Sylvain Garcia
sylvain.garcia@isynet.org

SAUVEGARDE ET RESTAURATION D'UN SYSTEME SOUS WINDOWS, CAS PARTICULIER D'UN CONTROLEUR DE DOMAINE

Les administrateurs systèmes doivent protéger leurs réseaux de la perte de données et des défaillances machines. Ce document fournit des indications pour **le rétablissement d'un contrôleur de domaine Windows 2000**. Car la sauvegarde et la restauration d'un système windows ne pause aucun problème particulier si tous ce qui suit est compris

Un domaine Windows 2000 n'a pas de PDC ni de BDC mais que des DC, ce qui facilite la tolérance de panne. ***En effet si l'on veut réaliser un premier pas vers un système de « sauvegarde » contre un crash, le mieux est de multiplier le nombre de Contrôleur de Domaine.***
Cependant il y a différent cas où il est important de restaurer un contrôleur de domaine ainsi que l'architecture Active Directory.

Le contrôleur de domaine Windows 2000 détient une copie de l'annuaire Active Directory, c'est le point qui peut nous amener à réaliser une restauration. Si par exemple une modification dans l'annuaire a été réalisée maladroitement ou via une infection, il est intéressant de pouvoir revenir en arrière.

Dans ce document nous décrirons quatre points : la sauvegarde du contrôleur de domaine puis trois méthode afin de restaurer un contrôleur de domaine, suivant le contexte.

Toutes les manipulations suivantes se feront grâce à l'utilitaire windows ***ntbackup***, qui ce lance en tapant tous simplement ***ntbackup*** dans le menu exécuter.

SAUVEGARDE

Pour ne sauvegarder que les donné utile à la restauration du DC il suffit de cocher « **Etat du système** » ce qui aura donc pour effet de sauvegarder tout les composants utiles à la restauration d'un DC.

Sur un contrôleur de domaine, "**état du système**" inclut,

- **Active Directory**,
- le dossier **SYSVOL** *(Sysvol est un répertoire partagé qui stocke la copie serveur des fichiers publics du domaine, qui sont répliqués entre tous les contrôleurs de domaine du domaine)*
- le **registre**
- les **fichiers de démarrage système**,
- la **base d'enregistrement de classes**
- si le contrôleur de domaine géré est un serveur de certificats, la **base de donnée de certificats**.

Ensuite il faut choisir le nom du fichier de destination puis cliquer sur « démarrer » et encore sur **Démarrer la sauvegarde**.

TOMBSTONE LIFETIME

Après la suppression d'un objet Active Directory, le système le maintient pendant une durée appelé tombstone lifetime. Après ce temps le système les l'enlève d'une façon permanente.

En restaurant l'Etat du Système, votre restauration doit tenir compte du fait que l'âge de votre sauvegarde ne doit pas dépasser le Tombstone Lifetime de l'annuaire Active Directory (par défaut il est de 60 jours). Si une sauvegarde plus vieille que la date de tombstone lifetime est restaurée, ntbackup rejettera toutes les données comme dépassé.
Par conséquent il est très important de faire des sauvegardes très régulièrement.

LA RESTAURATION

Il existe trois méthode pour restaurer un DC : **autoritaire (authoritative)**, **non-autoritaire (non-authoritative)** et **primaire (primary)**, par défaut la restauration est non-autoritaire.

Lorsque l'on parlera du « Mode de restauration Active Directory », il s'agira en fait d'appuyer sur la touche F8 au démarrage de l'ordinateur et de sélectionner le mode approprié. **Toutes les opérations de restauration doivent impérativement ce faire dans ce mode.**

RESTAURATION NON-AUTORITAIRE

Exécuter une **restauration non-autoritaire** quand au moins un autre DC dans le domaine est disponible.
Ne pas exécuter quand il n'y a plus de DC en fonctionnement.
En utilisant une restauration non-autoritaire, le DC reçoit les données Sysvol d'un autre DC vivant ; l'architecture Active Directory n'est pas restaurée, on garde celle qui est en fonctionnement.
Ce type de restauration néglige donc toutes les données Sysvol sauvegardées.

Procédure :

1- Booter en **Mode de restauration Active Directory**
2- Quand le PC démarre exécuter ***ntbackup*** (cliquer démarrer, puis executer, et taper ntbackup)
3- Cliquer sur **l'assistant de restauration**, puis sur suivant. Importer votre media, puis sélectionner et cocher l'entré « **état du système** », puis cliquer sur suivant.
4- Cliquer sur Terminer
5- Quand la procédure de restauration est fini, une boite de dialogue apparaît demandant de **redémarrer**, valider.
6- La restauration Terminé

RESTAURATION AUTORITAIRE

Exécuter une restauration autoritaire quand vous avez effacé accidentellement des données de Sysvol, et que cet effacement a été propagé sur tous les DC de domaine.
Si vous avez modifié votre architecture Active Directory, il est possible de revenir à une version antérieur à celle courante.
Ne pas exécuter une restauration autoritaire si le DC est le seul DC du domaine.
Les changements restaurés sur le DC seront automatiquement répliqués sur tous les DC de votre domaine.

Pour une restauration autoritaire, nous suivront la même procédure qu'en mode non-autoritaire, mais il faut annuler le redémarrage de la machine et exécuter ***ntdsutil***.

Par exemple, nous avons supprimer une OU et nous souhaitons la restaurer. Si nous utilisons une restauration non-autoritaire, les données seront récupéré des autres serveurs, ayant eux aussi l'OU supprimé, *c'est donc une mauvaise manipulation*

Ndsutils va nous permettre de marquer des objets dans Active Directory comme autoritaire. En fait chaque objet AD possède un numéro de version qui s'incrémente lors de changements et de mises à jour. Si on marque un objet comme autoritaire, son identifiant de version s'incrément de 100 000. Lorsque deux contrôleurs de domaine possèdent des numéros de version différents pour un même objet, celui qui possède l'identifiant le plus élevé est autoritaire et se réplique par dessus l'autre copie de l'objet.

Procédure :

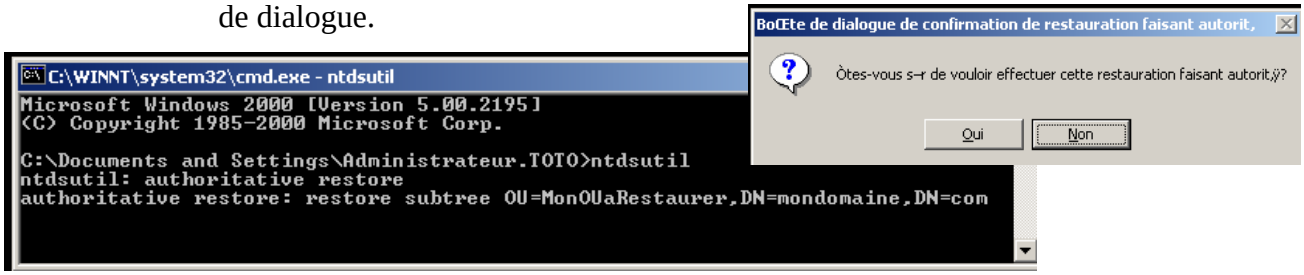
1- Booter en Mode de restauration Active Directory
2- Quand le PC démarre exécuter ntbackup (cliquer démarrer, puis executer, et taper ntbackup)
3- Cliquer sur l'assistant de restauration, puis sur suivant. Importer votre media, puis selectionner et cocher l'entré « état du système », puis cliquer sur suivant.
4- Cliquer sur Terminer
5- Quand la procédure de restauration est fini, une boite de dialogue apparaît demandant de redémarrer, ***Annuler*****.**

Ntdsutils

6- lancer une fenêtre MSDOS
7- taper au prompt **ntdsutil**, puis saisissez **authoritative restore**
8- Il est important de connaître le nom de l'objet a restaurer ou bien vous pouvez faire une restauration de l'ensemble de l'annuaire.

Pour une aide des commande a taper vous pouvez utiliser « ? »

Si vous voulez **restaurer une OU** utiliser la commande **restore subtree** et spécifier le chemin LDAP de l'OU, c'est-à-dire son DN (Distinguish Name). Puis valider la boite de dialogue.



Si vous voulez **restaurer tout l'arbre** de l'architecture Active Directory, vous pouvez taper **restore database.**

9- Pour quitter cet utilitaire utiliser la commande **quit**
10- Vous pouvez redémarrer, et la restauration est terminé

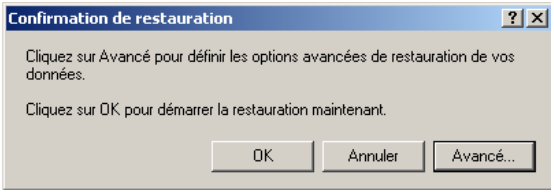
RESTAURATION PRIMAIRE

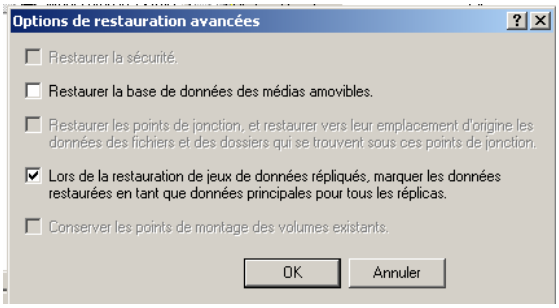
Utiliser la **restauration primaire (primary**) quand tous les DC de votre domaine sont perdus, et que vous voulez reconstruire le domaine de vos sauvegardes.
Ne pas exécuter ce type de restauration si il reste un DC de disponible.
Utiliser la restauration primaire pour le premier DC puis sur les autres DC exécuter en mode non autoritaire.
Bien sûr, lorsque dans un domaine il n'y a qu'un seul DC et que celui-ci vient à tomber, c'est ce type de restauration qu'il faut utiliser.

Procédure :

1- Booter en **Mode de restauration Active Directory**
2- Quand le PC démarre exécuter ***ntbackup*** (cliquer démarrer, puis executer, et taper ntbackup)
3- Ne pas se mettre en mode assistance de restauration, cliquer sur l'**onglet restauration**.
4- Faite un clique droit sur fichier, puis **fichier catalogue** et sélectionner votre sauvegarde.
5- Cocher **l'état du système**

6- **Démarrer** la sauvegarde, puis **valider** la première boite de dialogue
7- Sur la seconde boite de dialogue, cliquer sur **avancer** afin de déterminer le mode primary.
Dans les options avancées **sélectionnées** l'option pour marquer les données comme principale, comme sur l'image ci-dessous





8- Valider jusqu'à la fin, l'opération de restauration s'effectue, redémarrer et c'est terminé.

SAUVEGARDE ET RESTAURATION D'UN SYTEME WINDOWS SANS DC

Par rapport à toutes les manipulations qui on été faite, sauvegarder un système autre qu'un DC ne pose aucune complication.

Cependant pour une restauration d'un système windows autre qu'un DC il n'y a pas besoin de redémarrer en mode de restauration Active Directory.
Cet technique fonctionne aussi bien avec des serveurs, qu'avec des postes clients comme windows 2000 pro et Windows XP pro.

LIENS UTILES

White paper sur Windows 2000 Server Disaster Recovery Guidelines, *document très intéressant et explicatif :*
http://www.microsoft.com/windows2000/techinfo/administration/fileandprint/recovery.asp

Sauvegarder et restaurer Active Directory, *document en français mais succin.*
http://www.laboratoire-microsoft.org/articles/win/ad_sauve/

« Comment faire » de Microsoft : Réalisation d'une copie de sauvegarde complète du système d'exploitation Windows 2000 Server
http://support.microsoft.com/default.aspx?scid=kb;fr;328150

Securing Windows 2000 Active Directory - Backup and Restoration
http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_3__Backup_and_Restoration.html

Authoritative, primary, and normal restores
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/18f89932-80ee-4b50-9a1f-698cada42ccc.mspx