|  |  |
| --- | --- |
| formation-informatique-grenoble-cabare  http://[WWW.CABARE.NET](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](http://www.cabare.net) ©

**table des matiÈres**

[Intégration DC 2012r2 dans 1 Domaine 2008R2 3](#_Toc471822814)

[Planification de la migration 3](#_Toc471822815)

[Vérification Domaine 4](#_Toc471822816)

[Sauvegarde du DC 5](#_Toc471822817)

[Blocage de la réplication 5](#_Toc471822818)

[Vérification version schéma forêt et domaine 6](#_Toc471822819)

[Adprep pour la forêt 9](#_Toc471822820)

[Déblocage de la réplication 9](#_Toc471822821)

[Adprep pour le domaine 10](#_Toc471822822)

[Intégration nouveau serveur membre 2012 10](#_Toc471822823)

[Rôle AD DS Directory Services , DNS 12](#_Toc471822824)

[Assistant de configuration Active Directory (ex dcpromo) 18](#_Toc471822825)

[Test serveur et réplication générale 21](#_Toc471822826)

[Paramétrage IP pour le serveurs DNS et sur le Domaine 25](#_Toc471822827)

[Migration rôles FSMO 27](#_Toc471822828)

[Suppression Catalogue Global ancien serveur 30](#_Toc471822829)

[Suppression DNS ancien serveur 31](#_Toc471822830)

[Démontage ancien DC 33](#_Toc471822831)

[Erreur possible dcpromo /forceremoval: 34](#_Toc471822832)

[Nettoyage des méta données de l’AD: 36](#_Toc471822833)

[L'utilitaire NTDSUTIL: 38](#_Toc471822834)

[Gestion Synchronisation base de temps ntp: 39](#_Toc471822835)

[Vérification Niveau fonctionnel: 41](#_Toc471822836)

[Passage du niveau de domaine de 2003 à 2008r2 42](#_Toc471822837)

[Passage du niveau de Forêt de 2003 à 2008r2 42](#_Toc471822838)

[Migration de DHCP 44](#_Toc471822839)

[Principe de la migration 44](#_Toc471822840)

[Ajout du rôle dhcp sur le serveur 2012 44](#_Toc471822841)

[Exportation de la configuration du DHCP 2008 47](#_Toc471822842)

[Importation de la configuration dans le DHCP 2012 47](#_Toc471822843)

[Autorisation et activation des serveurs 48](#_Toc471822844)

[Migration réplication Sysvol 49](#_Toc471822845)

[Niveau fonctionnel 2008 49](#_Toc471822846)

[DFSRMIG - Migrer la réplication NTFSR en DFS-R 49](#_Toc471822847)

[Les 3 étapes de la migration 51](#_Toc471822848)

[1° étape - dfsrmig /setglobalstate 1 51](#_Toc471822849)

[2 étape - dfsrmig /setglobalstate 2 52](#_Toc471822850)

[3 étape - dfsrmig /setglobalstate 3 53](#_Toc471822851)

[Vérification 54](#_Toc471822852)

[Surveiller replication DFS Sysvol 55](#_Toc471822853)

[Rôle serveur de Fichier Option DFS 55](#_Toc471822854)

[Intégration DC 2008-2008R2 dans Domaine 2000-2003 62](#_Toc471822855)

[Adprep pour le schéma 62](#_Toc471822856)

[Vérification Adprep du schéma ADSIedit 63](#_Toc471822857)

[Adprep pour le domaine 65](#_Toc471822858)

[Vérification Adprep du domaine ADSIedit 65](#_Toc471822859)

[Niveaux Fonctionnels de Forêt 66](#_Toc471822860)

[Niveaux Fonctionnels de Domaine 68](#_Toc471822861)

[Utilitaire ADSIedit 69](#_Toc471822862)

# Intégration 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**



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

**Dcdiag /test :dns /e /v**

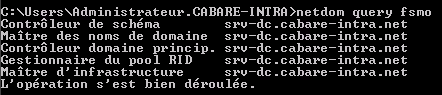


On peut aussi tester de manière plus approfondie la réplication sur chaque DC avec la commande et

**Repadmin /showrepl Repadmin /replsummary**

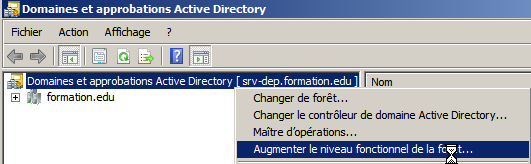
On note ou se trouvent les rôles FSMO par la commande

**Netdom query fsmo**

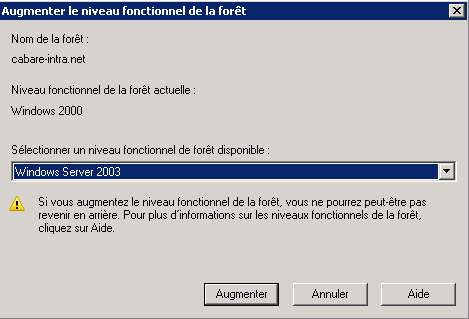


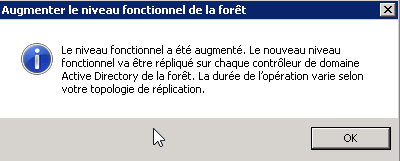
La Vérification du niveau fonctionnel en cours (2003 minimum) se fait dans **Domaines et approbations Active Directory**

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

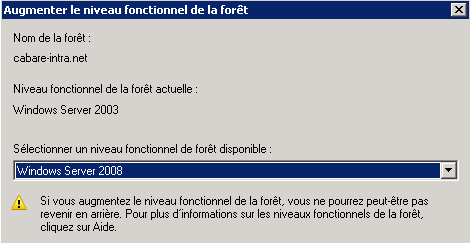


Le niveau actuel est précisé... ici dans l’exemple 2000, il faut être en 2003 minimum pour



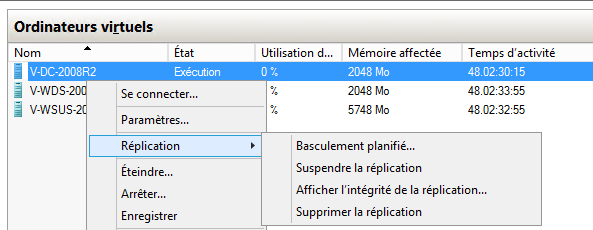
Si on doit augmenter le niveau fonctionnel, il faut attendre la réplication dans toute la forêt !

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.

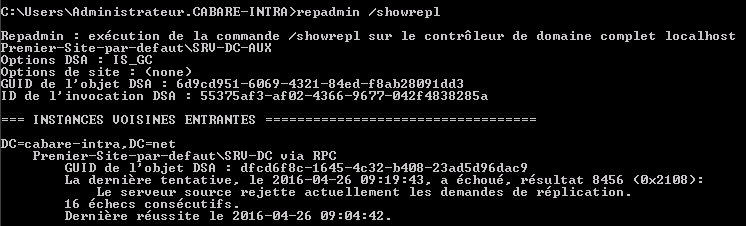
Pour cela:

**repadmin /options** *nom-serveur* **+disable\_outbound\_repl**



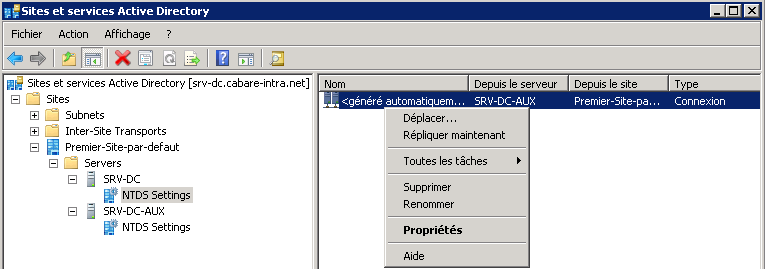
On peut vérifier avec la commande suivante (à exécuter sur le serveur qui essaye de se répliquer depuis le serveur que l’on a dévalidé):

**repadmin /showrepl**

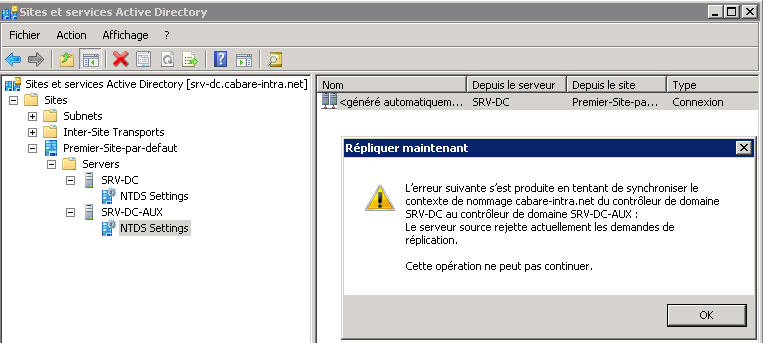


ou plus facilement depuis la console **Site et service Active Directory**

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

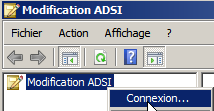


Mais plutôt si SRV-DC-AUX ne peut plus se répliquer depuis SRV-DC !



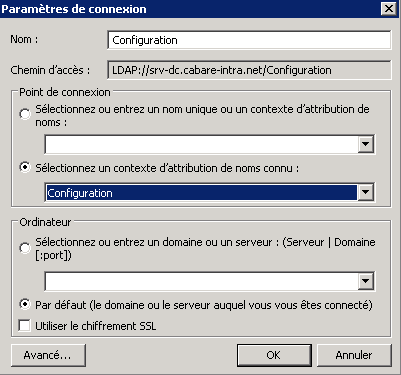
Dans le cas d’un environnement plus conséquent procéder de même pour tous les CD supplémentaires

## Vérification version schéma forêt et domaine

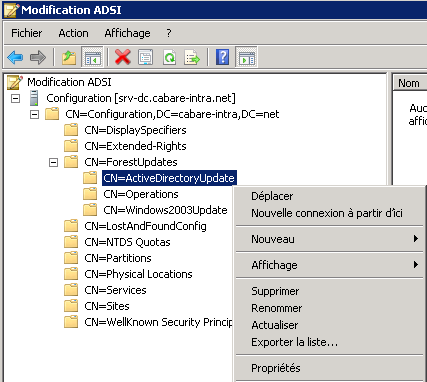
On sait que notre mode fonctionnel est 2003, on a bloqué notre CD avec le maitre de schéma, on va vérifier la version actuelle du schéma… via l’utilitaire **adsiedit.msc**

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

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



on obtient

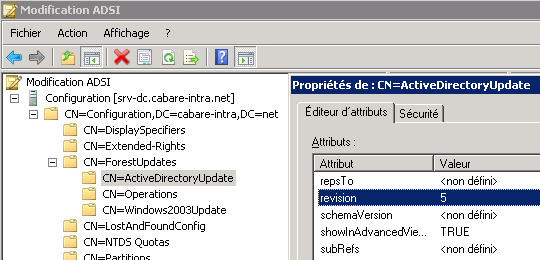


Développer **Configuration**, puis

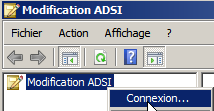
**CN=Configuration**, DC=domaine\_racine\_forêt

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

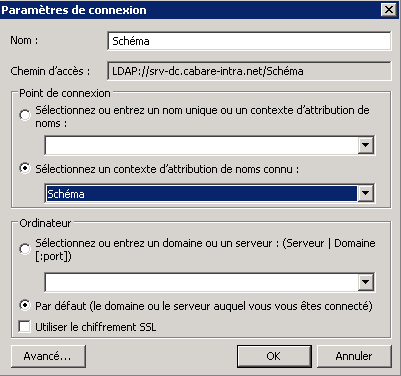
Vérifier que l’attribut **Revision** à pour valeur **4** pour 2008, ou **5** pour Windows Server 2008 R2,.

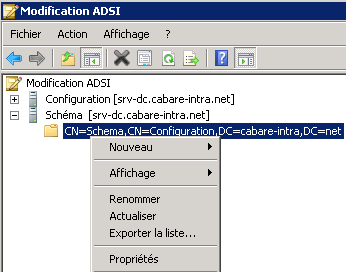


Il faut maintenant tester la version de schéma ... donc **Connexion**.



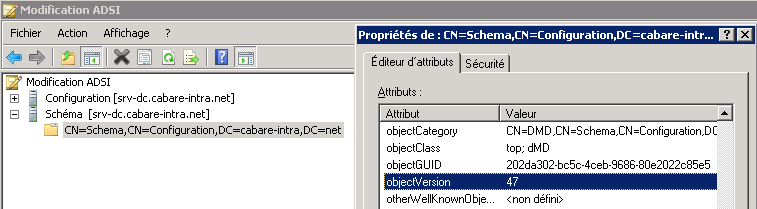
dans **Sélectionnez un contexte d’attribution de noms connu**, puis **Schéma**



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



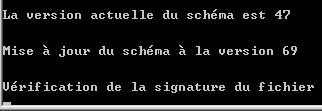
Les principales versions de schéma existantes sont

30 Windows 2003 31 Windows 2003 R2

44 Windows Server 2008 47 Windows server 2008r2

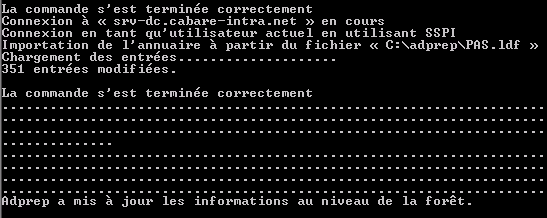
56 Windows Server 2012 69 Windows Server 2012r2

## Adprep pour la forêt

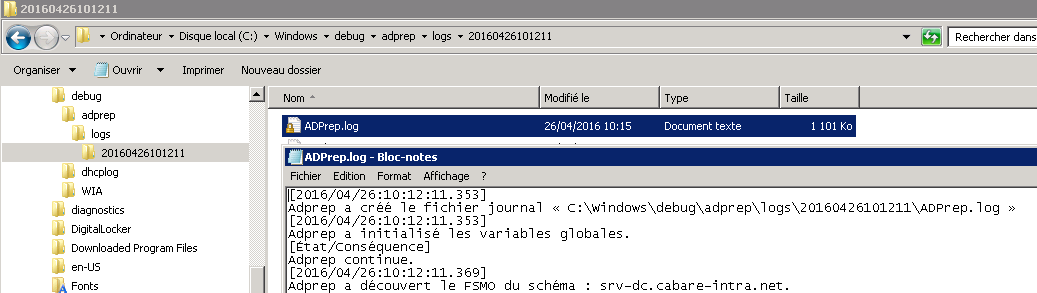
* Depuis le DVD de Windows Server 2012R2 copier le contenu du dossier **\support\adprep** dans un dossier Adprep sur le Serveur ayant le rôle de **contrôleur de schéma**.
* Taper: **Adprep.exe /forestprep**



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



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

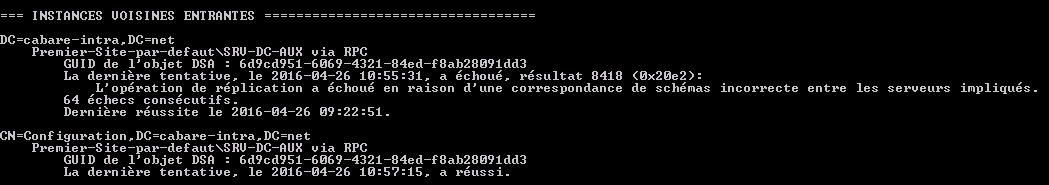
pour débloquer la réplication sortante on passe la commande avec – ( **à la place de +**) :

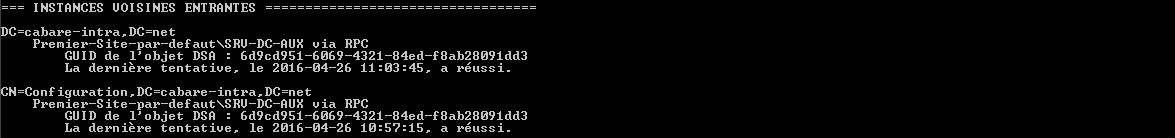
Pour cela:

**repadmin /options** *nom-serveur* **-disable\_outbound\_repl**

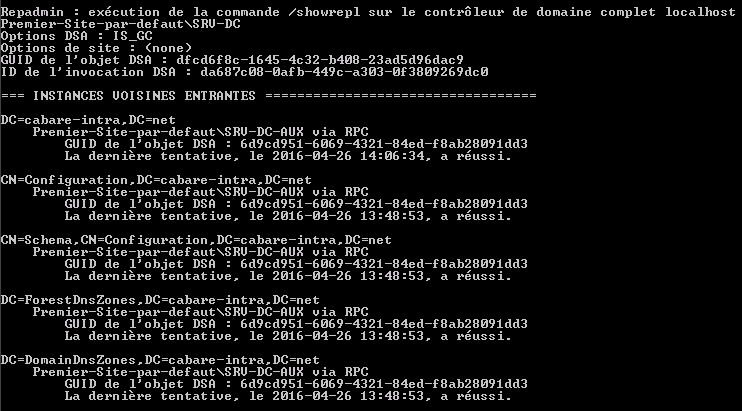


Il est important de na pas s’inquiéter sur les premiers messages envoyés par **repadamin / showrepl**, car il faut du temps pour que le schéma se propage…





Pour obtenir les 5 rôles



**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:

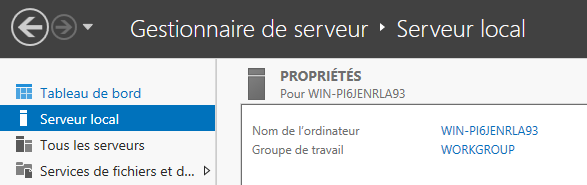
**adprep /rodcprep**

**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*

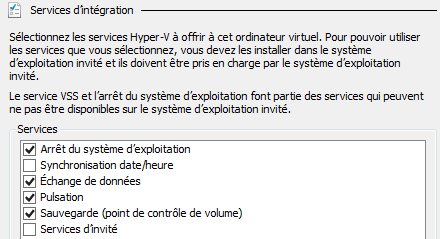


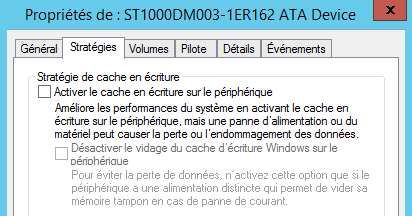
* Avec un adressage Ip correct (adresse, masque, dns)
* Joint au domaine dans les règles, (compte machine dans l’AD, hôte et pointeur correspondant dans le DNS) 

* Test avec nslookup

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



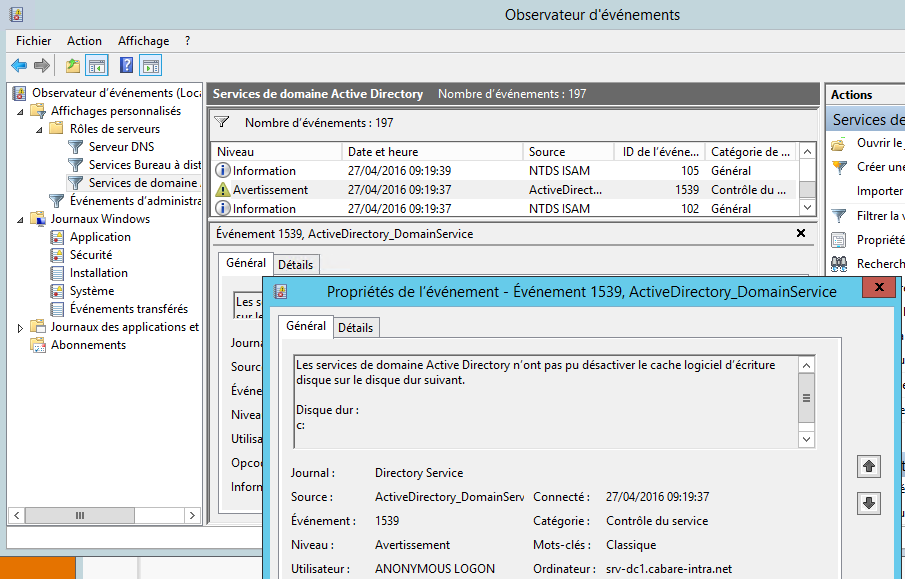
**N.B** : penser à désactiver pour une VM posée sur un disque IDE le cache en écriture disque

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

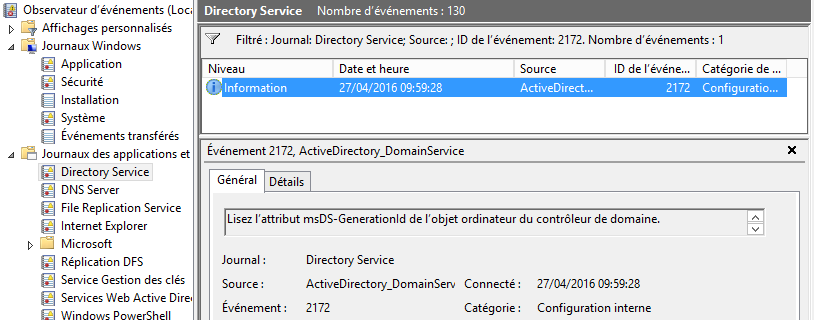
* Dévalider le cache dans le Bios
* Poser la Vm sur un disque SCSI !

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](http://support.microsoft.com/kb/2855336/fr)  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 !

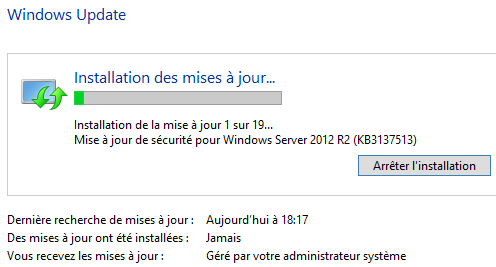


**N.B** : penser à ne pas faire de **snapshot** sur un **DC** sauf s’il intègre une gestion de l’évènement 2170. A partir de **Windows 2012** et si l'hyperviseur supporte le "**GenerationID**" il est possible d'utiliser des fonctionnalités supplémentaires tel que les "snapshot" ou le clonage de contrôleur 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



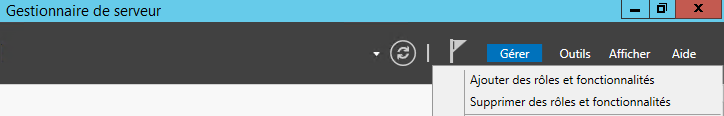
et ensuite ajouter 2 rôles qui permettront de prendre en charge le domaine

* Le rôle AD DS Directory Service
* Le rôle DNS

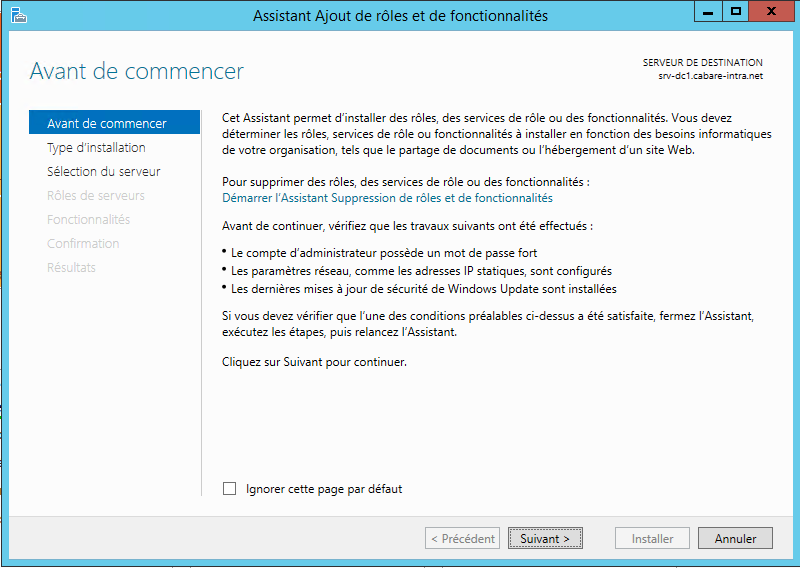
Soit dans le **Gestionnaire de serveur**, **Tableau de bord** puis dans **Configurer ce serveur local** on demande **Ajouter des rôles**



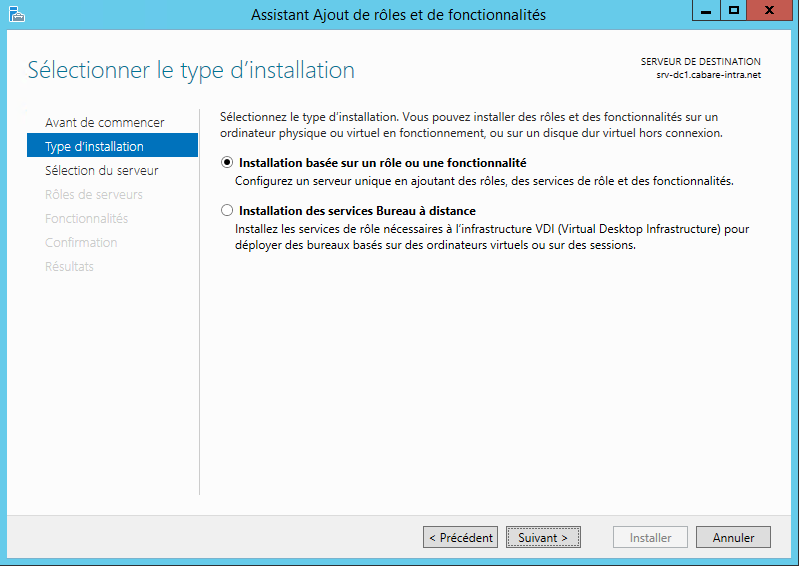
Sinon à tout moment, dans le **Gestionnaire de serveur**, en haut à droite on demande **Ajouter des rôles et des fonctionnalités**



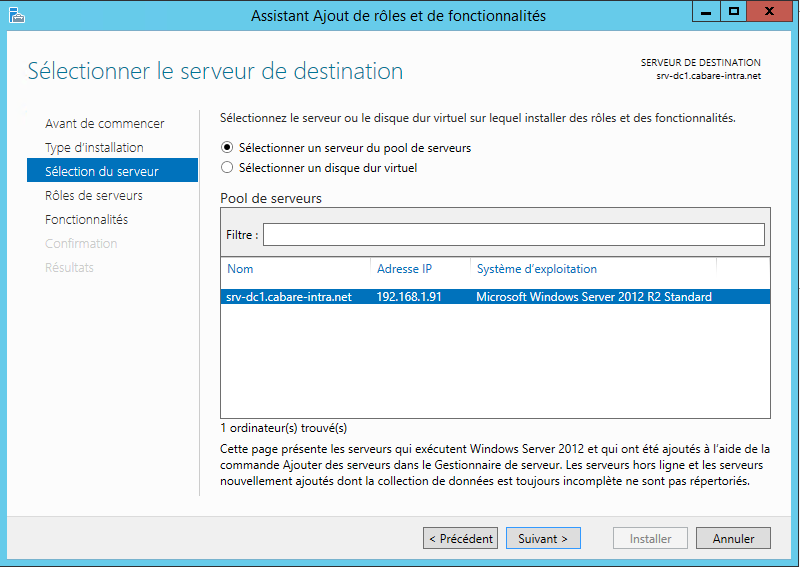
On déclanche l’assistant



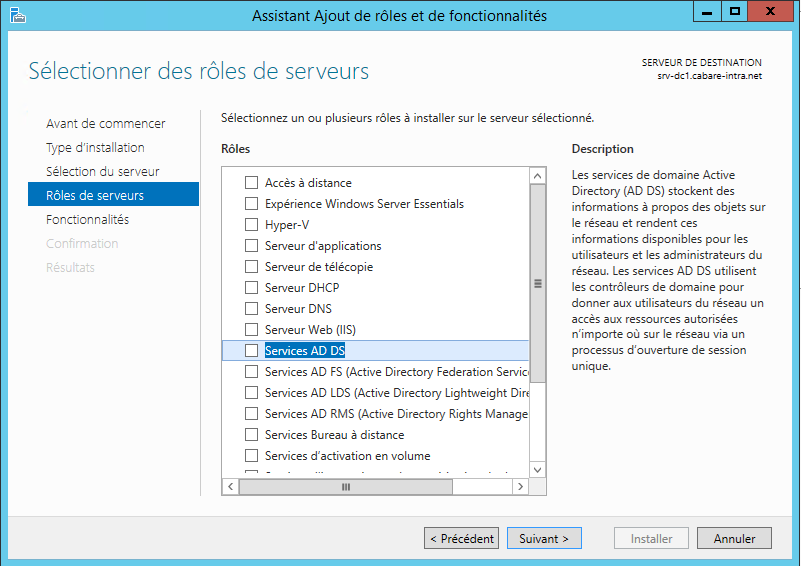
On demande d’ajouter un rôle

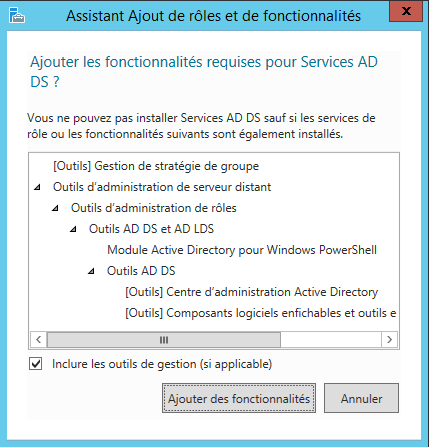


Sur notre serveur

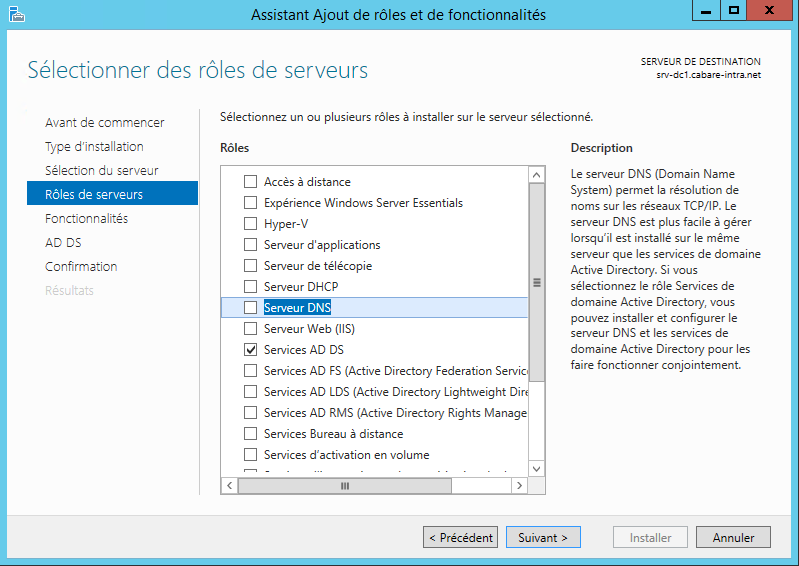


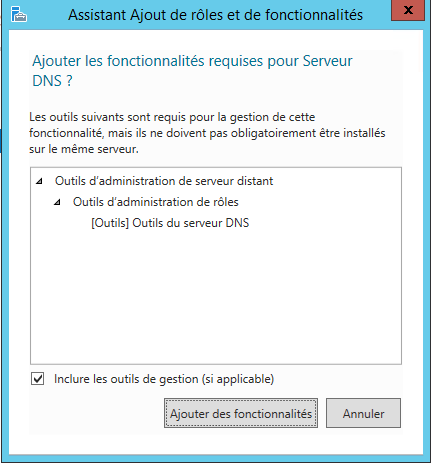
Les services **AD DS** (et les fonctionnalités associées)



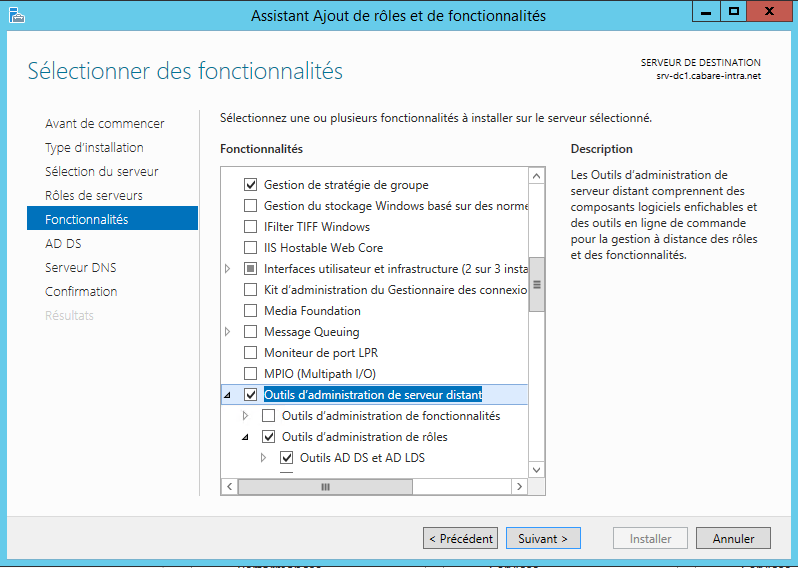


Puis le rôle **DNS** (et les fonctionnalités associées)

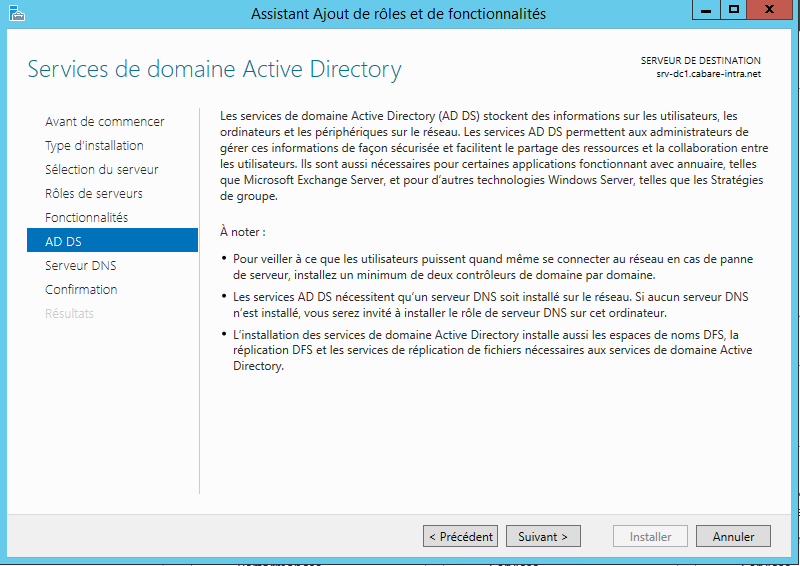




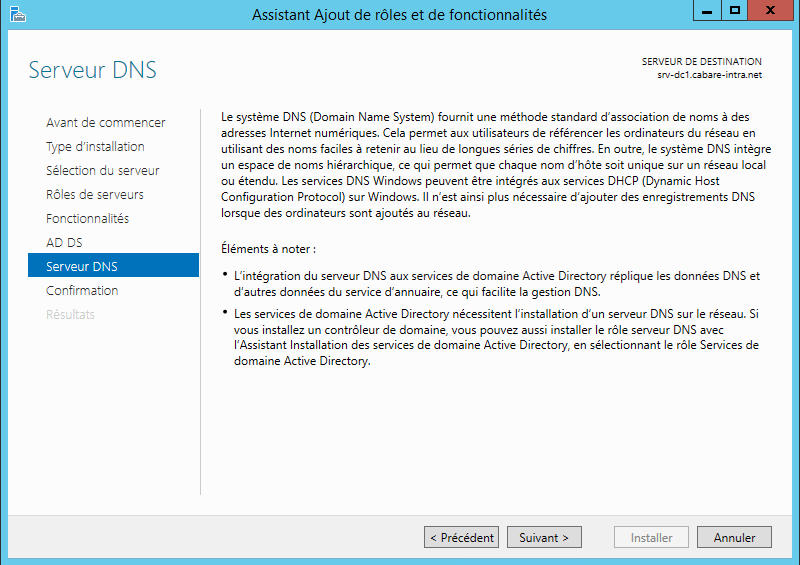
Du coup dans l’étape suivante des fonctionnalités on n’a rien à faire, ce qui doit être coché l’est déjà (cela s’est fait précédemment)

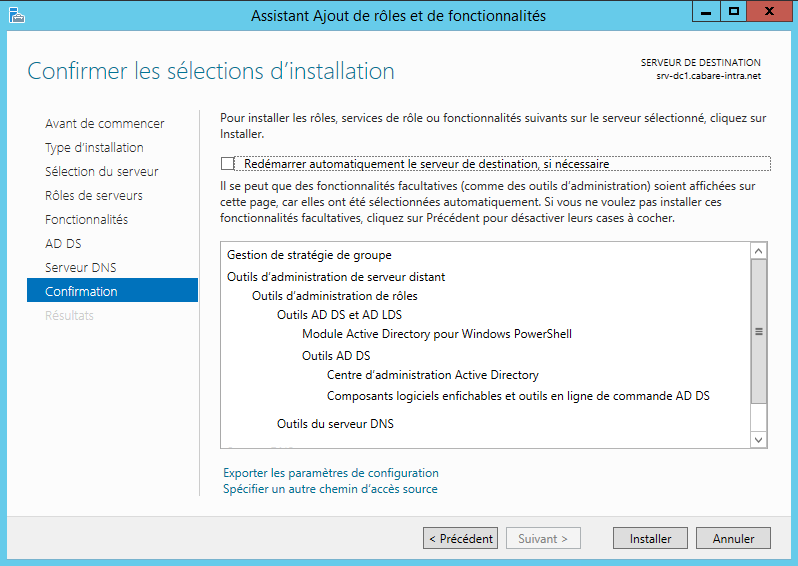


Ensuite on nous invite à penser à installer un 2° CD et un DNS au minimum…

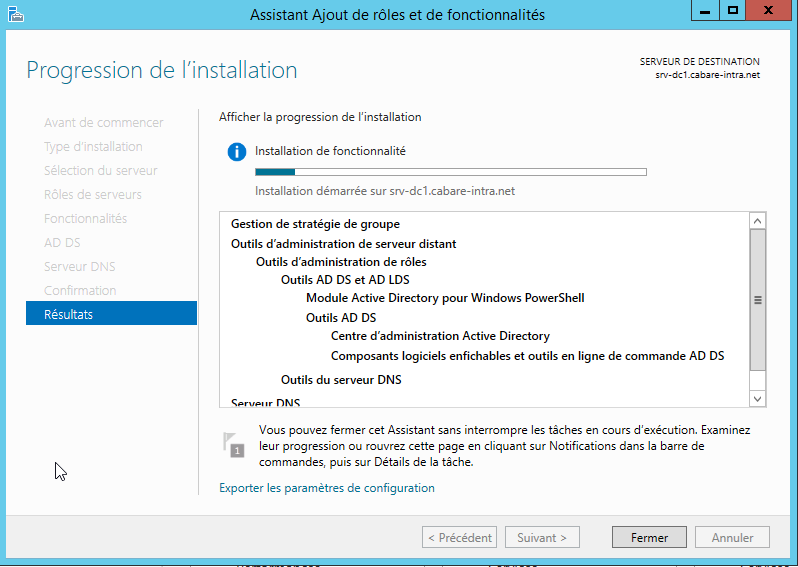


On nous conseille de stocker la zone DNS dans Active directement…

On confirme

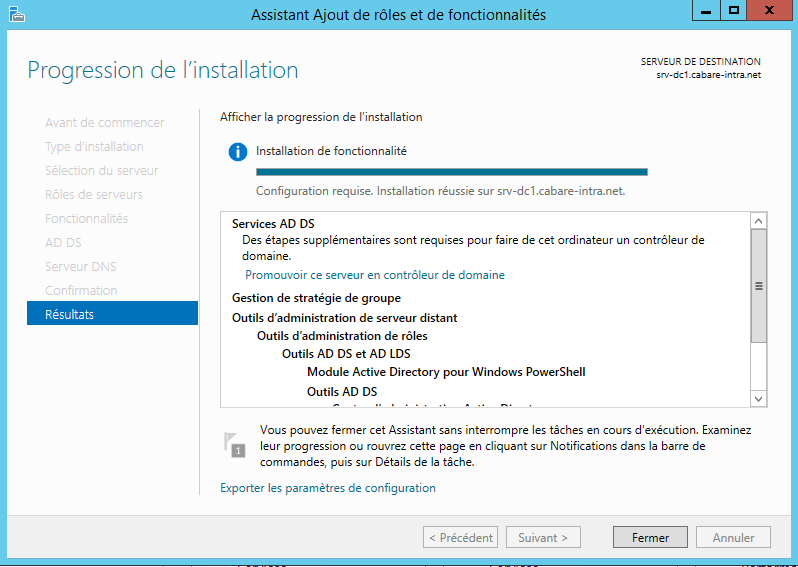
 on **Installe**

Et c’est terminé



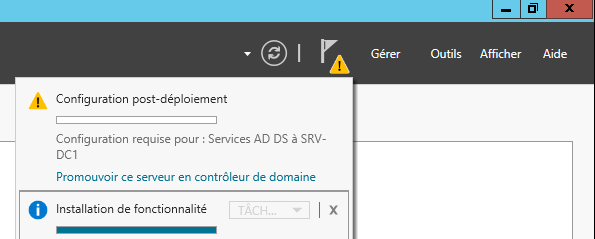
Lorsque l’on obtient la réussite de l’installation il sera possible de

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

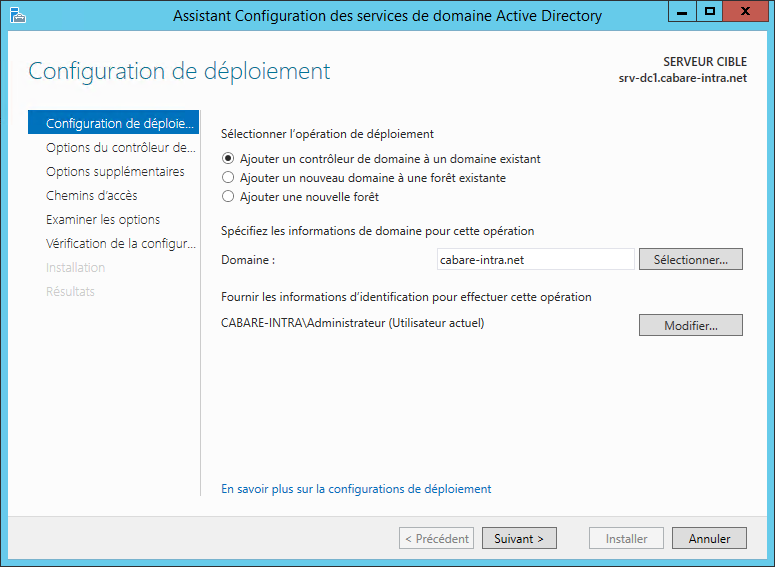


## Assistant de configuration Active Directory (ex dcpromo)

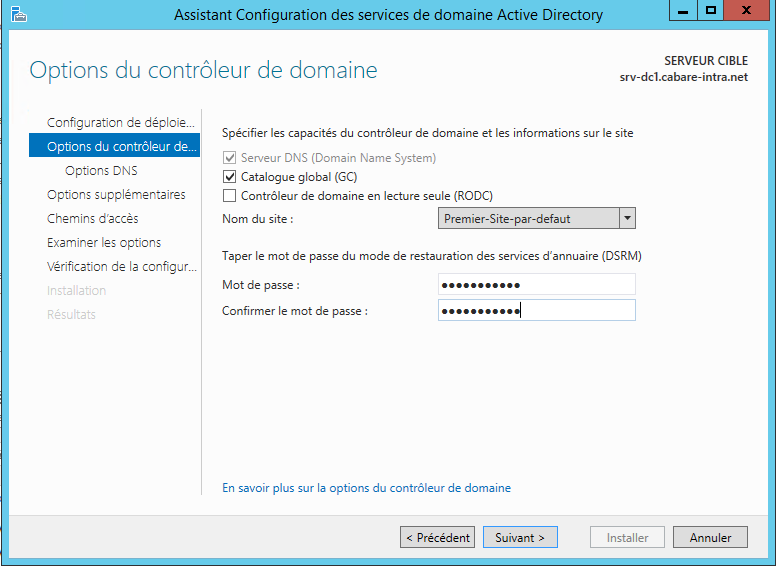
Peut importe de cliquer ou non sur le lien précédent **Promouvoir ce serveur en contôleur de domaine** car le **gestionnaire de serveur** nous le reproposera



Donc on veut ajouter un DC



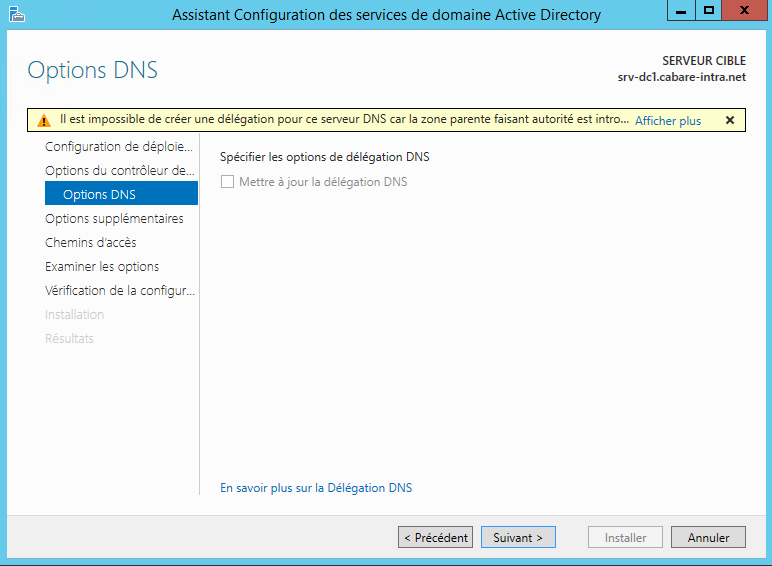
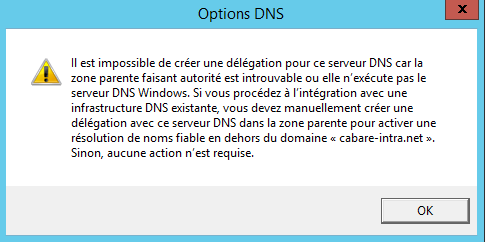
Qui sera aussi serveur DNS et Catalogue Global



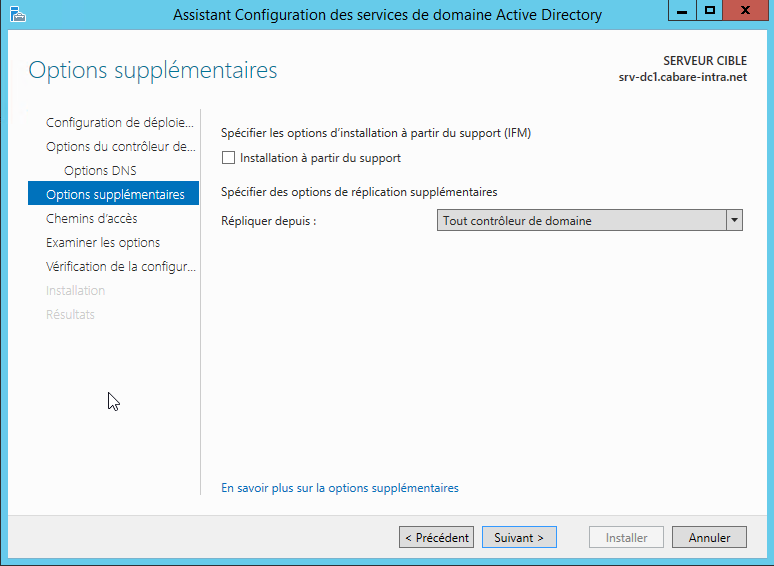
Mot de passe de restauration

*Restore2012*

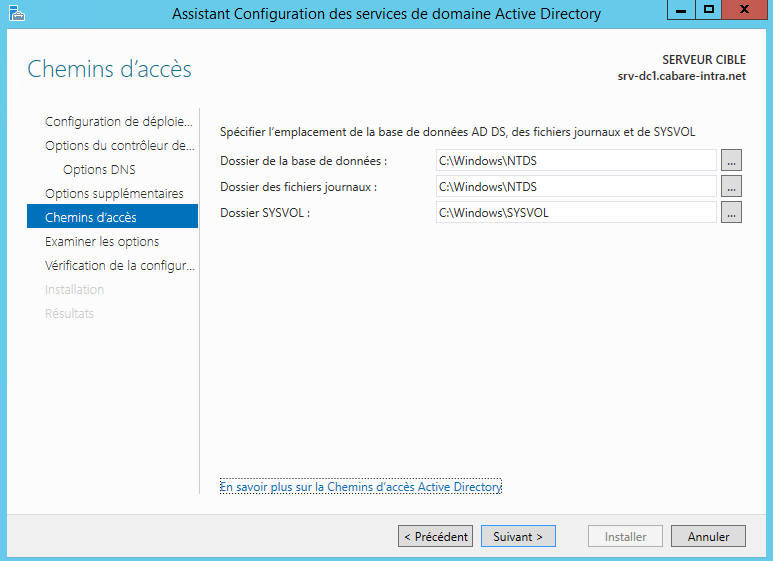
Ce message est normal car on est à la racine de la forêt



… on demande suivant



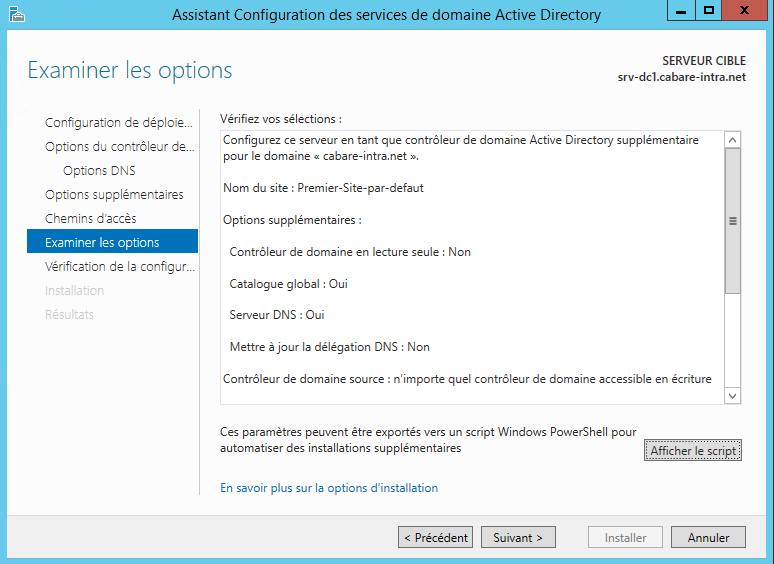
Il est préférable de laisser choisir le serveur avec lequel il trouve la meilleure bande passante… **Suivant**



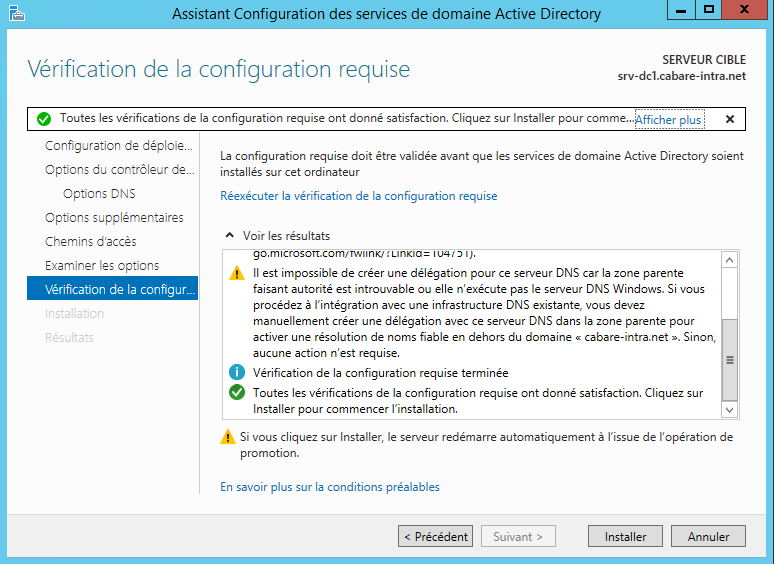
On lui laisse installer la Base AD et le réplica où il le souhaite par défaut…



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…

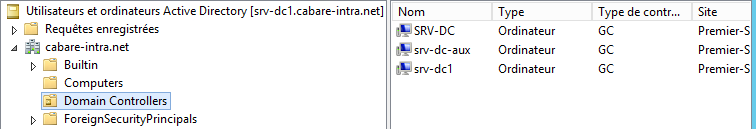
## Test serveur et réplication générale

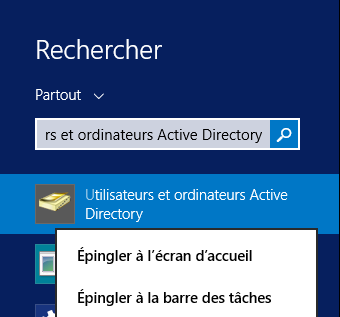
Dans le **Gestionnaire de serveur**, dans **Outils**

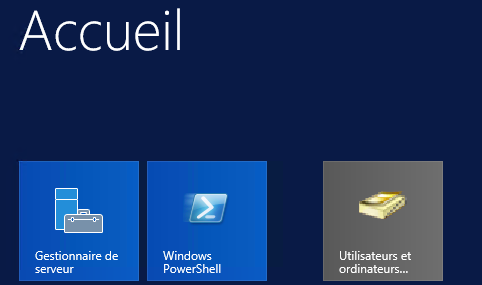


On demande, **Utilisateurs et ordinateurs Active Directory**

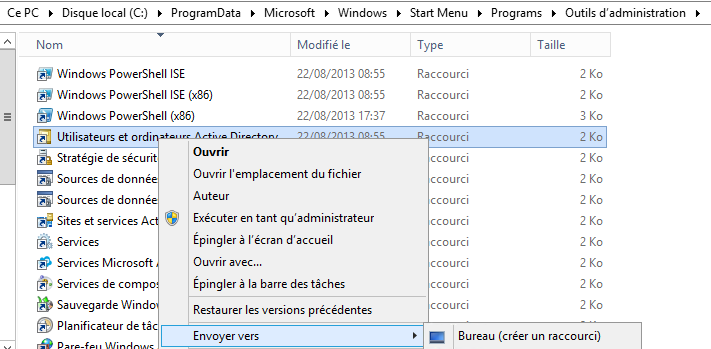
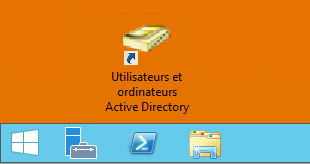
* Le compte de notre serveur **DC** doit faire partie de l’**UO Domain Controllers**



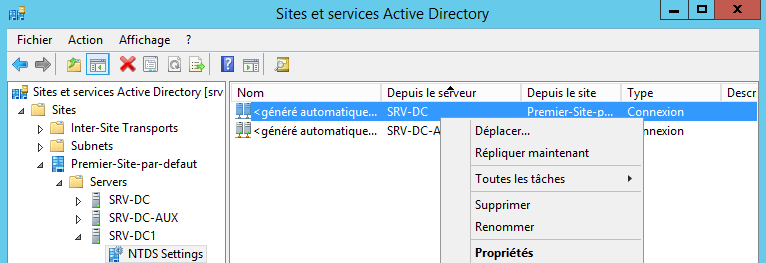
On peut aussi une fois pour toutes effectuer une recherche et **épingler** la mmc à **l’écran d’accueil,** Pour obtenir



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…



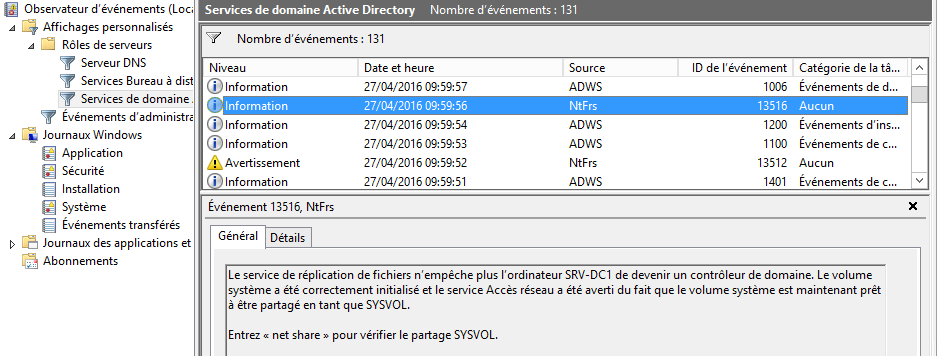
* La réplication doit être active entre le nouveau **srv-dc1** et les autres DC



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

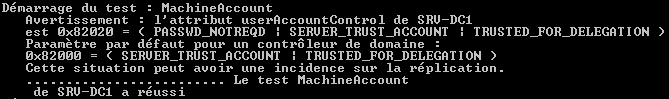


* Dans l’observateur d’évènement, on vérifie que la réplication soit bien terminée est que désormais notre serveur est bien contrôleur de domaine.



* 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



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)

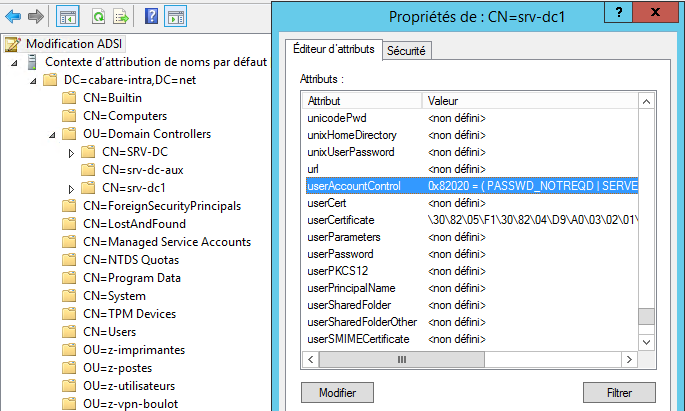
Domain controller: 0x82000 (532480)

Workstation/server: 0x1000 (4096)

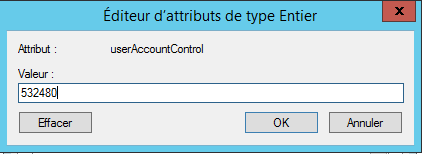
Ici on se retrouve avec la valeur 0x82020 (532512).

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

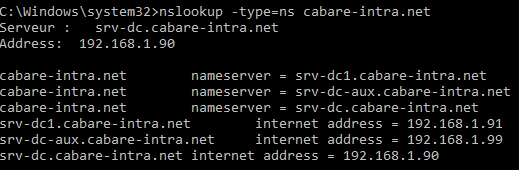
* qu'il dépends de lui-même, (1° serveur DNS)
* et du serveur dont il est le réplica (2° serveur DNS)

**Liste de tous les serveurs DNS disponibles sur le domaine :**

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

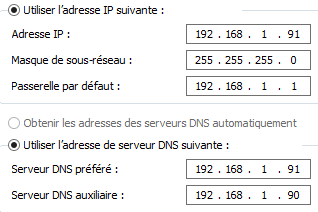
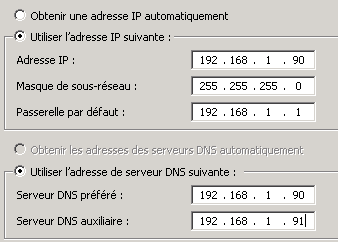
**Nslookup –type=ns domaine**

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

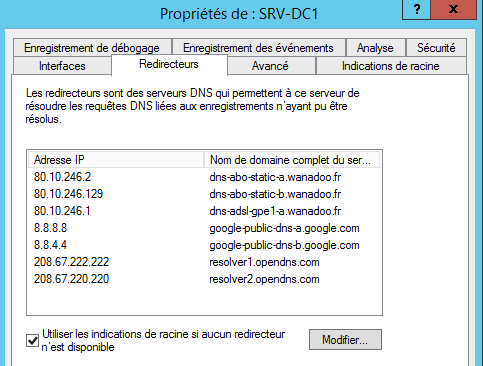


Donc si on garde uniquement *srv-dc1* et *srv-dc* cela donnerait

Sur srv-dc1 sur srv-dc

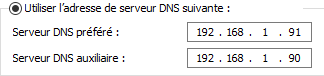
 

**Reglages redirecteurs :**

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

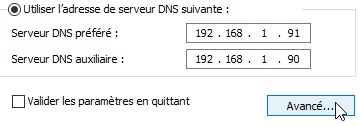
En effet ces réglages sont indiqués "hors zone" et donc non répliqués via AD, ils doivent donc être reconstruits sur chaque serveur DNS… !

**Paramétrage des clients Ip en dur:**

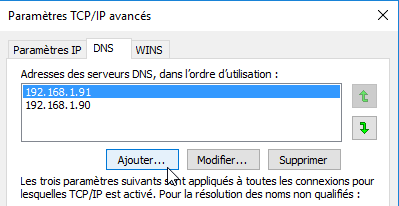
Il est juste nécessaire de spécifier pour les clients que le serveur DNS auxilliaire se trouve à telle adresse IP  (l’adresse de notre 2° CD avec son Serveur DNS…

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…**

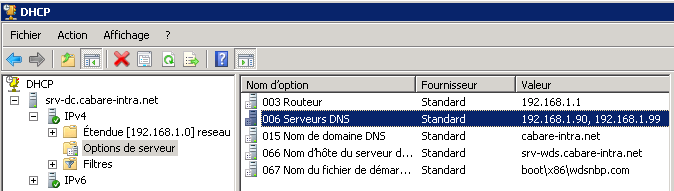


Puis onglet **DNS** et **Ajouter**

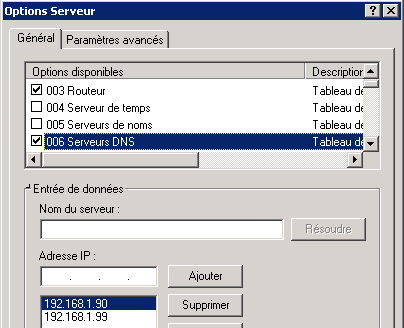
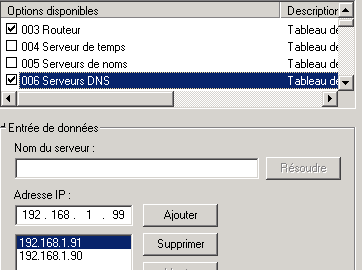


**Options de serveur DHCP :**

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



Pour passer de à



## Migration rôles FSMO

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 ?

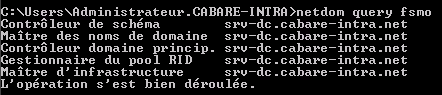
Sur le Domaine

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

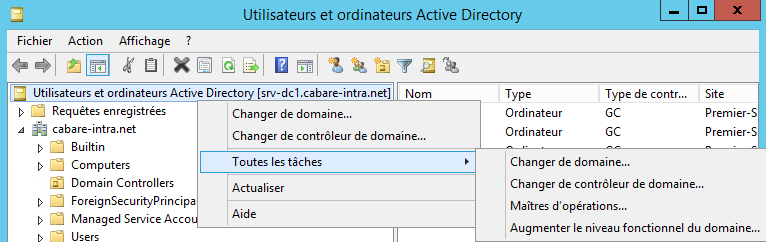
Sur la fôret (et l’ensemble des domaines))

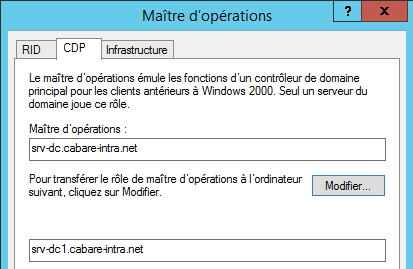
* **Maître d’attribution de nom de domaine** : GG Administrateurs de l’entreprise
* **Contrôleur de schéma** : GG Administrateurs du schéma

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



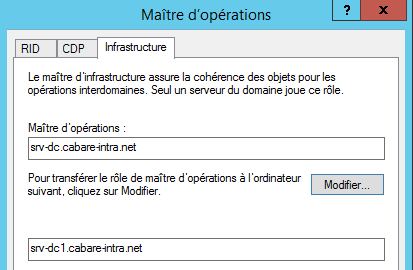
Avec la console **Utilisateur et ordinateur Active Directory** on peut trouver les 3 maîtres de domaine : clic droit **Toutes les tâches** / **Maîtres d’opérations…**

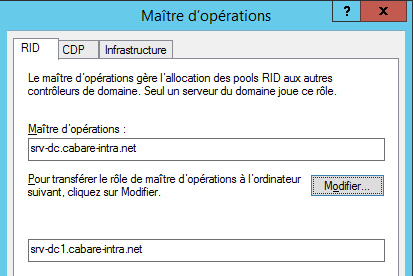




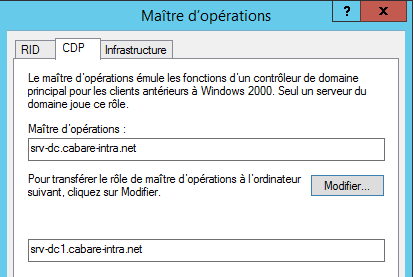
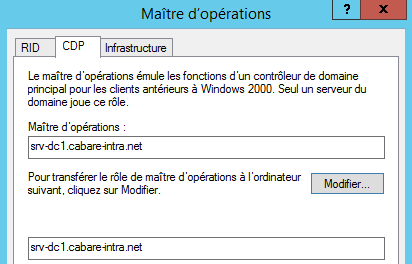
**N.B** : Il faut se placer sur le serveur sur lequel l’on veut tirer les rôles

* Emulateur CPD (NT 4.0)
* Maître identificateur Relatif RID
* Maître d’infrastructure

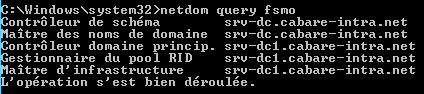




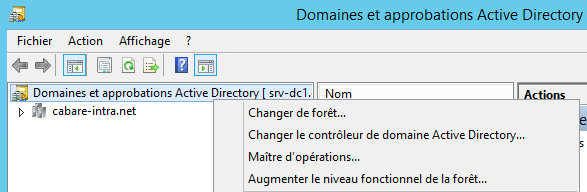
Le transfert se faisant simplement en demandant **Modifier…**, par exemple

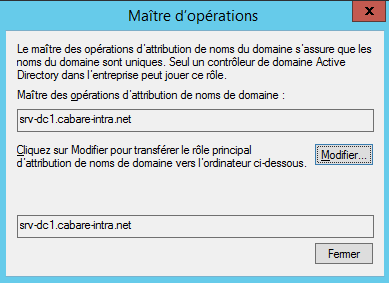


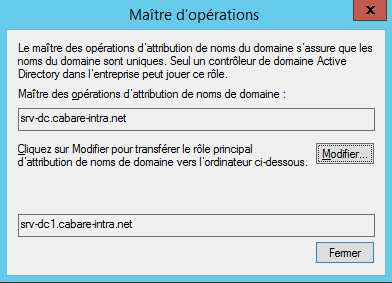
On peut vérifier par



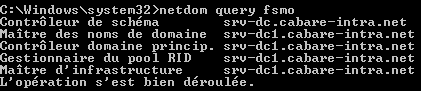
Avec la console **Domaine et approbation Active Directory** on peut trouver qui est maître d’attribution de nom de Domaine. En se plaçant sur **Domaines et approbations Active Directory** on demande clic droit **Maîtres d’opérations…**



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



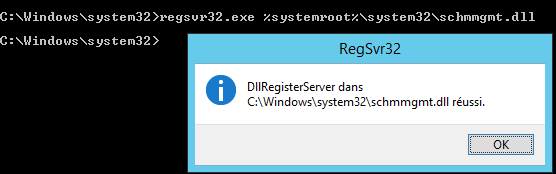
On peut vérifier par



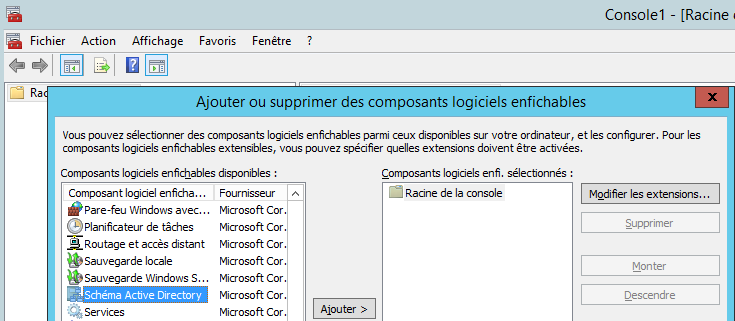
Reste le schéma…

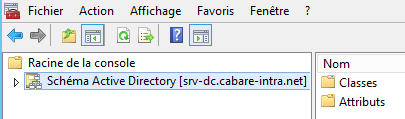
Pour localiser le maître de schéma, c’est le plus difficile. Il d’abords créer l’exécutable qui pourra ouvrir la console mmc

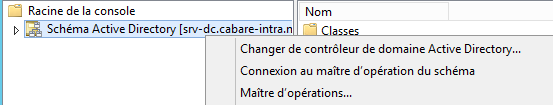
Via la commande **regsvr32.exe %systemroot%\system32\schmmgmt.dll**

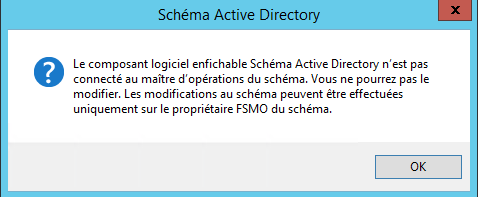


Puis on peut alors créer une console, via executer **mmc** dans laquelle on demande **Fichier / Ajouter ou supprimer des composants logiciels enfichables** et on choisit la console **Schéma active Directory**





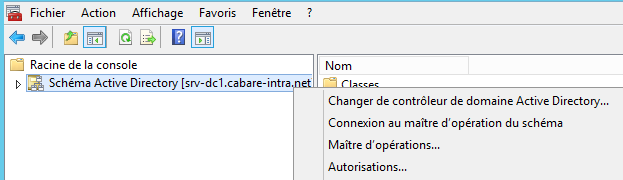
**N.B** : Si on est sur le serveur maître d’opération, il faut alors d’abords se connecter sur le serveur sur lequel on veut effectuer le transfert. **Via Changer de contrôleur de domaine Active Directory**. On peut aussi ouvrir la console directement sur le serveur sur lequel on veut transférer le rôle. 

**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…

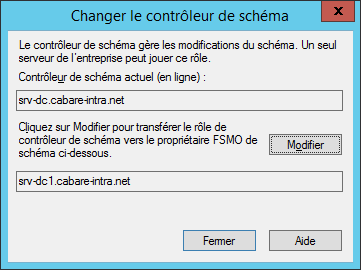
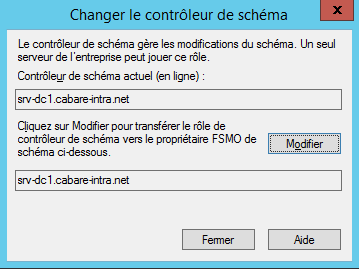
C’est normal, le rôle n’y est pas encore …

Donc on se place sur le serveur de destination puis

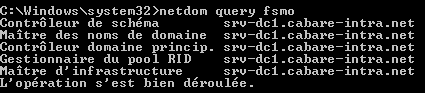


sur **Schéma Active Directory** on demande clic droit **Propriétés /** **Maîtres d’opérations…**

Et on tranfère le dernier rôle



Et c’est terminé

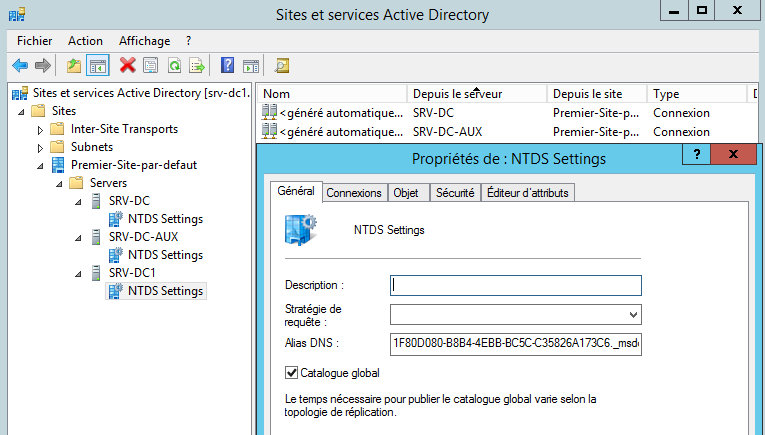


## Suppression Catalogue Global ancien serveur

**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**

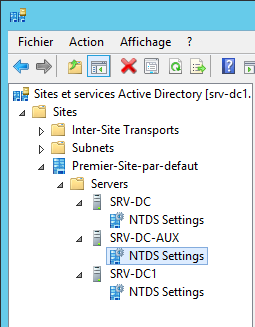
dans laquelle on demande les propriétés de **NTDS Settings** de notre serveur

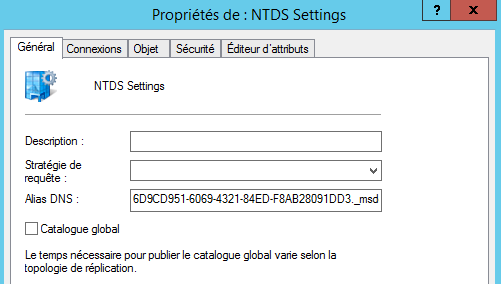
On sait ici que notre serveur est **Catalogue Global**

**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**,

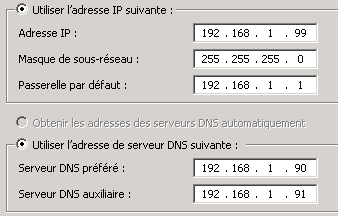
on demande **propriétés de NTDS Settings** et on décoche la case **Catalogue Global**



## Suppression DNS ancien serveur

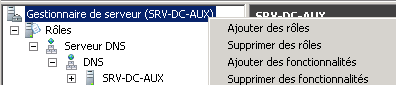
Il faut être sur d’avoir avant bien corrigé les adresses IP des serveurs DNS

* 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

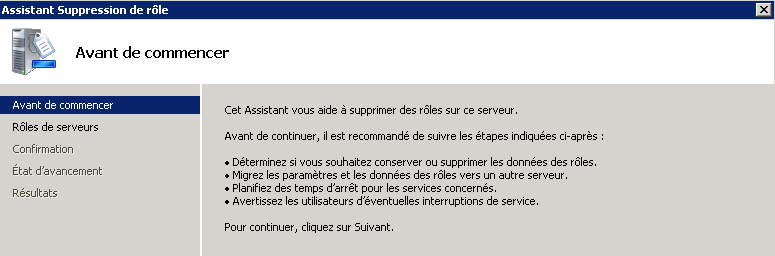


sur le serveur DNS 2008R2 à démonter, on indique les nouveaux serveur DNS du domaine (il n’est plus son propre serveur DNS ici notre serveur DNS en .99 utilise comme serveur DNS les .90 et .91)

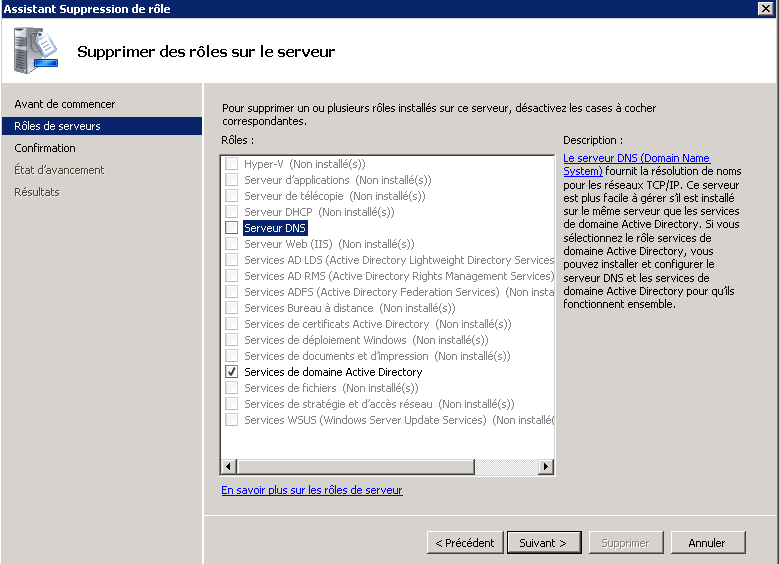
puis on va demander de supprimer un rôle

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

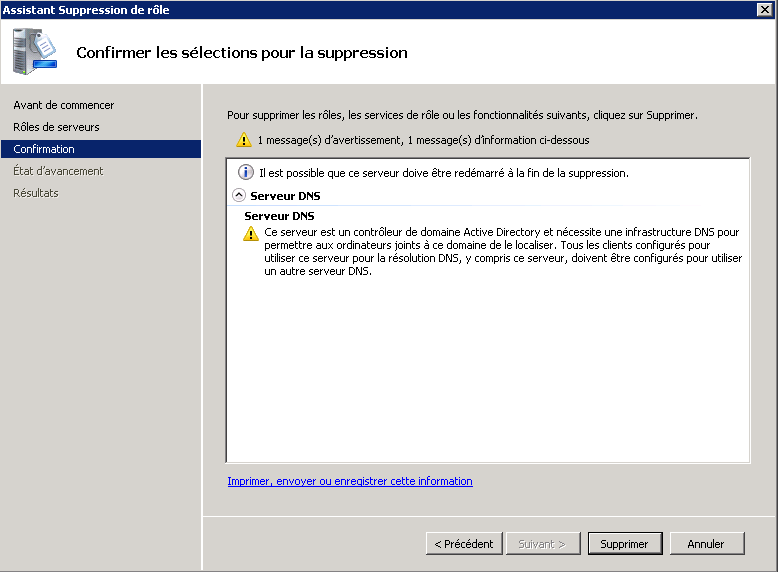
un assistant se déclanche

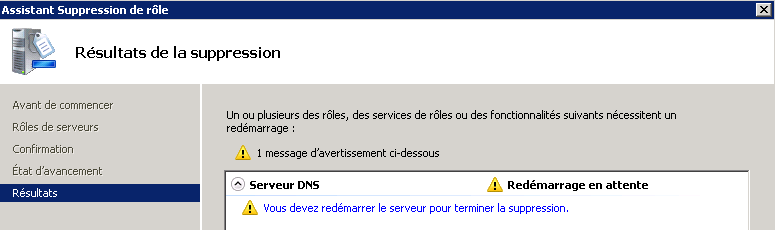


On décoche uniquement **Serveur DNS**

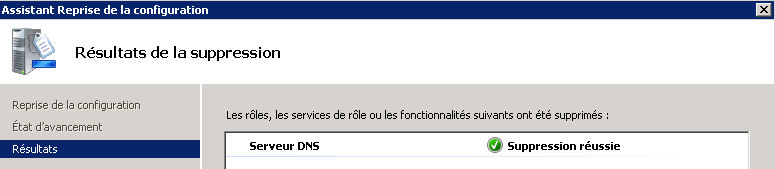


On a une mise en garde comme quoi il serait bon qu’il y ait d’autres DNS dans le domaine…





Et après un re démarrage



## Démontage ancien DC

Sur un serveur Windows 2008 et 2008 R2 il faudra

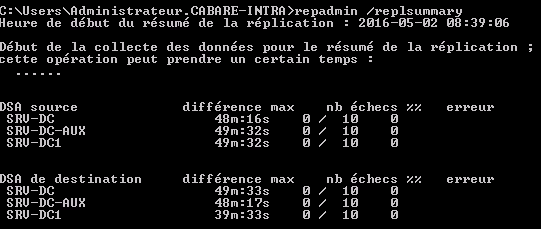
* Effectuer dcpromo
* après la rétrogradation du serveur supprimer le rôle AD DS ajout « ajout / suppression de rôle ».

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

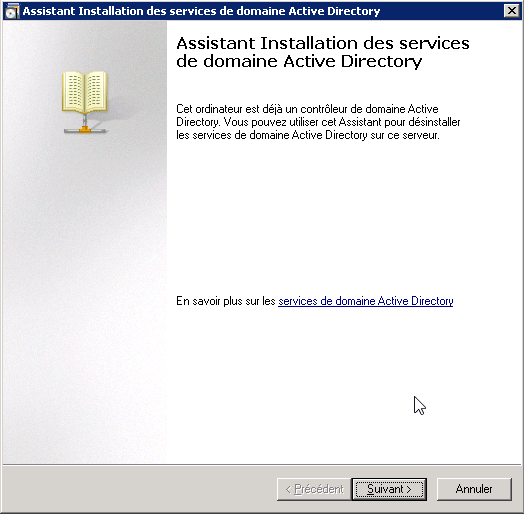
* il faut directement supprimer le rôle AD DS l’assistant de configuration se lancera automatiquement et permettra de rétrograder le DC.

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…

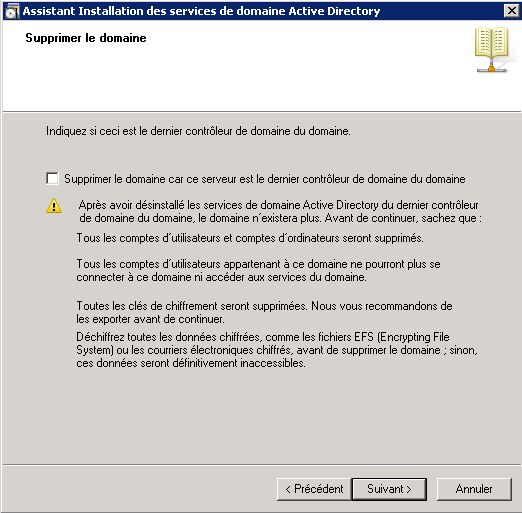
On pourrait même avant vérifier la bonne marche de la réplication par un **repadmin / replsummary**



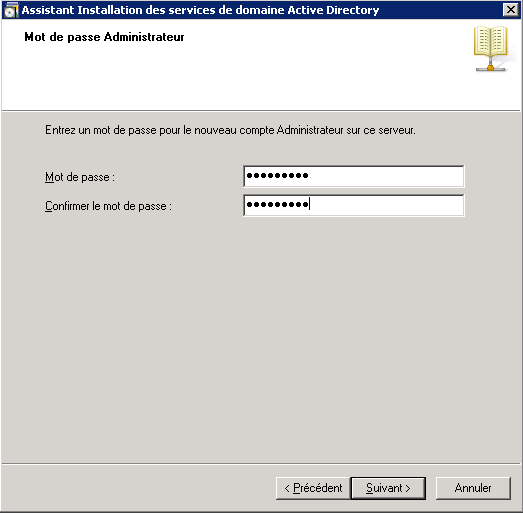
Faisons un **dcpromo** sur notre ancien serveur 2008R2 ***srv-dc-aux***



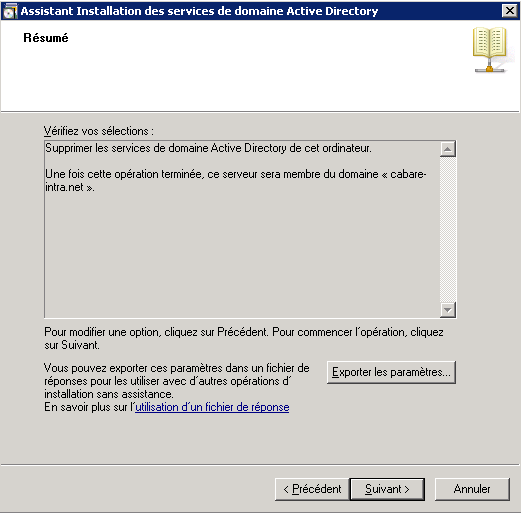
Surtout ne pas cocher…



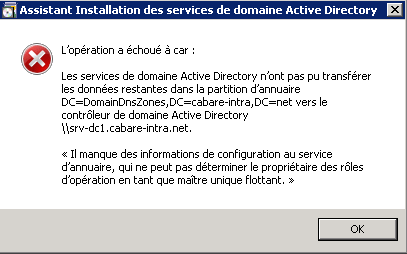
On saisie le nouveau mot de passe du futur serveur (pour pouvoir ouvrir une session locale



Et c’est fini…



## Erreur possible dcpromo /forceremoval:

On n’arrive pas à démonter un Dc…

Ou il est … hors service…

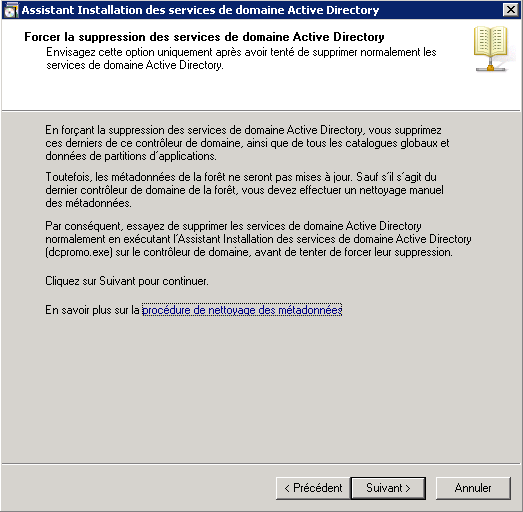
Il faut d’abords vérifier que les rôles soient bien transférés…. (**netdom query fsmo**) Et que la réplication fonctionne bien… (**repadmin /replsummary**)

* 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

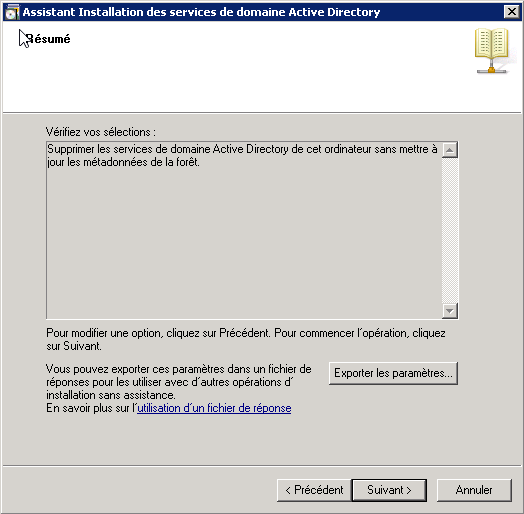
**N.B** : après un démontage forcé, il faut effectuer un netoyage de l’AD !

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

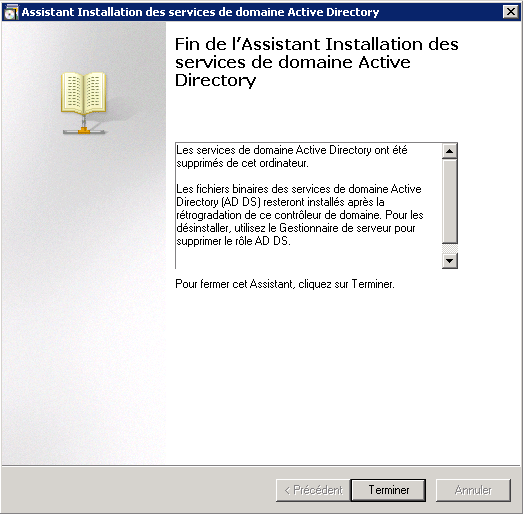




On a une confirmation



Et c’est términé



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

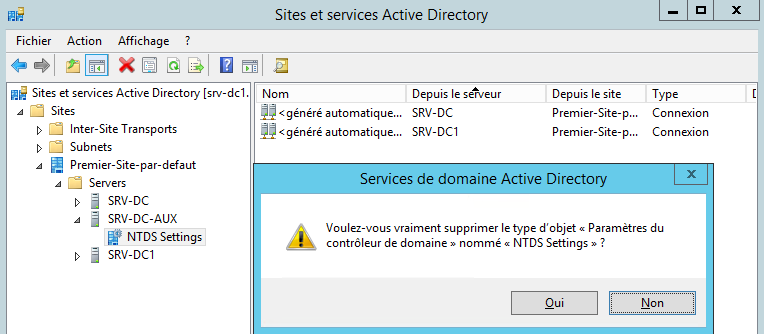
Dans le DNS il faut supprimer

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

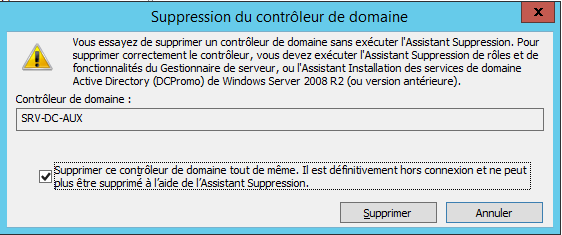
Depuis 2008 on n’est plus obligé de passer par **ntdsutil**, on utilise la console **Site et service Active Directory** on se place sur le serveur à effacer, sur sa zone **NTDS Settings**, que l’on supprime



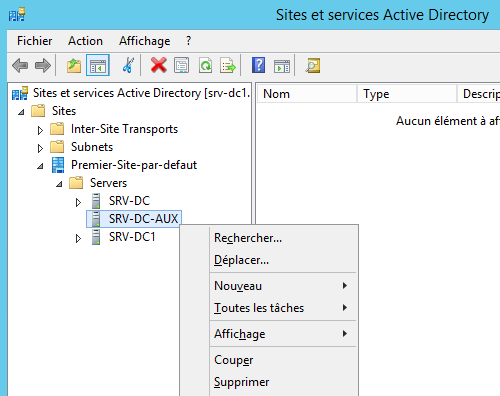
On confirme



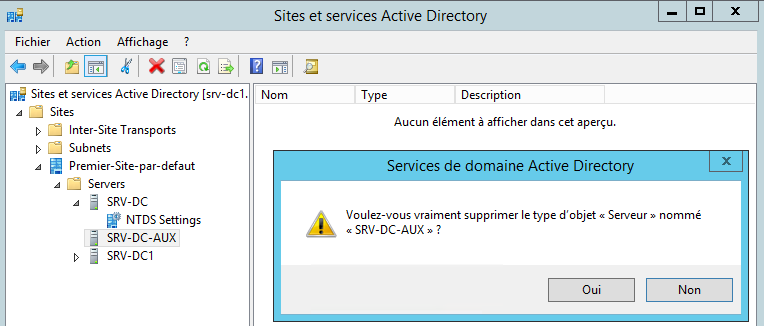
On valide la non accesibilité du serveur à détruire



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

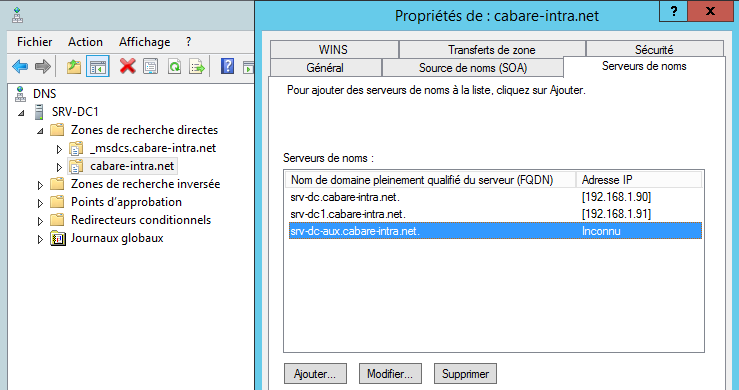


Et l’on confirme



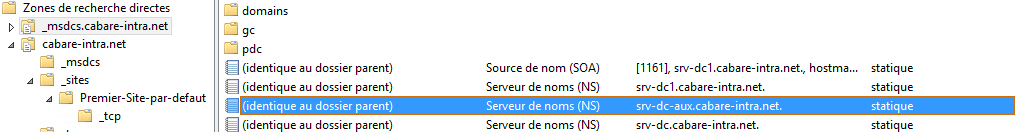
Pour le DNS il va falloir supprimer les indications de serveur de nom concernant notre serveur supprimé.

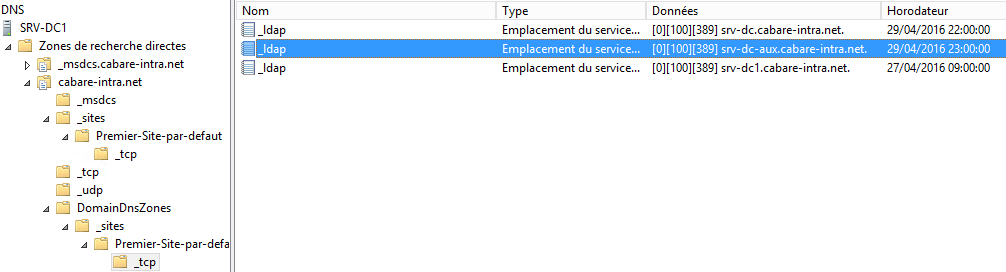
Dans la mmc **DNS**, on se place sur les **zone de recherche directe**, ici *cabare-intra.net* et *\_msdcs*.*cabare-intra.net* dans les **propriétés** on demande **Serveurs de noms**



**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**



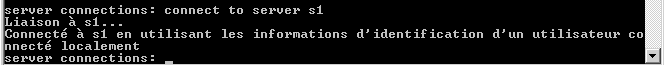
Le niveau qui nous intéresse ici est celui accessible par la commande **roles**



il faut ensuite taper la commande **connections**



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



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



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



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



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**









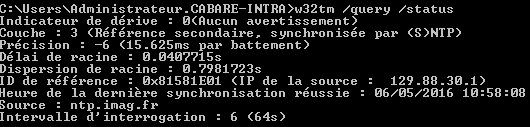




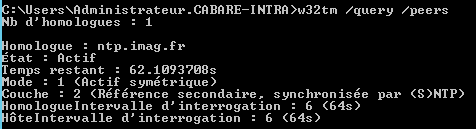
On peut vérifier avec un **/query /source** où il se synchronise



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



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



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**









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



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

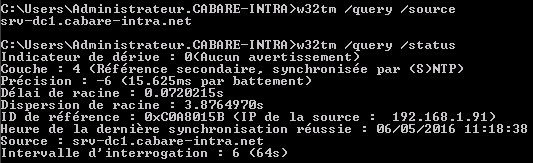
**Net stop w32time**

**w32tm /unregister**

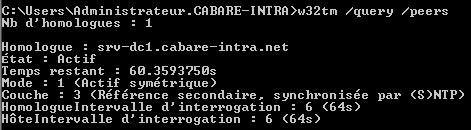
**w32tm /register** vérifiable par



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



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



## 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**:

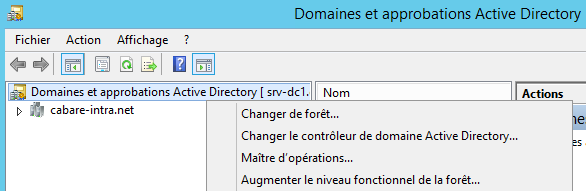
un **niveau fonctionnel 2008R2** qui par rapport à 2003 va offrir les possibilités suivantes:

* 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

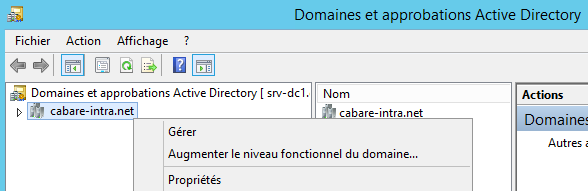
**N.B**: quelques fonctionnalités possibles uniquement sur des niveaux 2012 ne seront pas accessibles, mais elles ne sont pas dans un premier temps indispensable, elles concernent des stratégies d'authentification renforcée…

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

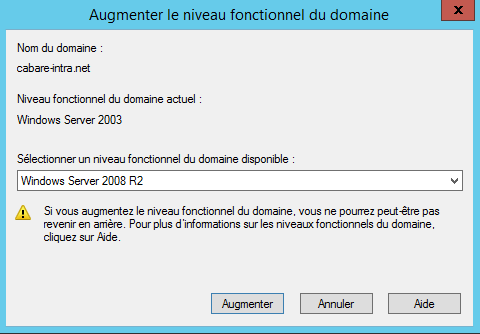
Dans la console **Domaine et approbation Active Directory**, sur **Domaine et approbation**, on a via clic droit le niveau fonctionnel de forêt,



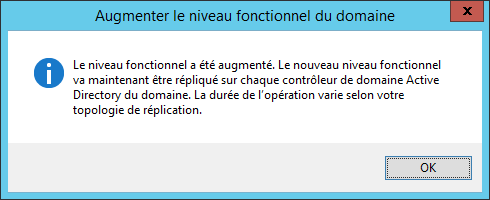
et sur le **domaine** on a via clic droit le niveau fonctionnel de domaine



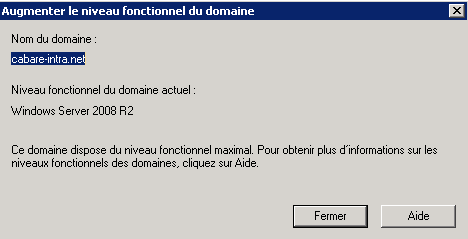
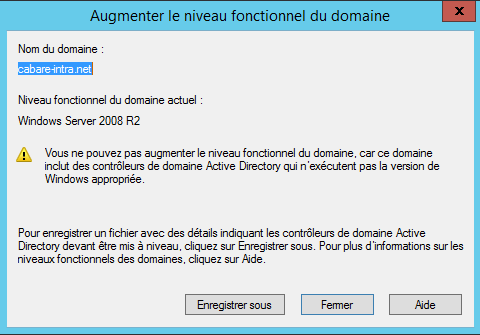
### Passage du niveau de domaine de 2003 à 2008r2

 **Augmenter**

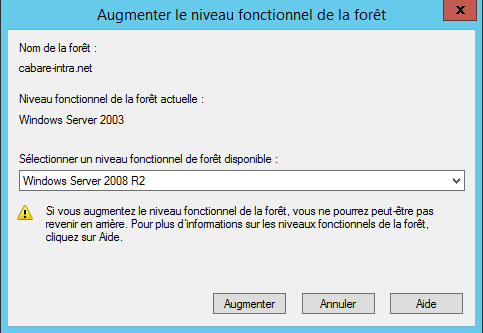
on est prévenu…Il serait bon de vérifier sur tous les CD le niveau…



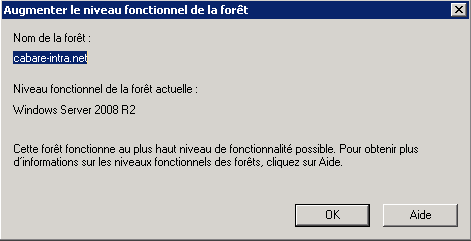
Sur un 2008R2 cela donne Sur un 2012 cela donne



### Passage du niveau de Forêt de 2003 à 2008r2

 **Augmenter**…

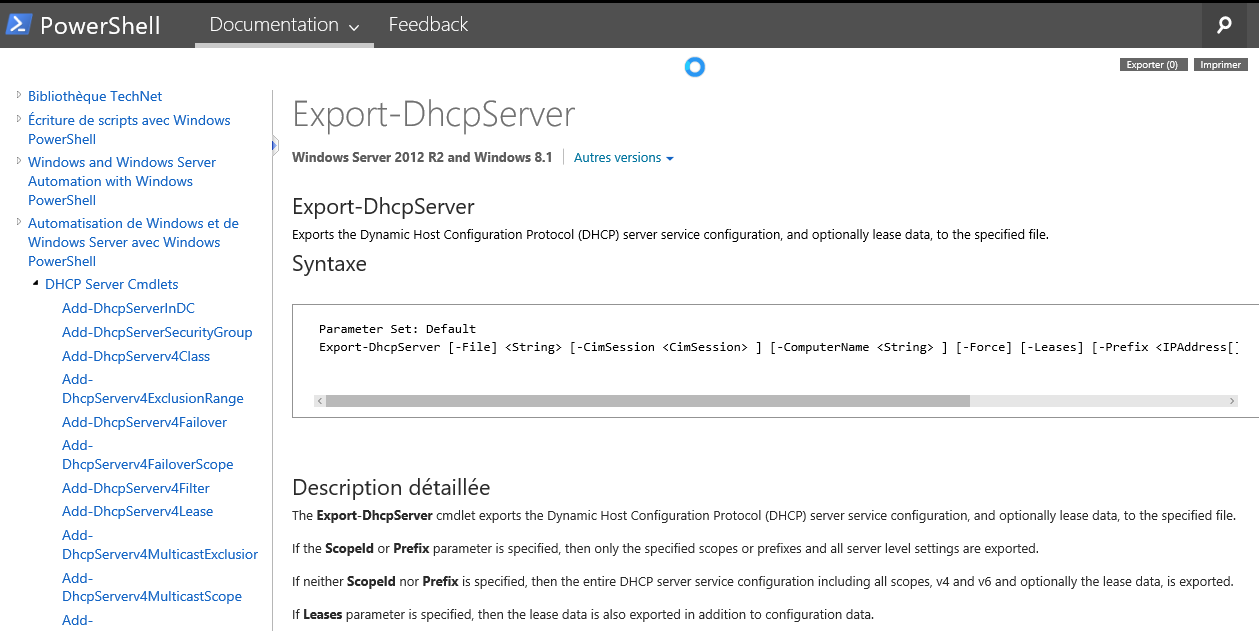
Sur un 2008R2 cela donne Sur un 2012 cela donne



# 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

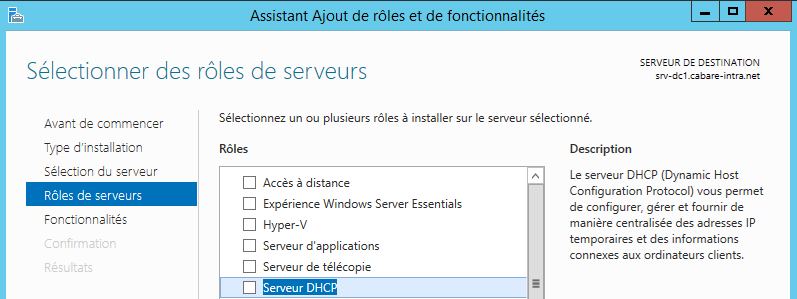


Le principe sera donc le suivant :

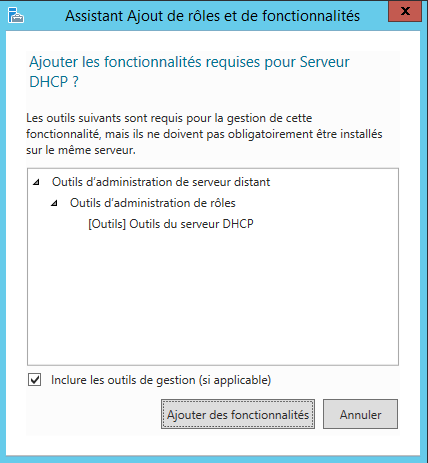
* Sur le serveur 2012R2 installer le **rôle dchp** mais sans étendue et sans activation
* Depuis le serveur 2012 executer la commande permettant de lancer l’export de la configuration dhcp du serveur 2008 dans un fichier xml (à distance donc)
* Depuis le serveur 2012 executer la commande pour récupérer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

## Ajout du rôle dhcp sur le serveur 2012

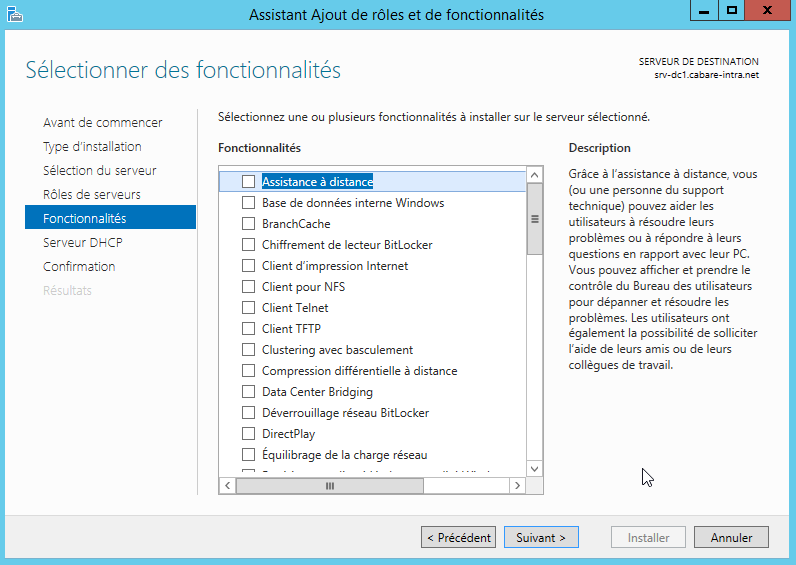
On ajouter le rôle dhcp sur notre serveur 2012 via le **gestionnaire de serveur**



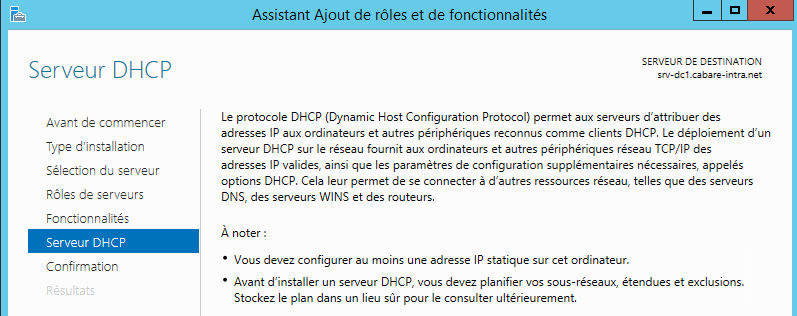
Et toutes les fonctions associées



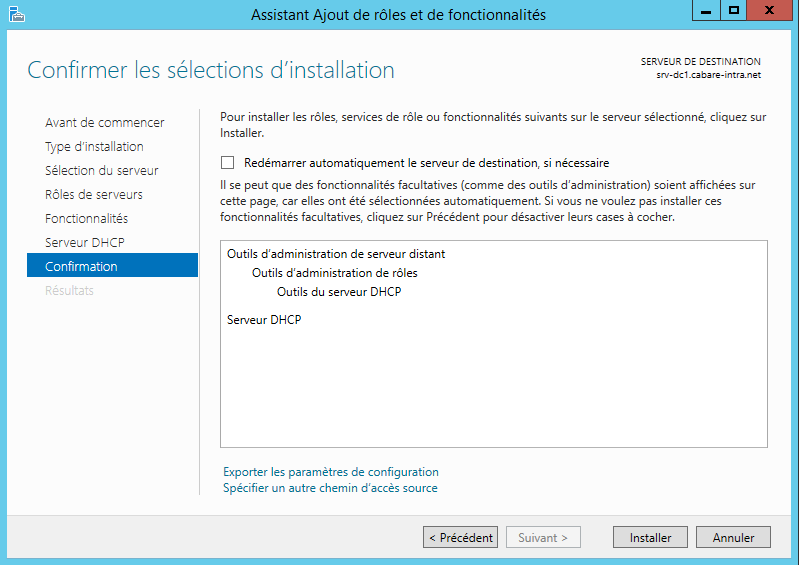
On ne modifie rien ensuite dans les fonctionnalités…



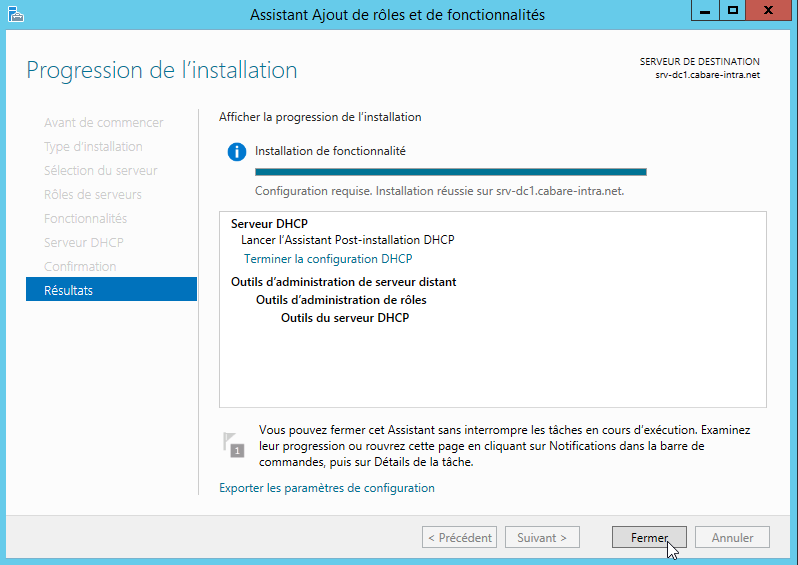
Une mise en garde apparait comme quoi il serait bon d’avoir une adresse IP



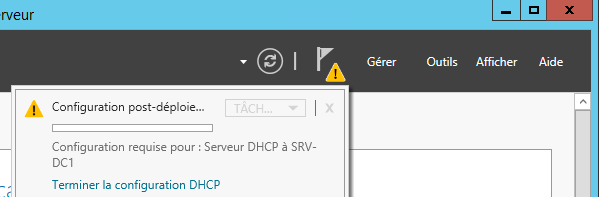
On confirme



Et c’est tout



Evidemment il faudra configurer le serveur…



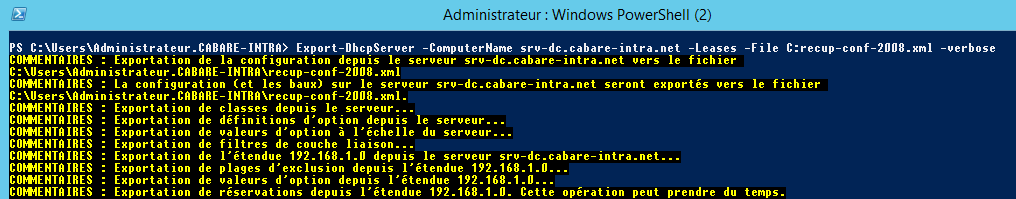
## Exportation de la configuration du DHCP 2008

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**

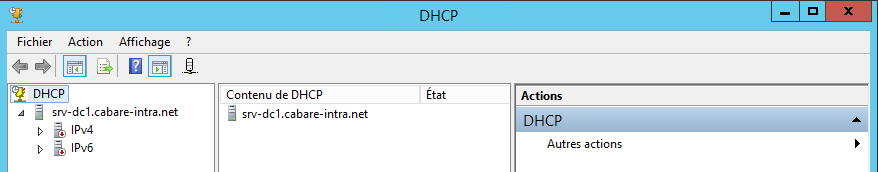


Cela crée un fichier xml



## Importation de la configuration dans le DHCP 2012

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

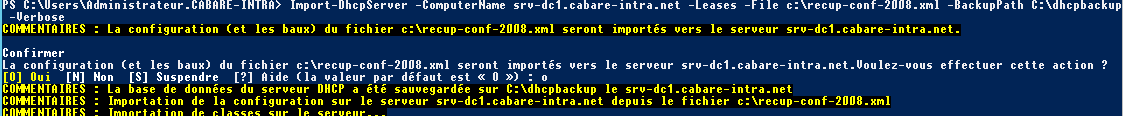


On va récupérer la configuration avec une commande powerschell du genre, ou *nomsrv* est le nom du serveur 2012r2 sur lequel est installé le nouveau serveur dhcp à configurer, et *:nomfichier.xml* est le nom du fichier de conf crée précedamment

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

Donc par exemple

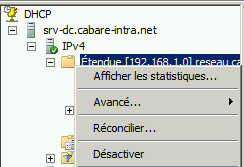
***Import-DhcpServer –ComputerName*** *srv-dc1.cabare-intra.net* ***-Leases –File*** *c:\recup-conf-2008.xml* ***-BackupPath*** *C:\dhcpbackup* ***–Verbose***

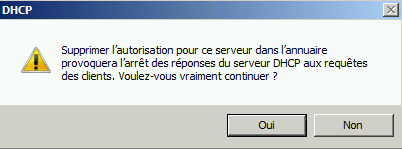


Et notre serveur est configuré !

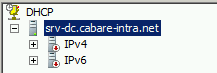
## Autorisation et activation des serveurs

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

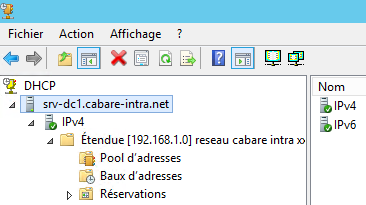
 et ensuite interdire l’ancien serveur DHCP2008R2



Pour obtenir



Reste à activer le nouveau serveur DHCP 2012…

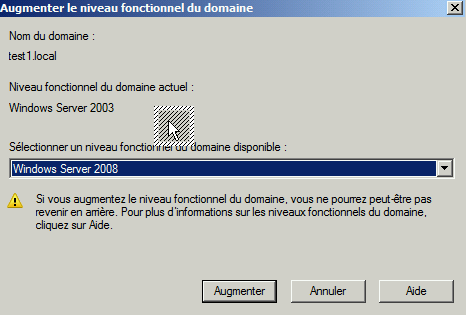


# Migration réplication Sysvol

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>

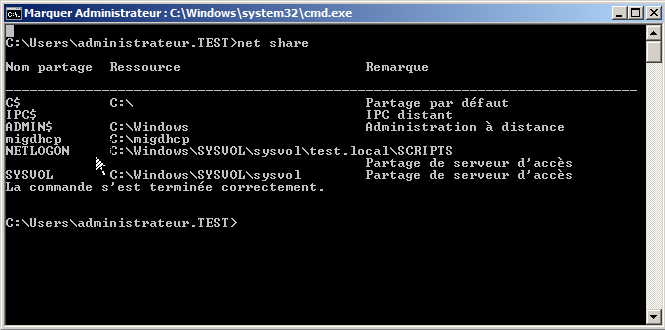


## DFSRMIG - Migrer la réplication NTFSR en DFS-R

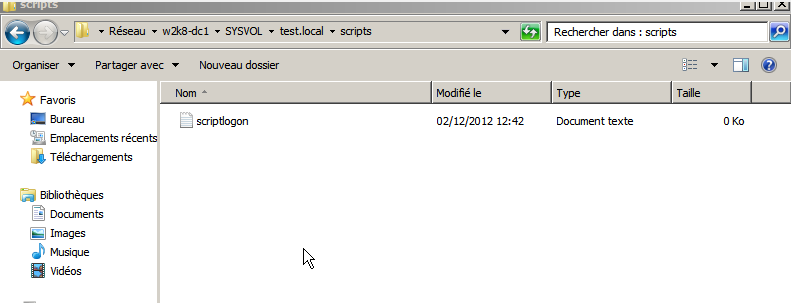
Le domaine ne contient que des DC en Windows 2008 R2 minimum, le niveau fonctionnel de la forêt et le niveau du domaine sont en 2008R2.

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

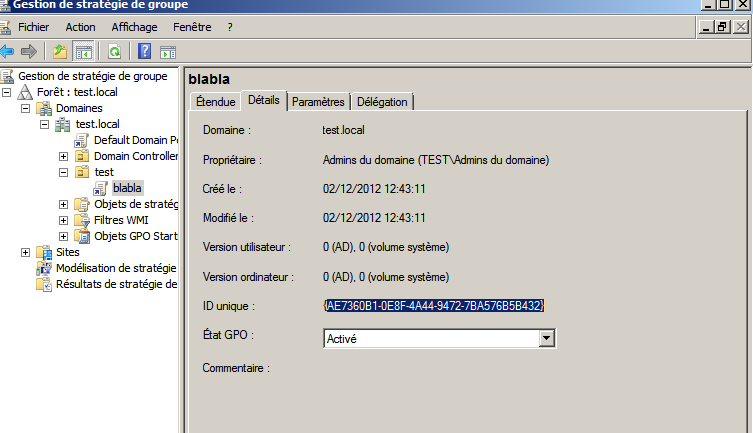
Ici le dossier partagé "sysvol" et le dossier "Netlogon" sont dans le dossier :"c:\windows\sysvol" (situation standard d'une réplication NTFRS)

1

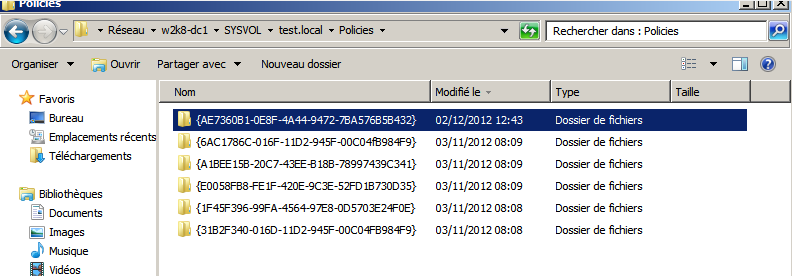
On ajoute un script de démo ***scritplogon*** dans le dossier « Netlogon »



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

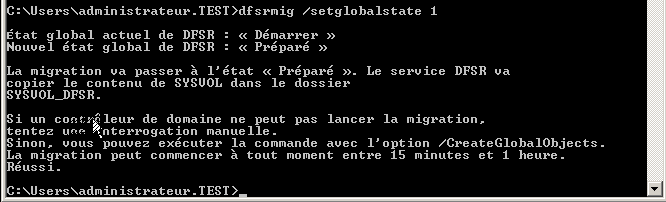
## 1° étape - dfsrmig /setglobalstate 1

Dans cette étape on crée le nouveau dossier **sysvol\_dfsr**.

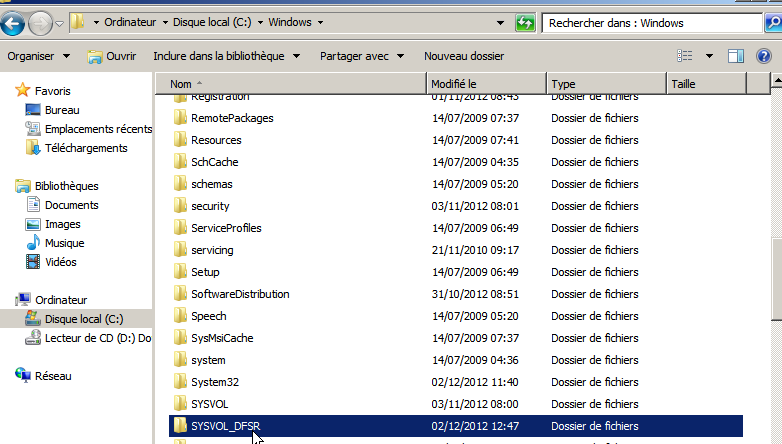
On passe du mode « démarrer » au mode « préparé » par la **commande**

**dfsrmig /setglobalstate 1**

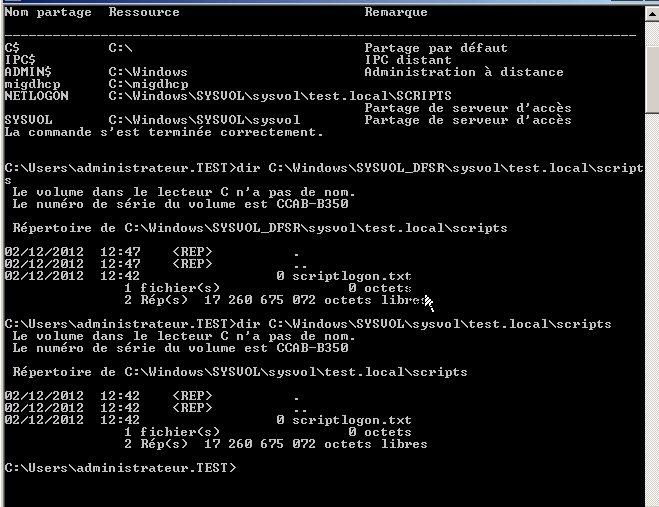
Le dossier c**:\\windows\\sysvol\_dfsr** est donc crée et initialisé avec une copie du dossier sysvol actuel.



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

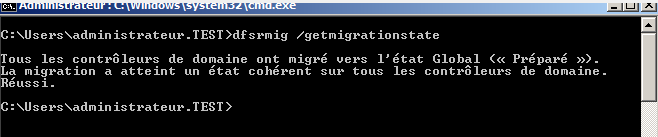


On vérifie par un **dir** sur les 2 dossiers ou sont stockés les scripts (partage netlogon), qu’ils sont identiques.



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**

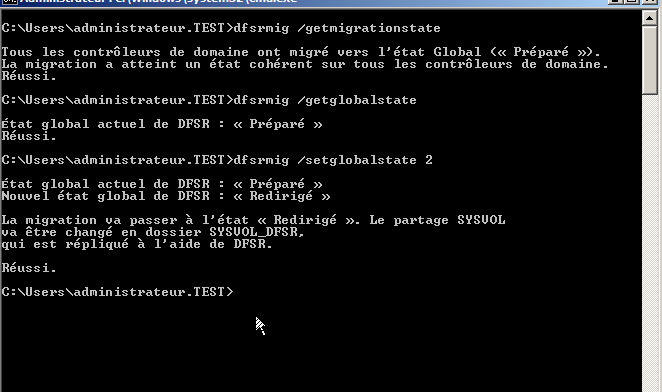


## 2 étape - dfsrmig /setglobalstate 2

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

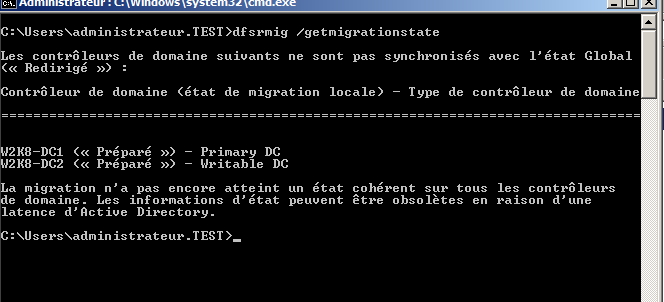
On passe du mode « préparé » au mode « redirigé » par la **commande**

**dfsrmig /setglobalstate 2**



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

**dfrsmig /getmigrationstate**

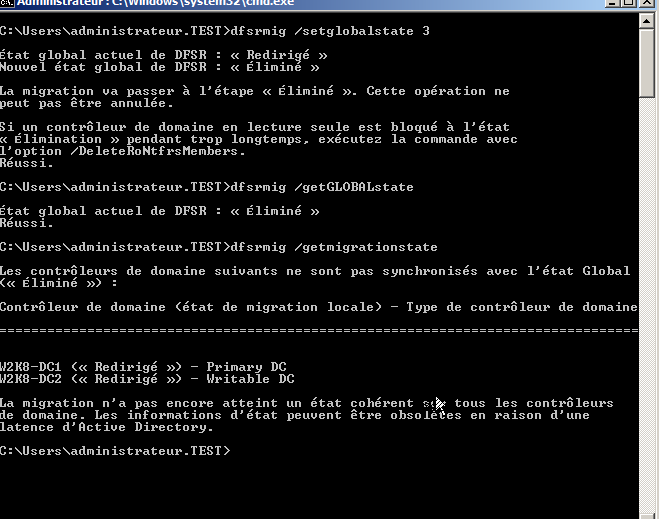


Mais après un laps de temps variable on doit obtenir une information comme quoi que tous les DC sont passés à l’étape redirigé.

## 3 étape - dfsrmig /setglobalstate 3

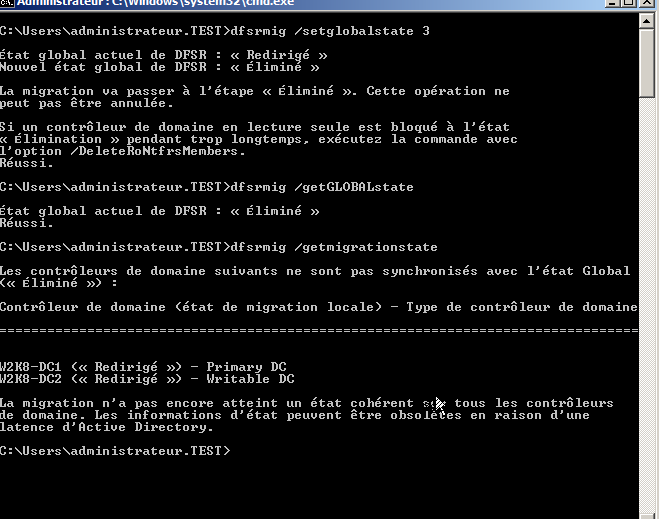
Nous allons passer à la dernière étape qui consiste à supprimer l’ancien dossier "sysvol". A partir de ce moment l’opération est irréversible. Cela se fait via la commande :

**dfsrmig /setglobalstate 3**

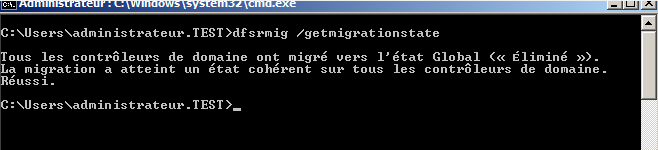


La commande de vérification peut encore une fois nous indiquer la nécessité … d'attendre

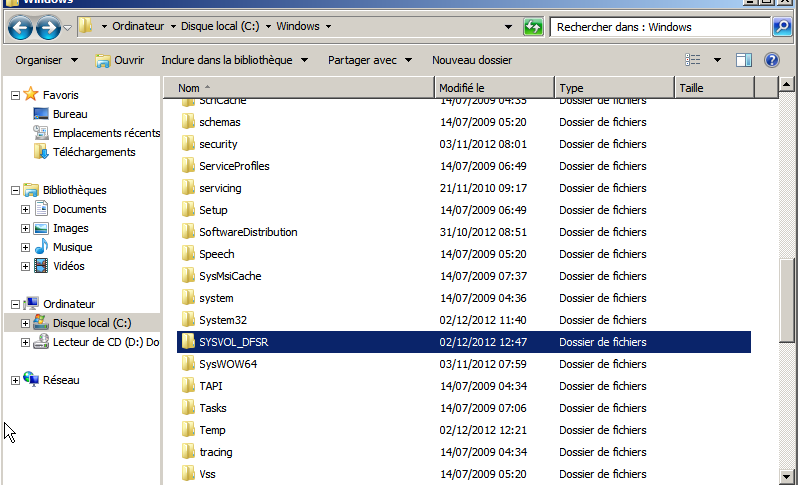
**dfrsmig /getmigrationstate**



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



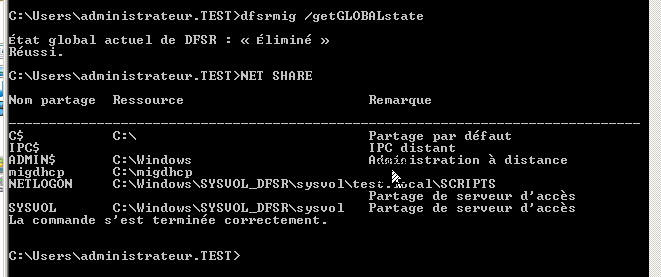
Après un délais, on peut constater la suppression du dossier « sysvol » dans le dossier Windows.



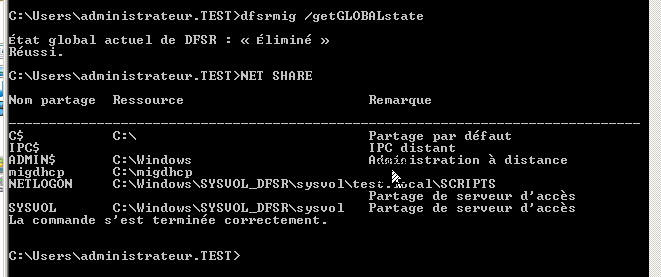
## Vérification

La commande pour vérifier dans quelle étape nous somme est

**dfrsmig /GetGlobalState :**



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



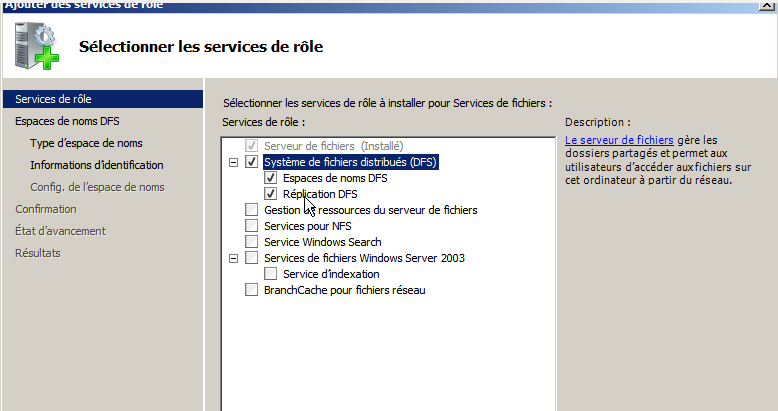
L’opération est terminée, mais nous souhaitons quand même surveiller l’état de la réplication.

# Surveiller replication DFS Sysvol

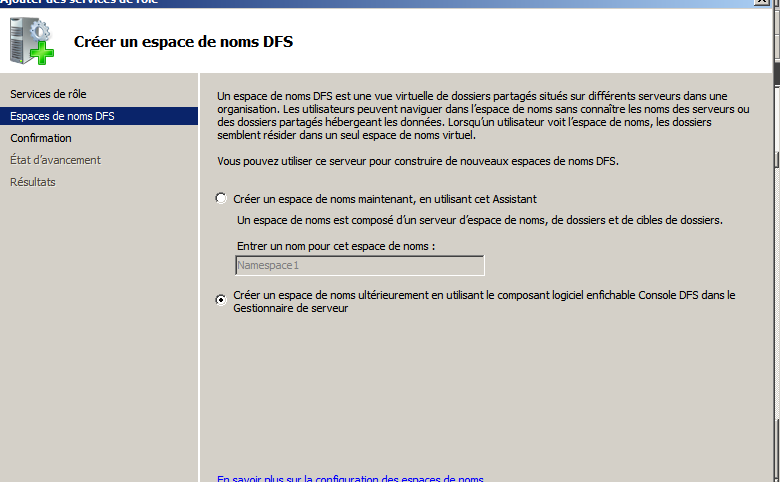
On souhaite juste surveiller l’état de la réplication

## 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.

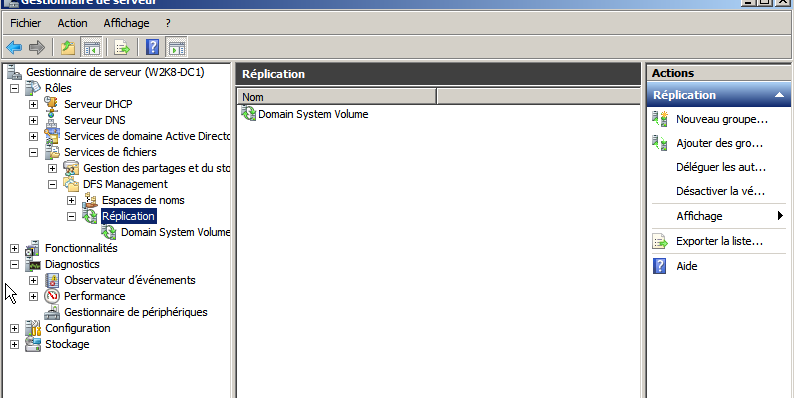


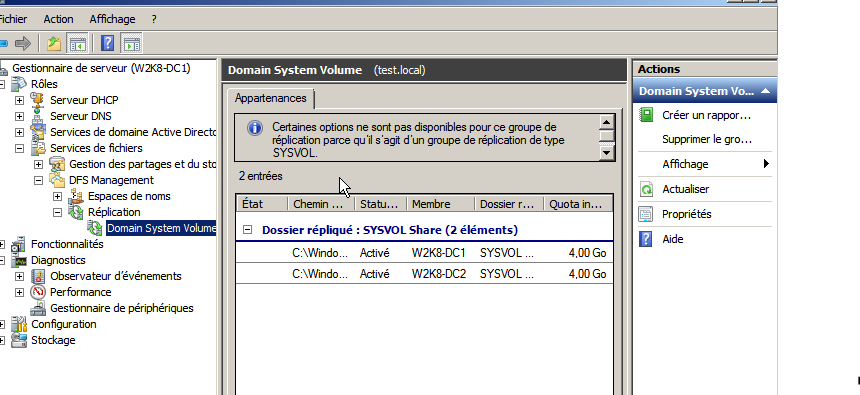
Nous n’allons pas créer d’espace de nom DFS, car l'objectif c'est juste d'utiliser les outils de réplication.



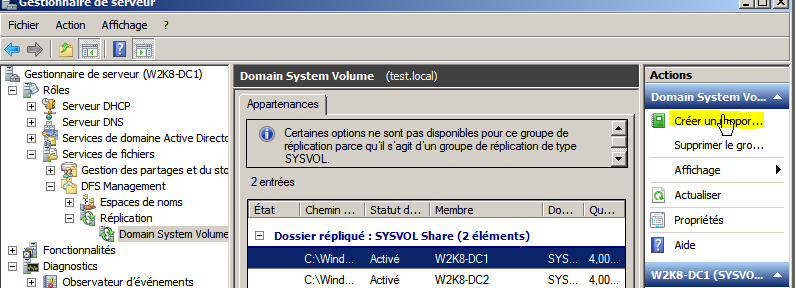
Dans la console gestion de serveur, sous **rôles / serveur de fichiers / DFS Management / Réplication**, nous trouvons « **Domain System volume** »  qui est la réplication du dossier « sysvol ».

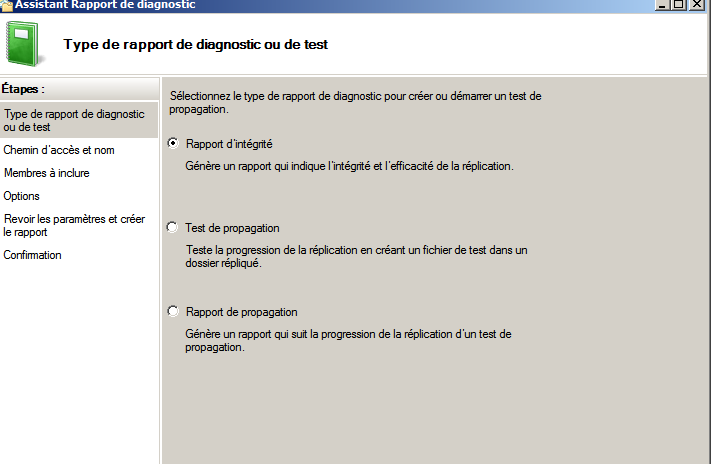
Sur la partie de droite dans la zone « actions », nous cliquons sur « créer un rapport… ».

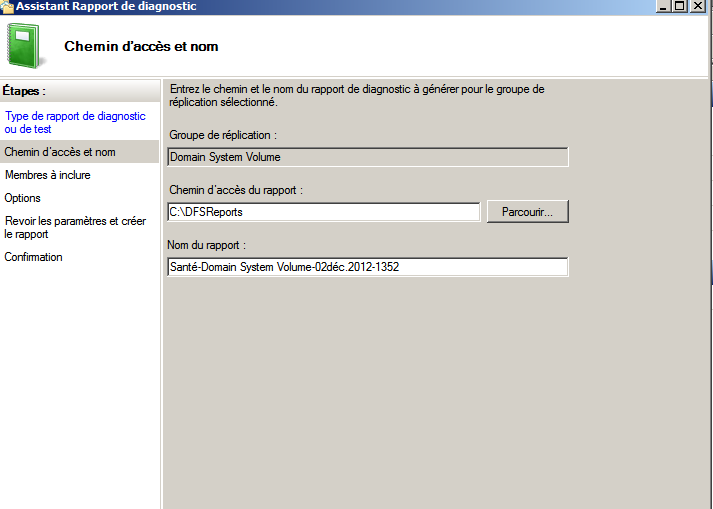


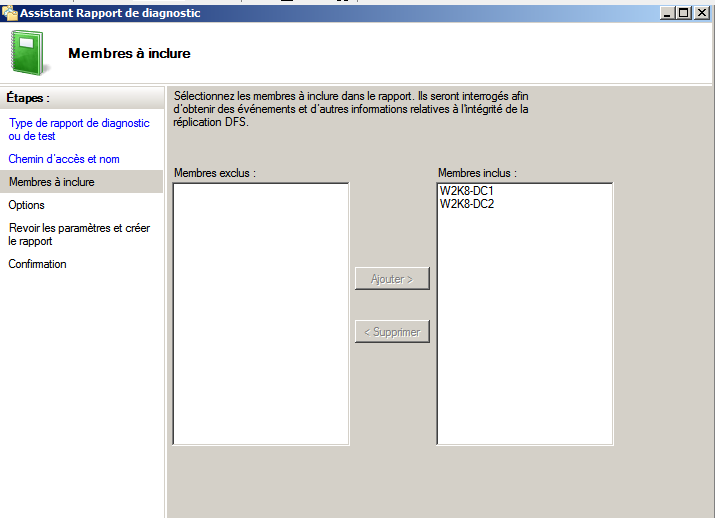


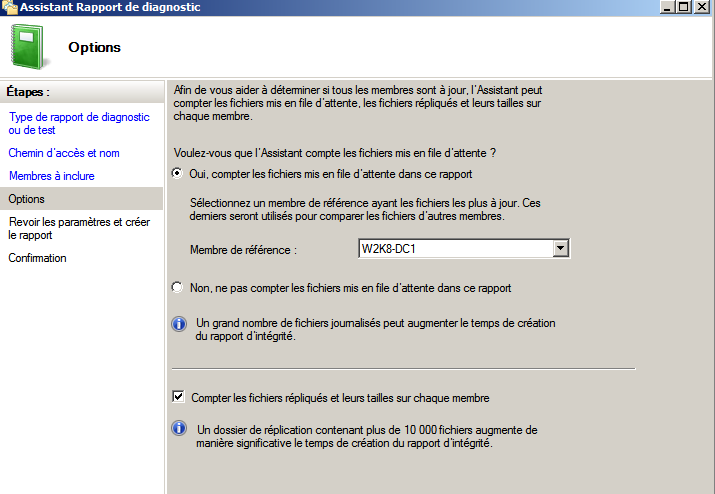
Nous allons utiliser l’option « créer un rapport » dans le volet d’action en haut à droite :

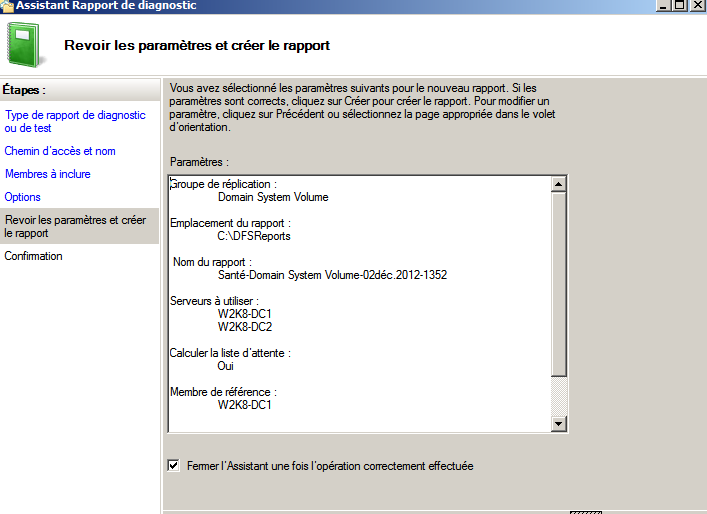


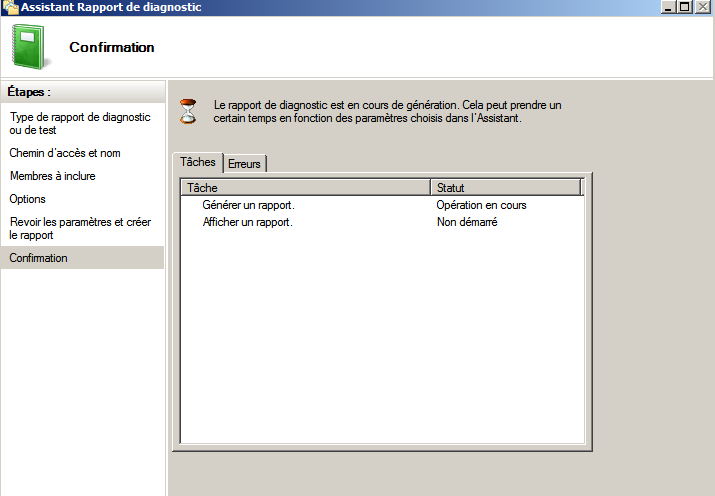




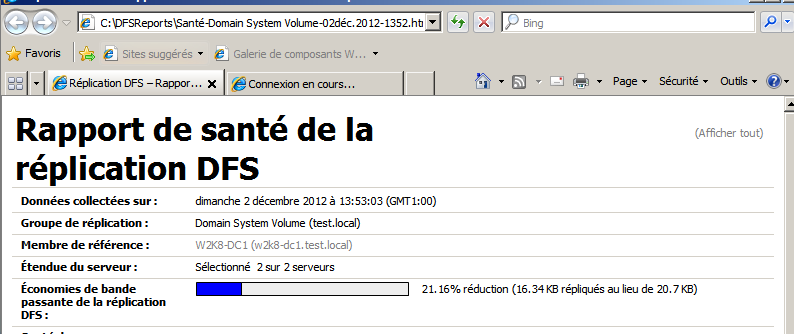


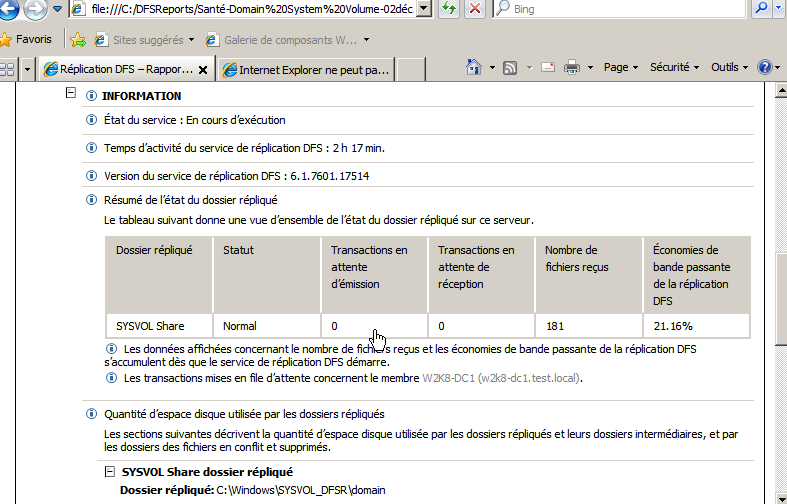




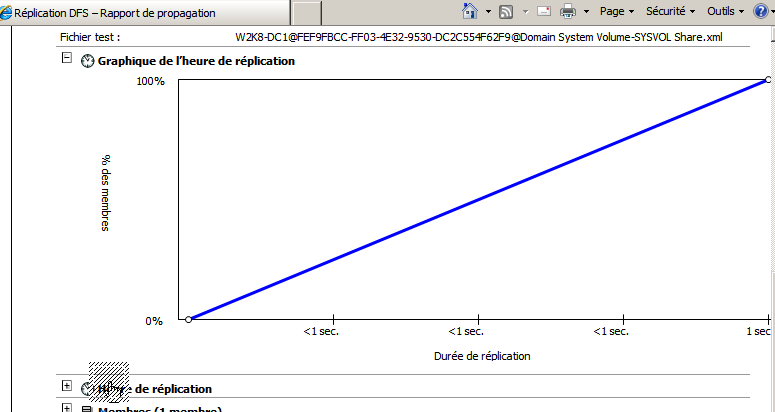


Dans le rapport on constate l'absence de dossier ou de fichier en conflit.





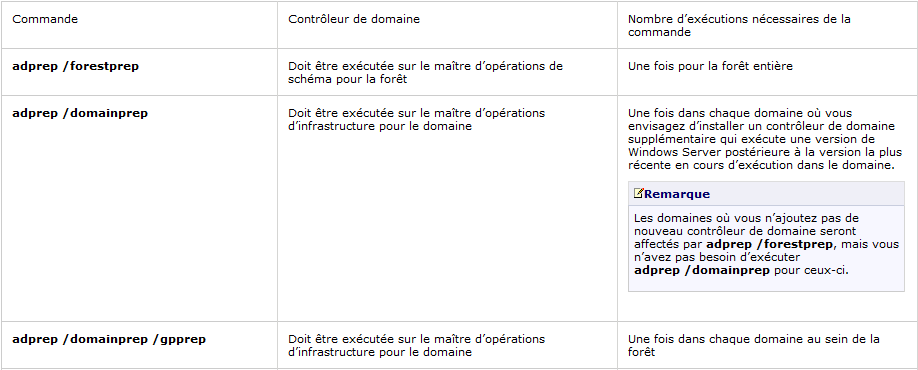
Il est possible de faire d’autres rapports comme un test de propagation :



# Intégration 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**



## 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**

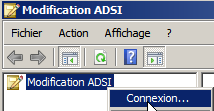
**N.B**: Attendez la réplication des modifications dans la forêt.

## Vérification Adprep du schéma ADSIedit

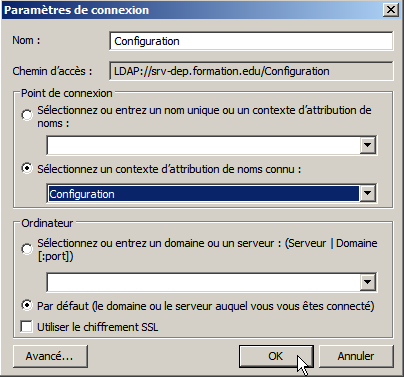
Au terme de la commande **adprep /forestprep**, un message apparaît dans la fenêtre Invite de commandes pour indiquer qu’Adprep a correctement mis à jour les informations au niveau de la forêt….

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

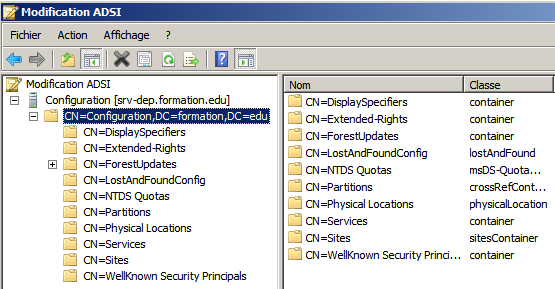
lancer la console **adsiedit.msc** puis clic droit / connexion.



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



on obtient



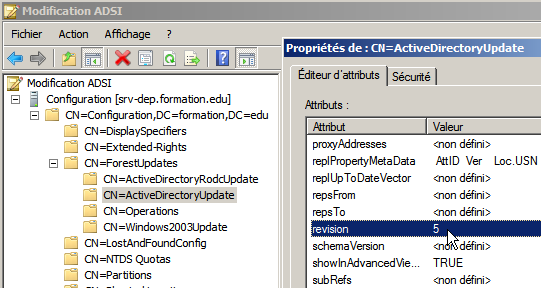
Développer **Configuration**, puis

CN=Configuration, DC=domaine\_racine\_forêt

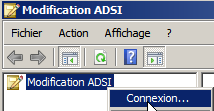
Développer sur CN=ForestUpdates.

Demander les propriétés de CN=ActiveDirectoryUpdate,

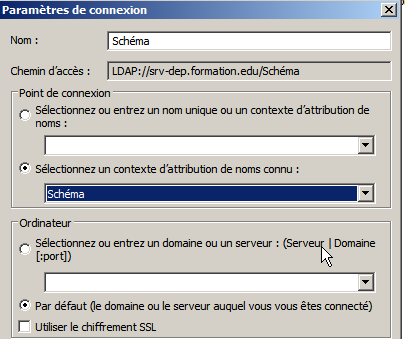
* Vérifiez que l’attribut **Revision** à pour valeur **4** pour 2008, ou **5** pour Windows Server 2008 R2,.



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

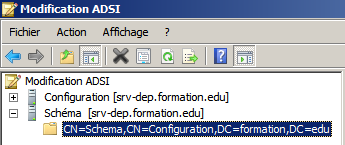


demander **Sélectionnez un contexte d’attribution de noms connu**, puis **Schéma**

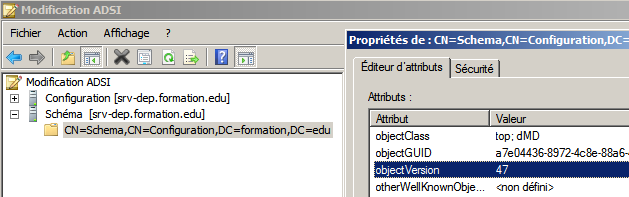


Développer **Schéma**, puis

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**

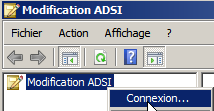
Ou **adprep32.exe / domainprep /gpprep**

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

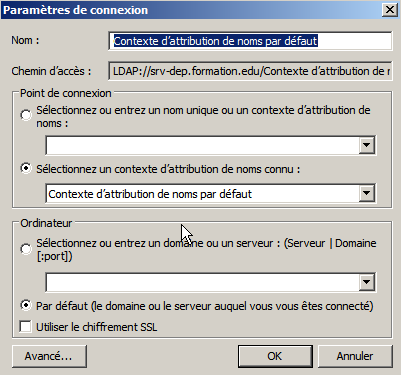
**N.B**: Attendez la réplication dans le domaine tout entier.

## Vérification Adprep du domaine ADSIedit

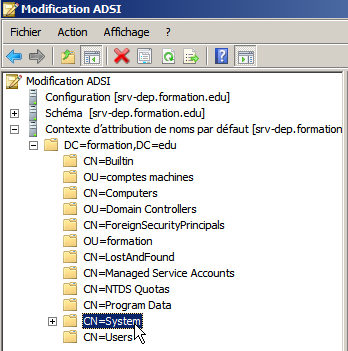
lancer la console **adsiedit.msc** puis clic droit / connexion.



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



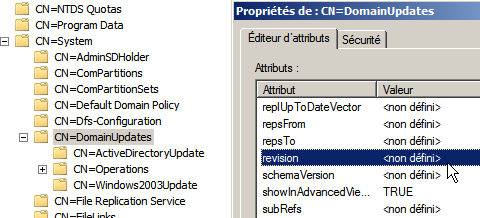
on obtient



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):**

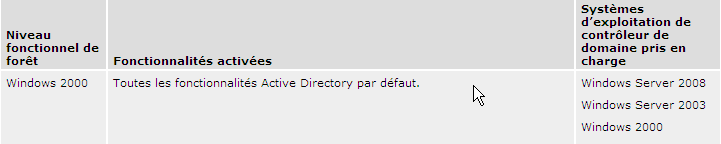
Ce niveau de fonctionnalité n’apporte rien de plus, mais requiert que tous les contrôleurs de domaines soient sous Windows 2008 Server (sécurité ?...)

**Windows 2003 version préliminaire :**

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

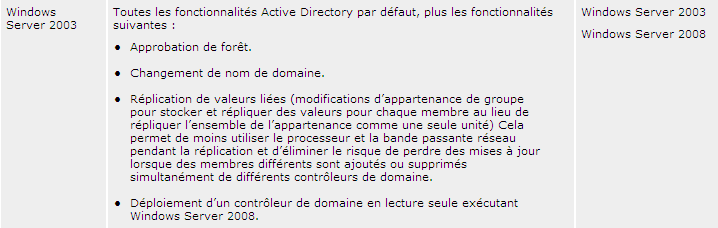
**NB** : Il faut augmenter le niveau fonctionnel de tous les domaines de la forêt avant de pouvoir augmenter celui de la forêt.

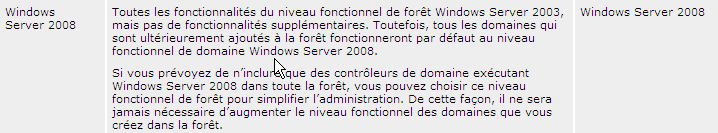
**NB** : Il est impossible de revenir à un niveau fonctionnel de domaine et de forêt inférieur, on ne peut qu'augmenter le niveau de fonctionnalités.



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

DNS sans le domaine

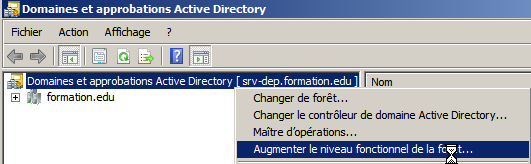




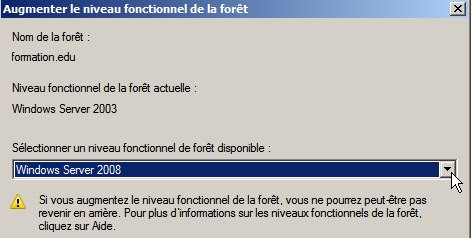
La modification se fait dans **Domaines et approbations Active Directory**

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 :**

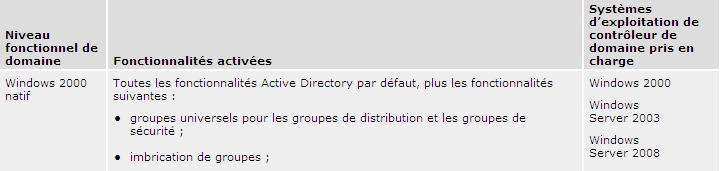
Le niveau fonctionnel le plus élevé pour un domaine. Il n’est accessible uniquement si le domaine ne possède que des contrôleurs de domaine sous Windows 2003 server. Avec ce niveau fonctionnel, toutes les fonctionnalités Active Directory pour le domaine sont disponibles.

**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 ?...)

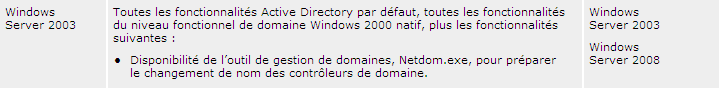
**Windows 2003 niveau préliminaire :**

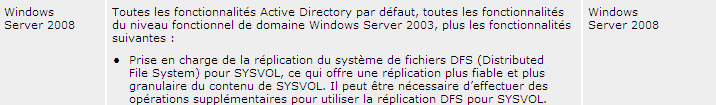
Ce niveau fonctionnel est utilisable si le domaine contient des contrôleurs de domaine sous NT 4.0 et des contrôleurs de domaine sous Windows 2003 server. Ce niveau fonctionnel est utilisé dans le cadre d’une migration.



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

DNS sans le domaine

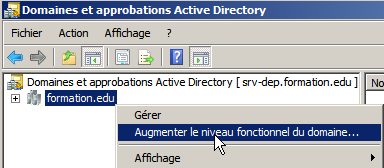


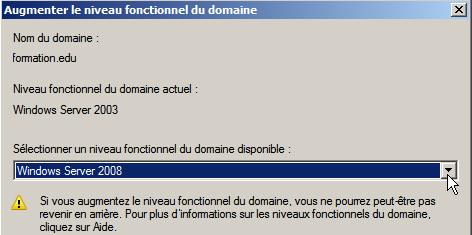


La modification se fait dans **Domaines et approbations Active Directory**

il faut se placer sur le domaine,

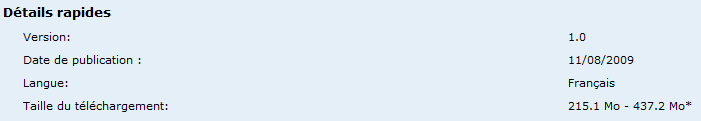
puis clic droit **Augmenter le niveau fonctionnel du domaine...**





## 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…



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