

# Base de connaissances

## Explorer la base NTDS.DIT de votre domaine Active Directory

with one comment

### Avant-propos

Dans Windows serveur 2008/2008 R2, il est possible d'effectuer des snapshots des volumes contenant la base de donnée de l'Active Directory et les fichiers des journaux. Une fois que l'on aura fait un instantané, on pourra exposer la base de donnée de l'Active Directory stockée dans l'instantané.

L'ensemble des informations d'un domaine Active Directory sont contenu dans un fichier de base de données nommé NTDS.DIT. Ces informations seront disponibles « hors ligne », autrement dit on va pouvoir regarder la base de donnée en se connectant à notre instantané.

### Outils

Dans cet article, nous aurons besoin de deux outils, [Ntdsutil.exe](#) et [Dsamain.exe](#). Ces outils sont disponibles si vous avez installé les services AD DS ou AD LDS, autrement dit Active Directory. Dans notre cas, l'un ne va pas sans l'autre. Ils ont besoin tout deux des droits administrateurs pour s'exécuter correctement.

### Manipulations

#### Monter une sauvegarde de la base

1. Lancez une invite de commande en tant qu'administrateur
2. Tapez la commande *Ntdsutil snapshot*
3. Entrez *List All*

4. Tapez *Mount 1*.

## Charger la base NTDS.DIT

Dans une invite de commande lancez en tant qu'administrateur, tapez la commande  
`dsamain -dbpath C:\$SNAP__VOLUME{C}\Windows\NTDS\ntds.dit -ldapport 3000`

## Explorer les données en LDAP

1. Lancez *LDP.exe*
2. Cliquez sur *Connection > Connect*
3. Changer le port en *3000*
4. Cliquez sur *View > Tree*

Il vous sera dès lors possible d'explorer la base NTDS.DIT de votre domaine Active Directory hors ligne.

Olivier

Written by olivier

24 mai 2013 à 10:42

Publié dans [Administration](#), [Microsoft](#)

Tagged with [Active Directory](#), [Windows Serveur 2008](#)

## Une Réponse

Subscribe to comments with [RSS](#).

Merci pour ton tutoriel

**Makeln**

13 février 2014 at [10:10](#)

[Réponse](#)

**Créez un site Web ou un blog gratuitement sur WordPress.com.**