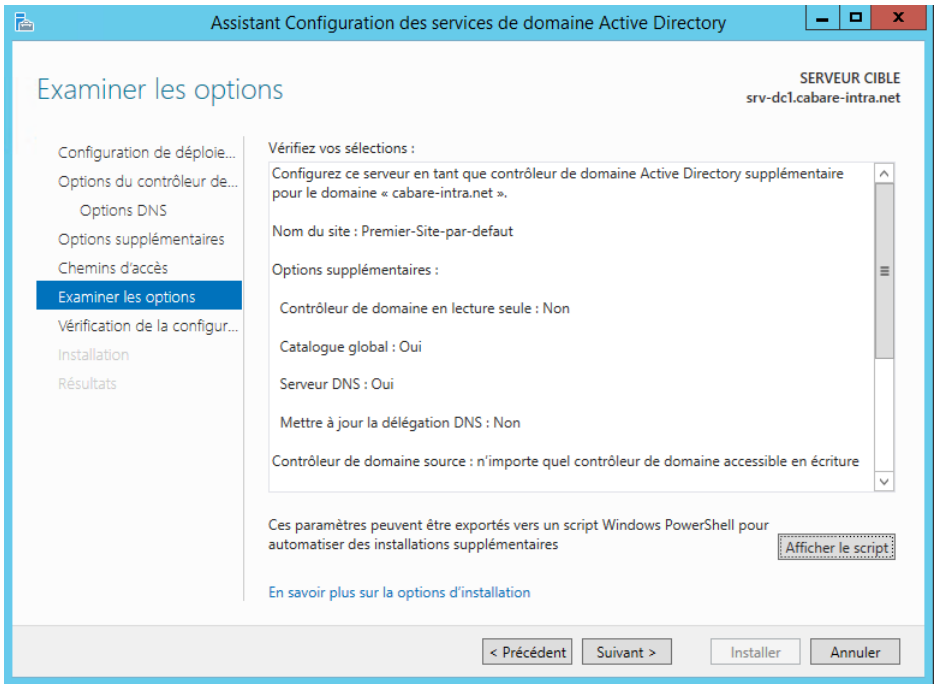
Il est préférable de laisser choisir le serveur avec lequel il trouve la meilleure bande passante… **Suivant**



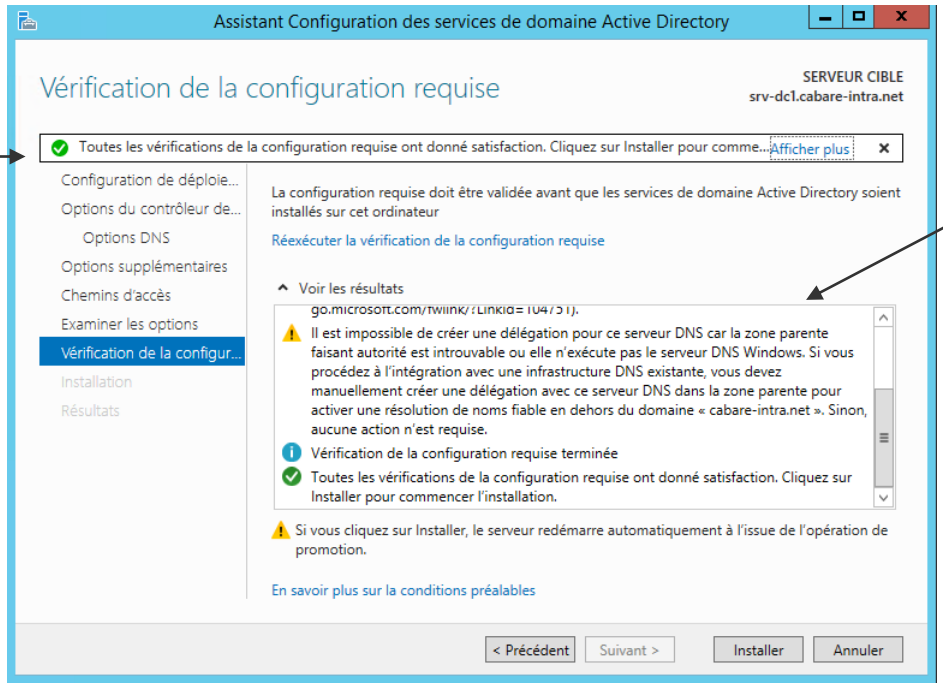
On lui laisse installer la Base AD et le réplica où il le souhaite par défaut…



On à une confirmation des paramètres



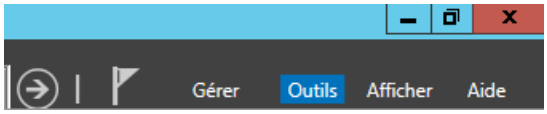
Et un test général est effectué avant l'execution réelle, si tout est ok on peut lancer l'installation après avoir lu les informations eventuelles



Il y aura ensuite re démarrage du serveur…

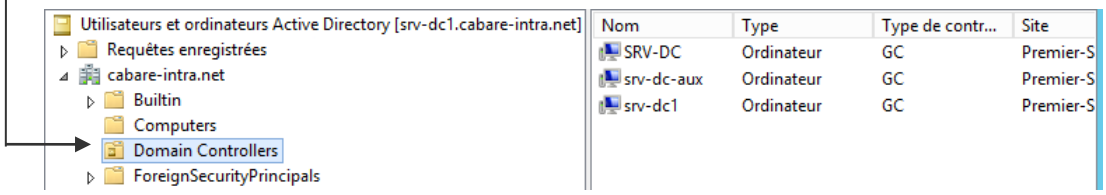
Test serveur et réplication générale

Dans le **Gestionnaire de serveur**, dans **Outils**

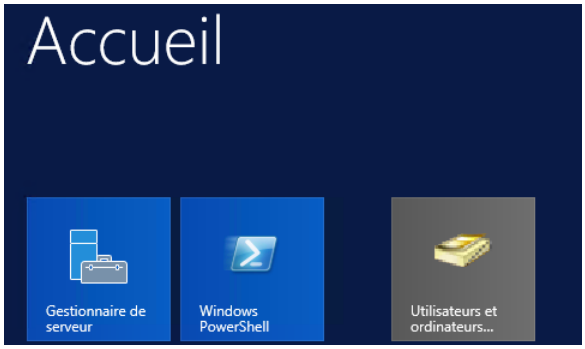


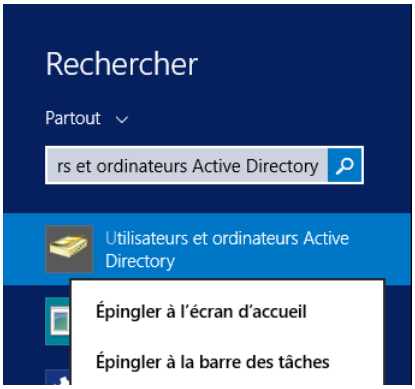
On demande, **Utilisateurs et ordinateurs Active Directory**

- Le compte de notre serveur **DC** doit faire partie de l'**UO Domain Controllers**

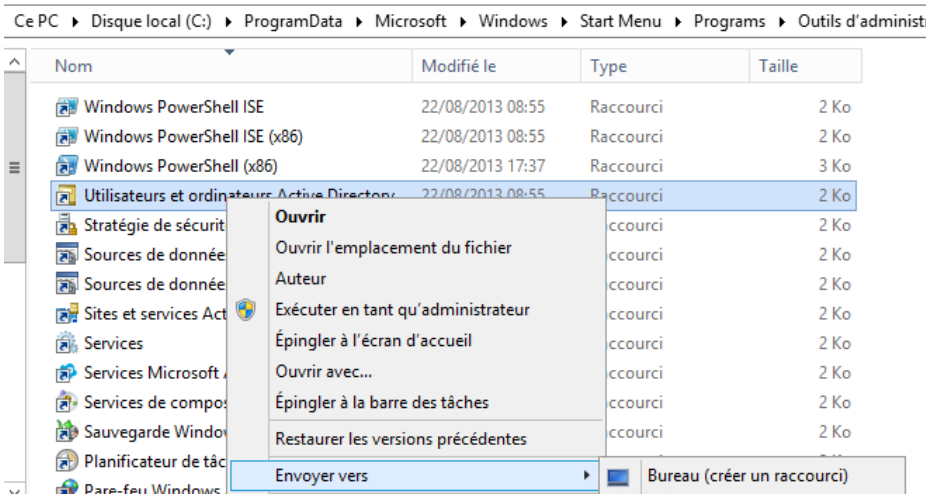


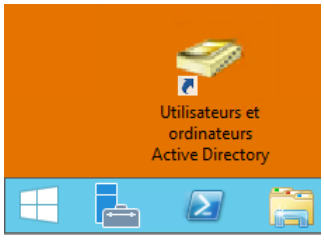
On peut aussi une fois pour toutes effectuer une recherche et **épingler** la mmc à **l'écran d'accueil,** Pour obtenir



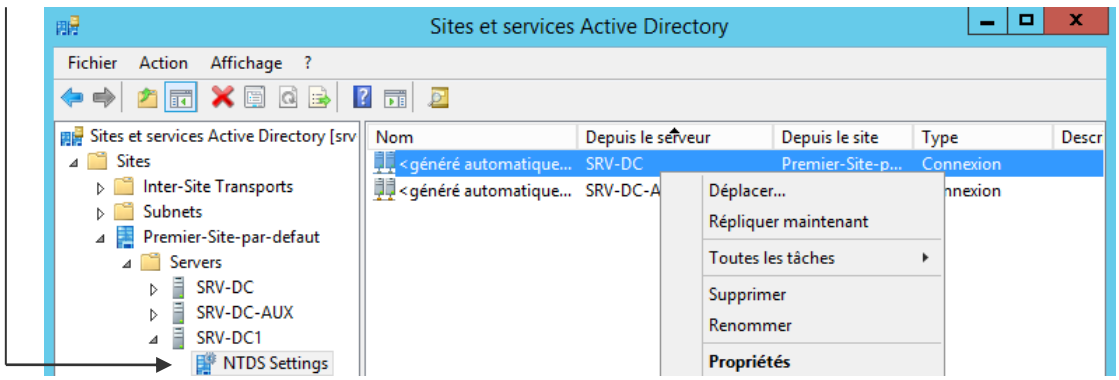


Ou, si l'on est « faché » avec l'interface metro et que l'on veut retrouver des raccourcis sur le bureau, on accède au dossier des outils d'administration et on copie les raccourcis sur le buro…

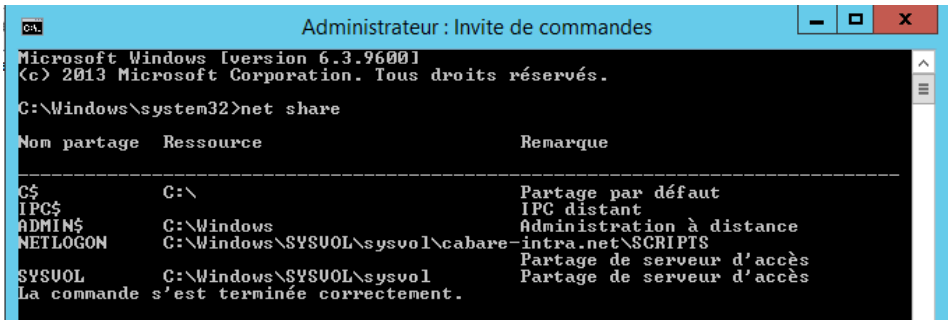




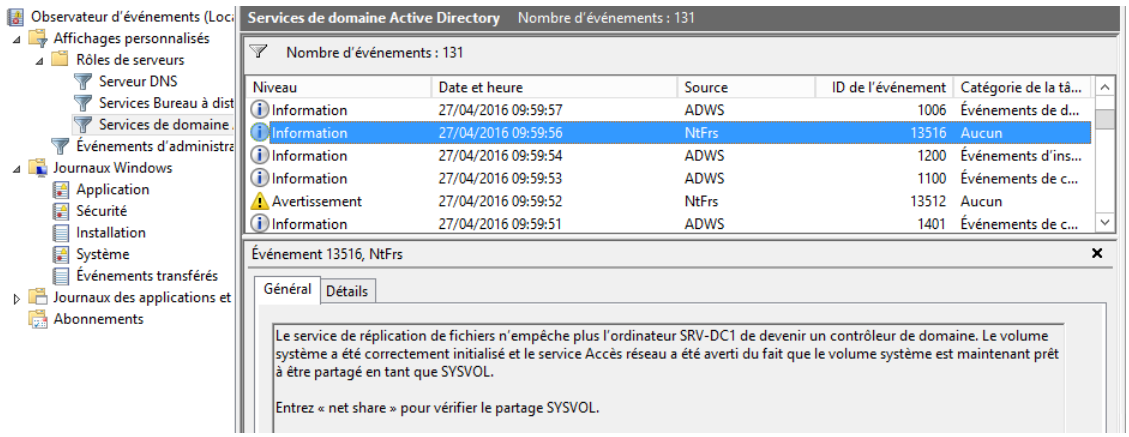
- La réplication doit être active entre le nouveau **srv-dc1** et les autres DC



- On vérifie avec **net share** les partages par défaut **netlogon** et **sysvol**



- Dans l'observateur d'évènement, on vérifie que la réplication soit bien terminée est que désormais notre serveur est bien contrôleur de domaine.



- Un **repadmin /showrepl** devrait être ok, voire un **repadmin /replsummary**

- Un **dcdiag** devrait sous 48 heure donner de bons résultats…

N.B : un message de type warning peut subsister sur le test **machineAccount** du genre

```
Démarrage du test : MachineAccount
   Avertissement : l'attribut userAccountControl de SRV-DC1
   est 0x82020 = ( PASSWD_NOTREQD | SERVER_TRUST_ACCOUNT | TRUSTED_FOR_DELEGATION )
   Paramètre par défaut pour un contrôleur de domaine :
   0x82000 = ( SERVER_TRUST_ACCOUNT | TRUSTED_FOR_DELEGATION )
   Cette situation peut avoir une incidence sur la réplication.
   ..... Le test MachineAccount
    de SRV-DC1 a réussi
```

Cela arrive si le compte machine a été créé manuellement avant la promotion du serveur en CD,

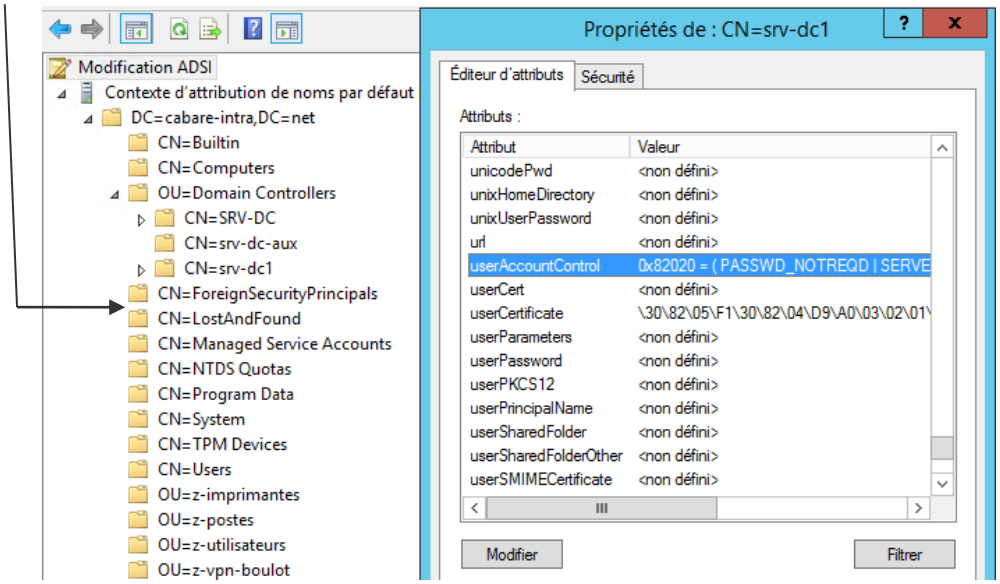
Les valeurs normales de l'attribut **userAccountControl** sont

Normal user :	0x200	(512)
Domain controller:	0x82000	(532480)
Workstation/server:	0x1000	(4096)

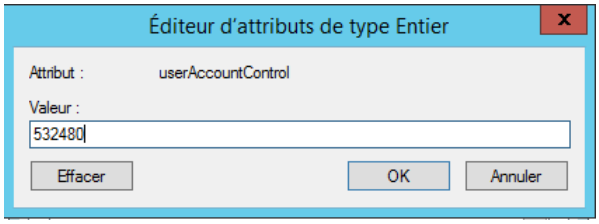
Ici on se retrouve avec la valeur 0x82020 (532512).

Cela peut se modifier via **adsiedit.msc**

On demande **contexte d'attribution de noms par défaut** / **DC** puis **OU= Domain Controllers** et on se place sur notre serveur **srv-dc1**



La valeur normale de l'attribut **userAccountControl** est de 0x82000 soit 532480 en décimal



Suite à quoi notre test **dcdiag** sera parfait…

Paramétrage IP pour le serveurs DNS et sur le Domaine

Reglages Adresses IP :

Chaque serveur DNS doit indiquer

- qu'il dépends de lui-même, (1° serveur DNS)
- et du serveur dont il est le réplica (2° serveur DNS)

Liste de tous les serveurs DNS disponibles sur le domaine :

La commande **nslookup** avec la syntaxe suivante :

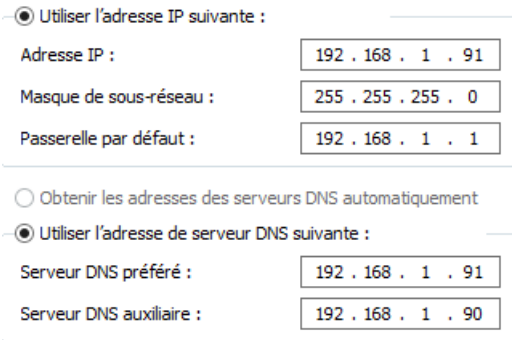
Nslookup –type=ns domaine

permet de lister tous les serveurs DNS (ici 3) enregistrés comme tels

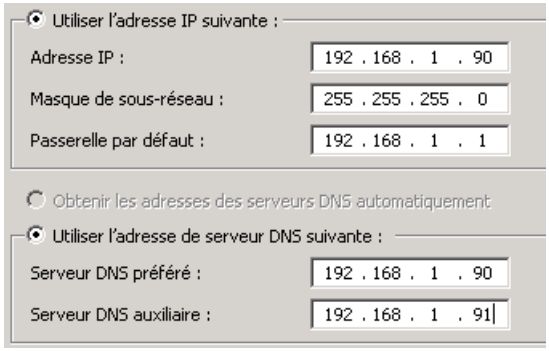
```
C:\Windows\system32>nslookup -type=ns cabare-intra.net
Serveur :   srv-dc.cabare-intra.net
Address:  192.168.1.90

cabare-intra.net        nameserver = srv-dc1.cabare-intra.net
cabare-intra.net        nameserver = srv-dc-aux.cabare-intra.net
cabare-intra.net        nameserver = srv-dc.cabare-intra.net
srv-dc1.cabare-intra.net        internet address = 192.168.1.91
srv-dc-aux.cabare-intra.net     internet address = 192.168.1.99
srv-dc.cabare-intra.net internet address = 192.168.1.90
```

Donc si on garde uniquement *srv-dc1* et *srv-dc* cela donnerait

Sur srv-dc1



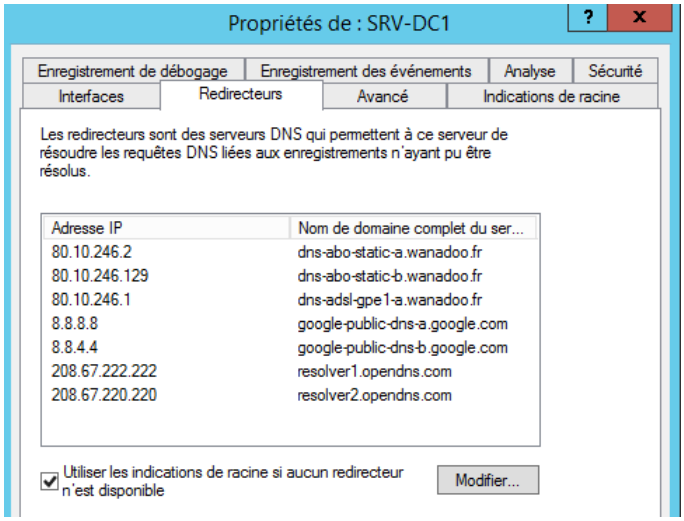
sur srv-dc



Reglages redirecteurs :

Si la notion de re-directeur est utilisée sur le 1° serveur DNS, il faut les re-paramétrer sur le 2° serveur DNS

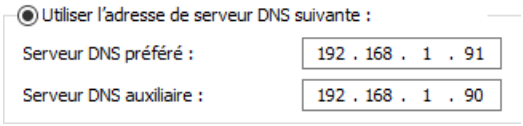
En effet ces réglages sont indiqués "hors zone" et donc non répliqués via AD, ils doivent donc être reconstruits sur chaque serveur DNS… !



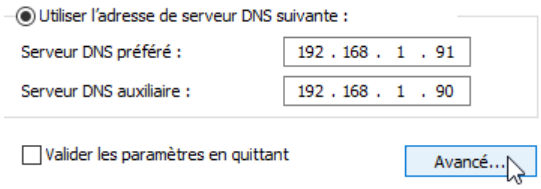
Paramétrage des clients Ip en dur:

Il est juste nécessaire de spécifier pour les clients que le serveur DNS auxilliaire se trouve à telle adresse IP (l'adresse de notre 2° CD avec son Serveur DNS…

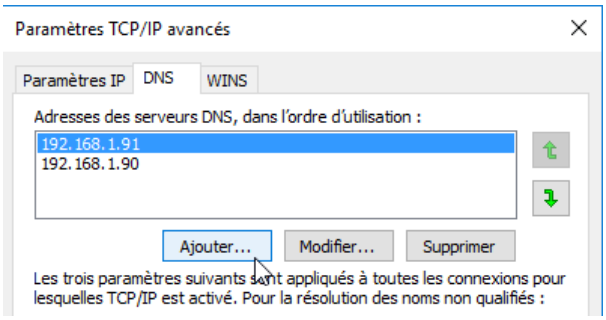
Il suffit d'indiquer dans les paramètres TCP/IP l'adresse de nos deux serveurs DNS,



N.B : s'il y a plus de 2 serveurs DNS on peut demander **Avancé…**

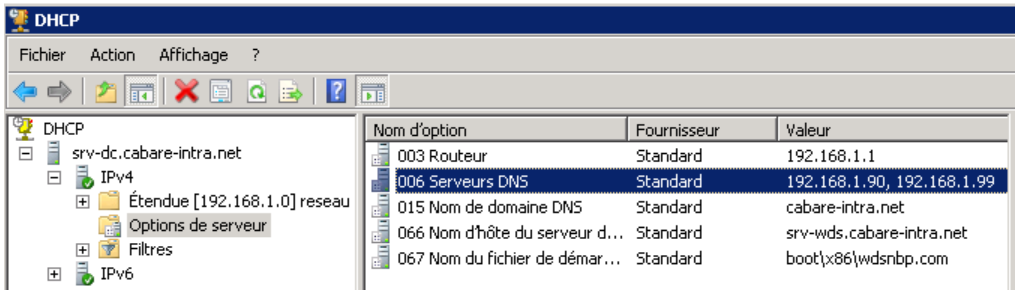


Puis onglet **DNS** et **Ajouter**

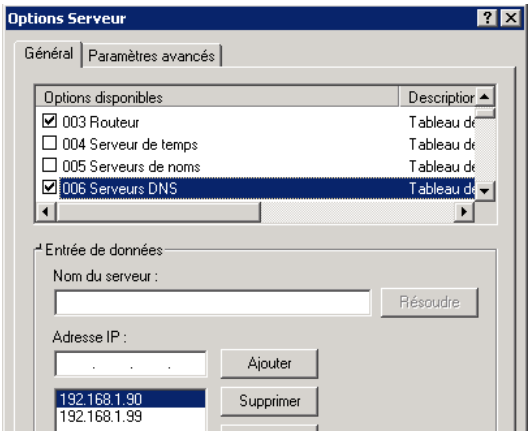


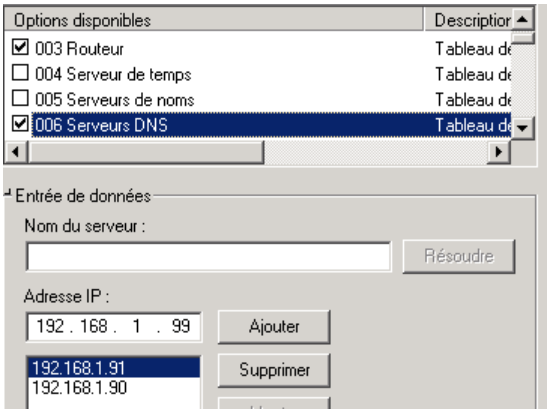
Options de serveur DHCP :

Si il y a un DHCP, il est necessaire de modifier l'option **006**, **serveurs DNS**



Pour passer de à





Le transfert ne peut se faire qu'entre 2 CD fonctionnels et en relation. On ne traitera pas ici la « **prise de rôle** » mais le « **transfert de rôle** » depuis srv-dc vers un nouveau serveur 2012 nommé *srv-dc1)*. Qui peut transférer les rôles ?

Sur le Domaine

- **Emulateur CPD (NT 4.0)** : GG Administrateurs du domaine
- **Maître identificateur Relatif RID** : GG Administrateurs du domaine
- **Maître d'infrastructure** : GG Administrateurs du domaine

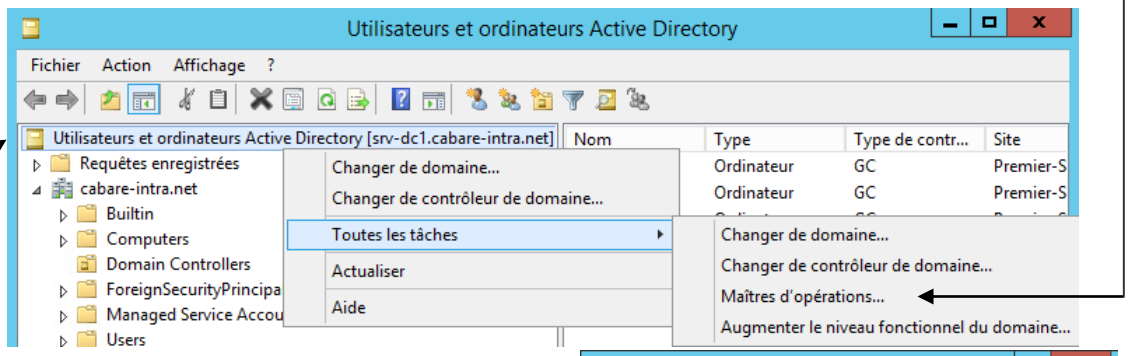
Sur la fôret (et l'ensemble des domaines))

- **Maître d'attribution de nom de domaine** : GG Administrateurs de l'entreprise
- **Contrôleur de schéma** : GG Administrateurs du schéma

On repère les rôles FSMO par la commande **Netdom query fsmo**

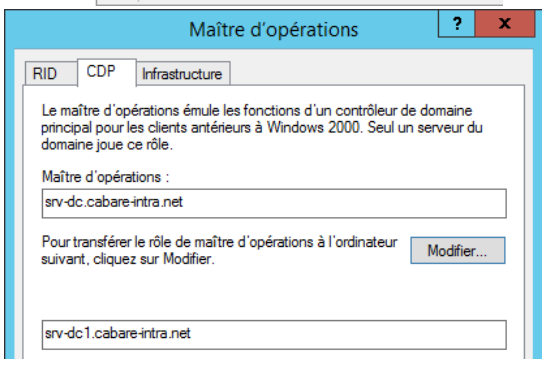
```
C:\Users\Administrateur.CABARE-INTRA>netdom query fsmo
Contrôleur de schéma         srv-dc.cabare-intra.net
Maître des noms de domaine   srv-dc.cabare-intra.net
Contrôleur domaine princip.  srv-dc.cabare-intra.net
Gestionnaire du pool RID     srv-dc.cabare-intra.net
Maître d'infrastructure      srv-dc.cabare-intra.net
L'opération s'est bien déroulée.
```

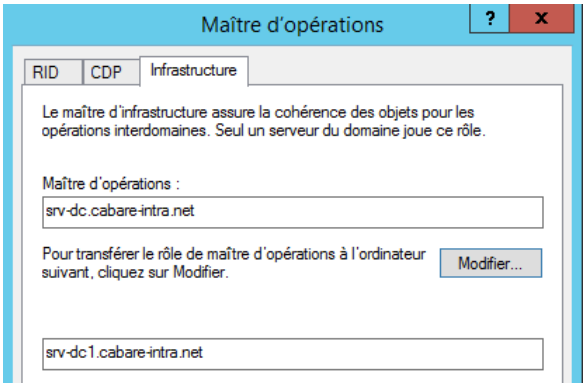
Avec la console **Utilisateur et ordinateur Active Directory** on peut trouver les 3 maîtres de domaine : clic droit **Toutes les tâches** / **Maîtres d'opérations…**

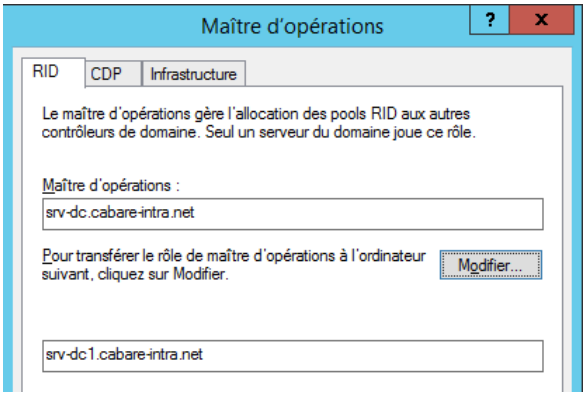


N.B : Il faut se placer sur le serveur sur lequel l'on veut tirer les rôles

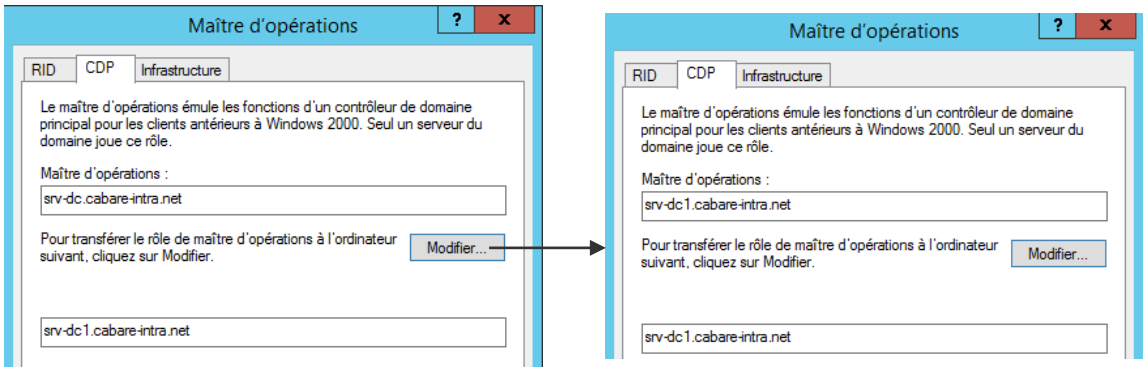
- Emulateur CPD (NT 4.0)
- Maître identificateur Relatif RID
- Maître d'infrastructure







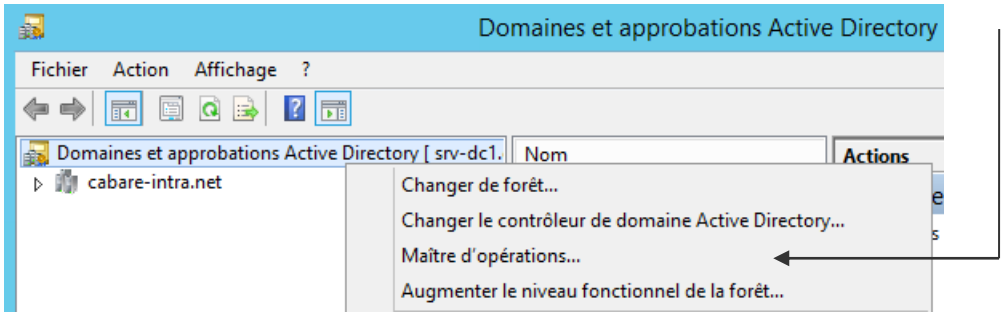
Le transfert se faisant simplement en demandant **Modifier…**, par exemple



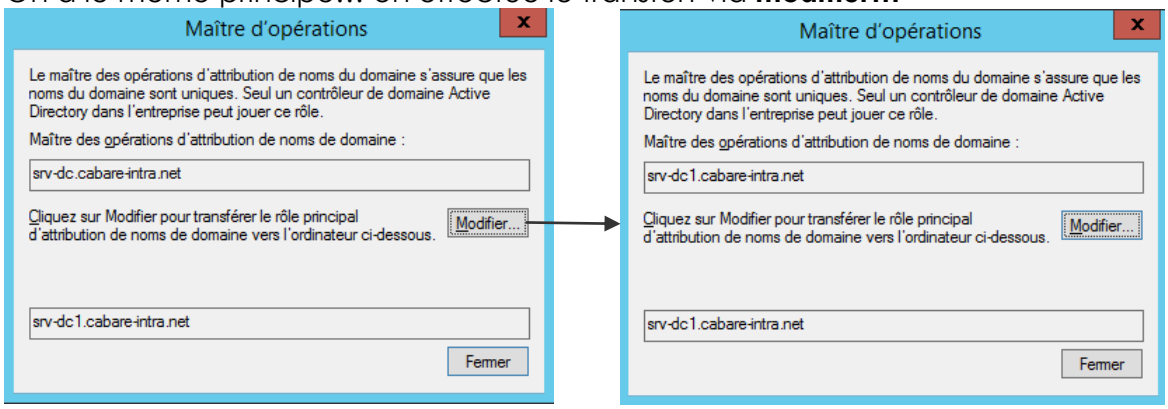
On peut vérifier par

```
C:\Windows\system32>netdom query fsmo
Contrôleur de schéma          srv-dc.cabare-intra.net
Maître des noms de domaine    srv-dc.cabare-intra.net
Contrôleur domaine princip.   srv-dc1.cabare-intra.net
Gestionnaire du pool RID      srv-dc1.cabare-intra.net
Maître d'infrastructure       srv-dc1.cabare-intra.net
L'opération s'est bien déroulée.
```

Avec la console **Domaine et approbation Active Directory** on peut trouver qui est maître d'attribution de nom de Domaine. En se plaçant sur **Domaines et approbations Active Directory** on demande clic droit **Maîtres d'opérations…**



On à le même principe… on effectue le transfert via **modifier…**



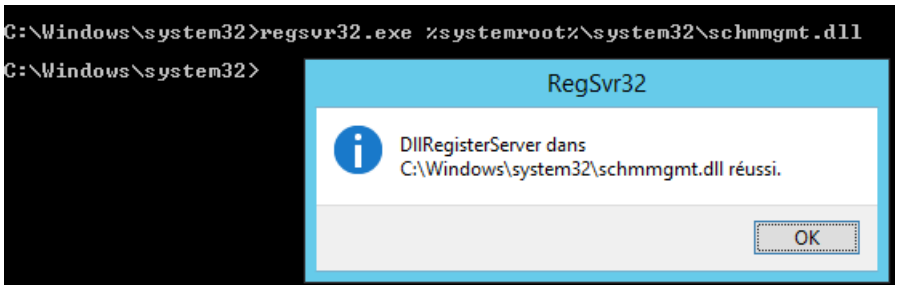
On peut vérifier par

```
C:\Windows\system32>netdom query fsmo
Contrôleur de schéma          srv-dc.cabare-intra.net
Maître des noms de domaine    srv-dc1.cabare-intra.net
Contrôleur domaine princip.   srv-dc1.cabare-intra.net
Gestionnaire du pool RID      srv-dc1.cabare-intra.net
Maître d'infrastructure       srv-dc1.cabare-intra.net
L'opération s'est bien déroulée.
```

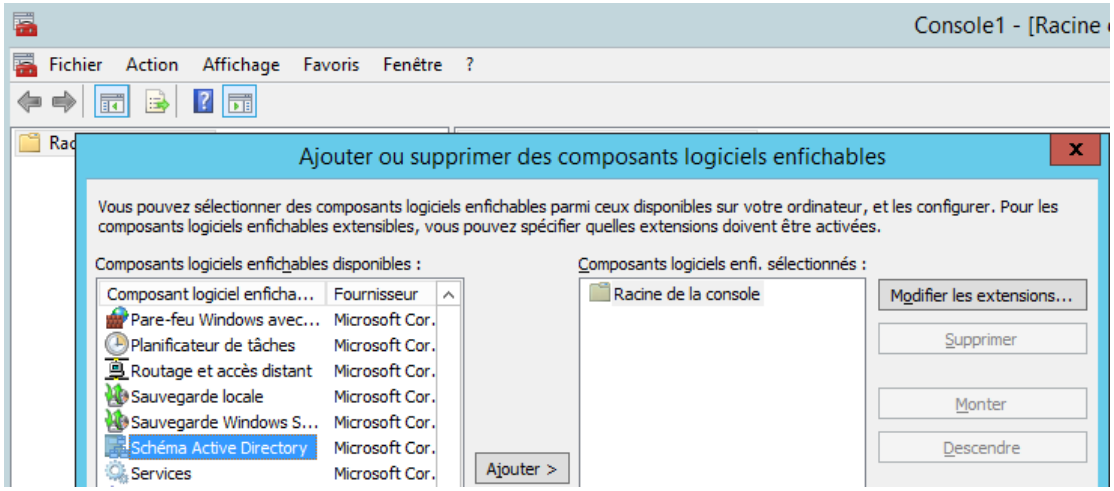
Reste le schéma…

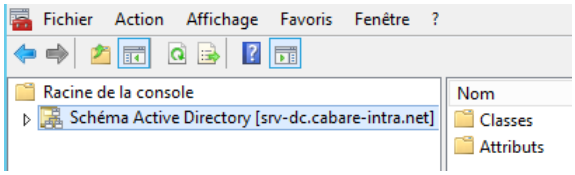
Pour localiser le maître de schéma, c'est le plus difficile. Il d'abords créer l'exécutable qui pourra ouvrir la console mmc

Via la commande **regsvr32.exe %systemroot%\system32\schmmgmt.dll**

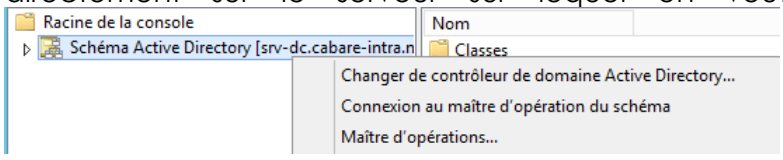


Puis on peut alors créer une console, via executer **mmc** dans laquelle on demande **Fichier / Ajouter ou supprimer des composants logiciels enfichables** et on choisit la console **Schéma active Directory**



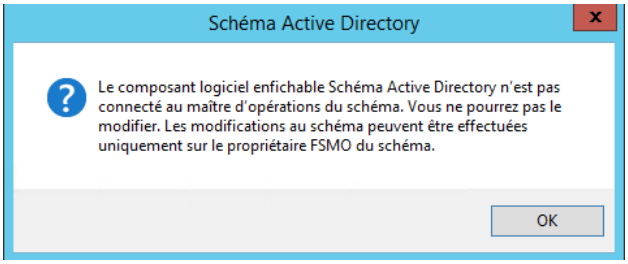


N.B : Si on est sur le serveur maître d'opération, il faut alors d'abords se connecter sur le serveur sur lequel on veut effectuer le transfert. **Via Changer de contrôleur de domaine Active Directory**. On peut aussi ouvrir la console directement sur le serveur sur lequel on veut transférer le rôle.



N.B : Mais lorsque l'on travaille avec le Contrôleur de schéma, on est toujours logué logiquement par défaut sur le serveur maître d'opération ! Il faut bien penser à se connecter sur le serveur sur lequel on veut effectuer le transfert…

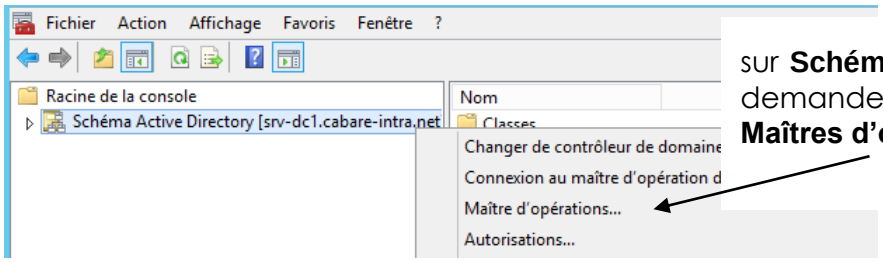
N.B : Ne pas préter attention aux messages indiquant que sur ce serveur on ne pourra pas administrer le schéma…



C'est normal, le rôle n'y est pas encore …

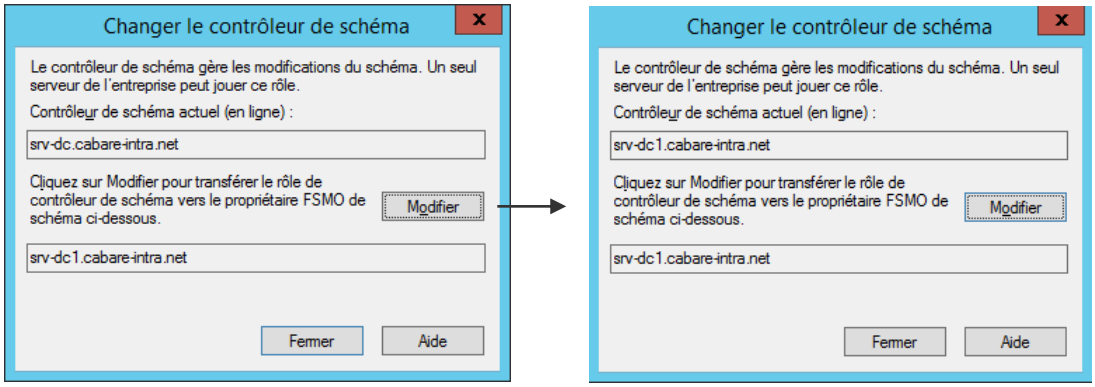
Donc on se place sur le serveur de

destination puis



sur **Schéma Active Directory** on demande clic droit **Propriétés / Maîtres d'opérations…**

Et on tranfère le dernier rôle



Et c'est terminé

```
C:\Windows\system32>netdom query fsmo
Contrôleur de schéma          srv-dc1.cabare-intra.net
Maître des noms de domaine    srv-dc1.cabare-intra.net
Contrôleur domaine princip.   srv-dc1.cabare-intra.net
Gestionnaire du pool RID      srv-dc1.cabare-intra.net
Maître d'infrastructure       srv-dc1.cabare-intra.net
L'opération s'est bien déroulée.
```

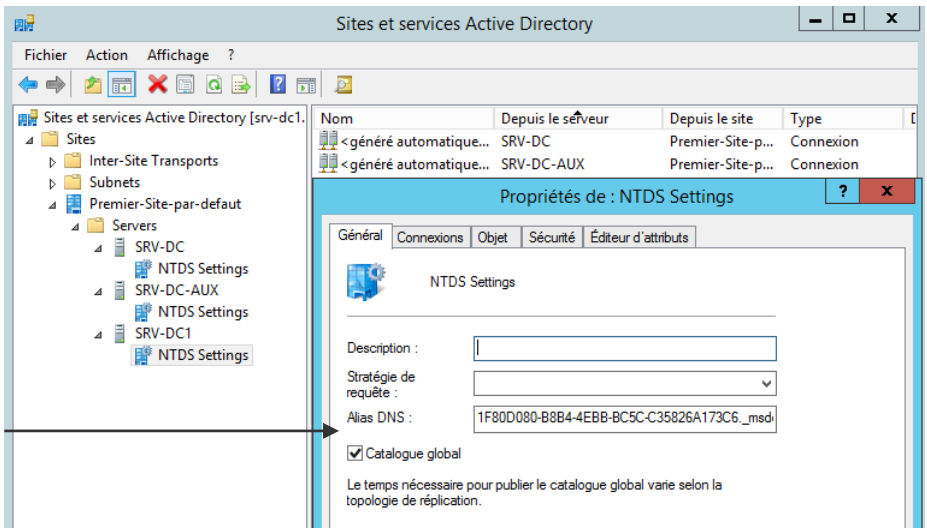
Suppression Catalogue Global ancien serveur

Localisation du Catalogue Global :

A part le **premier DC du premier domaine de la forêt**, Un DC n'est PAS par défaut serveur de Catalogue Global

On peut vérifier si un DC est serveur de catalogue global via la mmc **site et service Active Directory**

dans laquelle on demande les propriétés de **NTDS Settings** de notre serveur

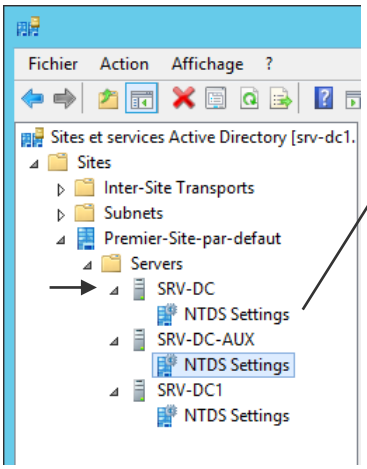


On sait ici que notre serveur est **Catalogue Global**

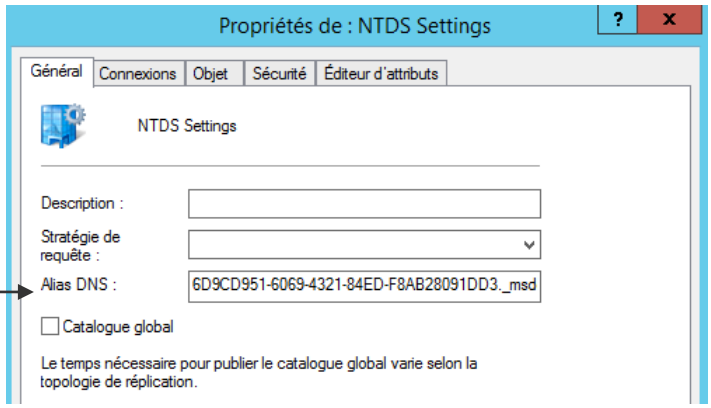
N.B: On ne transfère pas un serveur de Catalogue Global, mais on procède de la manière suivante :

1. on en active un 2°,
2. on attend une réplication,
3. puis on désactive le 1° (en faisant attention a ce qu'il ne s'agisse pas du CD qui a le rôle de maître d'attribution de nom de domaine de la foret) Si cela est nécessaire, on transfère également ces rôles…

Donc dans l'exemple on se place sur **SRV-DC-AUX**,



on demande **propriétés de NTDS Settings** et on décoche la case **Catalogue Global**

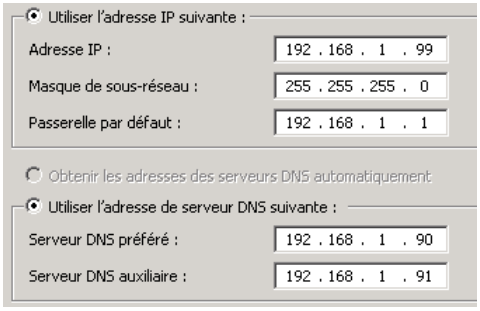


Suppression DNS ancien serveur

Il faut être sur d'avoir avant bien corrigé les adresses IP des serveurs DNS

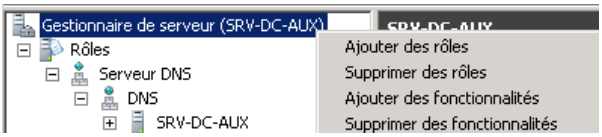
- sur toutes les machines du domaine avec une adresse IP en dur (remplacer la référence de l'ancien DNS par le nouveau installé)
- s'il ya un dhcp, avoir effectué le changement DNS dans les options

sur le serveur DNS 2008R2 à démonter, on indique les nouveaux serveur DNS du domaine (il n'est plus son propre serveur DNS ici notre serveur DNS en .99 utilise comme serveur DNS les .90 et .91)

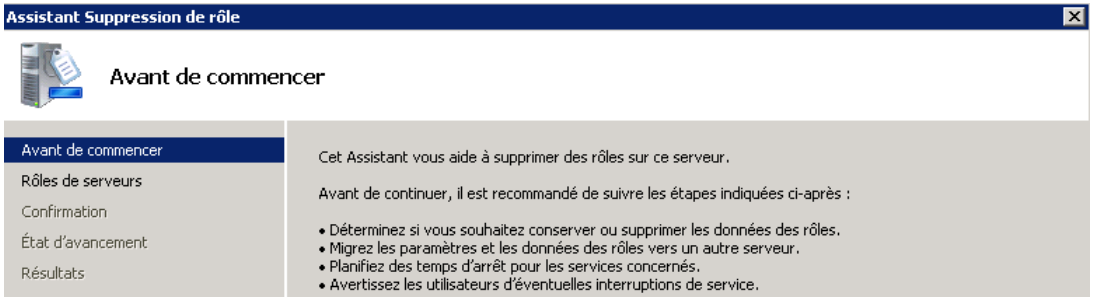


puis on va demander de supprimer un rôle

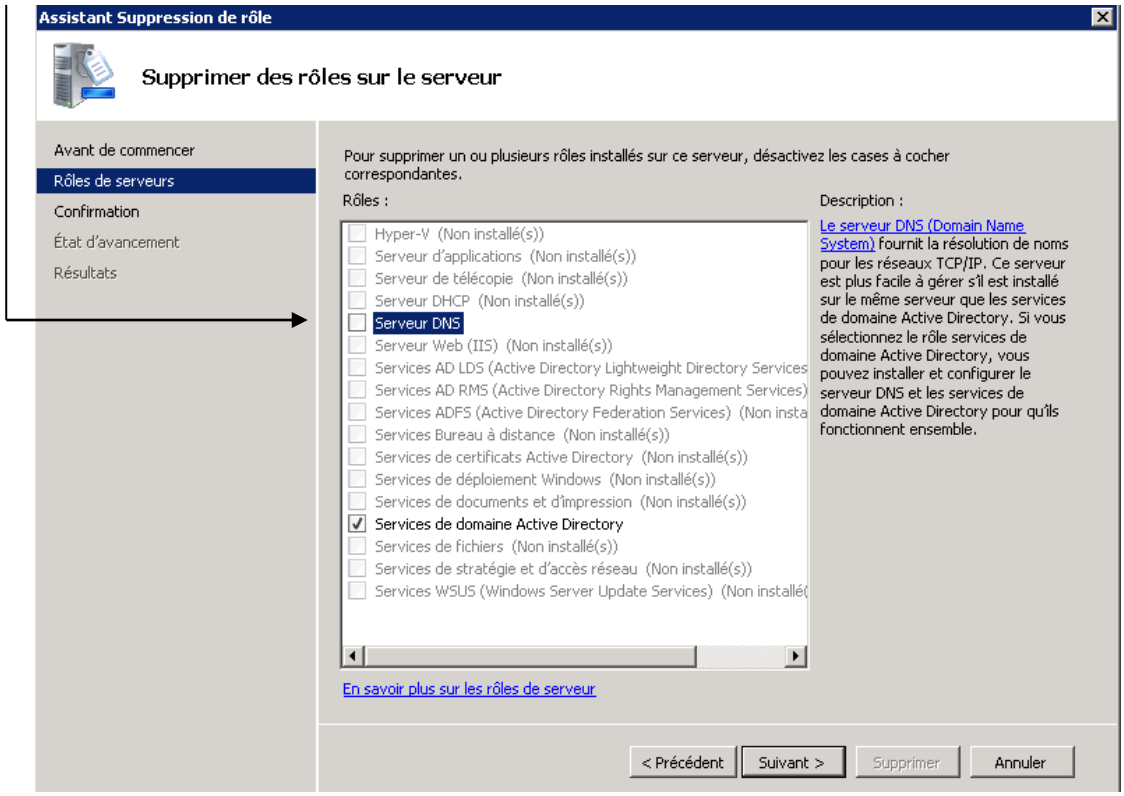
sur le **gestionnaire de serveur** via clic droit **Supprimer des rôles**



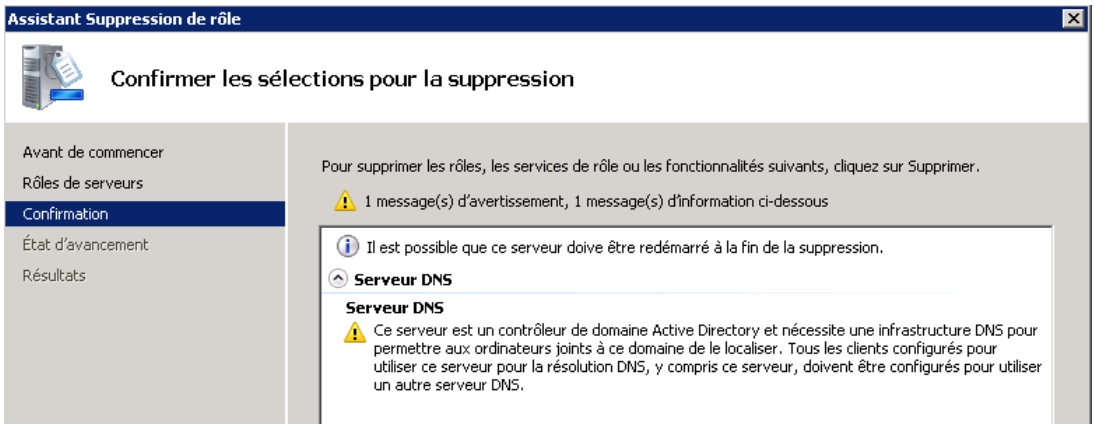
un assistant se déclanche

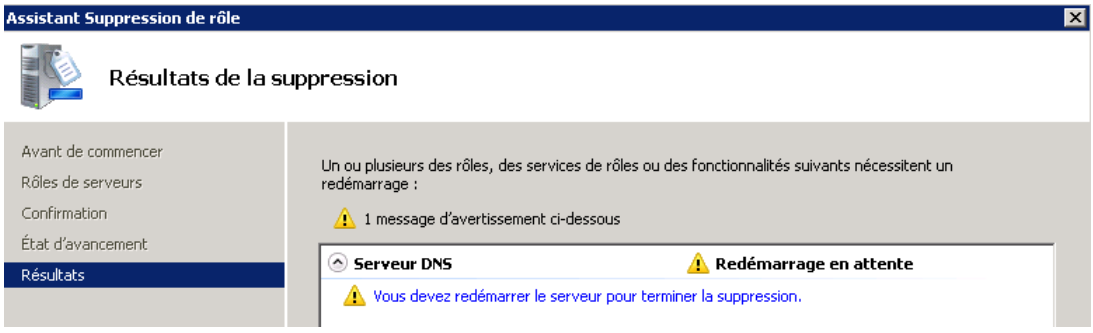


On décoche uniquement **Serveur DNS**

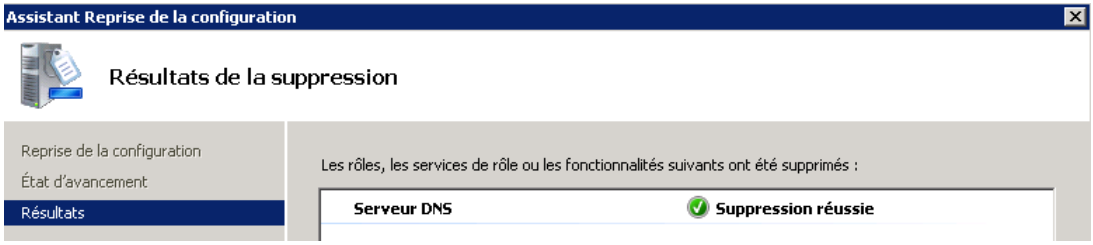


On a une mise en garde comme quoi il serait bon qu'il y ait d'autres DNS dans le domaine…





Et après un re démarrage



Démontage ancien DC

Sur un serveur Windows 2008 et 2008 R2 il faudra

- Effectuer dcpromo
- après la rétrogradation du serveur supprimer le rôle AD DS ajout « ajout / suppression de rôle ».

Sur un serveur en Windows 2012 et 2012 R2 l'assistant DCpromo n'existe plus.

- il faut directement supprimer le rôle AD DS l'assistant de configuration se lancera automatiquement et permettra de rétrograder le DC.

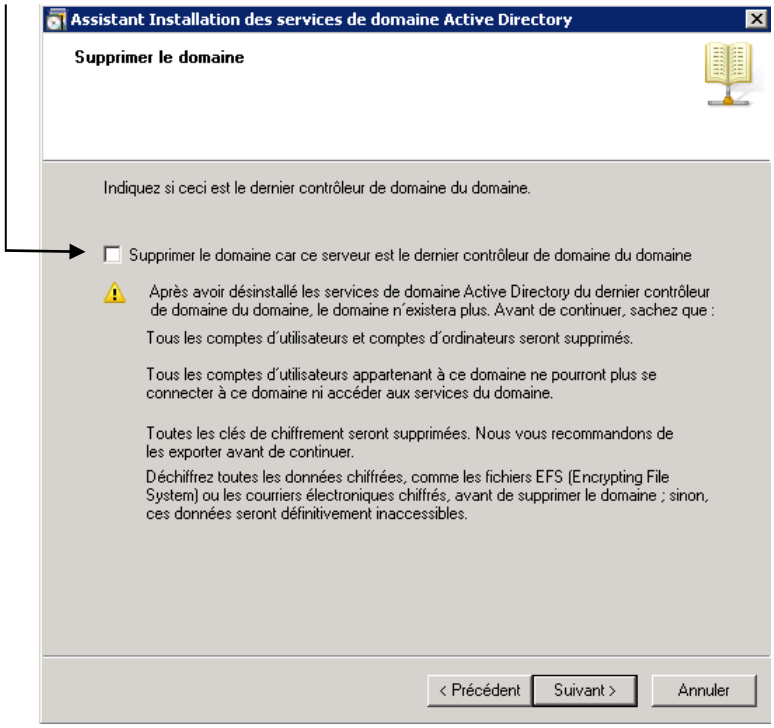
Il faut que sur cet ancien serveur les nouveaux DNS soient renseignés, de manière à ce que les information concernant le démontage circulent bien dans notre AD…

On pourrait même avant vérifier la bonne marche de la réplication par un **repadmin / replsummary**

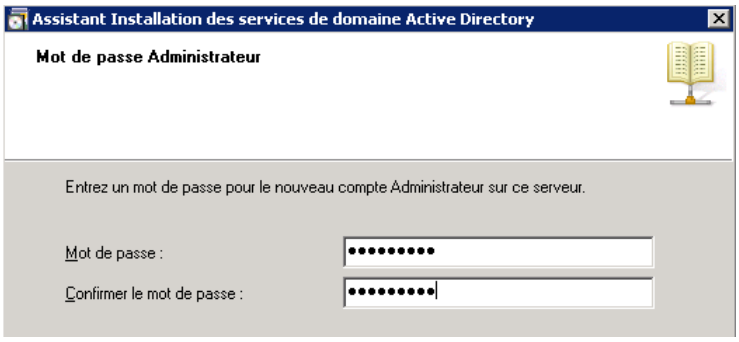
```
C:\Users\Administrateur.CABARE-INTRA>repadmin /replsummary
Heure de début du résumé de la réplication : 2016-05-02 08:39:06

Début de la collecte des données pour le résumé de la réplication ;
cette opération peut prendre un certain temps :
  ......


DSA source              différence max    nb échecs %%   erreur
 SRV-DC                     48m:16s    0 /  10    0
 SRV-DC-AUX                 49m:32s    0 /  10    0
 SRV-DC1                    49m:32s    0 /  10    0


DSA de destination      différence max    nb échecs %%   erreur
 SRV-DC                     49m:33s    0 /  10    0
 SRV-DC-AUX                 48m:17s    0 /  10    0
 SRV-DC1                    39m:33s    0 /  10    0
```

Faisons un **dcpromo** sur notre ancien serveur 2008R2 ***srv-dc-aux***

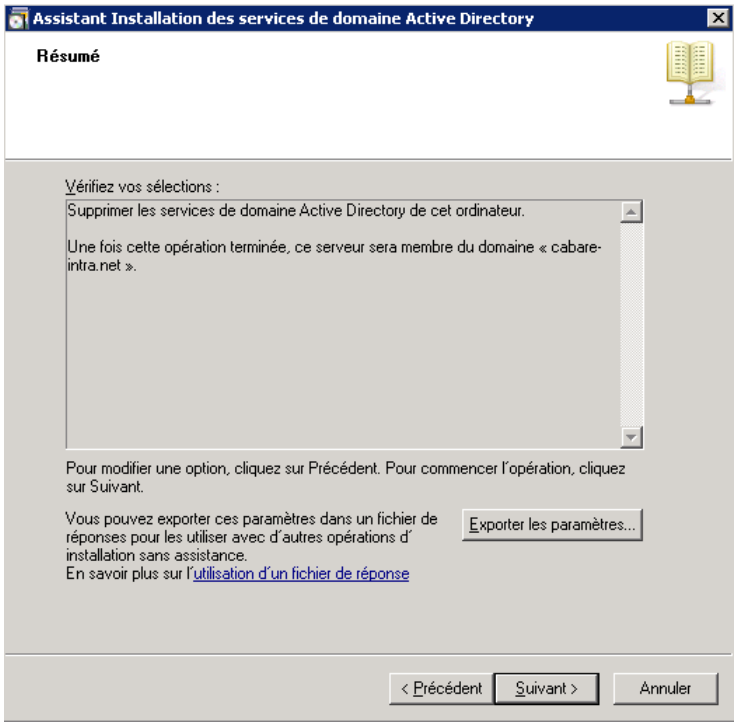
Surtout ne pas cocher…



On saisie le nouveau mot de passe du futur serveur (pour pouvoir ouvrir une session locale



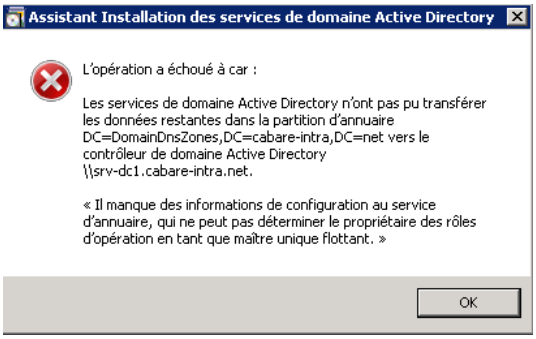
Et c'est fini…



Erreur possible dcpromo /forceremoval:

On n'arrive pas à démonter un Dc…

Ou il est … hors service…



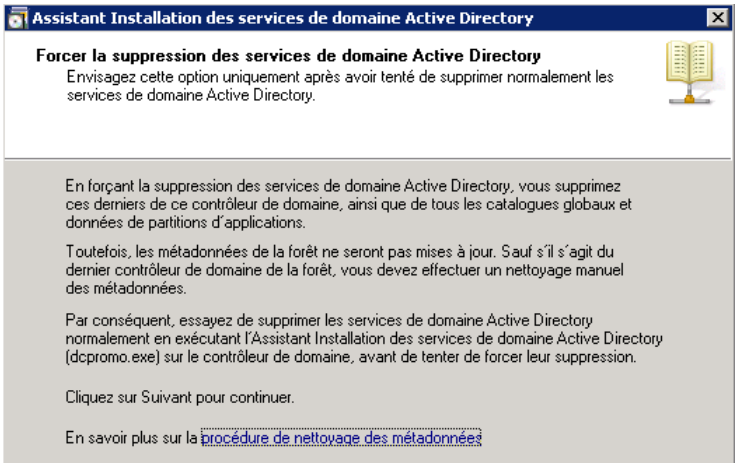
Il faut d'abords vérifier que les rôles soient bien transférés…. (**netdom query fsmo**) Et que la réplication fonctionne bien… (**repadmin /replsummary**)

- Si ce n'est pas le cas, il faut corriger, ou prendre les roles, et relancer la commande dcpromo
- Si c'est le cas il faut voir dans l'observateur d'evenement pourquoi ce CD ne veut pas se « demonter… »… en cas d'impossibilité à résoudre le problème, il faut alors forcer le démontage
- Si le serveur est Hors service, il faut forcer le démontage

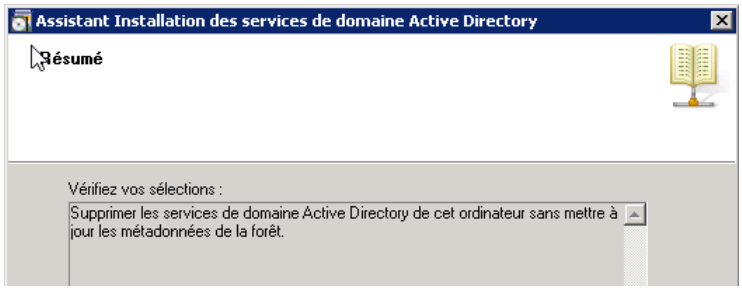
N.B : après un démontage forcé, il faut effectuer un netoyage de l'AD !

On va donc forcer le démontage via **dcpromo /forceremoval**

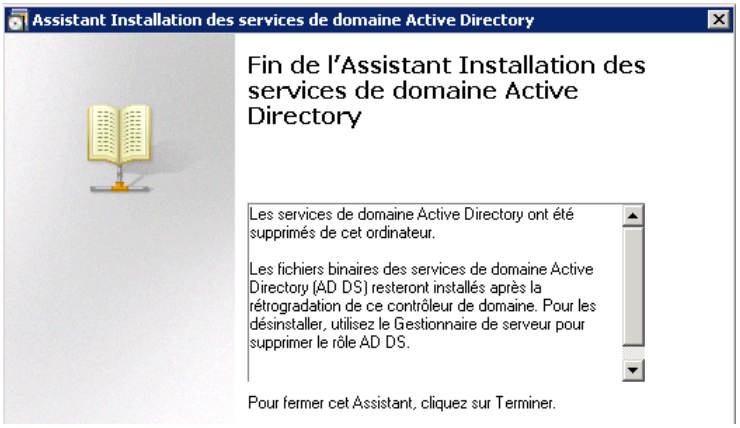
```
C:\Users\Administrateur.CABARE-INTRA>dcpromo /forceremoval_
```



On a une confirmation



Et c'est terminé



L'arrêt de ce serveur est définitif !

N.B : rien de pire ne peut arricer qu'un retour d'un CD déclaré Hors Circuit… il faut retirer ce poste de la circulation, un simple redemarrage par inadvertance pourrait être catastrophique pour le fonctionnement du Domaine complet !

Nettoyage des méta données de l'AD:

Il faut nettoyer les données dans l'AD et néttoyer le DNS

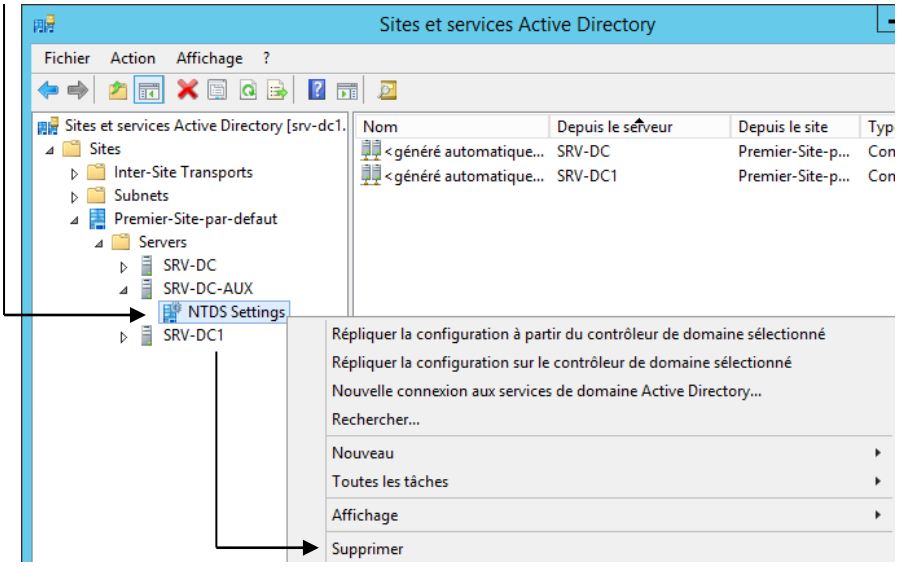
Dans l'AD il faut supprimer

- La zone NTDS du serveur à détruire
- Le serveur lui-même

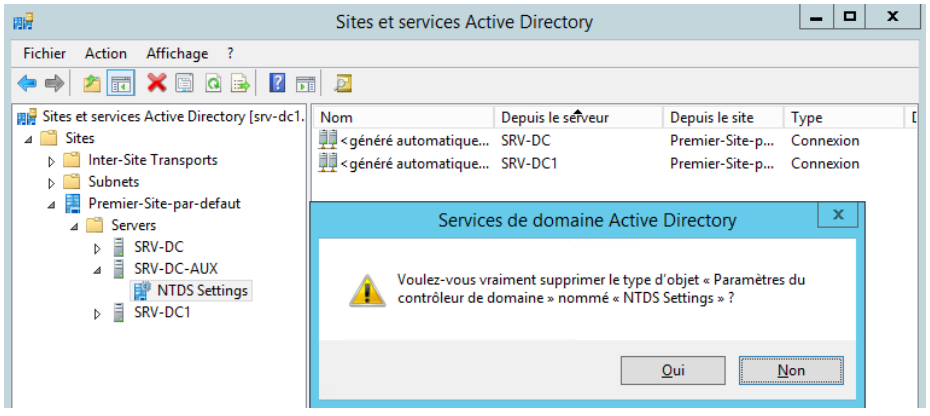
Dans le DNS il faut supprimer

- L'indication du serveur détruit comme serveurs de nom
- Tous les enregistrement de type SRV et NS du serveur détruit

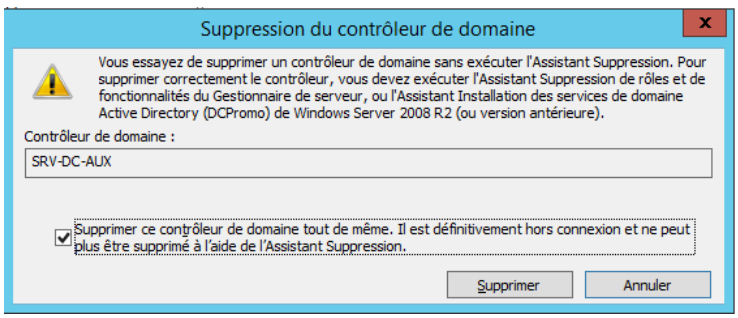
Depuis 2008 on n'est plus obligé de passer par **ntdsutil**, on utilise la console **Site et service Active Directory** on se place sur le serveur à effacer, sur sa zone **NTDS Settings**, que l'on supprime



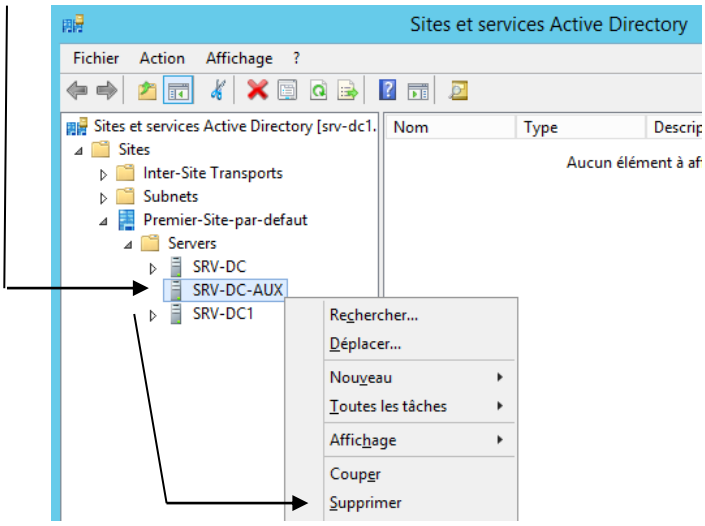
On confirme



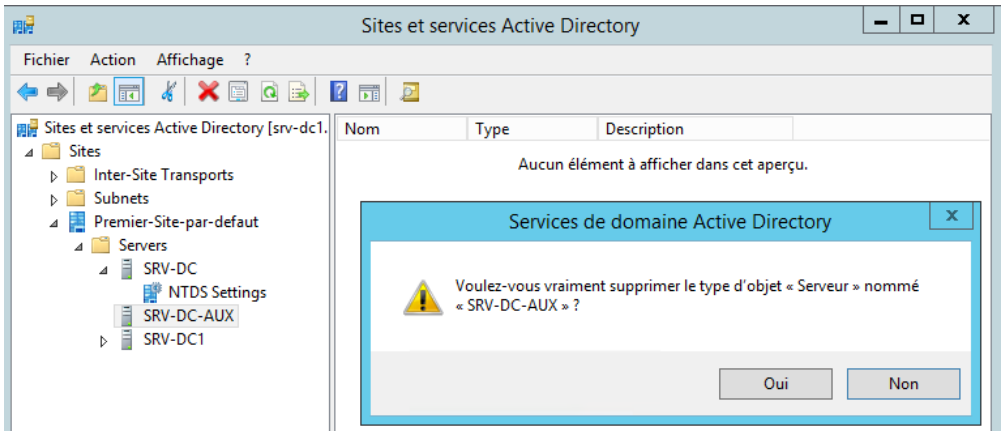
On valide la non accesibilité du serveur à détruire



via **Site et service Active Directory** on se place sur le serveur à effacer, , que l'on supprime

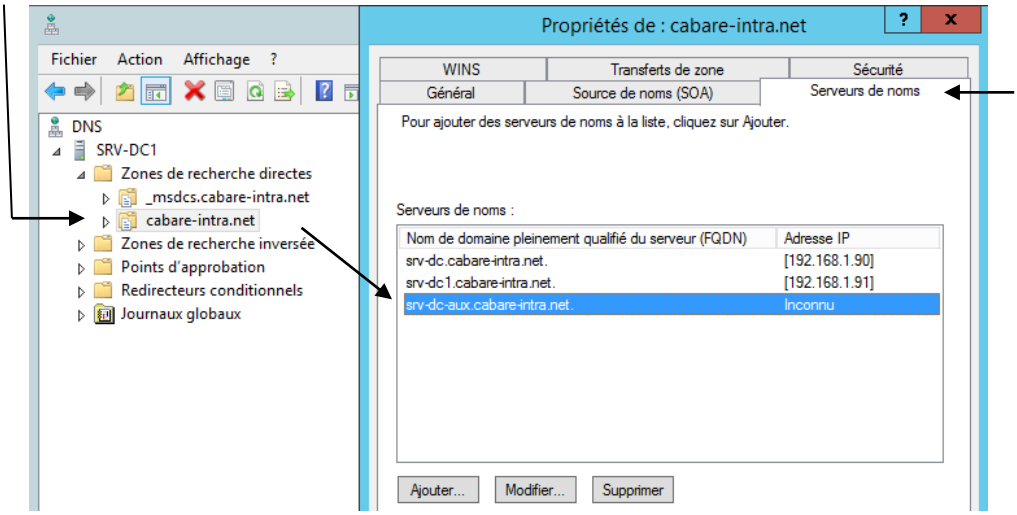


Et l'on confirme



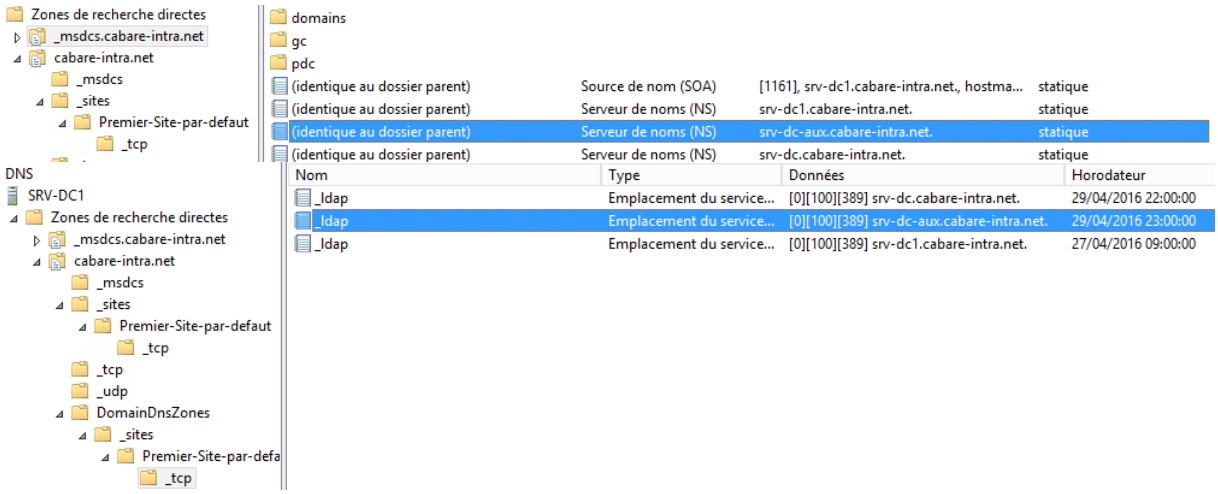
Pour le DNS il va falloir supprimer les indications de serveur de nom concernant notre serveur supprimé.

Dans la mmc **DNS**, on se place sur les **zone de recherche directe**, ici *cabare-intra.net* et *_msdcs.cabare-intra.net* dans les **propriétés** on demande **Serveurs de noms**



N.B : ces indications de serveurs n'étant pas répliquées, il faut les mettre à jours surtous les serveurs DNS restants

Toujours la console « **Gestionnaire DNS** » il faut parcourir les différentes zones et supprimer tout enregistrement relatif au contrôleur de domaine détruit qu'ils soient de type ***SRV***, ***A*** ou ***CNAME (et pointeurs…)***



L'utilitaire NTDSUTIL:

Cet utilitaire est un utilitaire en mode interactif, a niveau (genre netsh ou nslookup). On sort d'un niveau (ou de l'utilitaire) via la commande **quit**.

Il se lance par la commande **ntdsutil**

```
C:\>ntdsutil
ntdsutil: quit

C:\>_
```

Le niveau qui nous intéresse ici est celui accessible par la commande **roles**

```
ntdsutil: roles
fsmo maintenance:
```

il faut ensuite taper la commande **connections**

```
fsmo maintenance: connections
server connections: _
```

puis le nom du serveur sur lequel on désire effectuer une connection à travers la commande **connect to server *xxxxx***

```
server connections: connect to server s1
Liaison à s1...
Connecté à s1 en utilisant les informations d'identification d'un utilisateur co
nnecté localement
server connections: _
```

une fois la connection effectuée, on remonte au niveau précédant avec la commande **quit**,

```
server connections: quit
fsmo maintenance:
```

et la on peut taper **seize** suivit du rôle que l'on veut prendre…. Ou on peut taper **transfert** suivit du rôle que l'on veut transférer…. Au choix

seize pdc

seize RID master

seize infrastructure master

seize schema master

seize naming master

et l'on peut vérifier le succès de l'opération avec un **netdom query fsmo**

Gestion Synchronisation base de temps ntp:

A priori un DC 2008 existant, ici srv-dc est base de temps, il va chercher ici dans l'exemple ntp.imag.fr

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /source
ntp.imag.fr
```

et notre nouveau dc en 2012 est synchronisé celui-ci…

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /source
srv-dc.cabare-intra.net
```

Un seul CD de référence doit se synchroniser sur un serveur externe ntp.

Donc sur LE CD de référence (notre nouveau serveur 2012), on exécute

→ **w32tm /config /manualpeerlist:"ntp.obspm.fr" /syncfromflags:MANUAL**

→ **w32tm /config /reliable:YES**

w32tm /config /update

Net stop w32time

Net start w32time

W32tm /resync

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /config /manualpeerlist:"ntp.imag.fr" /syncfromflags:MANUAL
La commande s'est terminée correctement.

C:\Users\Administrateur.CABARE-INTRA>w32tm /config /reliable:YES
La commande s'est terminée correctement.

C:\Users\Administrateur.CABARE-INTRA>w32tm /config /update
La commande s'est terminée correctement.

C:\Users\Administrateur.CABARE-INTRA>net stop w32time
Le service Temps Windows s'arrête.
Le service Temps Windows a été arrêté.

C:\Users\Administrateur.CABARE-INTRA>net start w32time
Le service Temps Windows démarre.
Le service Temps Windows a démarré.

C:\Users\Administrateur.CABARE-INTRA>w32tm /resync
Envoi de la commande de resynchronisation à l'ordinateur local
La commande s'est terminée correctement.
```

On peut vérifier avec un **/query /source** où il se synchronise

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /source
ntp.imag.fr
```

Puis un **/query /status** si la synchronisation a réussi

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 3 (Référence secondaire, synchronisée par (S)NTP)
Précision : -6 (15.625ms par battement)
Délai de racine : 0.0407715s
Dispersion de racine : 0.7981723s
ID de référence : 0x81581E01 (IP de la source :  129.88.30.1)
Heure de la dernière synchronisation réussie : 06/05/2016 10:58:08
Source : ntp.imag.fr
Intervalle d'interrogation : 6 (64s)
```

Et enfin par **/query /peers** si c'est bien le seul serveur sur lequel il se synchronise..

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /peers
Nb d'homologues : 1

Homologue : ntp.imag.fr
État : Actif
Temps restant : 62.1093708s
Mode : 1 (Actif symétrique)
Couche : 2 (Référence secondaire, synchronisée par (S)NTP)
HomologueIntervalle d'interrogation : 6 (64s)
HôteIntervalle d'interrogation : 6 (64s)
```

Reste à faire prendre en compte sur tous les autres CD qui se synchronisaient à l'exterieur que un nouveau cd maitre de temps existe désormais (notre serveur 2012r2 nommé srv-dc1)

Donc sur notre ancien CD base de temps on exécute

→ **w32tm /config /syncfromflags:DOMHIER**

w32tm /config /update

Net stop w32time

Net start w32time

W32tm /resync

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /config /syncfromflags:DOMHIER
La commande s'est terminée correctement.
```

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /config /update
La commande s'est terminée correctement.
```

```
C:\Users\Administrateur.CABARE-INTRA>net stop w32time
Le service Temps Windows s'arrête.
Le service Temps Windows a été arrêté.
```

```
C:\Users\Administrateur.CABARE-INTRA>net start w32time
Le service Temps Windows démarre.
Le service Temps Windows a démarré.
```

On peut vérifier via **/query /source** qu'il se synchronise sur le nouveau dc 2012

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /source
srv-dc1.cabare-intra.net
```

N.B: si cela ne marche pas, il peut être necessaire de passer par un nettoyage des paramètres avec une sequence type du genre

Net stop w32time

w32tm /unregister

w32tm /register vérifiable par

```
C:\Users\Administrateur>w32tm /query /source
Local CMOS Clock
```

On peut vérifier avec un /**query /status** qu'il y arrive bien

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /source
srv-dc1.cabare-intra.net

C:\Users\Administrateur.CABARE-INTRA>w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 4 (Référence secondaire, synchronisée par (S)NTP)
Précision : -6 (15.625ms par battement)
Délai de racine : 0.0720215s
Dispersion de racine : 3.8764970s
ID de référence : 0xC0A8015B (IP de la source :  192.168.1.91)
Heure de la dernière synchronisation réussie : 06/05/2016 11:18:38
Source : srv-dc1.cabare-intra.net
Intervalle d'interrogation : 6 (64s)
```

Et enfin par **/query /peers** qu'il utilise uniquement LE CD 2012R2 de référence

```
C:\Users\Administrateur.CABARE-INTRA>w32tm /query /peers
Nb d'homologues : 1

Homologue : srv-dc1.cabare-intra.net
État : Actif
Temps restant : 60.3593750s
Mode : 1 (Actif symétrique)
Couche : 3 (Référence secondaire, synchronisée par (S)NTP)
HomologueIntervalle d'interrogation : 6 (64s)
HôteIntervalle d'interrogation : 6 (64s)
```

Vérification Niveau fonctionnel:

Si on est sûr que l'on 'utilisera plus jamais de CD 2003, ou de CD 2008, et donc que la version minimale d'un CD sera 2008R2, 2012 ou 2012R2… alors il est conseillé de choisir

- au **niveau Forêt**:

un **niveau fonctionnel 2008R2** (et pas 2008, qui n'apporte rien par rapport à 2003) qui par rapport à 2003 va offrir les possibilités suivantes

- Corbeille AD

N.B: les niveaux fonctionnels de forets 2012 et 2012R2 n'amènent aucunes nouvelles fonctionnalités par rapport au niveau 2008R2

- au **niveau Domaine**:

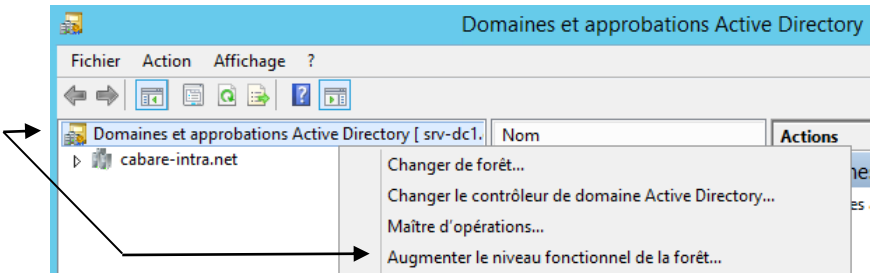
un **niveau fonctionnel 2008R2** qui par rapport à 2003 va offrir les possibilités suivantes:

- prise en charge de la réplication du système de fichiers DFS (Distributed File System) pour SYSVOL
- prise en charge d'AES (Advanced Encryption Services) 128 et 256 pour le protocole d'authentification Kerberos
- informations sur la dernière ouverture de session interactive
- stratégies de mot de passe affinées

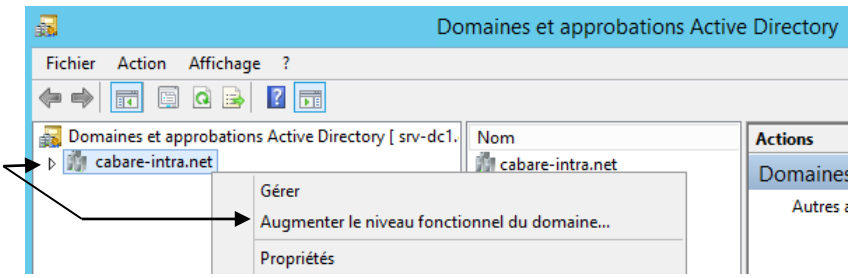
N.B: quelques fonctionnalités possibles uniquement sur des niveaux 2012 ne seront pas accessibles, mais elles ne sont pas dans un premier temps indispensable, elles concernent des stratégies d'authentification renforcée…

Il faut donc mettre à niveau tous les Domaine, puis la forêt. Si on a 1 seul domaine, il faut que tous les Cd soient à niveau, puis on passe le domaine, puis la forêt

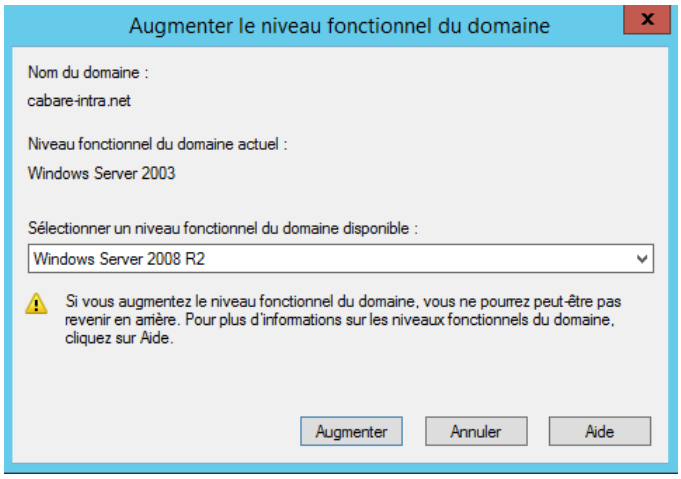
Dans la console **Domaine et approbation Active Directory**, sur **Domaine et approbation**, on a via clic droit le niveau fonctionnel de forêt,



et sur le **domaine** on a via clic droit le niveau fonctionnel de domaine

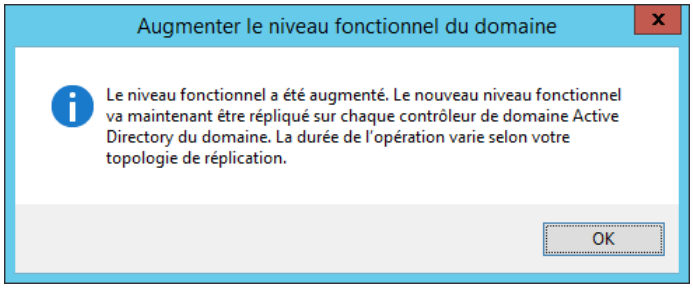


Passage du niveau de domaine de 2003 à 2008r2

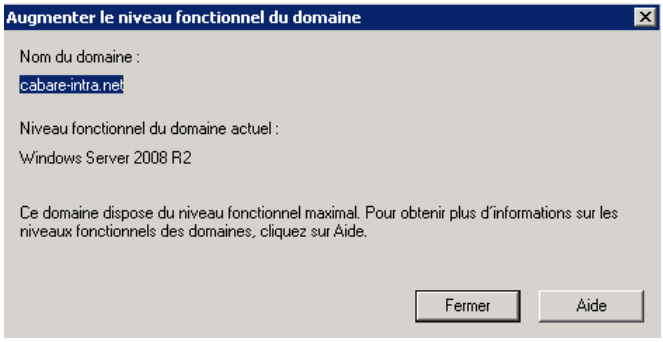


Augmenter

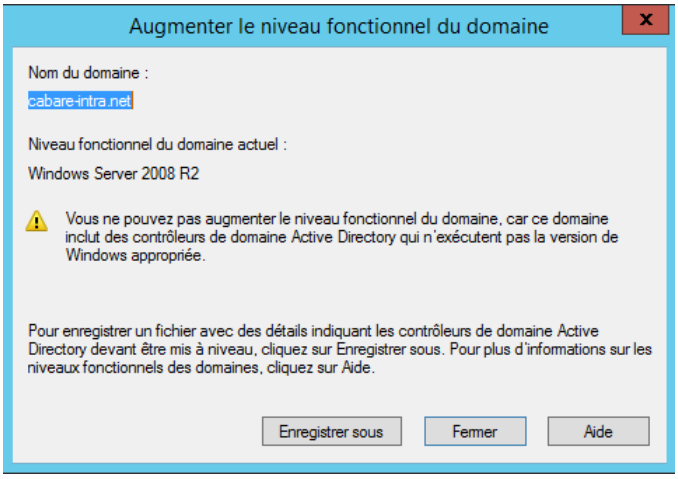
on est prévenu…Il serait bon de vérifier sur tous les CD le niveau…



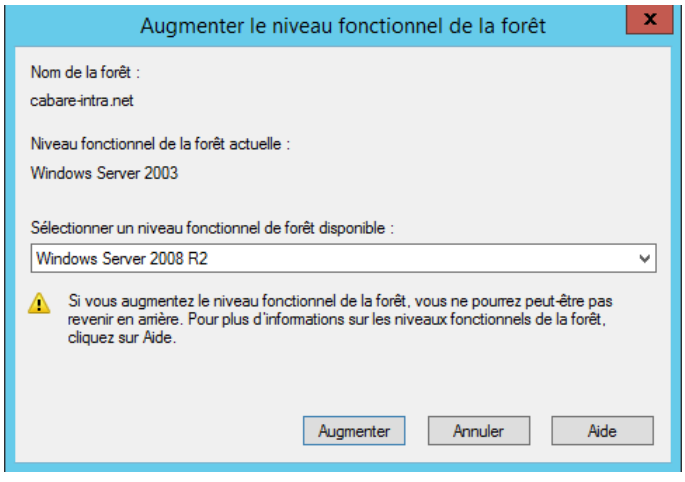
Sur un 2008R2 cela donne



Sur un 2012 cela donne

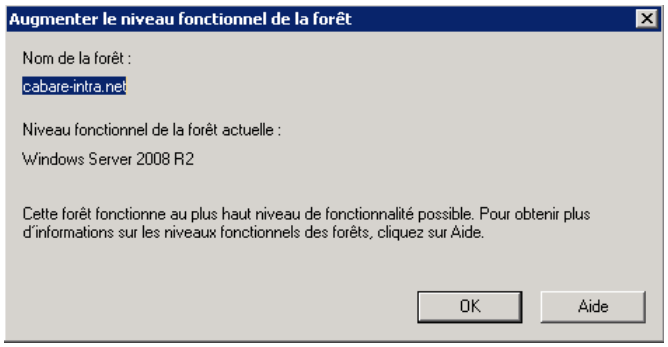


Passage du niveau de Forêt de 2003 à 2008r2

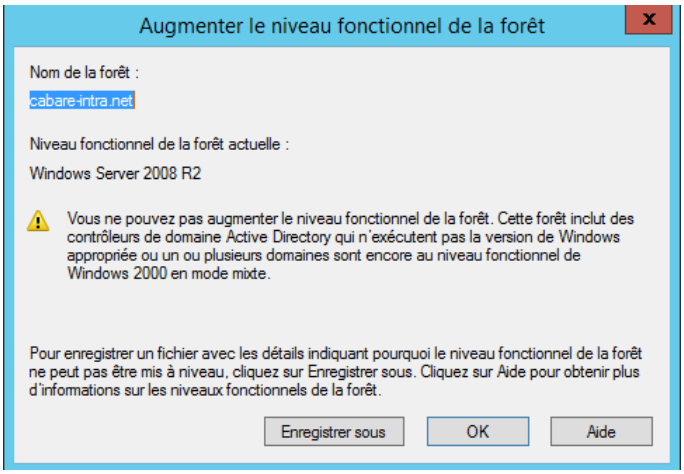


Augmenter…

Sur un 2008R2 cela donne



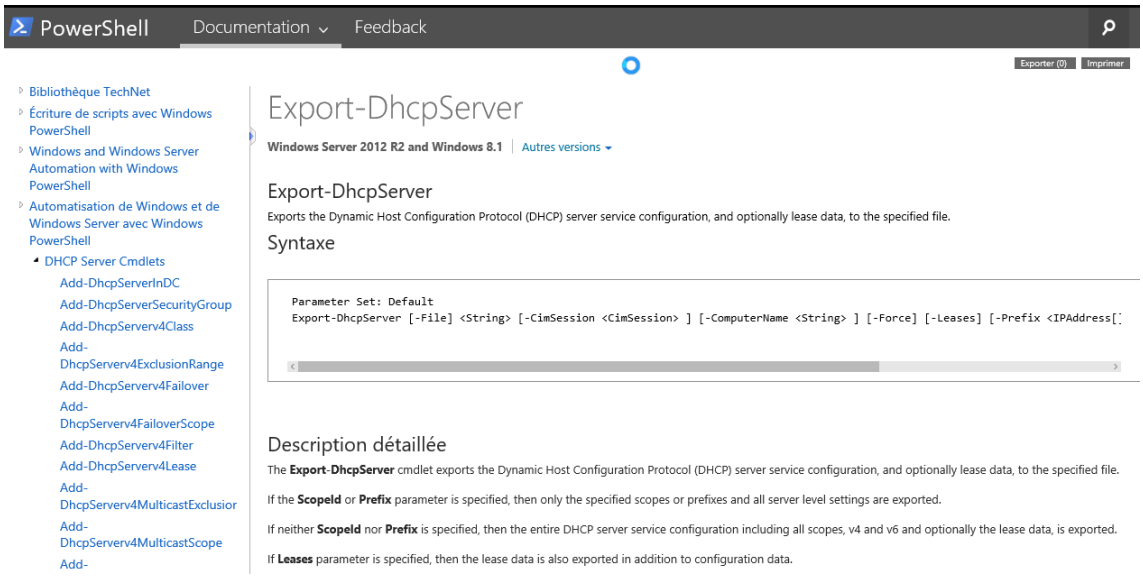
Sur un 2012 cela donne



MIGRATION DE DHCP

Principe de la migration

Il existe sur 2012R2 de nouvelles commandes powerschell permettant de récupérer une configuration dhcp existante sur un serveur 2008r2

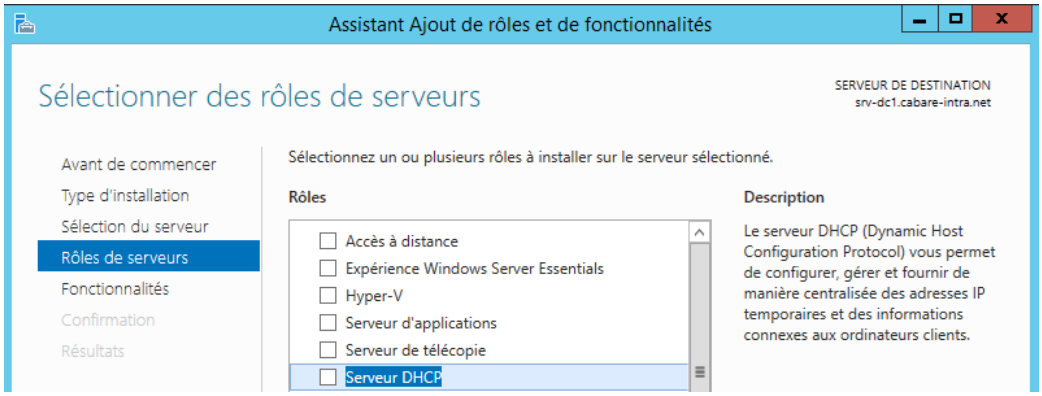


Le principe sera donc le suivant :

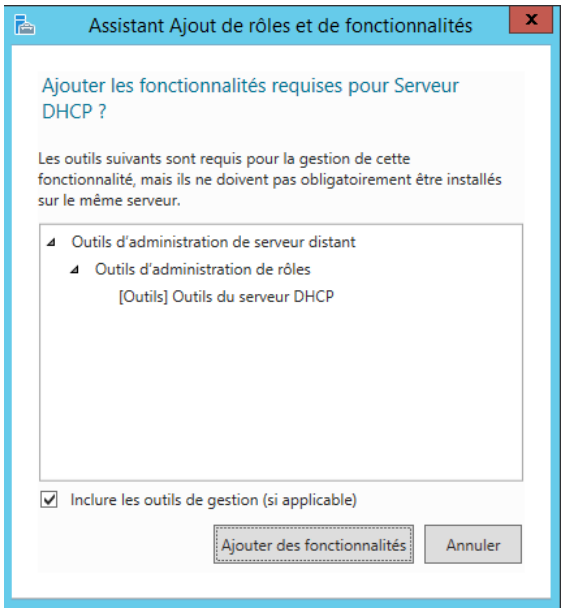
- Sur le serveur 2012R2 installer le **rôle dchp** mais sans étendue et sans activation
- Depuis le serveur 2012 executer la commande permettant de lancer l'export de la configuration dhcp du serveur 2008 dans un fichier xml (à distance donc)
- Depuis le serveur 2012 executer la commande pour récupérer ce fichier de configuration
- **Désactiver – interdire** l'ancien Serveur et **Activer – autoriser** le nouveau Serveur

Ajout du rôle dhcp sur le serveur 2012

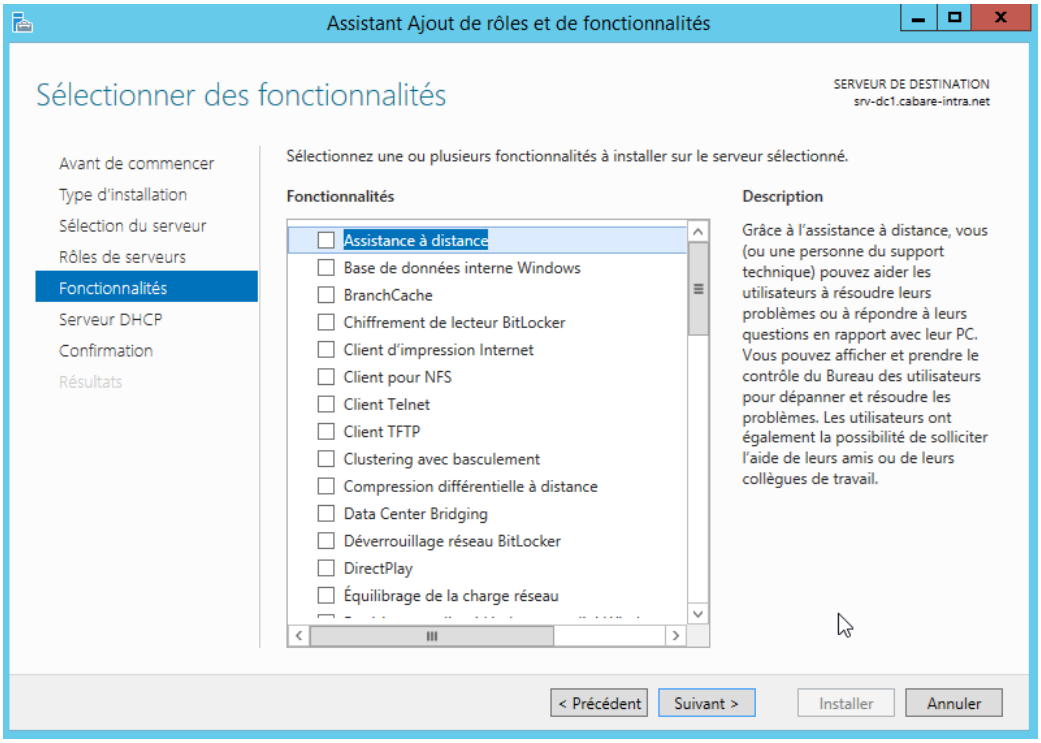
On ajouter le rôle dhcp sur notre serveur 2012 via le **gestionnaire de serveur**



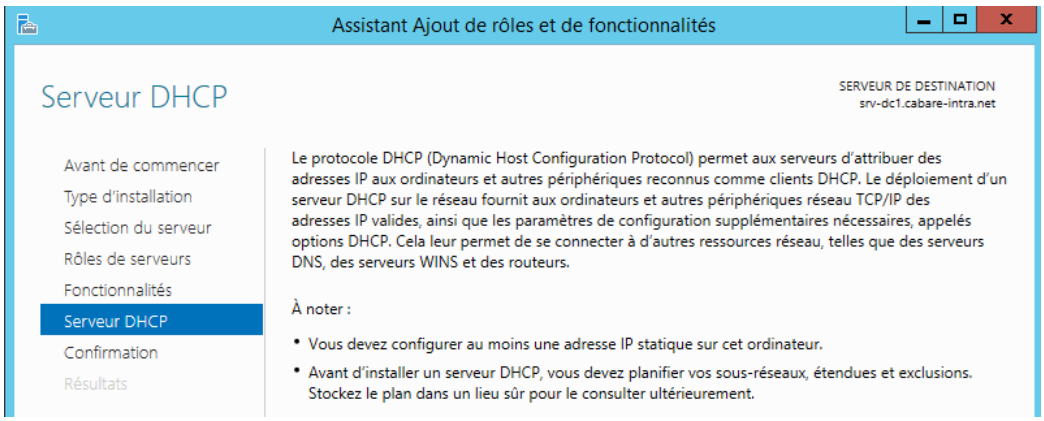
Et toutes les fonctions associées



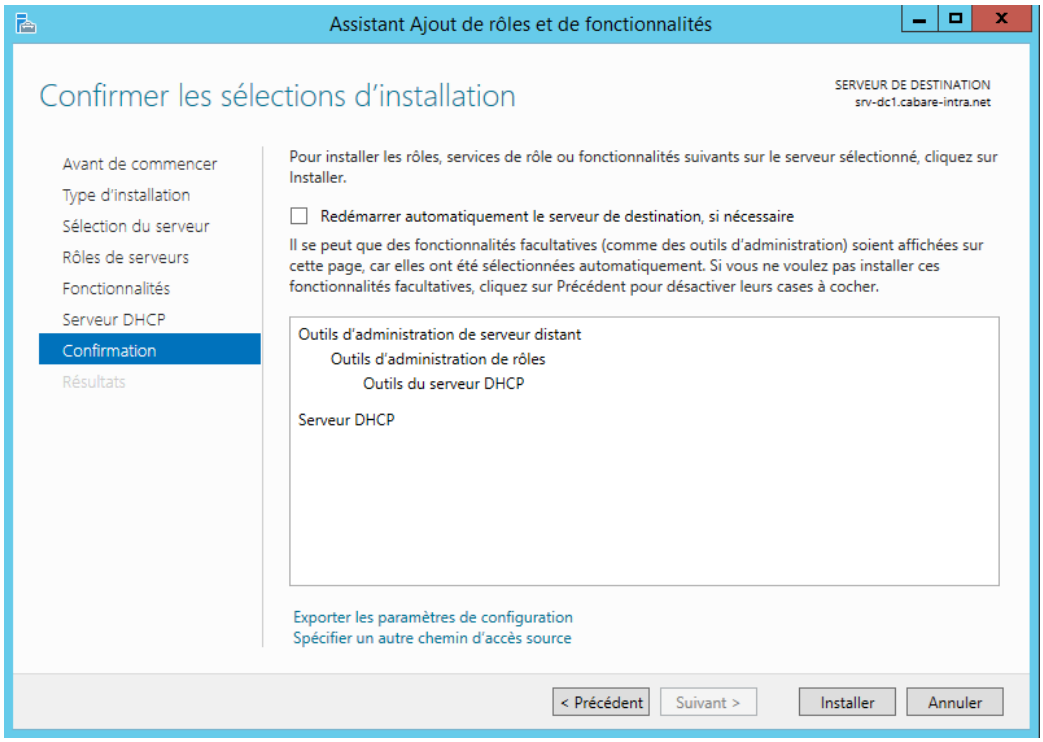
On ne modifie rien ensuite dans les fonctionnalités…



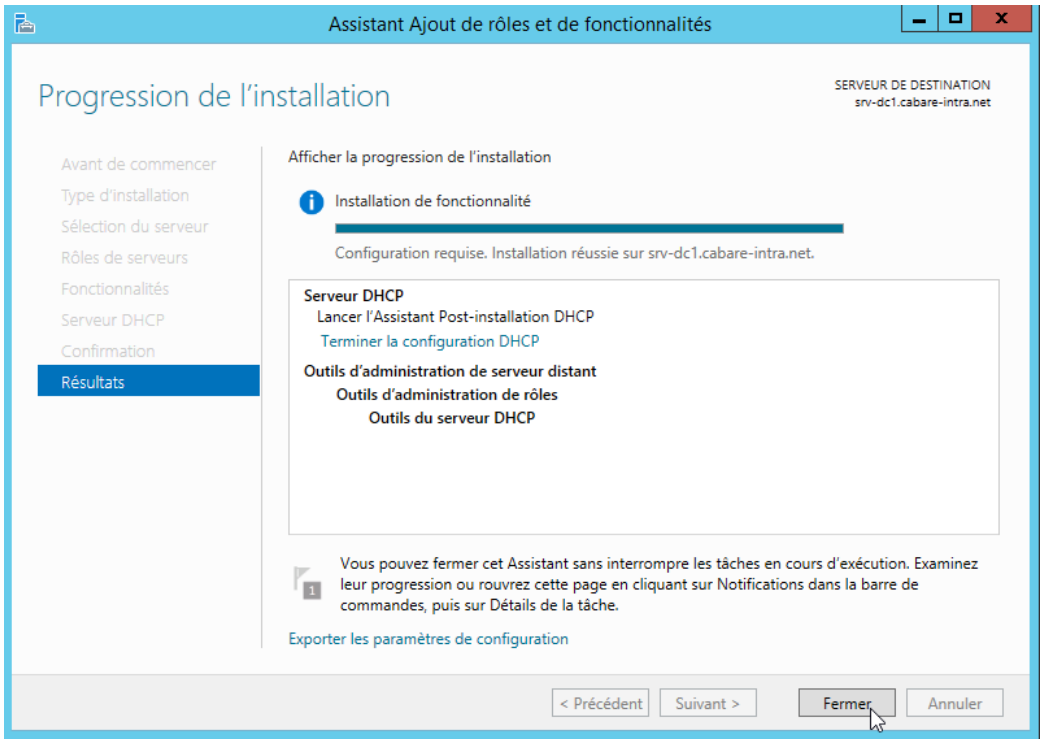
Une mise en garde apparait comme quoi il serait bon d'avoir une adresse IP



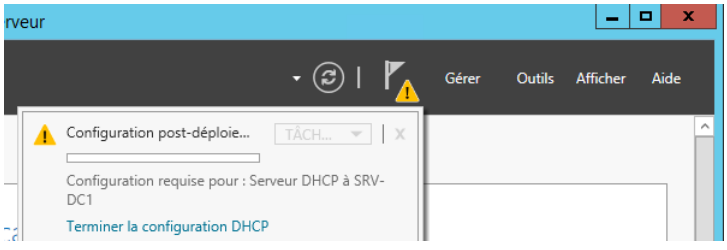
On confirme



Et c'est tout



Evidemment il faudra configurer le serveur…



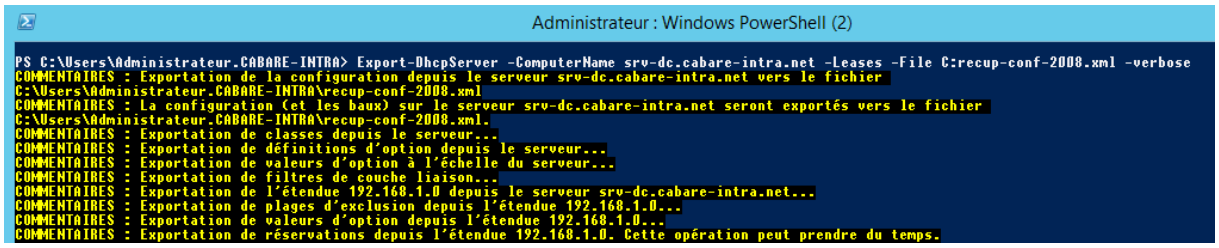
Exportation de la configuration du DHCP 2008

En powershell avec une commande du genre, ou *nomsrv* est le nom du serveur 2008r2 sur lequel est installé le dhcp que l'on veut récupérer et *nomfichier.xml* est le nom du fichier de conf que l'on veut obtenir

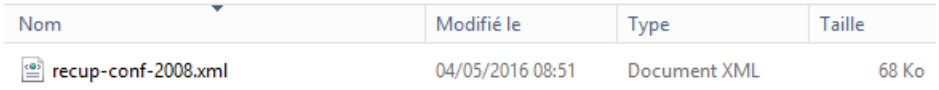
Export-DhcpServer –ComputerName *nomsrv* **-Leases -File** *c:nomfichier.xml* **-verbose**

Donc par exemple

Export-DhcpServer –ComputerName *srv-dc.cabare-intra.net* **-Leases -File** *c:\recup-conf-2008.xml* **-verbose**

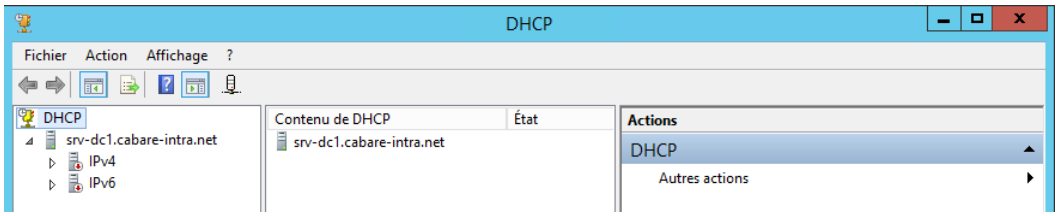


Cela crée un fichier xml



Importation de la configuration dans le DHCP 2012

Pour l'instant notre serveur DHCP est « vide » sans configuration

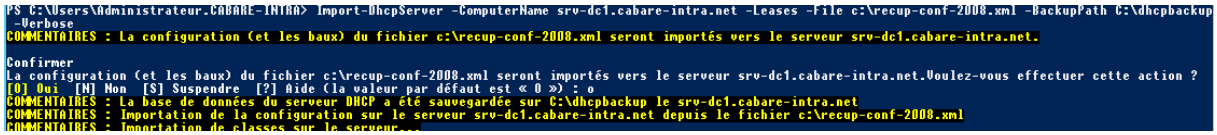


On va récupérer la configuration avec une commande powerschell du genre, ou *nomsrv* est le nom du serveur 2012r2 sur lequel est installé le nouveau serveur dhcp à configurer, et *:nomfichier.xml* est le nom du fichier de conf crée précedamment

Import-DhcpServer –ComputerName *nomsrv* ***-Leases –File*** *c:nomfichier.xml* ***-BackupPath*** *C:\dhcpbackup* ***–Verbose***

Donc par exemple

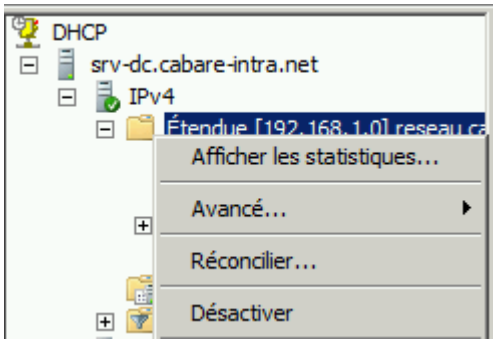
Import-DhcpServer –ComputerName *srv-dc1.cabare-intra.net* ***-Leases –File*** *c:\recup-conf-2008.xml* ***-BackupPath*** *C:\dhcpbackup* ***–Verbose***



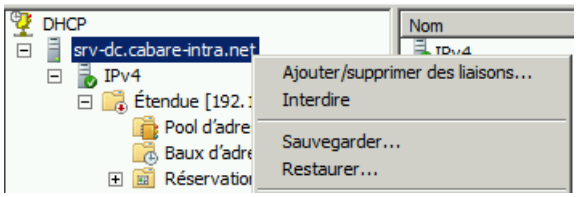
Et notre serveur est configuré !

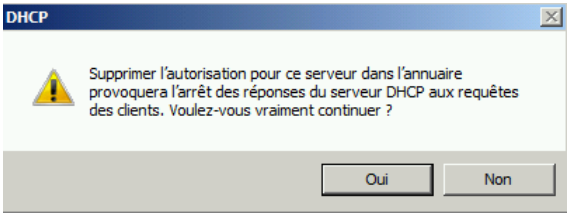
Autorisation et activation des serveurs

Ne pas oublier de désactiver l'étendue sur l'ancien serveur (2 précautions valent mieux qu'une

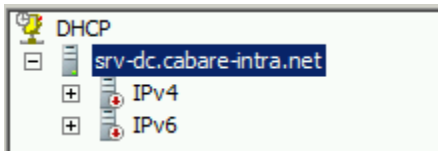


et ensuite interdire l'ancien serveur DHCP2008R2

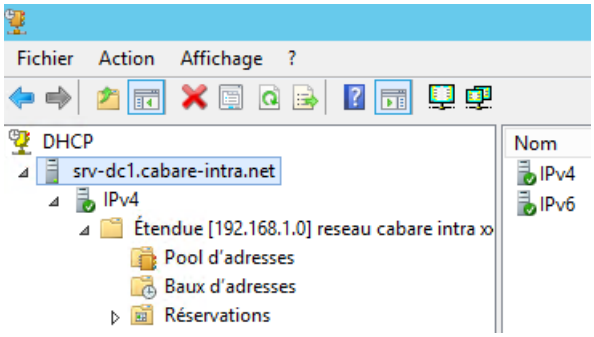




Pour obtenir



Reste à activer le nouveau serveur DHCP 2012…

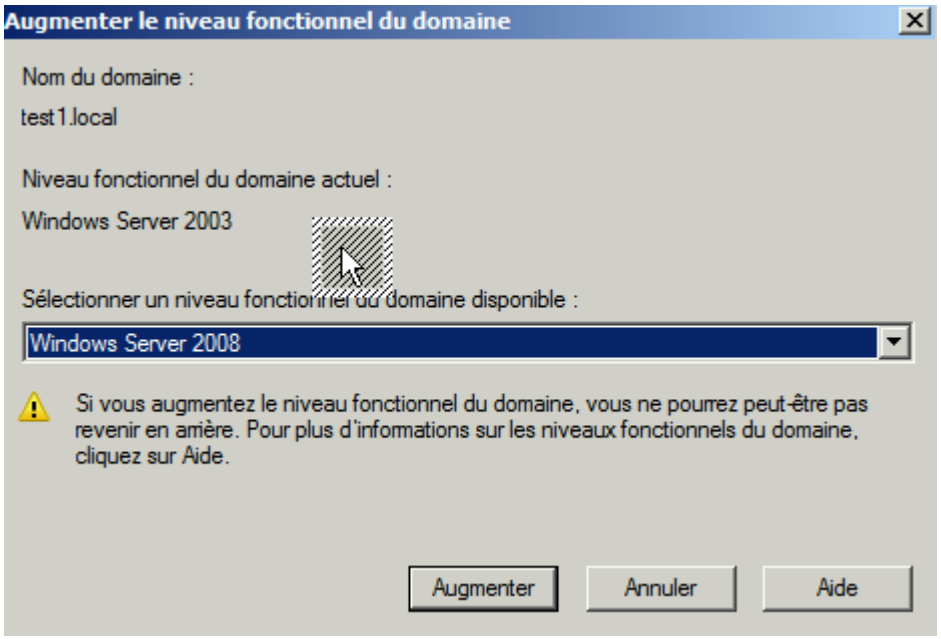


MIGRATION REPLICATION SYSVOL

lors de la création du domaine en « migration », celui-ci n'étant pas « Natif » Windows 2008 ou supérieur, Sysvol utilise l'ancienne réplication NTFRS et non la nouvelle technologie DFS-R

Niveau fonctionnel 2008

Pour migrer en DFS-R le niveau fonctionnel doit être au minimum 2008 et il faut exécuter l'assistant 'dfsrmig » voir : http://pbarth.fr/node/75

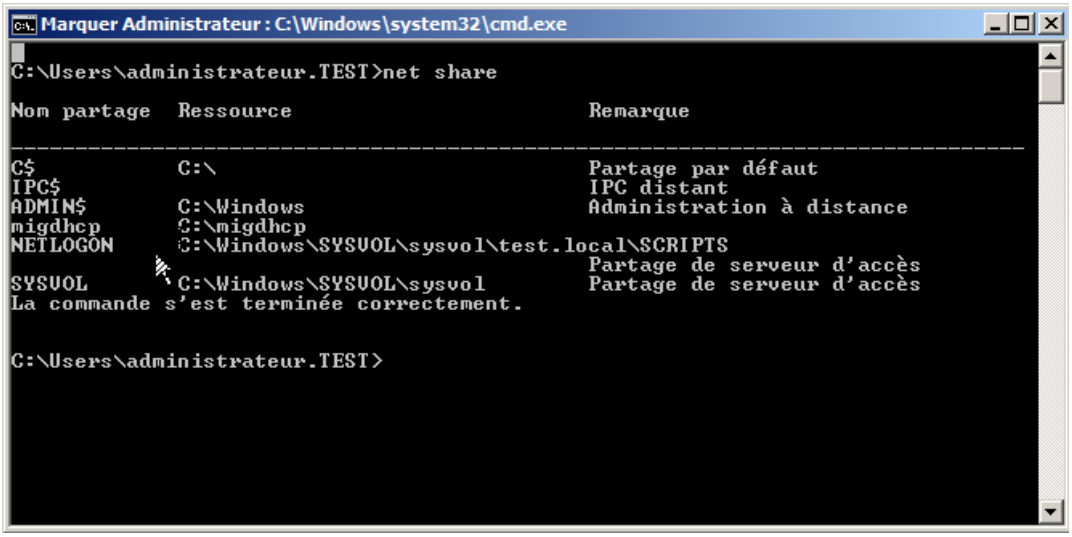


DFSRMIG - Migrer la réplication NTFSR en DFS-R

Le domaine ne contient que des DC en Windows 2008 R2 minimum, le niveau fonctionnel de la forêt et le niveau du domaine sont en 2008R2.

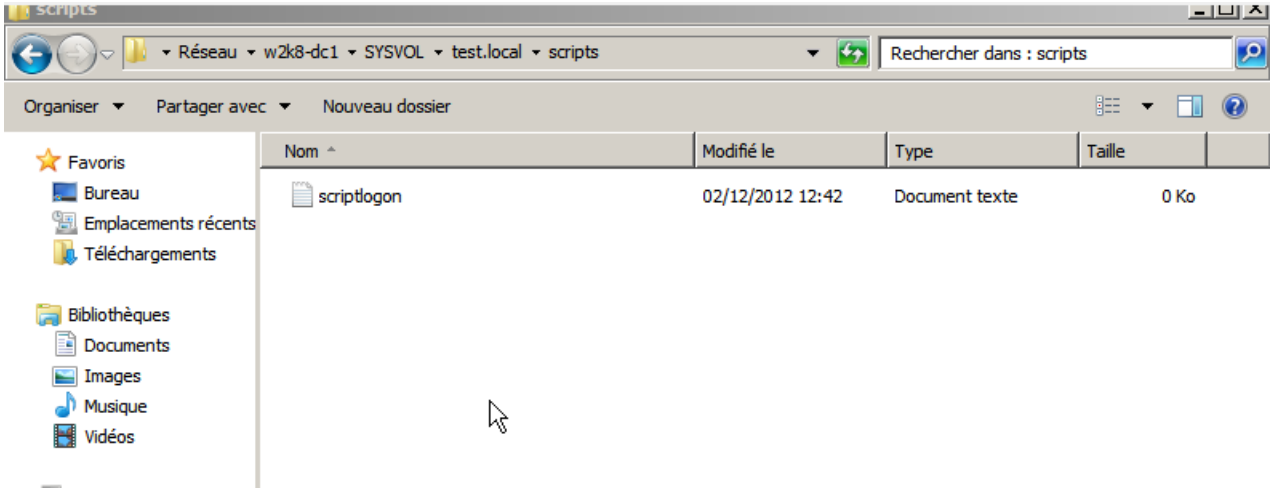
L'outil permettant d''effectuer la migration est **dfsrmig**. (cet outil existe est en standard depuis Windows 2008 R2.)

Ici le dossier partagé "sysvol" et le dossier "Netlogon" sont dans le dossier :"c:\windows\sysvol" (situation standard d'une réplication NTFRS)

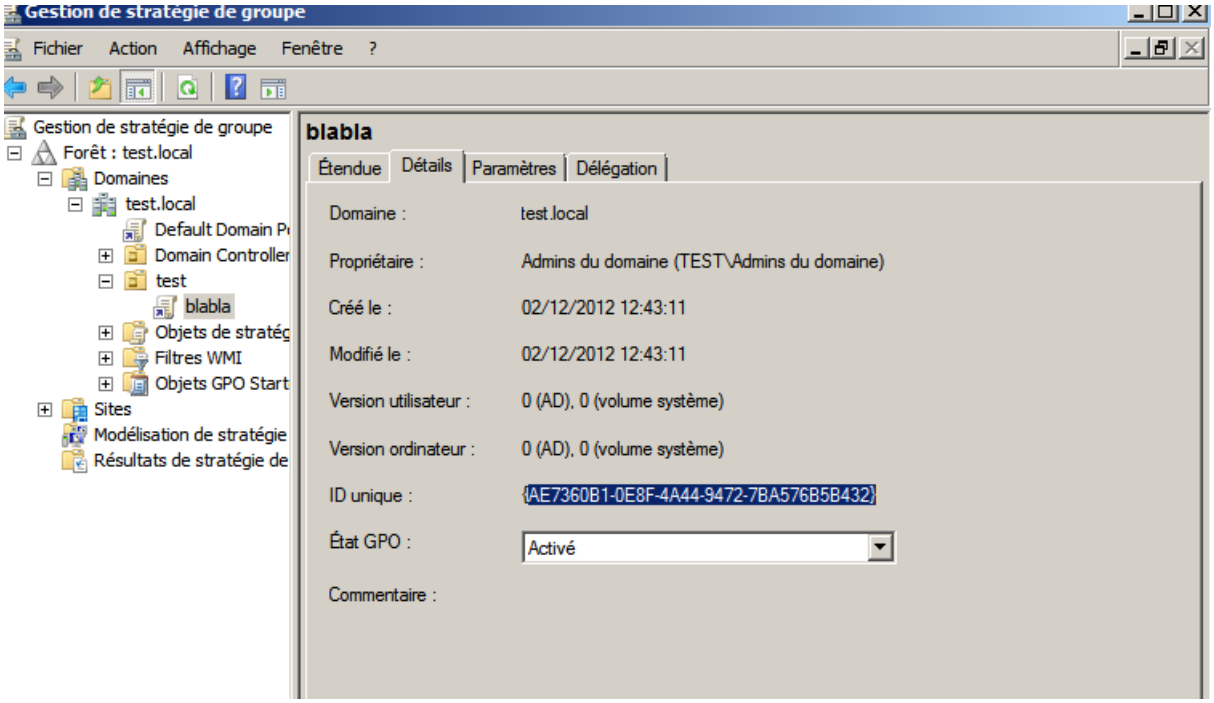


1

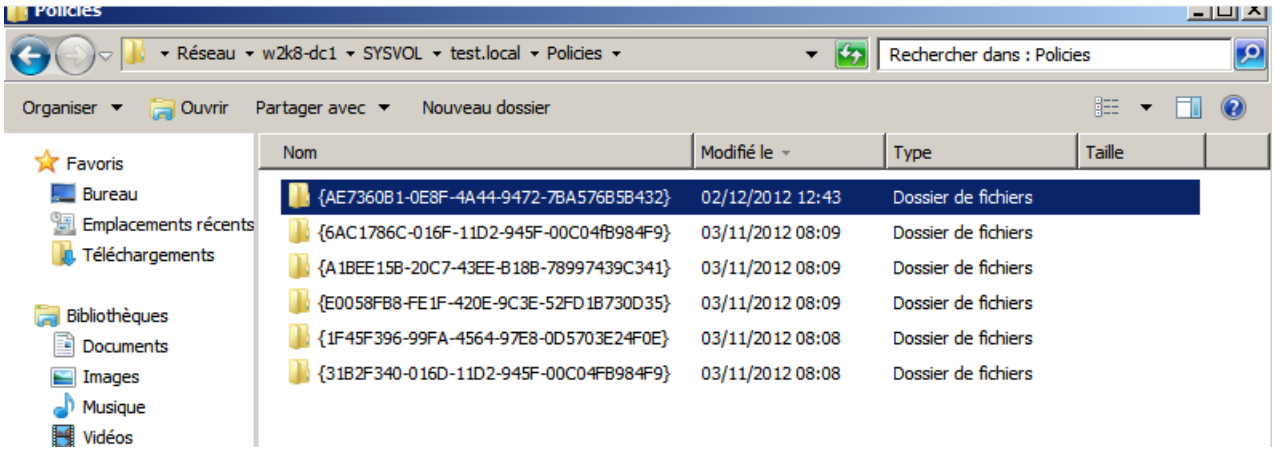
On ajoute un script de démo ***scritplogon*** dans le dossier « Netlogon »



Et une GPO ***blabla*** qui sera dans le dossier « sysvol\policies »



On retrouve dans le dossier « policies » notre stratégie de groupe identifiable par l'intermédiaire de "l'ID unique"



Les 3 étapes de la migration

La migration se fait en 3 étapes : (on part de l'état démarrer)

- **phase démarrer vers préparé**
  création du nouveau dossier sysvol_dfsr
- **phase préparé vers redirigé**
  les partages sont déplacés sur les nouveaux dossiers
- **phase redirigé vers éliminé**
  les anciens dossiers sont supprimés

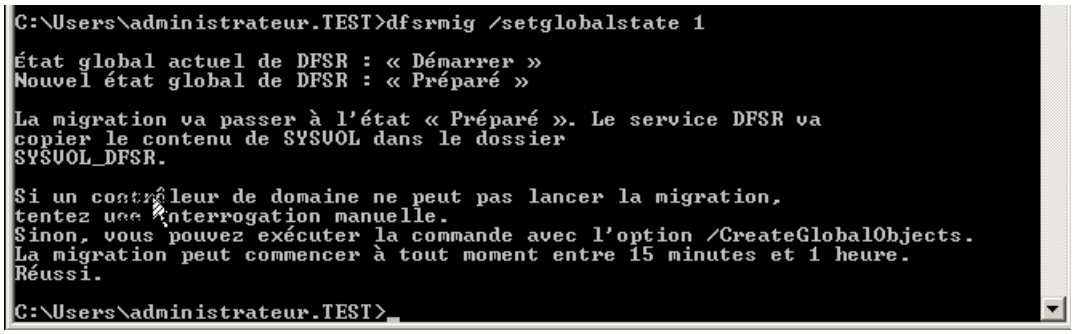
1° étape - dfsrmig /setglobalstate 1

Dans cette étape on crée le nouveau dossier **sysvol_dfsr**.

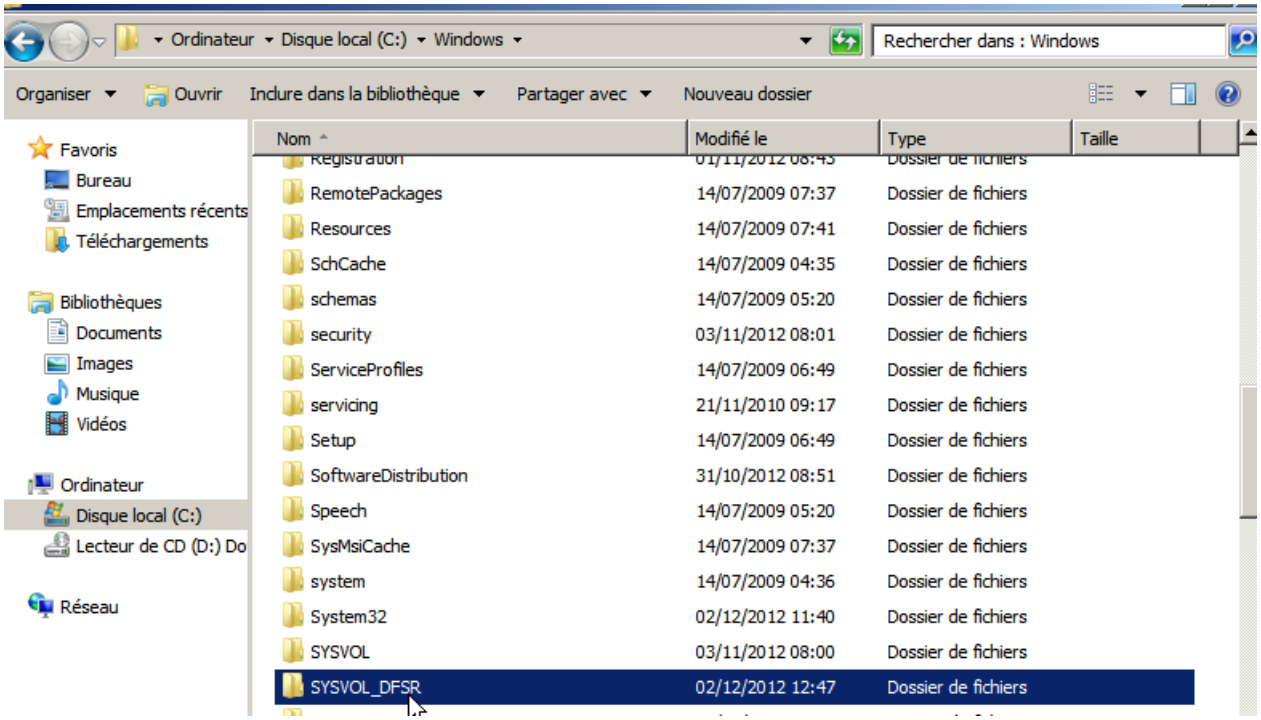
On passe du mode « démarrer » au mode « préparé » par la **commande**

dfsrmig /setglobalstate 1

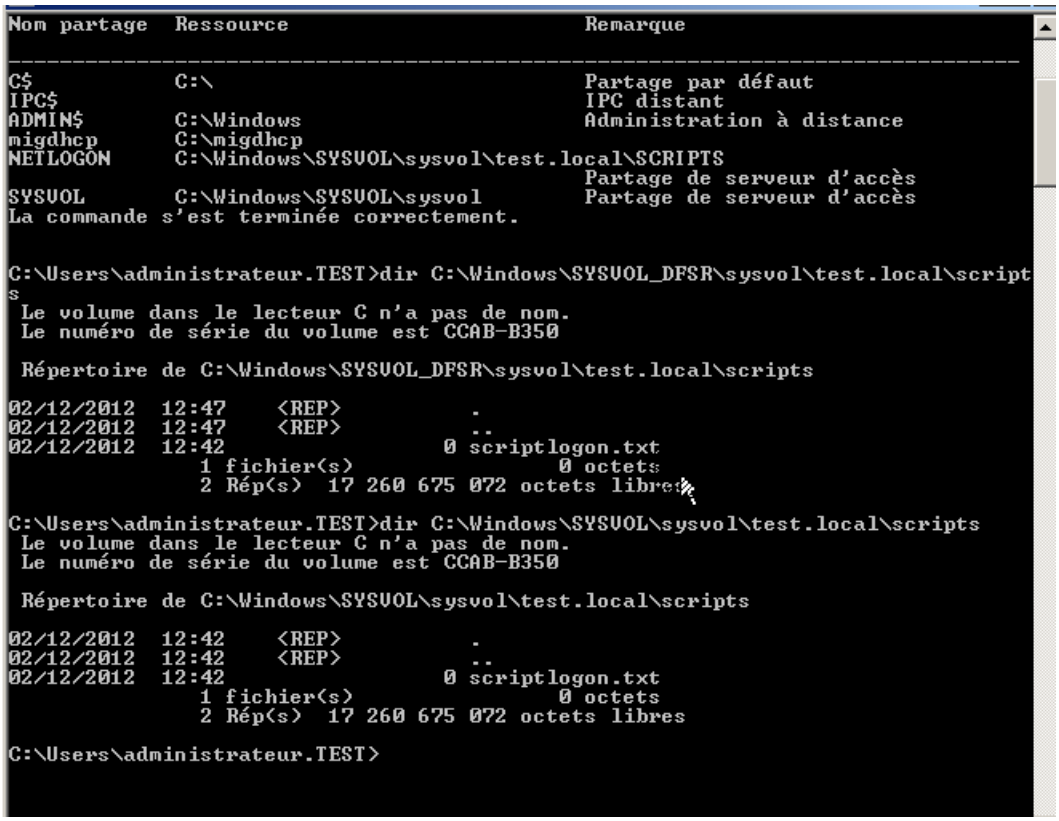
Le dossier c**:\\windows\\sysvol_dfsr** est donc crée et initialisé avec une copie du dossier sysvol actuel.



Dans l'image ci-dessous nous voyons que le dossier « **sysvol_dfsr** » a été créé, mais le partage pointe toujours sur l'ancien dossier.

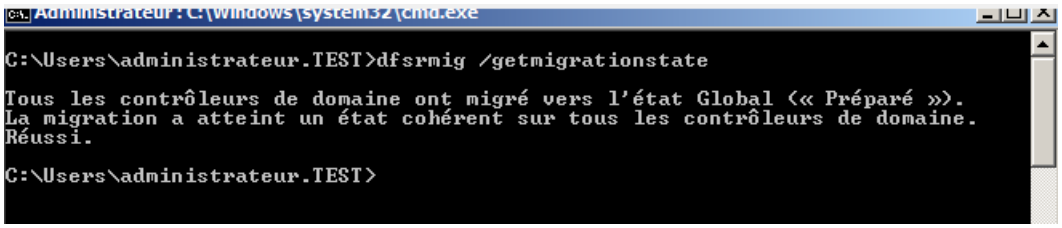


On vérifie par un **dir** sur les 2 dossiers ou sont stockés les scripts (partage netlogon), qu'ils sont identiques.



Dans le cas ou l'on à plusieurs contrôleurs de domaine, on valide que la phase 1 est bien terminée sur l'ensemble des DC par la commande

dfrsmig /getmigrationstate

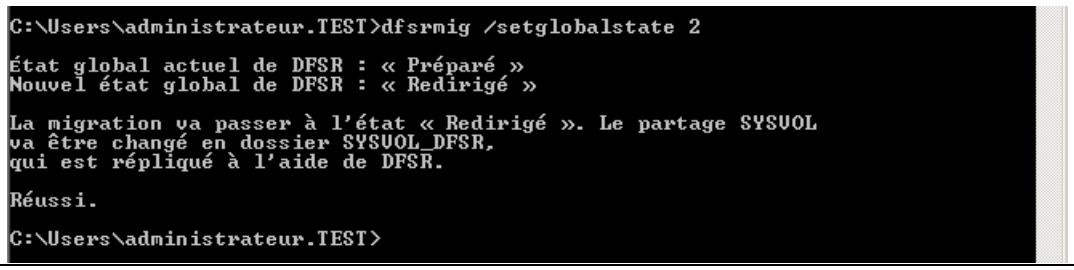


2 étape - dfsrmig /setglobalstate 2

Dans cette étape les partages « sysvol » et « netlogon » vont être modifiés pour basculer sur les nouveaux dossiers.

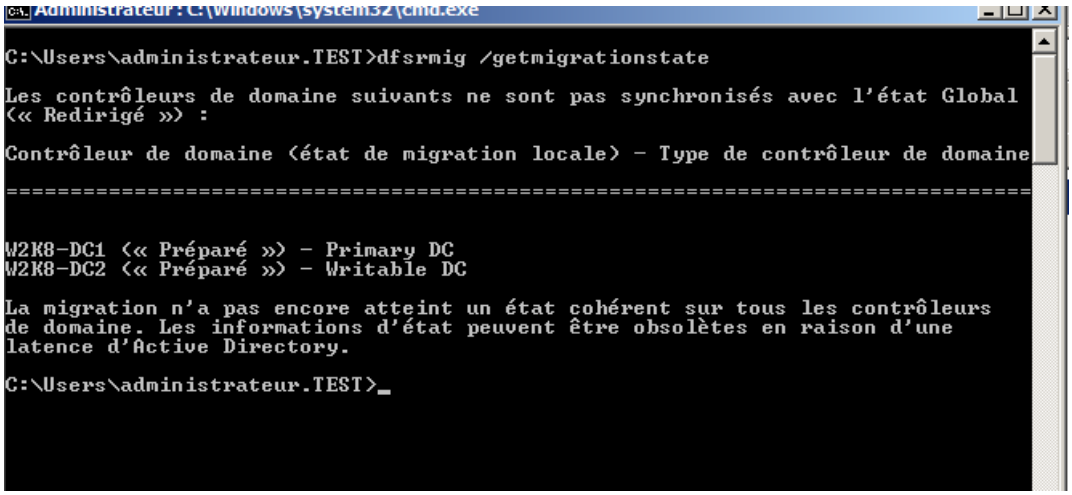
On passe du mode « préparé » au mode « redirigé » par la **commande**

dfsrmig /setglobalstate 2



La commande de vérification peut nous indiquer la nécessité … d'attendre

dfrsmig /getmigrationstate

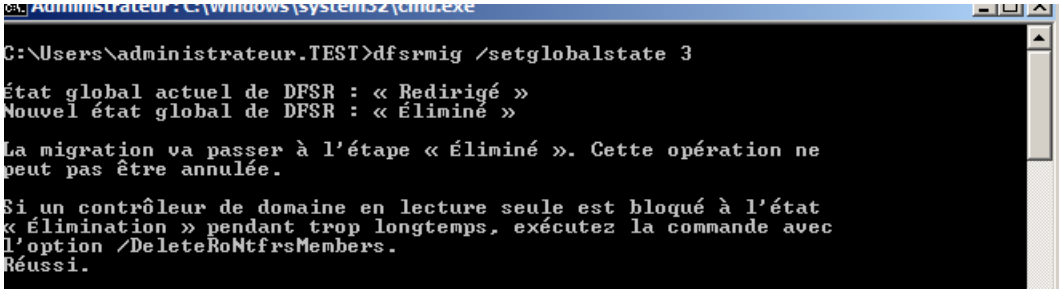


Mais après un laps de temps variable on doit obtenir une information comme quoi que tous les DC sont passés à l'étape redirigé.

3 étape - dfsrmig /setglobalstate 3

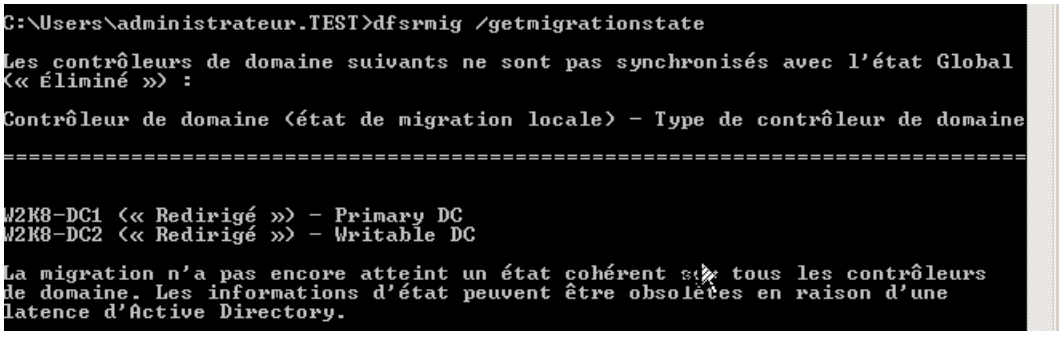
Nous allons passer à la dernière étape qui consiste à supprimer l'ancien dossier "sysvol". A partir de ce moment l'opération est irréversible. Cela se fait via la commande :

dfsrmig /setglobalstate 3

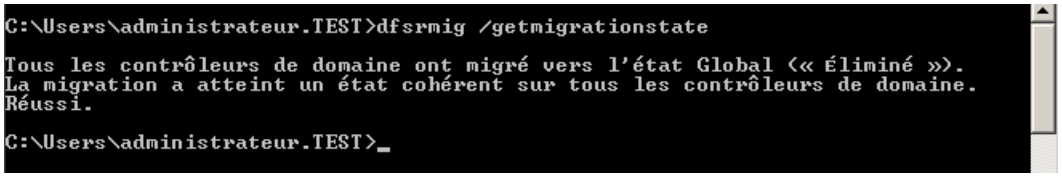


La commande de vérification peut encore une fois nous indiquer la nécessité … d'attendre

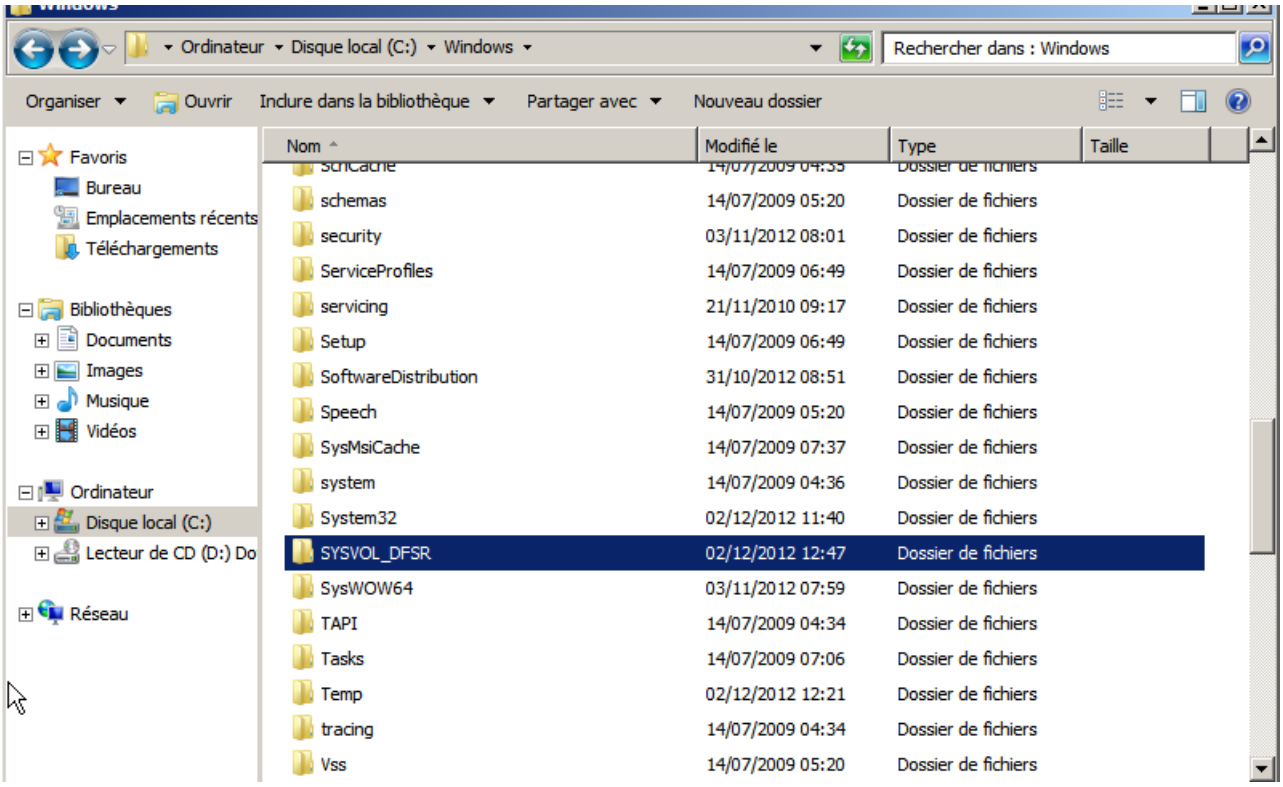
dfrsmig /getmigrationstate



Mais après un laps de temps variable on doit obtenir une information comme quoi que tous les DC sont passés à l'étape éliminé.



Après un délais, on peut constater la suppression du dossier « sysvol » dans le dossier Windows.



Vérification

La commande pour vérifier dans quelle étape nous somme est

dfrsmig /GetGlobalState :

```
C:\Users\administrateur.TEST>dfsrmig /getGLOBALstate

État global actuel de DFSR : « Éliminé »
Réussi.
```

Et un **net share** nous confirme que les partages sont bien sur les nouveaux dossiers.

```
C:\Users\administrateur.TEST>NET SHARE
Nom partage  Ressource                        Remarque
-------------------------------------------------------------------------------
C$           C:\                              Partage par défaut
IPC$                                          IPC distant
ADMIN$       C:\Windows                       Administration à distance
migdhcp      C:\migdhcp
NETLOGON     C:\Windows\SYSVOL_DFSR\sysvol\test.local\SCRIPTS
                                              Partage de serveur d'accès
SYSVOL       C:\Windows\SYSVOL_DFSR\sysvol    Partage de serveur d'accès
La commande s'est terminée correctement.
```

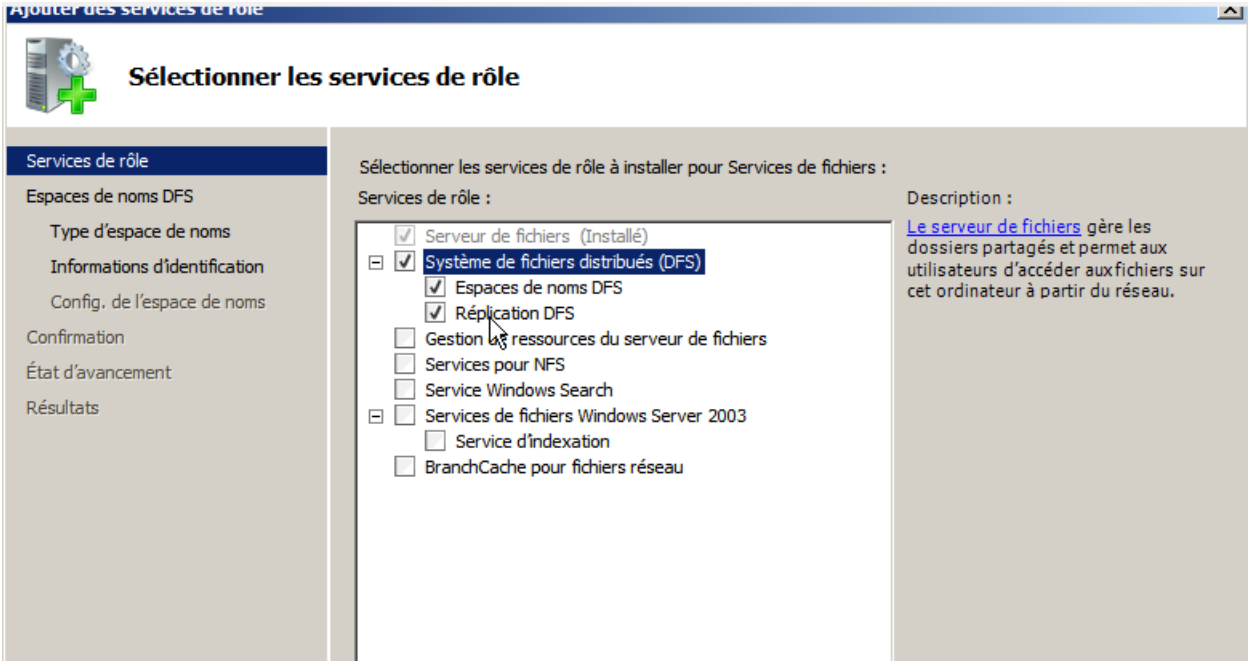
L'opération est terminée, mais nous souhaitons quand même surveiller l'état de la réplication.

SURVEILLER REPLICATION DFS SYSVOL

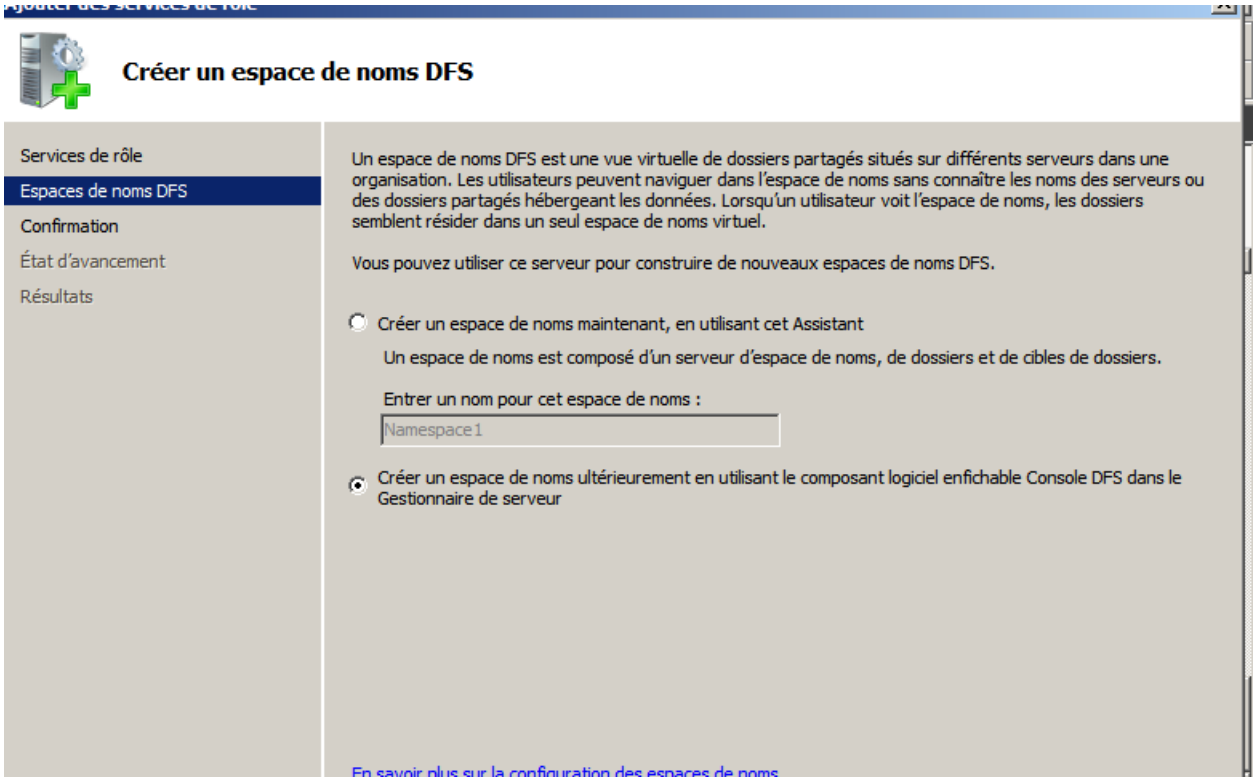
On souhaite juste surveiller l'état de la réplication

Rôle serveur de Fichier Option DFS

On installe le rôle serveur de fichier avec les options DFS. Cela va nous ajouter la console DFS, qui nous permettra de voir la réplication DFS.

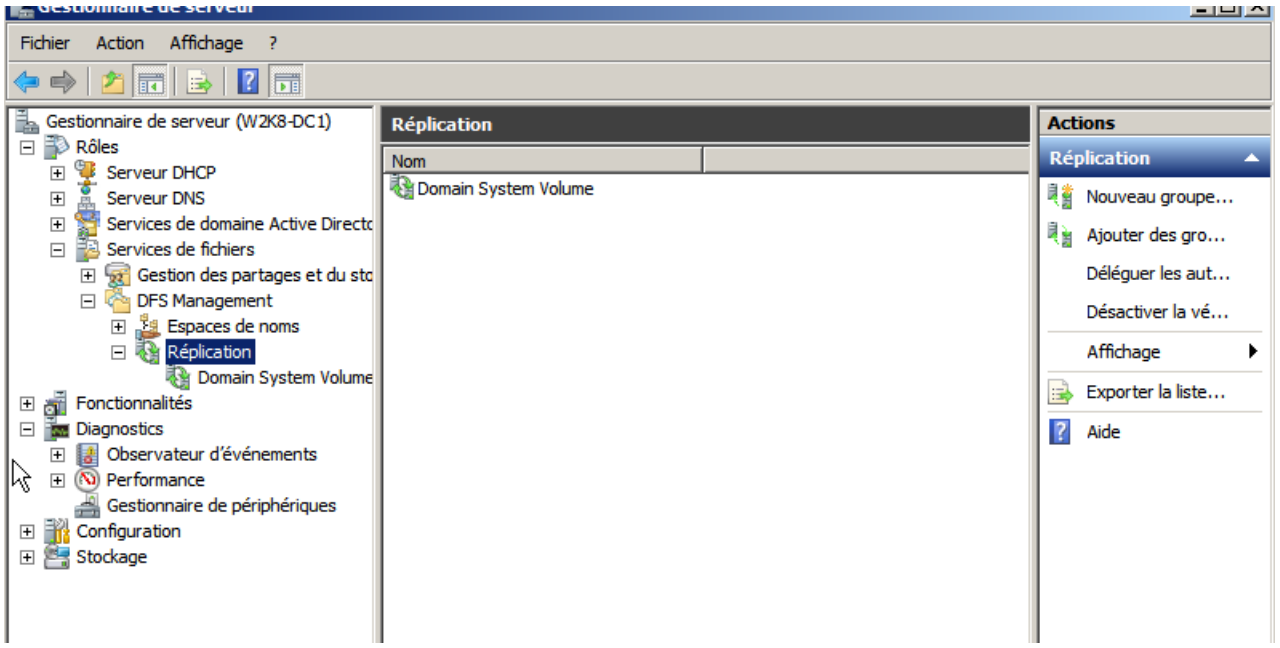


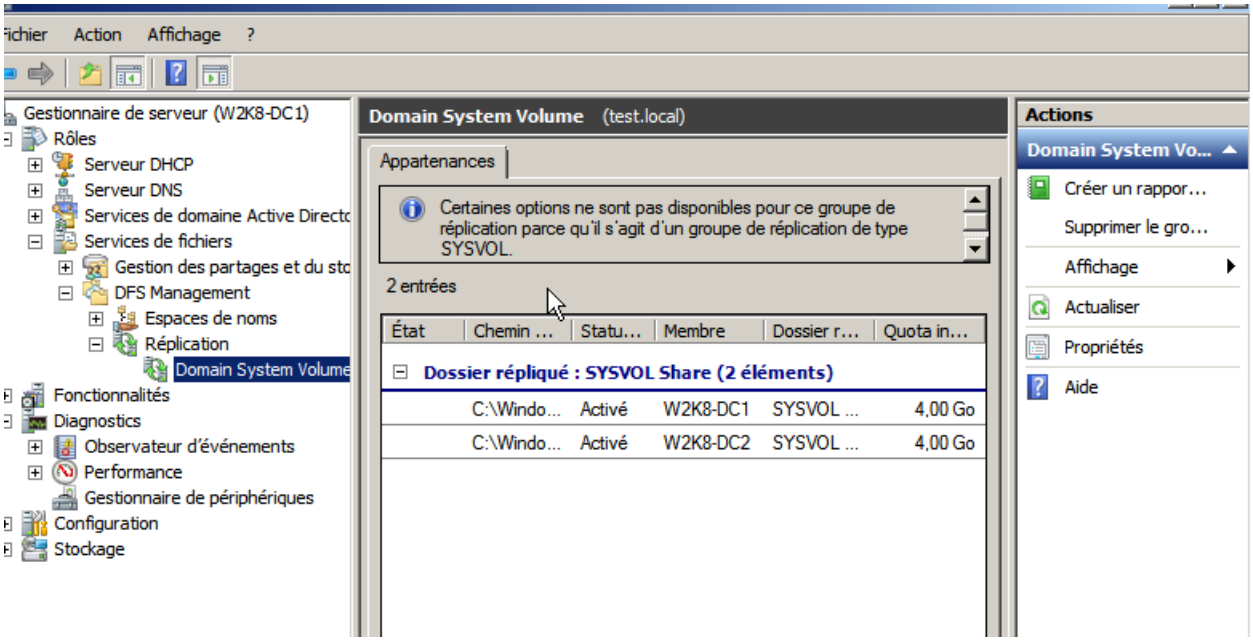
Nous n'allons pas créer d'espace de nom DFS, car l'objectif c'est juste d'utiliser les outils de réplication.



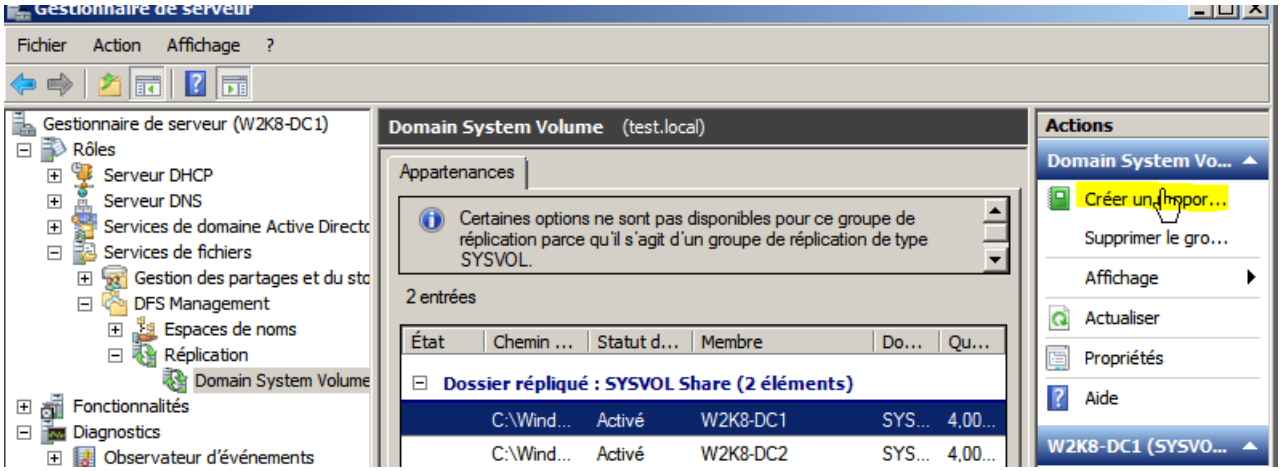
Dans la console gestion de serveur, sous **rôles / serveur de fichiers / DFS Management / Réplication**, nous trouvons « **Domain System volume** » qui est la réplication du dossier « sysvol ».

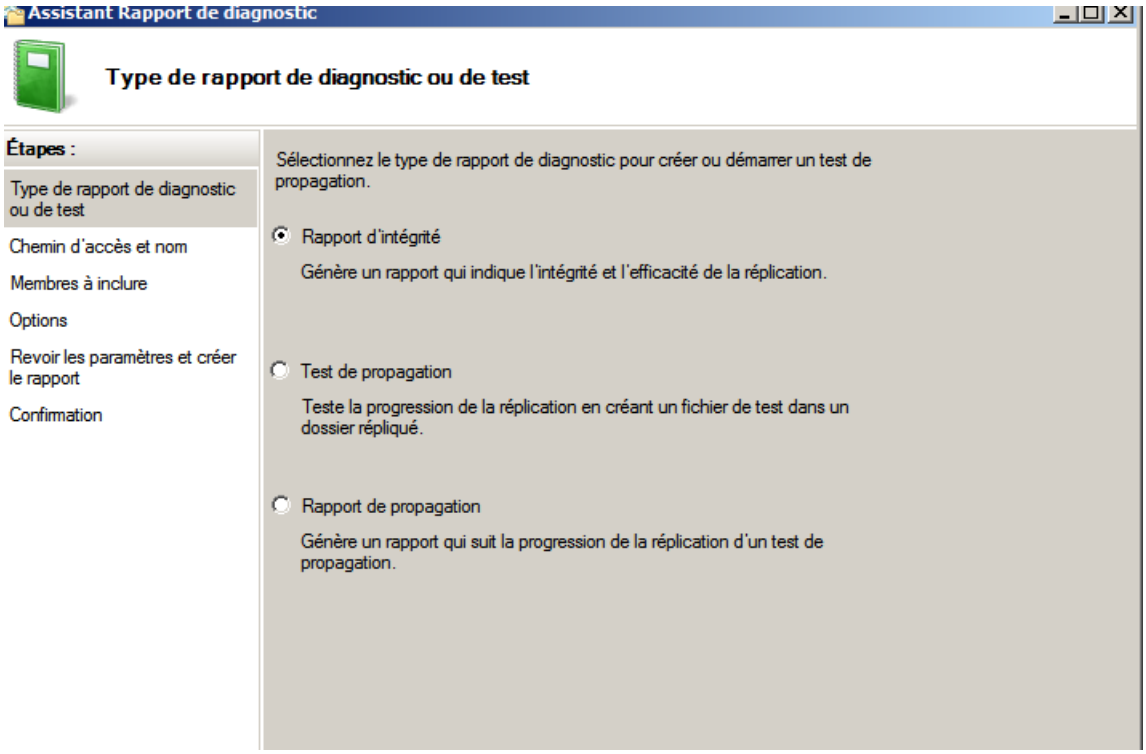
Sur la partie de droite dans la zone « actions », nous cliquons sur « créer un rapport… ».

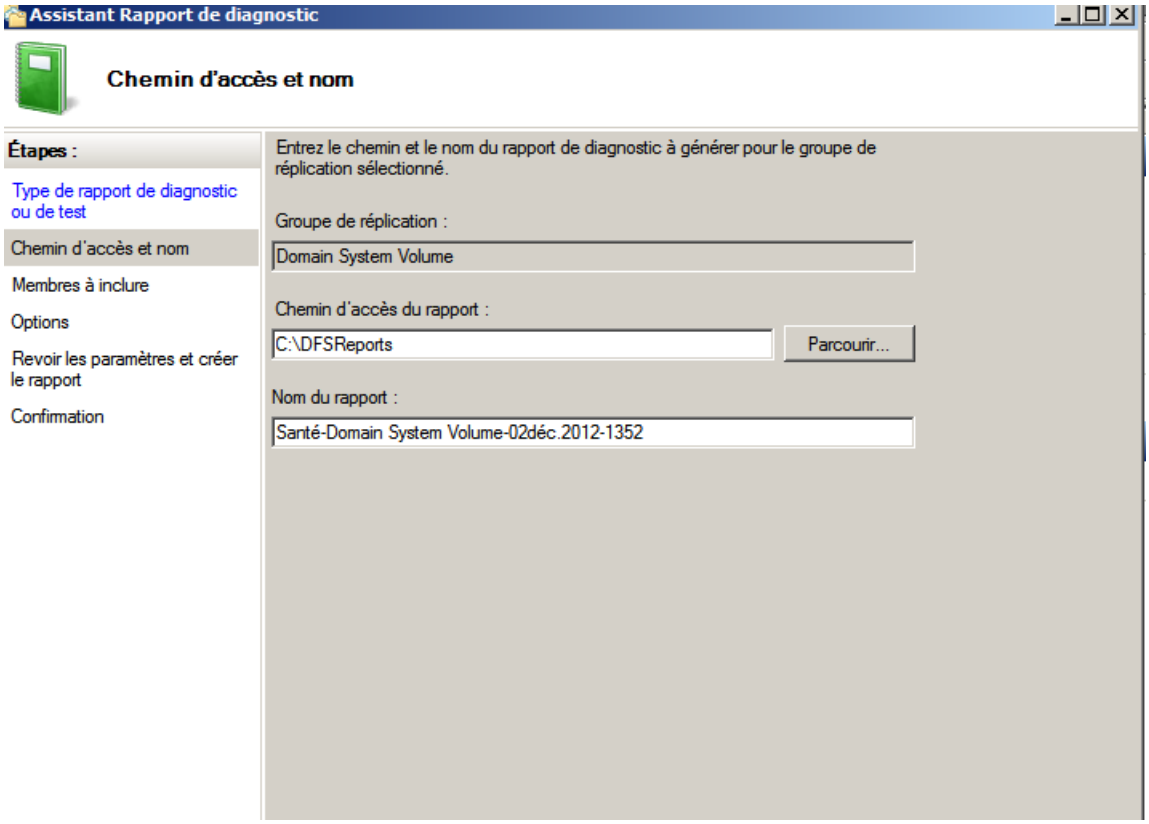


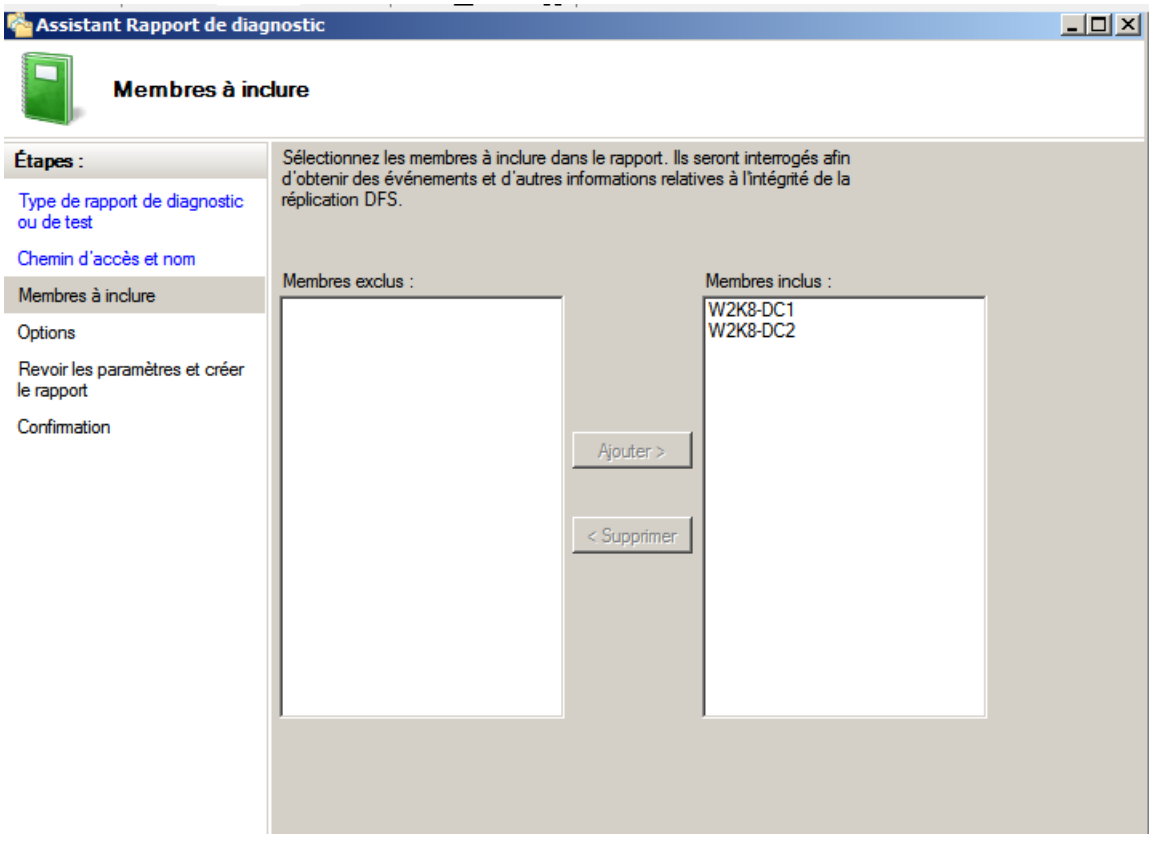


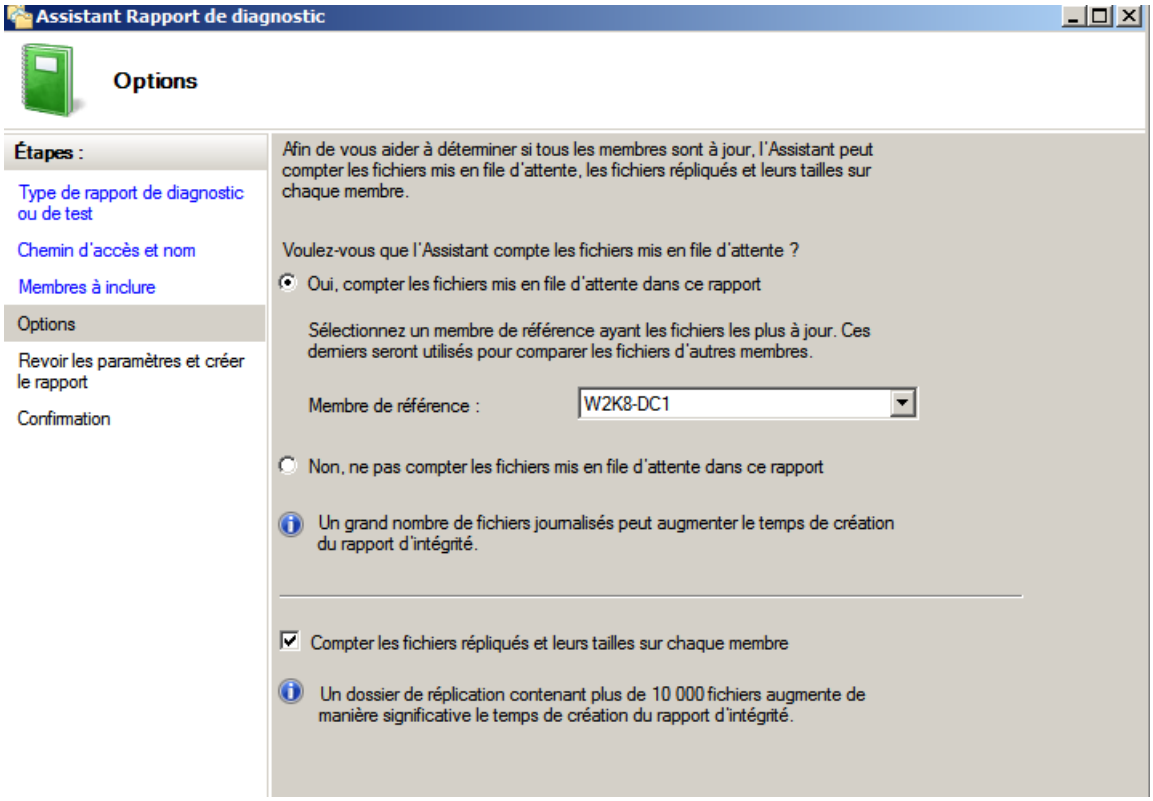
Nous allons utiliser l'option « créer un rapport » dans le volet d'action en haut à droite :

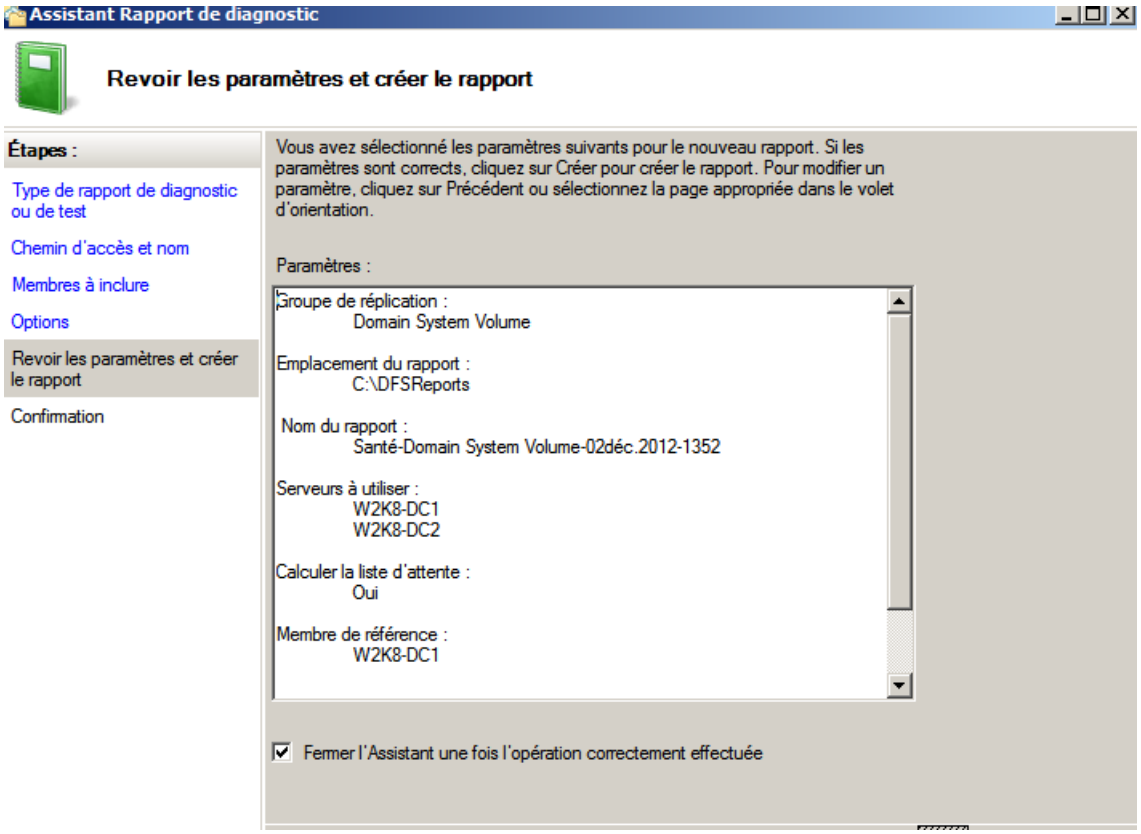

Gestionnaire de serveur
Fichier Action Affichage ?
Gestionnaire de serveur (W2K8-DC1)
Rôles
Serveur DHCP
Serveur DNS
Services de domaine Active Directc
Services de fichiers
Gestion des partages et du stc
DFS Management
Espaces de noms
Réplication
Domain System Volume
Fonctionnalités
Diagnostics
Observateur d'événements
Domain System Volume (test.local)
Appartenances
Certaines options ne sont pas disponibles pour ce groupe de réplication parce qu'il s'agit d'un groupe de réplication de type SYSVOL.
2 entrées
État Chemin ... Statut d... Membre Do... Qu...
Dossier répliqué : SYSVOL Share (2 éléments)
C:\Wind... Activé W2K8-DC1 SYS... 4,00...
C:\Wind... Activé W2K8-DC2 SYS... 4,00...
Actions
Domain System Vo...
Créer un impor...
Supprimer le gro...
Affichage
Actualiser
Propriétés
Aide
W2K8-DC1 (SYSVO...

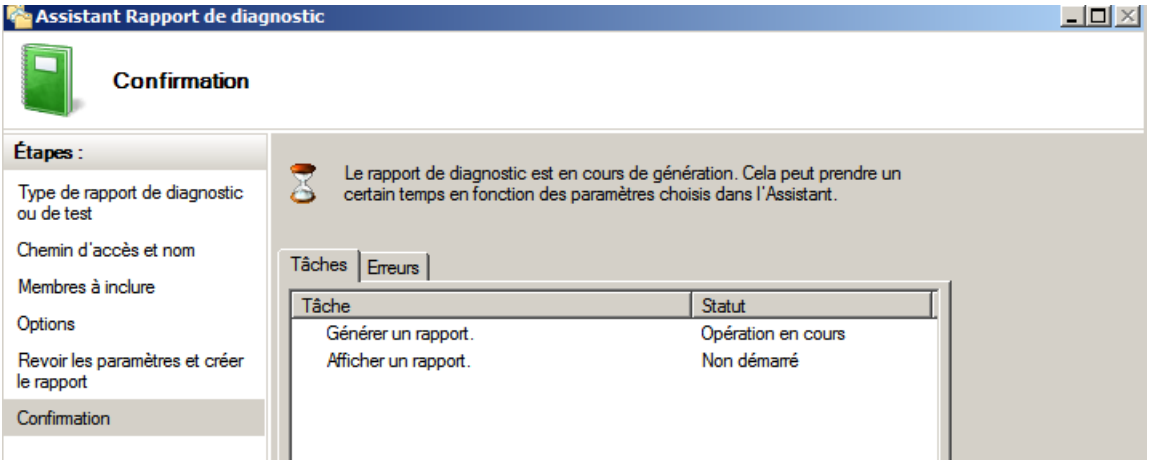

Assistant Rapport de diagnostic
Type de rapport de diagnostic ou de test
Étapes :
Type de rapport de diagnostic ou de test
Chemin d'accès et nom
Membres à inclure
Options
Revoir les paramètres et créer le rapport
Confirmation
Sélectionnez le type de rapport de diagnostic pour créer ou démarrer un test de propagation.
Rapport d'intégrité
Génère un rapport qui indique l'intégrité et l'efficacité de la réplication.
Test de propagation
Teste la progression de la réplication en créant un fichier de test dans un dossier répliqué.
Rapport de propagation
Génère un rapport qui suit la progression de la réplication d'un test de propagation.


Assistant Rapport de diagnostic
Chemin d'accès et nom
Étapes :
Type de rapport de diagnostic ou de test
Chemin d'accès et nom
Membres à inclure
Options
Revoir les paramètres et créer le rapport
Confirmation
Entrez le chemin et le nom du rapport de diagnostic à générer pour le groupe de réplication sélectionné.
Groupe de réplication :
Domain System Volume
Chemin d'accès du rapport :
C:\DFSReports
Parcourir...
Nom du rapport :
Santé-Domain System Volume-02déc.2012-1352

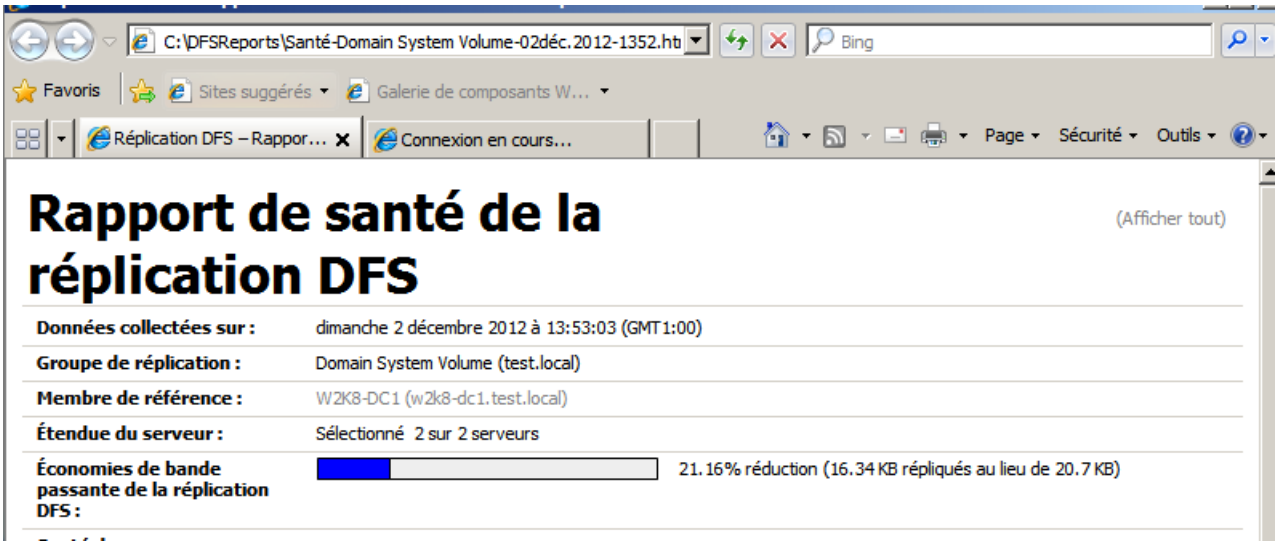

Assistant Rapport de diagnostic
Membres à inclure
Étapes :
Type de rapport de diagnostic ou de test
Chemin d'accès et nom
Membres à inclure
Options
Revoir les paramètres et créer le rapport
Confirmation
Sélectionnez les membres à inclure dans le rapport. Ils seront interrogés afin d'obtenir des événements et d'autres informations relatives à l'intégrité de la réplication DFS.
Membres exclus :
Membres inclus :
W2K8-DC1
W2K8-DC2
Ajouter >
< Supprimer

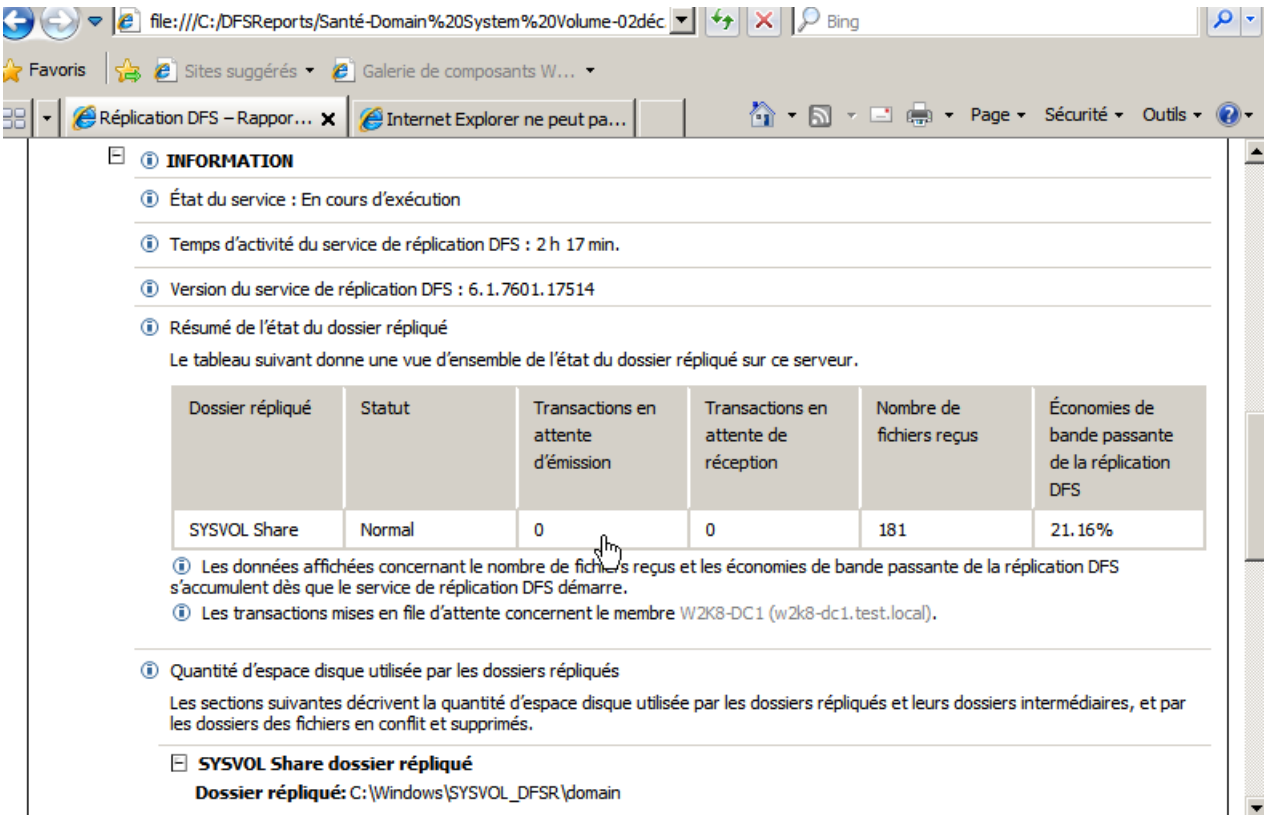

Assistant Rapport de diagnostic
Options
Étapes :
Type de rapport de diagnostic ou de test
Chemin d'accès et nom
Membres à inclure
Options
Revoir les paramètres et créer le rapport
Confirmation
Afin de vous aider à déterminer si tous les membres sont à jour, l'Assistant peut compter les fichiers mis en file d'attente, les fichiers répliqués et leurs tailles sur chaque membre.
Voulez-vous que l'Assistant compte les fichiers mis en file d'attente ?
Oui, compter les fichiers mis en file d'attente dans ce rapport
Sélectionnez un membre de référence ayant les fichiers les plus à jour. Ces derniers seront utilisés pour comparer les fichiers d'autres membres.
Membre de référence :
W2K8-DC1
Non, ne pas compter les fichiers mis en file d'attente dans ce rapport
Un grand nombre de fichiers journalisés peut augmenter le temps de création du rapport d'intégrité.
Compter les fichiers répliqués et leurs tailles sur chaque membre
Un dossier de réplication contenant plus de 10 000 fichiers augmente de manière significative le temps de création du rapport d'intégrité.


Assistant Rapport de diagnostic
Revoir les paramètres et créer le rapport
Étapes :
Type de rapport de diagnostic ou de test
Chemin d'accès et nom
Membres à inclure
Options
Revoir les paramètres et créer le rapport
Confirmation
Vous avez sélectionné les paramètres suivants pour le nouveau rapport. Si les paramètres sont corrects, cliquez sur Créer pour créer le rapport. Pour modifier un paramètre, cliquez sur Précédent ou sélectionnez la page appropriée dans le volet d'orientation.
Paramètres :
Groupe de réplication :
Domain System Volume
Emplacement du rapport :
C:\DFSReports
Nom du rapport :
Santé-Domain System Volume-02déc.2012-1352
Serveurs à utiliser :
W2K8-DC1
W2K8-DC2
Calculer la liste d'attente :
Oui
Membre de référence :
W2K8-DC1
Fermer l'Assistant une fois l'opération correctement effectuée

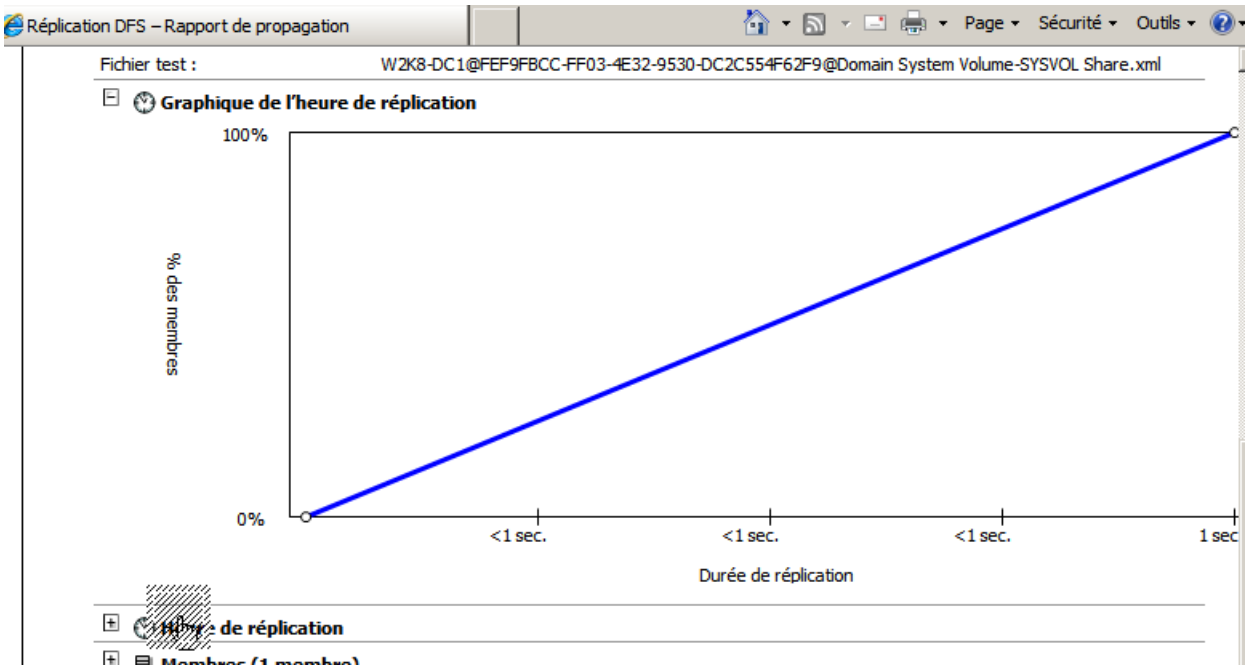


Dans le rapport on constate l'absence de dossier ou de fichier en conflit.





Il est possible de faire d'autres rapports comme un test de propagation :


Réplication DFS – Rapport de propagation
Page
Sécurité
Outils
Fichier test :
W2K8-DC1@FEF9FBCC-FF03-4E32-9530-DC2C554F62F9@Domain System Volume-SYSVOL Share.xml
Graphique de l'heure de réplication
100%
0%
% des membres
<1 sec.
<1 sec.
<1 sec.
1 sec
Durée de réplication

INTEGRATION DC 2008-2008R2 DANS DOMAINE 2000-2003

Avant de pouvoir ajouter un contrôleur de domaine doté de Windows Server 2008 ou 2008R2 dans un environnement Active Directory fonctionnant sous Windows 2000 Server ou Windows Server 2003, vous devez mettre à jour le schéma Active Directory

Adprep est le processus par lequel vous devez passer avant de pouvoir faire passer vos DC **Win2003** à une compatibilité avec un DC **Windows 2008 r2**

Commande	Contrôleur de domaine	Nombre d'exécutions nécessaires de la commande
adprep /forestprep	Doit être exécutée sur le maître d'opérations de schéma pour la forêt	Une fois pour la forêt entière
adprep /domainprep	Doit être exécutée sur le maître d'opérations d'infrastructure pour le domaine	Une fois dans chaque domaine où vous envisagez d'installer un contrôleur de domaine supplémentaire qui exécute une version de Windows Server postérieure à la version la plus récente en cours d'exécution dans le domaine. **Remarque** Les domaines où vous n'ajoutez pas de nouveau contrôleur de domaine seront affectés par **adprep /forestprep**, mais vous n'avez pas besoin d'exécuter **adprep /domainprep** pour ceux-ci.
adprep /domainprep /gpprep	Doit être exécutée sur le maître d'opérations d'infrastructure pour le domaine	Une fois dans chaque domaine au sein de la forêt

Adprep pour le schéma

Vous devez mettre à jour le schéma à partir du contrôleur de domaine qui héberge le rôle de **maître d'opérations de schéma**

- Insérez le DVD de Windows Server 2008 dans le lecteur CD ou DVD. Copiez le contenu du dossier **\support\adprep** dans un dossier Adprep dans le contrôleur de schéma.
- Ouvrez une invite de commandes, placez vous dans les dossiers copiés. À l'invite de commandes, tapez:

  Adprep.exe /forestprep

  Ou **adprep32.exe /forestprep**

  Si on envisage à terme d'installer un contrôleur de domaine en lecture seule (RODC) il faut alors aussi passer la commande:

  adprep /rodcprep

  Ou **adprep32.exe /rodcprep**

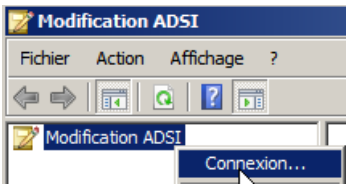
N.B: Attendez la réplication des modifications dans la forêt.

Vérification Adprep du schéma ADSIedit

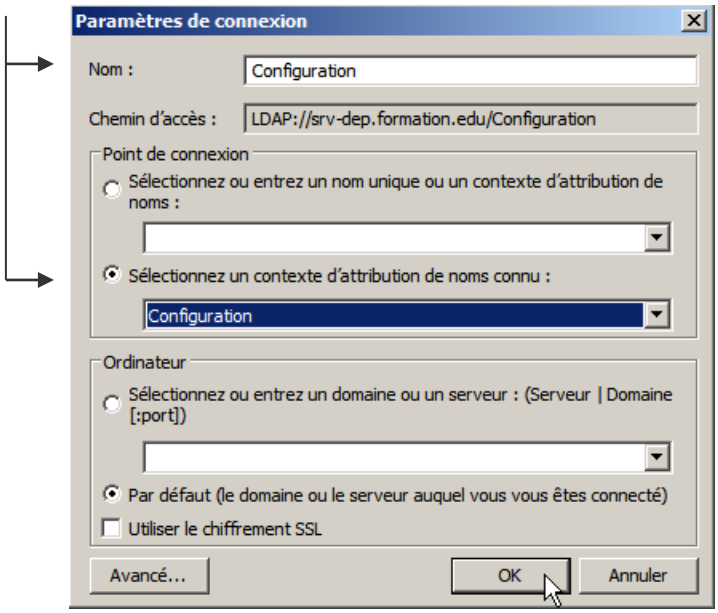
Au terme de la commande **adprep /forestprep**, un message apparaît dans la fenêtre Invite de commandes pour indiquer qu'Adprep a correctement mis à jour les informations au niveau de la forêt….

On peut vérifier à postériori que la commande adprep /forestprep s'est correctement déroulée via **ADSIEdit**

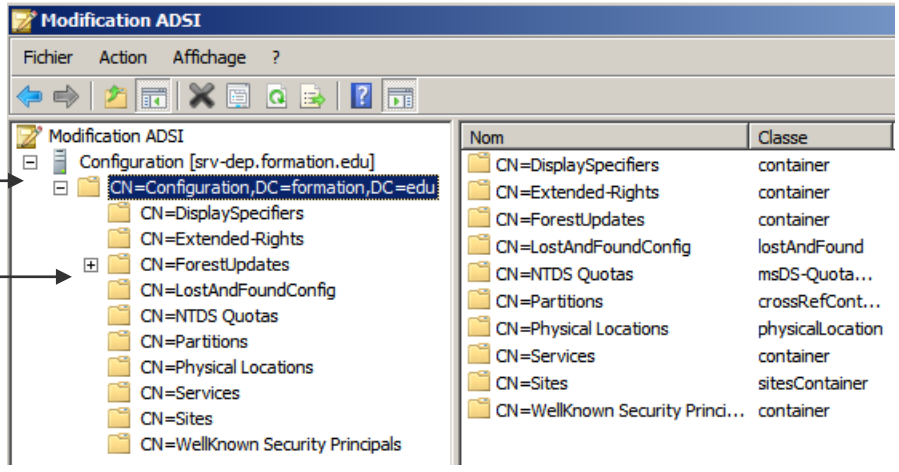
lancer la console **adsiedit.msc** puis clic droit / connexion.



demander **Sélectionnez un contexte d'attribution de noms connu**, puis **Configuration**



on obtient



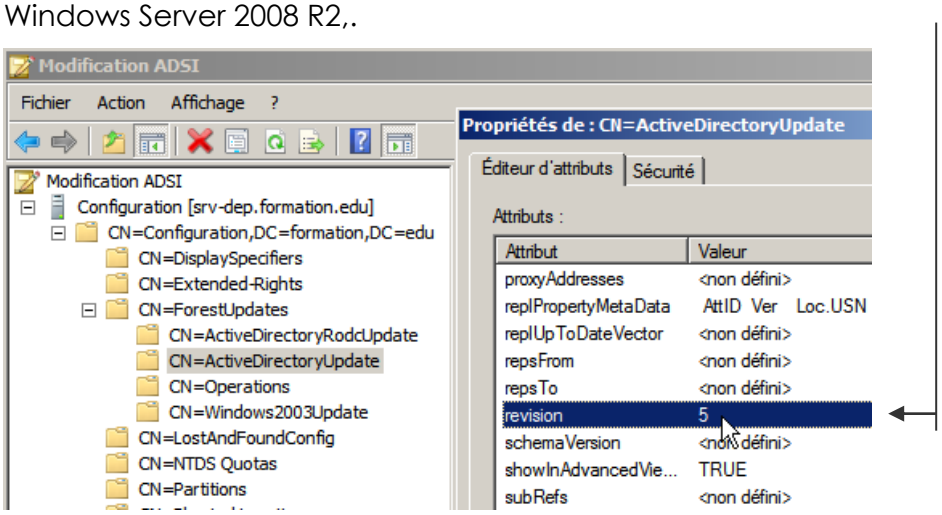
Développer **Configuration**, puis

CN=Configuration, DC=domaine_racine_forêt

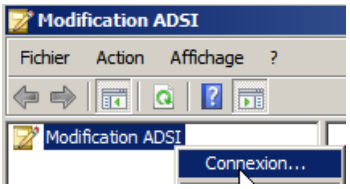
Développer sur CN=ForestUpdates.

Demander les propriétés de CN=ActiveDirectoryUpdate,

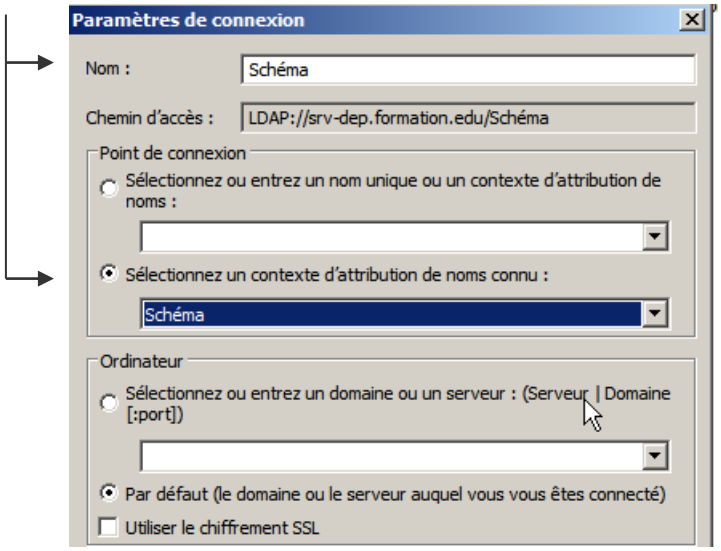
- Vérifiez que l'attribut **Revision** à pour valeur **4** pour 2008, ou **5** pour Windows Server 2008 R2,.



Il faut maintenant tester Modification ADSI, ... donc Connexion.

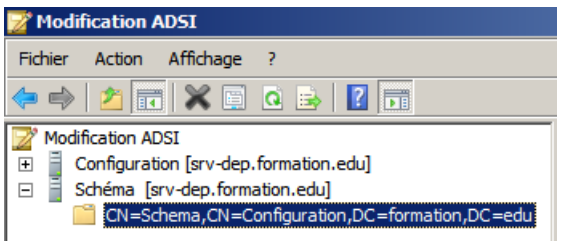


demander **Sélectionnez un contexte d'attribution de noms connu**, puis **Schéma**

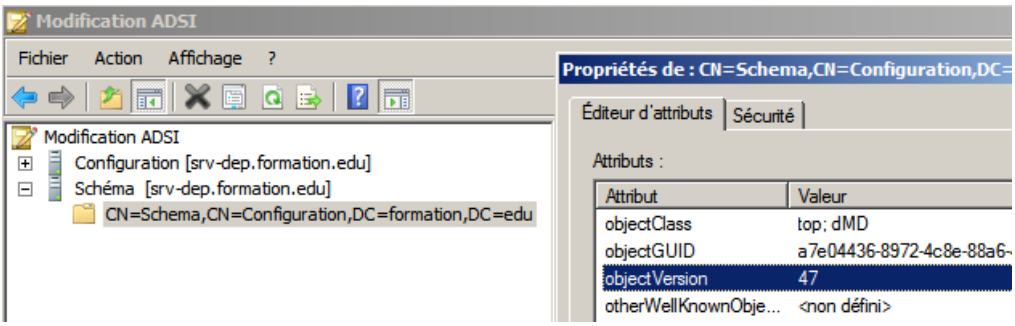


Développer **Schéma**, puis

demander les propriétés de CN=Schema,CN=Configuration,DC=domaine_racine_forêt,



pour Windows 2008 l'attribut **objectVersion** pour valeur **46** pour 2008 ou **47** pour Windows 2008 R2



Adprep pour le domaine

Sur contrôleur de domaine qui héberge le rôle de **maître d'infrastructure**

- Ouvrez une invite de commandes, taper

  adprep /domainprep

  Ou **adprep32.exe / domainprep**

  N.B: désactivation de l'éventuel anti-virus…

  adprep /domainprep /gpprep

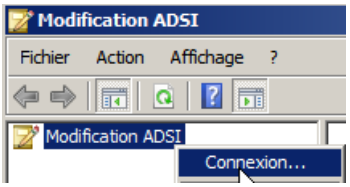
  Ou **adprep32.exe / domainprep /gpprep**

N.B: Le domaine 2003 doit être en mode "2000 natif" minimum…

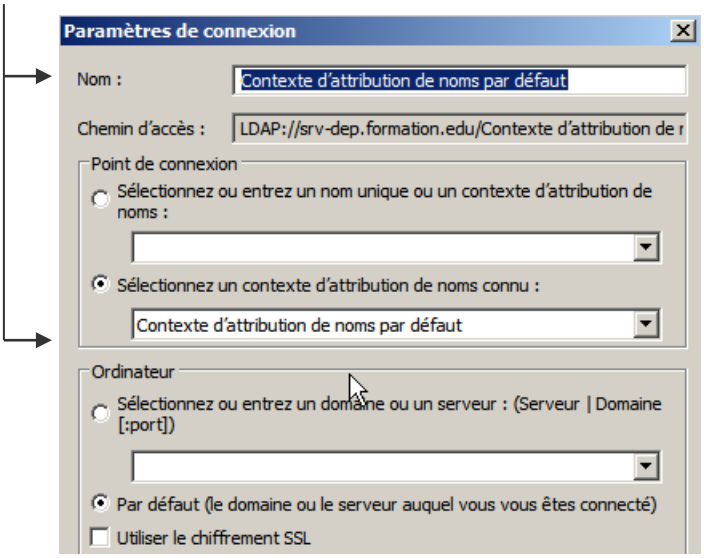
N.B: Attendez la réplication dans le domaine tout entier.

Vérification Adprep du domaine ADSIedit

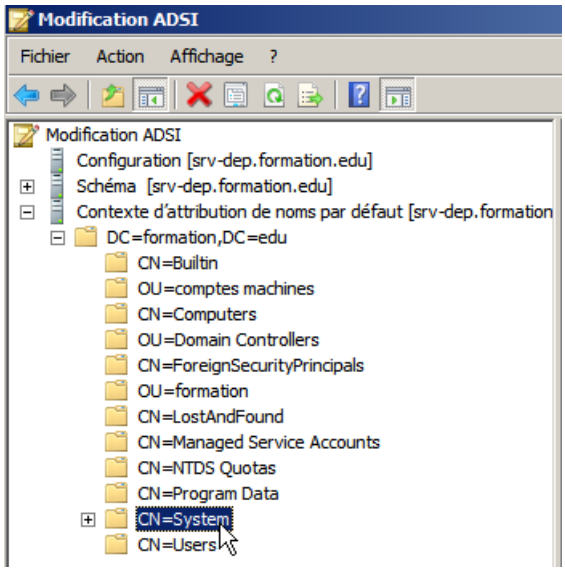
lancer la console **adsiedit.msc** puis clic droit / connexion.



demander **Sélectionnez un contexte d'attribution de noms connu**, puis **Contexte**



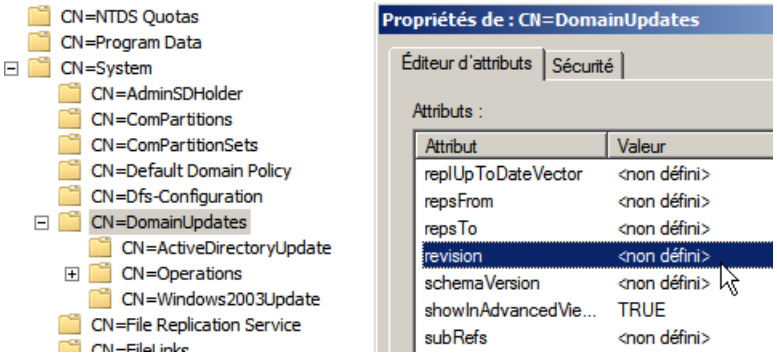
on obtient



Développer Contexte d'attribution de noms par défaut, sur le conteneur portant le nom unique du domaine, puis sur CN=System.

Demander les propriétés de CN=DomaineUpdates

pour Windows 2008 l'attribut **revision** pour valeur 4 ou plus



Si 1 seul domaine dans une forêt, le maitre d'infrastructure étant désactivé, la révision est non marquée…

Niveaux Fonctionnels de Forêt

Windows 2000 :

Par défaut, ce niveau permet une compatibilité avec des contrôleurs de domaine sous NT4.0, Windows 2000 et Windows 2003.

Windows 2003 :

Ce niveau de fonctionnalité requiert que tous les contrôleurs de domaines soient sous Windows 2003 Server

Windows 2008 (équivalent à 2003):

Ce niveau de fonctionnalité n'apporte rien de plus, mais requiert que tous les contrôleurs de domaines soient sous Windows 2008 Server (sécurité ?...)

Windows 2003 version préliminaire :

Ce niveau est utilisé lors de migrations de NT 4.0 vers Windows 2003 Server.

NB : Il faut augmenter le niveau fonctionnel de tous les domaines de la forêt avant de pouvoir augmenter celui de la forêt.

NB : Il est impossible de revenir à un niveau fonctionnel de domaine et de forêt inférieur, on ne peut qu'augmenter le niveau de fonctionnalités.

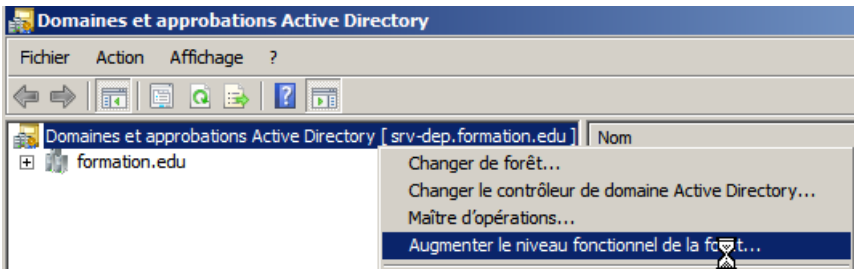
N.B: le choix du niveau conditionne le type des autres serveurs…

Niveau fonctionnel de forêt	Fonctionnalités activées	Systèmes d'exploitation de contrôleur de domaine pris en charge
Windows 2000	Toutes les fonctionnalités Active Directory par défaut.	Windows Server 2008 Windows Server 2003 Windows 2000
Windows Server 2003	Toutes les fonctionnalités Active Directory par défaut, plus les fonctionnalités suivantes : • Approbation de forêt. • Changement de nom de domaine. • Réplication de valeurs liées (modifications d'appartenance de groupe pour stocker et répliquer des valeurs pour chaque membre au lieu de répliquer l'ensemble de l'appartenance comme une seule unité) Cela permet de moins utiliser le processeur et la bande passante réseau pendant la réplication et d'éliminer le risque de perdre des mises à jour lorsque des membres différents sont ajoutés ou supprimés simultanément de différents contrôleurs de domaine. • Déploiement d'un contrôleur de domaine en lecture seule exécutant Windows Server 2008.	Windows Server 2003 Windows Server 2008
Windows Server 2008	Toutes les fonctionnalités du niveau fonctionnel de forêt Windows Server 2003, mais pas de fonctionnalités supplémentaires. Toutefois, tous les domaines qui sont ultérieurement ajoutés à la forêt fonctionneront par défaut au niveau fonctionnel de domaine Windows Server 2008. Si vous prévoyez de n'inclure que des contrôleurs de domaine exécutant Windows Server 2008 dans toute la forêt, vous pouvez choisir ce niveau fonctionnel de forêt pour simplifier l'administration. De cette façon, il ne sera jamais nécessaire d'augmenter le niveau fonctionnel des domaines que vous créez dans la forêt.	Windows Server 2008

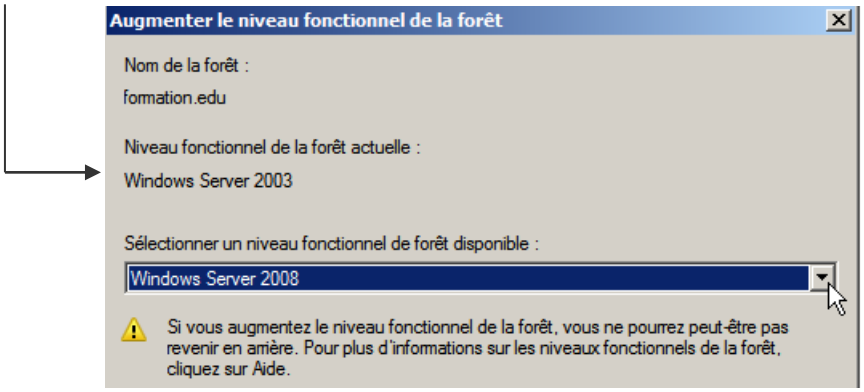
La modification se fait dans **Domaines et approbations Active Directory**

il faut se placer sur la forêt,

puis clic droit **Augmenter le niveau fonctionnel de la forêt...**



Le niveau actuel est précisé...



Niveaux Fonctionnels de Domaine

Windows 2000 mixte (n'existe plus sous 2008):

Permet de contenir au sein du domaine des contrôleurs de domaine Windows 2003, Windows 2000 et également des contrôleurs secondaires de domaine Windows NT 4.0.

Windows 2000 natif :

Si le domaine ne contient que des contrôleurs de domaine sous Windows 2000 et Windows 2003. Ce niveau fonctionnel permet d'activer certaines fonctionnalités du domaine dans Active Directory.

Windows 2003 :

Le niveau fonctionnel le plus élevé pour un domaine. Il n'est accessible uniquement si le domaine ne possède que des contrôleurs de domaine sous Windows 2003 server. Avec ce niveau fonctionnel, toutes les fonctionnalités Active Directory pour le domaine sont disponibles.

Windows 2008 (équivalent à 2003):

Ce niveau de fonctionnalité n'apporte rien de plus, mais requiert que tous les contrôleurs de domaines soient sous Windows 2008 Server (sécurité ?...)

Windows 2003 niveau préliminaire :

Ce niveau fonctionnel est utilisable si le domaine contient des contrôleurs de domaine sous NT 4.0 et des contrôleurs de domaine sous Windows 2003 server. Ce niveau fonctionnel est utilisé dans le cadre d'une migration.

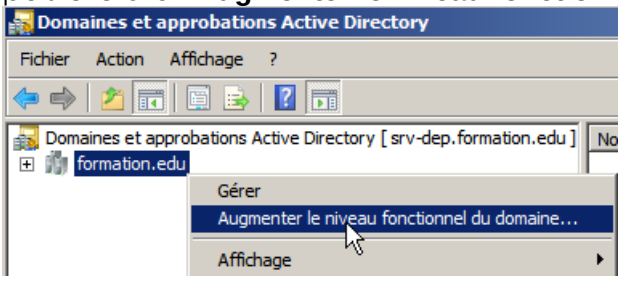
N.B: le choix du niveau conditionne le type des autres serveurs…

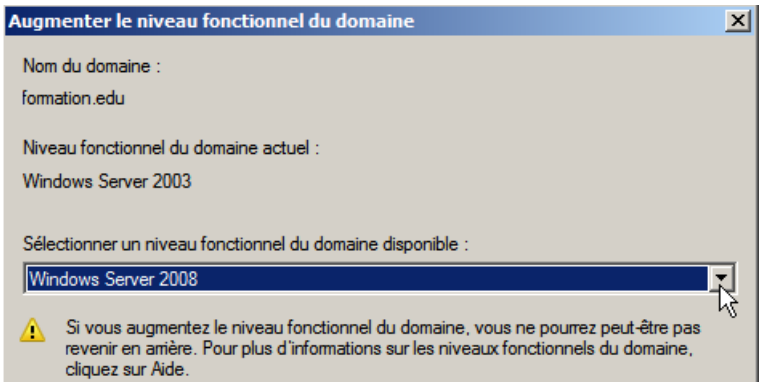
Niveau fonctionnel de domaine	Fonctionnalités activées	Systèmes d'exploitation de contrôleur de domaine pris en charge
Windows 2000 natif	Toutes les fonctionnalités Active Directory par défaut, plus les fonctionnalités suivantes : • groupes universels pour les groupes de distribution et les groupes de sécurité ; • imbrication de groupes ;	Windows 2000 Windows Server 2003 Windows Server 2008
Windows Server 2003	Toutes les fonctionnalités Active Directory par défaut, toutes les fonctionnalités du niveau fonctionnel de domaine Windows 2000 natif, plus les fonctionnalités suivantes : • Disponibilité de l'outil de gestion de domaines, Netdom.exe, pour préparer le changement de nom des contrôleurs de domaine.	Windows Server 2003 Windows Server 2008
Windows Server 2008	Toutes les fonctionnalités Active Directory par défaut, toutes les fonctionnalités du niveau fonctionnel de domaine Windows Server 2003, plus les fonctionnalités suivantes : • Prise en charge de la réplication du système de fichiers DFS (Distributed File System) pour SYSVOL, ce qui offre une réplication plus fiable et plus granulaire du contenu de SYSVOL. Il peut être nécessaire d'effectuer des opérations supplémentaires pour utiliser la réplication DFS pour SYSVOL.	Windows Server 2008

La modification se fait dans **Domaines et approbations Active Directory**

il faut se placer sur le domaine,

puis clic droit **Augmenter le niveau fonctionnel du domaine...**





Utilitaire ADSIedit

- L'utilitaire ADSIEdit est installé par défaut sur les CD 2008 ou 2008 R2.
- Pour l'avoir en Environnement 2003 Sp2 ou XP sp3 il faut installer les supports Tools (présents sur le CD 2003 SRV en Support\Tools ou téléchargeables sur le site de microsoft)
- Pour l'avoir sur un client Seven, il faudrait installer RSAT…

Détails rapides

Version:	1.0
Date de publication :	11/08/2009
Langue:	Français
Taille du téléchargement:	215.1 Mo - 437.2 Mo*

Ensuite via **Exécuter / ADSIEdit.msc**, puis cliquez sur OK.