Microsoft

Base de registre

TP Installation système d'exploitation

Lionel POZET
[Date]

La **base de registre** (**BDR**) est une base de données utilisée par le système d'exploitation Windows. Elle contient les données de configuration du système d'exploitation et des autres logiciels installés désirant s'en servir.

Le plus souvent, les utilisateurs modifient la base de registre de façon transparente, via une interface graphique. Il existe des cas où aucune interface graphique n'est prévue : il est alors nécessaire d'utiliser l'outil Regedit, mais dans ce cas, il n'y a pas de garde-fou, le logiciel ne vérifie aucun des paramètres modifiés par l'utilisateur, qui peut donc endommager le système.

Utilitaire *regedit*

L'interface graphique actuelle de `regedit` de Microsoft permet de :

- Modifier la base de registre
- D'attribuer des droits spécifiques sur les clés de la base registre; l'interface graphique pour modifier les droits est semblable à celle qui permet de modifier les droits NTFS.

Répertoire de la base de registre

Par défaut, c'est dans le répertoire `%SystemRoot%\System32\Config` que sont stockés les fichiers de ruche suivants :

- *Components*
- *default*
- *SAM* (Security Account Manager)
- *Security*
- *Software*
- *System*

Les informations concernant un utilisateur sont stockées dans le répertoire correspondant à la variable d'environnement `%UserProfile%`. Par exemple, pour un utilisateur dont le login est "dupont", la valeur `%UserProfile%` sera par défaut `"C:\Documents and settings\dupont"`. Il y a un fichier de ruche `NTUSER.DAT` par utilisateur.

Le répertoire `%SystemRoot%\repair` contient une sauvegarde de la base de registre ; elle est utilisée par Windows pour certains cas de figure. De plus, sous Windows XP, la restauration du système les stocke dans le répertoire `\System Volume Information` du disque système.

Des fichiers journaux (extension .LOG) et des fichiers de sauvegarde (extension .SAV) sont utilisés en interne par Windows pour pallier des coupures de courant intempestives ou toute autre forme d'arrêt brutal.

Les emplacements physiques des différentes ruches utilisées lors du dernier boot sont indiqués sous la clé *hivelist* de *[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control*.

Le contenu de la base de registre

2 Hkey de base

La base de registre est partagée en différentes sections logiques. Elles sont généralement connues par les noms les définissant quand on y accède via l'interface graphique de Windows; les noms commencent tous par 'HKEY' (une abréviation de *Handle to a KEY*, gestionnaire de clé).

Les 2 HKEY de base sont :

- *HKEY_LOCAL_MACHINE* (*HKLM*) contient les informations qui sont générales à tous les utilisateurs de l'ordinateur :
    - Matériel
    - Sécurité
    - SAM (Security Account Manager)
    - Logicielle, la sous-branche "Classes" correspond à *HKEY_CLASSES_ROOT*
    - Système, elle contient notamment la sous-branche *CurrentControlSet* (NB : *CurrentControlSet\Control\Class* contient des informations sur les classes).

- *HKEY_USERS* contient les informations spécifiques de chaque utilisateur. La sous-branche correspondant à l'utilisateur courant est l'équivalent de

Les 4 autres HKEY sont

- *HKEY_CURRENT_CONFIG* contient des informations qui sont mises à jour immédiatement, elles sont régénérées après chaque boot.

- *HKEY_CLASSES_ROOT* (*HKCR*) contient les informations sur les applications enregistrées ; cela inclut entre autres les associations entre extensions de fichiers et identifiants de classe d'objet OLE, ce qui permet de lancer automatiquement l'exécutable correspondant. Cela correspond à *HKEY_LOCAL_MACHINE\SOFTWARE\Classes*. Exemple : "*.bat*" et "*XML*" sont respectivement associés à "*batfile*" et "*XML script engine*".

- *HKEY_CURRENT_USER* (*HKCU*) contient les informations concernant l'utilisateur Attention, cette ruche n'est visible que si l'utilisateur associé est connecté

Chacune de ces clés est divisée en sous-clé(s), qui peuvent contenir d'autre(s) sous-clé(s) et ainsi de suite, constituant toute une arborescence.

Typage des valeurs

Chaque clé peut contenir des valeurs typées : il existe une quinzaine de types de données possibles, voici les plus courantes :

- Binaire *REG_BINARY*, création possible avec REGEDIT

- Entier :
  - *Dword REG_DWORD*, 32 bits, création possible avec REGEDIT
  - Qword *REG_QWORD* 64 bits, création possible avec REGEDIT

- Chaîne de caractères
  - Chaîne simple *REG_SZ*, création possible avec REGEDIT
  - Chaîne extensible *REG_EXPAND_SZ*, permet d'utiliser des variables d'environnement, création possible avec REGEDIT
  - Chaîne multiple *REG_MULTI_SZ*, création possible avec REGEDIT

- NONE, REG_NONE : signifie donnée non typée !

Minuscule et majuscule

Contrairement à ce qui est habituel sous Windows, des casses de caractères différentes donnent des résultats différents. Exemple : les valeurs "no" et "No" peuvent donner des résultats très différents.

Espace dans les noms de clés

Le caractère espace (" ") peut être utilisé dans les noms de clés, bien que ce soit rare (exemple : la clé optionnelle *Use Search Asst*).

Utilitaires en ligne de commande pour modifier la base de registre

L'utilitaire ***REG.EXE*** permet de faire toutes sortes d'opération sur les clefs de la base de registre, en ligne de commande. Il est donc parfaitement manageable. Il est en natif sur tous les postes.

Utilitaires pour supprimer les entrées inutilisées de la base de registre

Il existe aussi des logiciels pour éliminer les entrées inutilisées de la base de registre. Citons par exemple CCleaner

REMARQUE : Ces utilitaires ne sont pas validés par Microsoft et, tout pertinents qu'ils soient, rien ne garantit qu'ils ne perturberont pas le fonctionnement du système, comme rien ne prouve leur efficacité présumée. L'utilisateur reste seul responsable des inconvénients éventuels subis.

Le nettoyage de la base de registre repose sur plusieurs concepts génériques :

- Nombre de programmes utilisant la base de registre ne la nettoient pas lors de la désinstallation. On peut parler de désinstallation malpropre. Cela a pour effet de garder en mémoire des paramètres inutiles.
- La base de registre est moins rapide au fur et à mesure de son accroissement.
- Certaines entrées peuvent devenir obsolètes au fur et à mesure de la vie du poste et de mauvais interaction/update des programmes. Dans certains cas, des dll restent enregistrés alors que le fichier dll proprement dit n'existe plus. Une partie de l'algorithme des nettoyeurs de base de registre se fonde sur cette technique pour détecter les entrées périmées.