# BASE DE REGISTRE

- Apparition sous W3.X en remplacement des fichiers de configuration .ini. Elle sert à associer un fichier  avec l'application qui permet de le visualiser.
- Des la première version de NT, elle est étendue elle comprend un ensemble de clés hiérarchiques et de valeurs. La sauvegarde physique de la base  est  appelée “ruche”.
- Elle remplace aujourd’hui la plupart des fichiers de conf W exception faite du Boot.ini (XP)

Le Registre contient:

- les profils de chaque utilisateur de l'ordinateur
- les informations relatives au matériel du système, aux programmes et aux paramètres de propriétés.

Windows utilise  ces informations dès le démarrage du système et lors de son fonctionnement.

- Dans %SystemRoot%\System32\Config sont stockés les fichiers de ruche suivants :
  - Components
  - default
  - SAM (Security Account Manager)
  - Security
  - Software
  - System

# 2003/XP/2000/VISTA/SEVEN/2008

# INFORMATIONS UTILISATEUR

Les informations  utilisateur sont dans le répertoire correspondant à la variable d'environnement %UserProfile%.

Le fichier  NTUSER.DAT.

- HKEY_LOCAL_MACHINE (HKLM)  informations qui sont générales à tous les utilisateurs.
- HKEY_USERS  informations spécifiques à chaque utilisateur.
- HKEY_CURRENT_CONFIG  informations mises à jour immédiatement,  régénérées après chaque boot.
- HKEY_CLASSES_ROOT (HKCR)  informations sur les applications enregistrées (associations entre extensions de fichiers eidentifiants de classe d'objet OLE HKEY_CURRENT_USER (HKCU) informations concernant l'utilisateur connecté.  Sous-branche de HKEY_USERS.

# GESTIONNAIRE DE CLÉ

**Trois types de valeurs** :

Chaîne, Binaire, et DWORD

**Cinq types de données :**

REG_BINARY  Donnée binaire.

REG_DWORD Données par un nombre de quatre octets  est couramment utilisé pour les valeurs booléennes.

REG_EXPAND_SZ  Chaine de données extensible dont la chaîne contient une variable qui sera remplacée quand elle est appelée par une application.

REG_MULTI_SZ  Chaine multiple,  utilisé pour représenter les valeurs qui contiennent des valeurs de liste ou multiples, chaque entrée étant séparée par un caractère NULL.

REG_SZ  Chaine standard, valeurs de texte contrôlables.

# STRUCTURE DES CLÉS

# GUID / CLSID

Un grand nombre de clés et de valeurs de clés sont affichées par regedit sous un format analogue :

- GUID (Globally Unique IDentifier)
  16 octets

- CLSID sont utilisés uniquement pour différencier les classes des objets.

HKEY_CLASSES_ROOT\CLSID

- Run:  programmes à lancer au démarrage, après le lancement de l'Explorateur Windows.
- RunOnce : programmes qui ne se lancent qu'une fois (la clé est supprimée après le démarrage).
- RunService  programmes à lancer avant l'affichage du Bureau.
- RunOnceService  programmes qui ne servent qu'une fois, comme les scripts d'installation.

# CLÉS RUN

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

# CLÉS RUN

- Outil de consultation de la base de registre
- Permet l'accès en modification.
- Permet de faire une sauvegarde/restauration de la base de registre, partielle ou complète.

# OUTIL REGEDIT.

Sauvegarde automatique du registre a chaque mise a jour du système.

rstrui.exe.

Permet de voir la liste des points de restauration.

Sauvegarde manuelle de la clé avant modification.

# SECURITÉ

# UTILITAIRES DIVERS

- Nettoyer le registre.
  - RegCleaner
- Journaliser les modifications du registre
  - Regshot

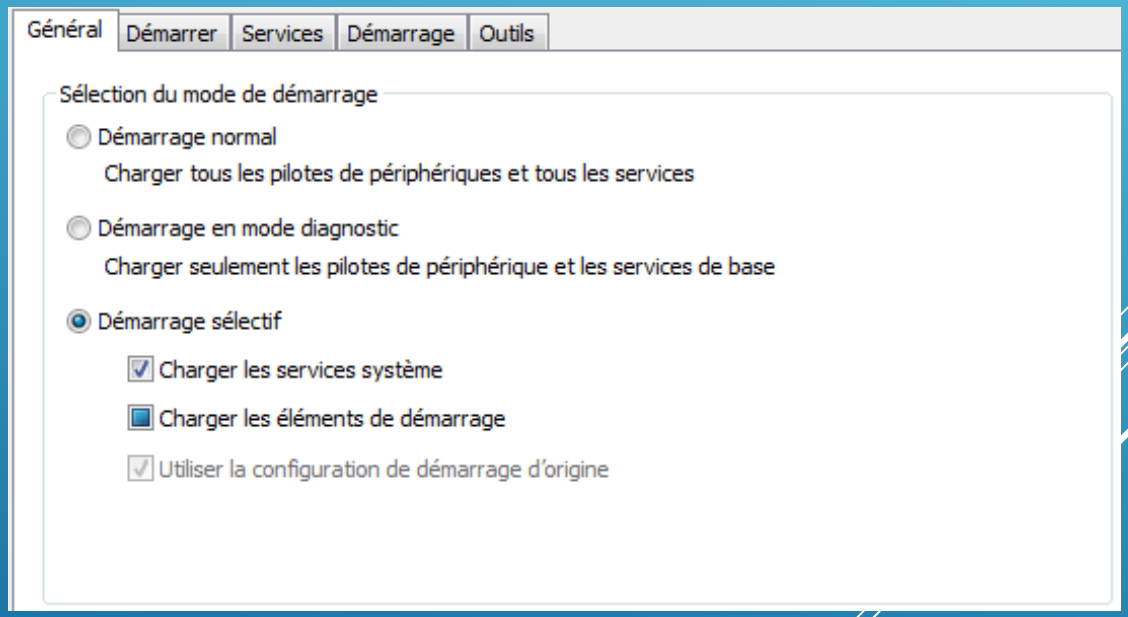
# MSCONFIG

l'éditeur de configuration système

Dans une session administrateur:

Menu Démarrer puis Exécuter et tapez msconfig.

- Onglet "Général"
- Onglet "SYSTEM.INI"
- Onglet "WIN.INI"
- Onglet "BOOT.INI"
- Onglet "Services"
- Onglet "Démarrage"




# L'OUTIL

- Démarrage normal

Windows va charger tous les pilotes de périphériques, programmes et services par défaut.

- Démarrage en mode diagnostic

Windows charge les périphériques et les services de base ainsi que le service RPC.

correspond au mode sans échec avec connexion réseau

- Démarrage en mode sélectif

Windows charge les pilotes, les services ou les programmes de votre choix.

# ONGLET GENERAL

Permet de configurer Windows au niveau de la machine.

Sous Windows 2000 ou XP compatibilité des anciens systèmes d'exploitation.

Absent sous Seven.

# ONGLET SYSTEM.INI

System.ini

Permet de configurer Windows au niveau de la machine.

Sous Windows 2000 ou XP compatibilité des anciens systèmes d'exploitation.

Absent sous Seven.

Win.ini

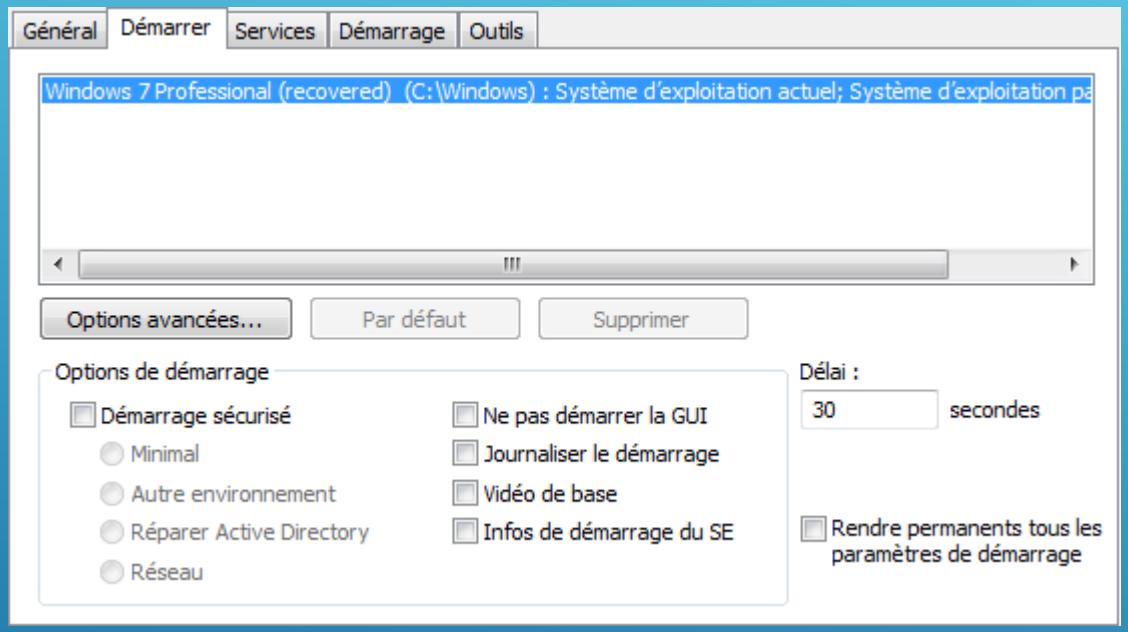
les paramètres relatifs à l'utilisateur.

Absent sous Seven

# ONGLETS SYSTEM.INI/WIN.INI

Configure le fichier **boot.ini** sous XP.

Configure le démarrage sous Vista Seven.

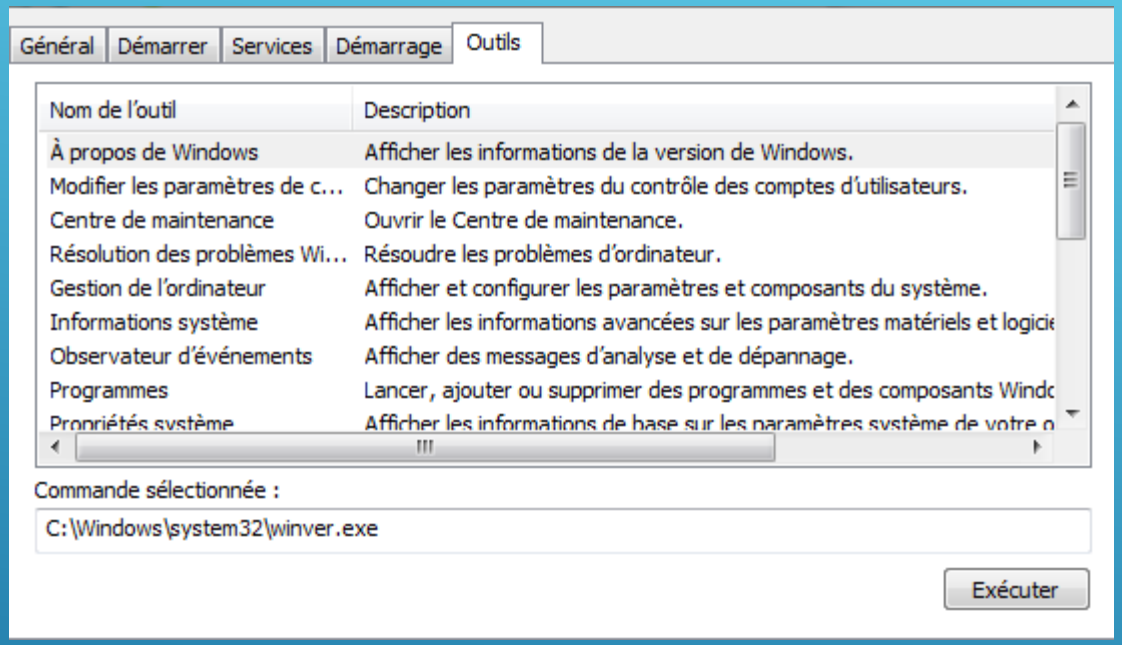



# ONGLET BOOT.INI / DÉMARRER

- Permet de voir les services qui sont lancés, arrêtés ou démarrés sur le système.
- Permet de voir les programmes qui se lancent au démarrage.

# ONGLETS SERVICES ET DÉMARRAGE

Accès a de nombreux outils systèmes.




# ONGLETS OUTILS