Restaurer SYSVOL dans un domaine avec un unique contrôleur de domaine sans sauvegarde de l'état du système

I. Présentation de ce document :

A. Où trouver ce document :

Ce document a été écrit par M. Guillaume MATHIEU. Une version électronique est disponible sur http://msreport.free.fr.
Une version au format PDF peut être téléchargée à l'adresse suivante :
http://msreport.free.fr/articles/Restaurer_SYSVOL.pdf

B. Objectifs :

Ce document a pour but de vous présenter :

- Le rôle du répertoire SYSVOL sur un contrôleur de domaine.
- Le contenu (et l'importance) d'une sauvegarde de l'état du système.
- Comment restaurer le répertoire SYSVOL lorsque celui-ci a été supprimé ou quand des fichiers à l'intérieur de ce répertoire ont été supprimés.
- Comment restaurer les 2 stratégies par défaut lors de la création d'un domaine Active Directory.

Microsoft fournit déjà une procédure http://support.microsoft.com/kb/315457/en-us pour restaurer ce répertoire mais uniquement lorsque que l'on a plusieurs contrôleurs de domaine dans le même domaine. La procédure Microsoft permet de forcer le contrôleur de domaine qui rencontre des problèmes avec SYSVOL à aller récupérer totalement le répertoire SYSVOL d'un autre contrôleur de domaine (comme lorsque l'on fait un dcpromo pour ajouter un nouveau contrôleur de domaine dans le domaine).

Ce document propose une solution dans le cas où l'on a un seul contrôleur de domaine dans notre domaine avec un SYSVOL endommagé et que l'on ne dispose pas de sauvegarde de l'état du système ou d'une sauvegarde complète du serveur.

Que dit Microsoft dans ce cas précis ?
La réponse est sans appel. Restaurer une sauvegarde de l'état du système. Cette article est fait pour ceux qui n'ont pas de sauvegarde.

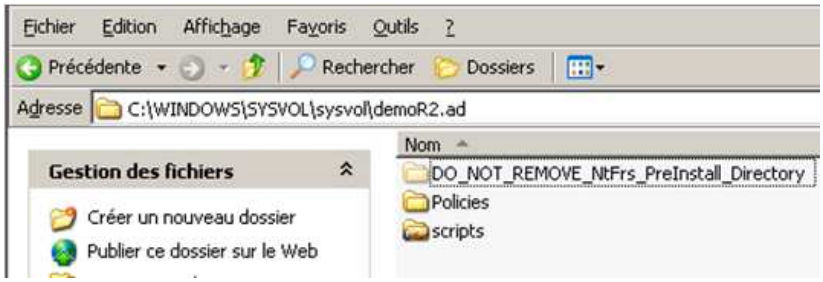
Attention cette procédure n'est pas sans risque. Donc effectuer une sauvegarde au préalable avec NTBACKUP.

II. Le répertoire SYSVOL :

Sysvol est un répertoire présent sur tous les contrôleurs de domaine Active Directory.
Il stocke entre autres tous les scripts utilisateurs ainsi que les objets de stratégie de groupe.
Le contenu de ce répertoire est répliqué sur tous les contrôleurs de domaine de votre domaine. C'est le service NTFRS (Service de réplication de fichiers) qui s'occupe de la réplication de ce répertoire.

Sysvol contient deux partages créés automatiquement par le système :

- SYSVOL : ce partage est créé automatiquement par le système lorsque l'on démarre le service NTFRS (Service de réplication de fichiers)
- Netlogon : ce partage est créé automatiquement par le système lorsque l'on démarre le service NETLOGON (Ouverture de session réseau).



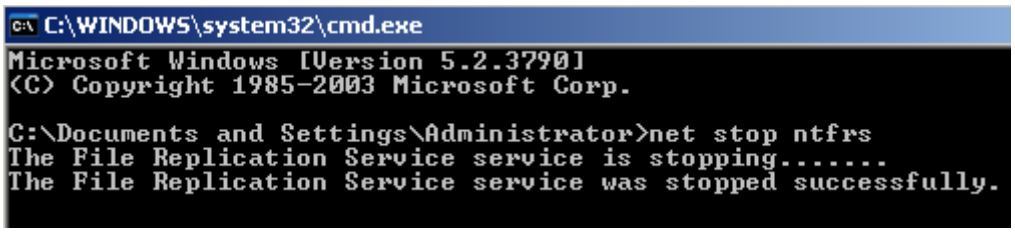
III.Reproduire le problème :

Cette étape n'est pas à faire (c'est un véritable massacre)! Elle me permet de reproduire le problème que l'on va corriger en étape IV en partant d'un contrôleur de domaine valide :

Les problèmes reproduits sont :

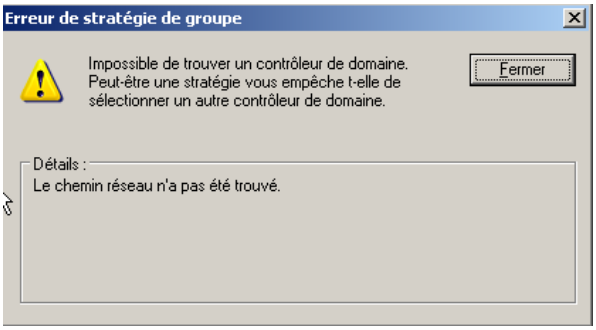
- Tout le contenu du répertoire SYSVOL a été supprimé sur votre contrôleur de domaine.
- Les objets de stratégies de groupe Default Domain Policy (stratégie du domaine par défaut) et/ou Default Domain Controller Policy (stratégie par défaut des contrôleurs de domaine) ont été supprimés ou sont corrompus.

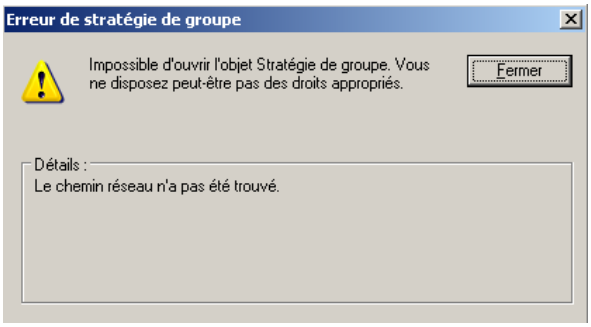
On arrête le service NTFRS qui gère la réplication du dossier sysvol.
Une fois le service arrêté, on peut supprimer le contenu du sysvol.



Plusieurs messages apparaissent comme quoi cela va supprimer partage Netlogon et SYSVOL et que ces répertoires sont empêcher le fonctionnement d'Active Directory.
Le dossier Sysvol est maintenant vide.
On peut redémarrer le service NTFRS. Le service NTFRS redémarre mais on obtient les erreurs suivantes :

- Quand on essaie d'éditer une stratégie de groupe, on obtient les erreurs suivantes :





<u>Les erreurs suivantes sont présentes dans le journal « Service de réplication de fichier » :</u>

Type de l'événement :Erreur
Source de l'événement : NtFrs
Catégorie de l'événement : Aucun
ID de l'événement : 13555
Date : 1/31/2008
Heure : 10:46:26 PM

Utilisateur : N/A
Ordinateur : W2K3R2-DC
Description :
Le service de réplication de fichiers est en état d'erreur. Les fichiers ne vont pas se répliquer vers ou à partir d'un ou plusieurs jeux de réplicas sur cet ordinateur tant que les étapes suivantes n'ont pas été effectuées…

Type de l'événement :Erreur
Source de l'événement : NtFrs
Catégorie de l'événement : Aucun
ID de l'événement : 13552
Date : 1/31/2008
Heure : 10:46:26 PM
Utilisateur : N/A
Ordinateur : W2K3R2-DC
Description :
Le service de réplication de fichiers ne peut pas ajouter cet ordinateur au jeu de réplica suivant :
"DOMAIN SYSTEM VOLUME (SYSVOL SHARE)"

Type de l'événement :Erreur
Source de l'événement : NtFrs
Catégorie de l'événement : Aucun
ID de l'événement : 13539
Date : 1/31/2008
Heure : 10:46:25 PM
Utilisateur : N/A
Ordinateur : W2K3R2-DC
Description :
Le service de réplication de fichiers ne peut pas répliquer c:\windows\sysvol\domain car le nom de chemin du répertoire dupliqué est le nom de chemin incomplet d'un répertoire local existant et accessible.

IV. Restaurer sysvol a un état normal de fonctionnement :

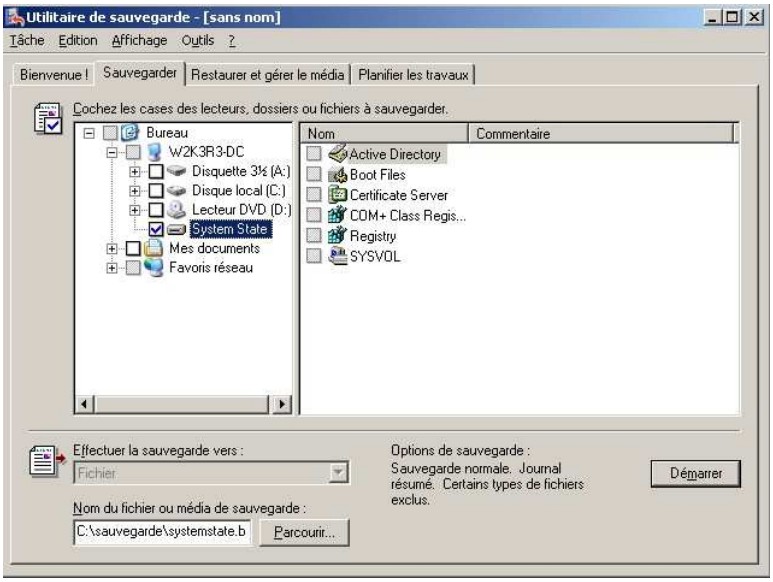
Attention cette procédure n'est à faire que qu'en vous avez qu'un seul contrôleur de domaine dans votre domaine et que vous avez pas de sauvegarde de l'état du système valide. Si vous n'êtes pas dans ce cas, appliquer rigoureusement l'article Microsoft suivant http://support.microsoft.com/kb/315457/en-us

Cette article vous explique comment regénérer les stratégies de groupe par défaut, c'est à dire la « default domain policy » et la « default domain controller policy ». **Vous perdez toutes les autres stratégies ainsi que vos scripts ainsi que toute la topologie DFS (saud si vous lez avez copier ce qui vous reste de répertoire sysvol).**

A. Etape 1 : sauvegarde de l'état du système :

Effectuer une sauvegarde de l'état du système et/ou une sauvegarde complète de votre contrôleur de domaine. On pourra revenir en arrière ainsi.

Taper Démarrer | Exécuter puis ntbackup. Sélectionner « System State » et faire une sauvegarde sur bande ou sous forme de fichier (à stocker sur une autre machine).



Le system state contient tous les fichiers liés à Active Directory, le ntds.dit (la base de données Active Directory), le répertoire sysvol (enfin ce qui vous en reste), le registre (le fichier de configuration de Windows), la base de certificats et tous les objets COM.

Il est probable que le system state détecte des problèmes du à l'absence de fichiers dans le répertoire sysvol ou l'absence de répertoire sysvol.

B. Etape 2 : sauvegarde manuel du contenu du répertoire sysvol :

Arrêter le service NTFRS.
Copier le contenu du répertoire sysvol (les scripts, les GPO).
Supprimer tout le contenu de votre répertoire c:\windows\sysvol.

C. Etape 3 : recréer l'arborescence SYSVOL de base :

On va détourner l'article http://support.microsoft.com/kb/315457/en-us afin de récrer un répertoire SYSVOL propre à l'aide des indications une arborescence sysvol complète.
Le service NTFRS doit être arrêté à cette étape.

Recréer les répertoires suivants :

- C:\windows\SYSVOL
- C:\windows\SYSVOL\domain
- C:\windows \SYSVOL\staging\domain
- C:\windows \SYSVOL\staging areas
- C:\windows \SYSVOL\domain\Policies
- C:\windows \SYSVOL\domain\scripts
- C:\windows \SYSVOL\SYSVOL

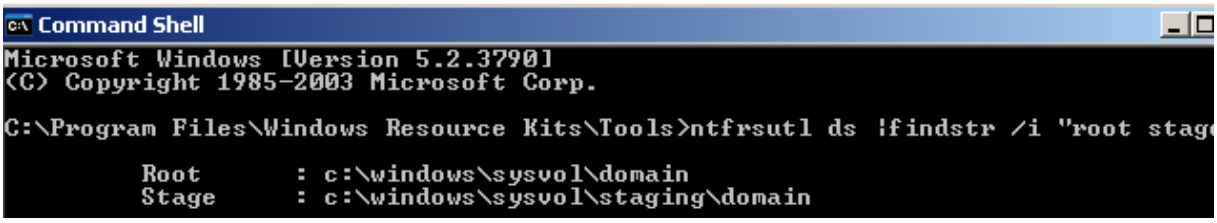
Remarque :
Par défaut sous Windows 2003, sysvol est dans c:\windows.
Sous Windows 2000, c'est dans c:\winnt.
Et lors du dcpromo, on peut mettre sysvol dans un autre répertoire donc pas de copier coller sans réféchir des chemins ci-dessous.

D. Etape 4 : recréer les liens physiques

Il faut redémarrer le service NTFRS à cette étape :

Le répertoire C:\windows\SYSVOL\SYSVOL\nom_du_domaine_dns est lié au répertoire c:\windows\sysvol\domain. C'est-à-dire que ces deux répertoires pointent sur les même données.
C'est la même chose pour le répertoire C:\windows\SYSVOL\staging areas\ nom_du_domaine_dns c:\windows\SYSVOL\staging\domain
C'est un peu comme les liens physiques sous Linux.

Taper la commande suivante :
ntfrsutl ds |findstr /i "root stage

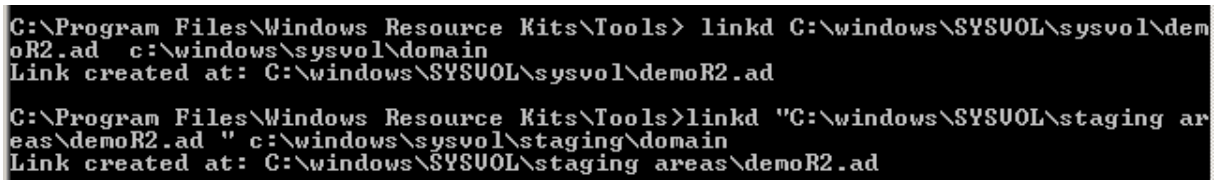


Dans notre cas, taper la commande :

linkd “C:\windows\SYSVOL\SYSVOL\demoR2.ad” c:\windows\SYSVOL\domain
linkd "C:\windows\SYSVOL\staging areas\demoR2.ad " c:\windows\SYSVOL\staging\domain

L’utilitraire linkd est disponible sur le ressource kit de Windows Server 2003
Il faut le télécharger à cette adresse puis l’intaller :
http://www.microsoft.com/Downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en

Il faut ensuite lancer une invite de commande depuis le répertoire du ressorce kit.
Taper les deux commandes linkd (voir ci-dessus).
On doit obtenir le message suivant :

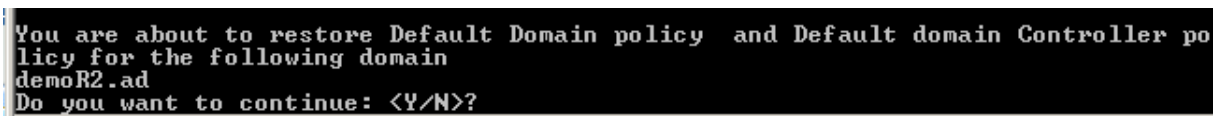


E. Etape 5 : recréer la default domain policy et la default domain controller policy

Pour cela, on va utiliser un outil qui s’appelle dcgpofix. Il est intégré dans le système d’exploitation.

Pour plus d’informations sur dcgpofix, voir article ci-dessous :
http://support.microsoft.com/kb/932445/en-us
http://support.microsoft.com/?kbid=842162

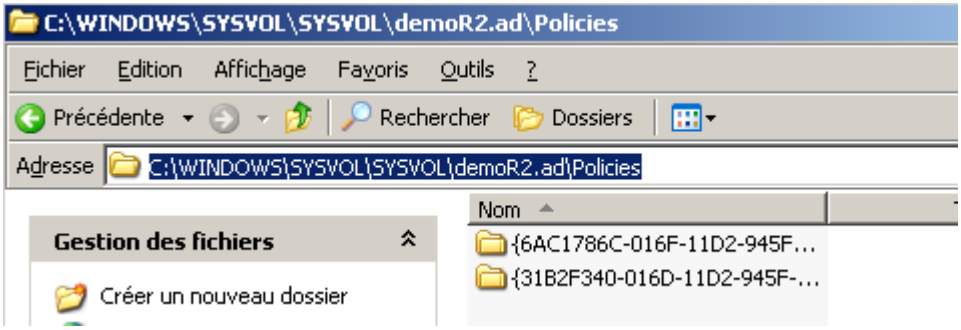
Si le schéma Windows 2003 est en R2, il faut exécuter la commande dans une fenêtre invite de commande (cmd):
dcgpofix.exe /ignoreschema
Sinon
dcgpofix.exe



Taper Y

Taper Y

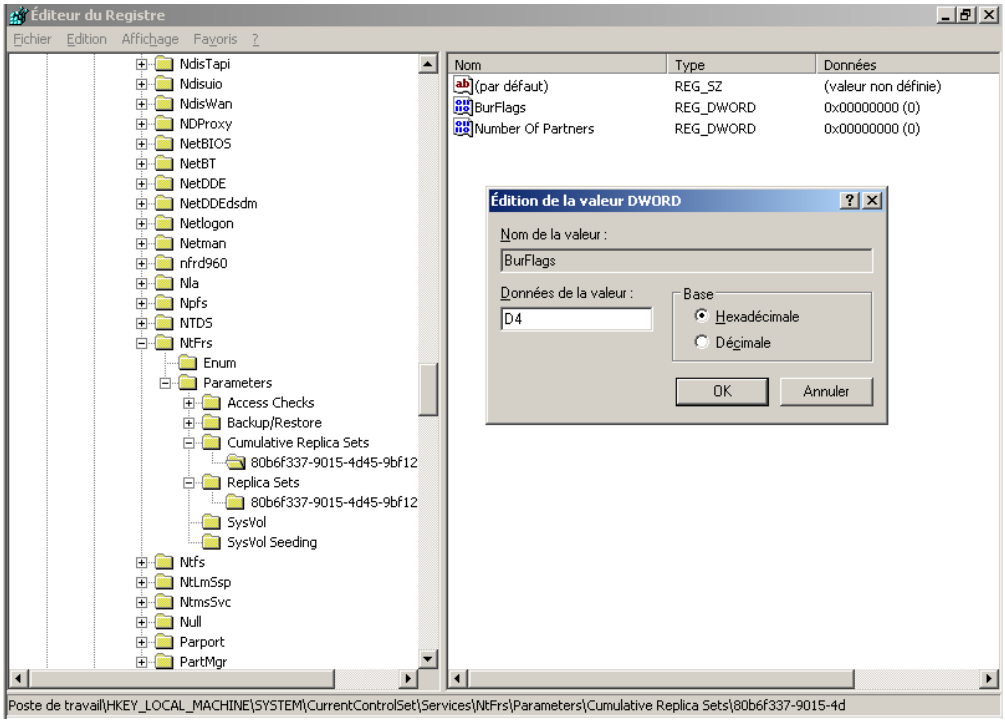
Les deux stratégies ont bien été recréer.



On a bien la stratégie qui est de nouveau éditable.

F. Etape 6 : réinitialiser sysvol :

Il faut arrêter le service NTFRS.
Il faut positionner la clé BurFlags à D4 (voir article http://support.microsoft.com/kb/315457/en-us).
Cette clé se trouve dans HKEY_LOCCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Cumulative Replica Sets\guid_domaine
Où guid domaine est le guid de votre domaine.



Redémarrer le service NTFRS puis le service NETLOGON.
Les partages sysvol et netlogon doivent être recréés.

G. Etape 7 : vérification :

Dans le journal « Service de réplication de fichiers », on doit avoir ces deux messages d'informations.

Type de l'événement :Informations
Source de l'événement : NtFrs
Catégorie de l'événement : Aucun
ID de l'événement : 13516
Date : 1/31/2008
Heure : 11:47:30 PM
Utilisateur : N/A
Ordinateur : W2K3R2-DC
Description :
Le service de réplication de fichiers n'empêche plus l'ordinateur W2K3R2-DC de devenir un contrôleur de domaine. Le volume système a été correctement initialisé et le service Accès réseau a été averti du fait que le volume système est maintenant prêt à être partagé en tant que SYSVOL.

Type de l'événement :Informations
Source de l'événement : NtFrs
Catégorie de l'événement : Aucun
ID de l'événement : 13553
Date : 1/31/2008

Heure : *11:47:29 PM*
Utilisateur : *N/A*
Ordinateur : *W2K3R2-DC*
Description :
Le service de réplication de fichiers a correctement ajouté cet ordinateur au jeu de réplica suivant :
"DOMAIN SYSTEM VOLUME (SYSVOL SHARE)"

Si vous n'avez pas ces deux messages d'informations et mais le message d'erreur ci-dessous, réappliquer l'étape 6 :

Type de l'événement :Erreur
Source de l'événement : *NtFrs*
Catégorie de l'événement : *Aucun*
ID de l'événement : *13559*
Date : *1/31/2008*
Heure : *11:33:50 PM*
Utilisateur : *N/A*
Ordinateur : *W2K3R2-DC*
Description :
Le service de réplication des fichiers a détecté que le chemin d'accès de la racine du réplica a été modifié de "c:\windows\sysvol\domain" à "c:\windows\sysvol\domain". Si il s'agit d'un choix intentionnel, le fichier du nom NTFRS_CMD_FILE_MOVE_ROOT doit être créé sous le nouveau chemin d'accès de la racine.
Ceci a été détecté pour le jeu de réplicas suivant :
"DOMAIN SYSTEM VOLUME (SYSVOL SHARE)"

SYSVOL a été restauré avec succès.