Introduction au Registre Windows XP

Complément de cours du module R3

IUT R&T 1ère année

David Mercier

Introduction (1/2)

Module R3 = administration des systèmes d'exploitation (SE), en particulier, administration d'un ensemble de postes gérés par un serveur.

Un des principaux SE est Windows.

En son cœur : une structure globale qui reprend :

- les informations système,
- ainsi que les informations des utilisateurs.

Cette base est appelée ***base de Registre (BDR)***, ou plus simplement, ***Registre***.

Introduction (2/2)

Nous ne détaillerons pas en profondeur cette structure complexe;

Simplement éclaircir certains points qui peuvent vous servir en tant qu'administrateur d'un parc de machines mises sur le réseau.

Nous vous demandons de connaître :

- la structure générale de cette base,
- son fonctionnement au travers de quelques outils ou tâches liées à l'administration.

Plan

- Accès au Registre
- Structure du Registre
- Utiliser le Registre
- Programmes facilitant la gestion du Registre

Plan

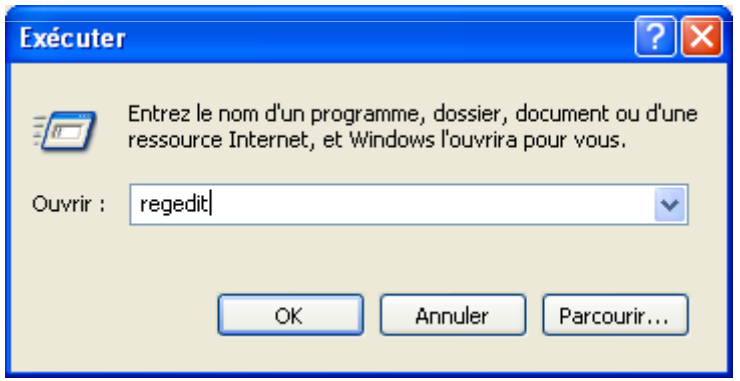
- Accès au Registre
- Structure du Registre
- Utiliser le Registre
- Programmes facilitant la gestion du Registre

Accès au Registre

Lecture et modification du contenu du Registre : un éditeur spécifique est nécessaire.

RegEdit = application dédiée.

- **Démarrer | Exécuter | regedit**



Remarque : il existe d'autres applications mieux outillées

- Exemples : Vilma registry explorer, RegCool, …

Plan

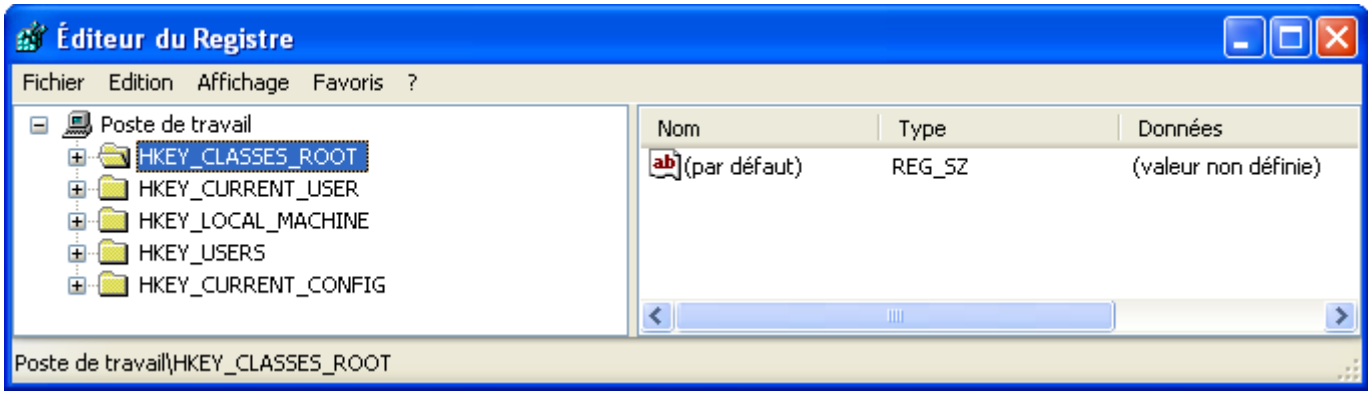
- Accès au Registre
- Structure du Registre
- Utiliser le Registre
- Programmes facilitant la gestion du Registre

Structure du Registre

Présentation

Le **Registre Windows** est séparé en deux volets :

- Volet de gauche : liste des clés, constituant des dossiers, contenant les entrées ou valeurs du Registre. Structure arborescente.
- Volet de droite : valeurs associées à la clé à gauche.

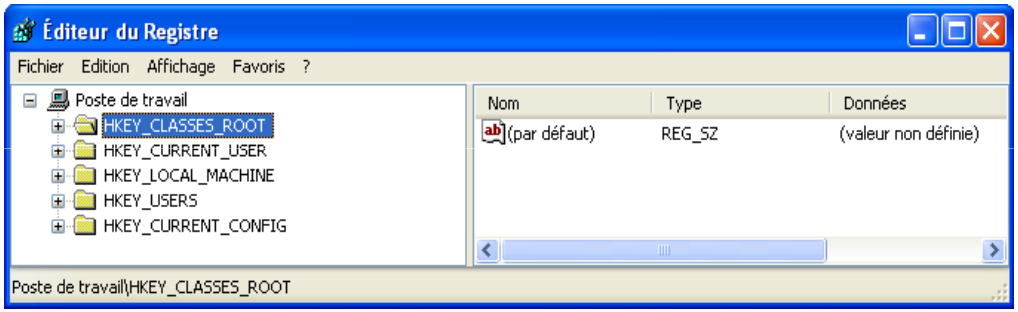


Structure du Registre

Les clés principales

Les clés principales sont :

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG



Chaque clé principale contient une arborescence de sous-clés qui renferment, à leur tour, de multiples ramifications.

Structure du Registre

Les clés principales et leurs alias

De ces 5 **branches**, seules les clés HKEY_LOCAL_MACHINE et HKEY_USERS ont une existence propre. Ces clés sont sauvegardées dans un certain nombre de fichiers système.

Clé principale	Clé miroir
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current	HKEY_CURRENT_CONFIG
Fusion de HKEY_LOCAL_MACHINE\Software\Classes et HKEY_CURRENT_USER\Software\Classes	HKEY_CLASSES_ROOT
HKEY_USERS\ < SID de l'utilisateur >	HKEY_CURRENT_USER

Remarque : un *SID (Security Identifier)* est une valeur unique permettant d'identifier un utilisateur ou un groupe d'utilisateurs. Certains SID ont des valeurs constantes.
Ex : S-1-5-18 : compte service utilisé par le système.

Structure du Registre

Les abréviations des clés principales

Clé principale	Abréviation utilisée
HKEY_LOCAL_MACHINE	HKLM
HKEY_CURRENT_USER	HKCU
HKEY_CURRENT_CONFIG	HKCC
HKEY_USERS	HKU
HKEY_CLASSES_ROOT	HKCR

Structure du Registre

La branche HKEY_CLASSES_ROOT (HKCR)

Cette clé permet le stockage des extensions de Shell, des composants OLE, des serveurs ActiveX ainsi que des informations de classe COM.

Remarques :

- ***Shell*** = coquille dans laquelle vient se loger un SE. En résumé, c'est ce qui définit l'apparence du système. Pour Windows, c'est l'explorateur.

MICROSOFT

- ***COM*** (*Component Object Model*) = modèle/standard de programmation pour le développement de composants réutilisables et communicants.
- ***OLE (Object Linking and Embedding)*** = architecture de communication inter-applications basée sur le modèle COM. C'est un protocole et un système d'objets distribués.
- ***ActiveX*** = désigne différentes technologies basées sur le modèle COM. Ex : contrôles ActiveX sur une page web (précédemment connus sous le nom de contrôles OLE).

Au début de cette clé, sont énumérées les extensions de fichiers.

Structure du Registre

La branche HKEY_CURRENT_USER (HKCU)

Cette clé gère les paramètres de l'utilisateur actif.

- HKCU\AppEvents : recense les évènements système et les sons correspondants (EventLabels);
- HKCU\Console : définit les paramètres de la console permettant l'accès à l'invite de commande;
- HKCU\Control Panel : gère l'ensemble des paramètres définis dans le panneau de configuration;
- HKCU\Environment : définit les variables d'environnement appliquées au Shell et à l'invite de commande;
- HKCU\Keyboard Layout : définit la configuration du clavier;
- HKCU\Printers : les paramètres d'impression;
- HKCU\Software : liste des applications installées sur la machine.

Structure du Registre

La branche HKEY_LOCAL_MACHINE (HKLM)

Cette clé gère les paramètres matériels.

- HKLM\HARDWARE : contient les informations concernant les composants matériels et les périphériques installés;
- HKLM\SAM (Security Account Manager) : paramètres de sécurité des comptes utilisateurs;
- HKLM\SECURITY : définit les paramètres de sécurité locale;
- HKLM\SOFTWARE : liste des applications installées sur la machine;
- HKLM\SYSTEM : définit les services et les pilotes périphériques ainsi que les options de configuration du système.

Structure du Registre

Les branches HKU et HKCC

La branche HKU contient autant de sous-clés que d'utilisateurs déclarés sur la machine.

La branche HKCC contient des informations sur le profil matériel utilisé par l'ordinateur local au démarrage.

Exemple : informations utilisées pour configurer les pilotes de périphérique à charger et la résolution d'écran à adopter.

Rappel : c'est une copie de HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current

Structure du Registre

Les fichiers de ruche

Le Registre est stocké dans un certains nombre de fichiers, appelés des **ruches** (*hives* en anglais).

Rangés dans \Windows\system32\config, on trouve :

Nom du fichier de ruche	Branche associée dans le Registre
Default	HKU\.Default
SAM	HKLM\SAM
Security	HKLM\Security
Software	HKLM\Software
System	HKLM\System

L'arborescence HKCU se trouve dans le fichier Ntuser.dat, présent pour chaque profil utilisateur dans : \Documents and Settings\ Nom_utilisateur

Structure du Registre

Les valeurs

Il existe différents types de valeurs. Voici la liste des plus courantes :

Nom de la valeur	Abréviation utilisée	Description
Valeur chaîne	REG_SZ	Texte ou valeurs booléennes (No pour FAUX et Yes pour VRAI).
Valeur binaire	REG_BINARY	Suites d'octets pouvant être cryptées.
Valeur DWORD	REG_DWORD	Valeurs booléennes (0 pour FAUX et 1 pour VRAI) ou valeurs numériques au format hexadécimal codées sur 32 bits.
Valeur de chaîne multiple	REG_MULTI_SZ	Listes de chaînes séparées par le caractère ASCII zéro
Valeur de chaîne extensible	REG_EXPAND_SZ	Enregistre des données sous forme de variables dont le système assurera la traduction.

Structure du Registre

Quelques variables système

Nom de la variable	Emplacement correspondant dans l'Explorateur
%systemroot%	Répertoire Windows (ex C:\Windows, D:\windows).
%SystemDrive%	Lettre du lecteur racine sur laquelle Windows est installé.
%ProgramFiles%	\Program Files
%Userprofile%	\Documents and Settings\Nom_de_l'utilisateur
%AllUsersProfile%	L'emplacement du répertoire All Users

Plan

- Accès au Registre
- Structure du Registre
- Utiliser le Registre
- Programmes facilitant la gestion du Registre

Utiliser le Registre

Créer/Supprimer/Renommer une clé ou une valeur

Créer une clé :

- **Edition** | **Nouveau** | **Clé**
- Ou bouton droit souris **Nouveau** | **Clé**

Créer une valeur :

- **Edition** | **Nouveau** | **Valeur…**
- Ou bouton droit souris **Nouveau** | **Valeur…**

Renommer | supprimer :

- **Edition** | **Renommer** ou bouton droit souris **Renommer** ou **F2**
- **Edition** | **Supprimer** ou bouton droit souris **Supprimer** ou **Suppr**

Utiliser le Registre

Remarques

Modifier le Registre : Quels sont les risques ?

- Aucun risque lié à la création d'une multitude de clés.
- En revanche, il est dangereux de supprimer des clés que l'on n'a pas créées.

Respect de la casse ?

- Non, l'emploi des majuscules et minuscules assurent simplement une meilleure visibilité des noms de clés et valeurs.

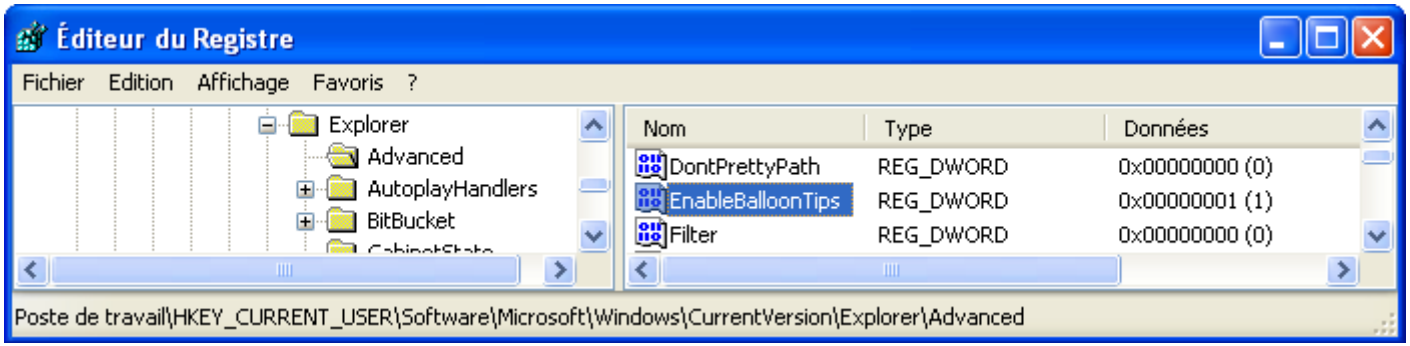
Utiliser le Registre

Modifier une valeur : un exemple

Pour certains, les info-bulles deviennent vite agaçantes, en effet, il faut presque à chaque fois les fermer…

Voici une solution utilisant le registre pour les désactiver.

- Rendez vous à la clé **HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Explorer\Advanced**
- L'entrée en charge de la gestion des infos-bulles est la suivante :
  - Nom : **EnableBalloonTips**,
  - Type **: DWORD**,
  - la valeur **0** désactive les infos-bulles, la valeur **1** les active.



Utiliser le Registre

Appliquer les modifications apportées au Registre

Plusieurs solutions

Méthode 1

- F5

Méthode 2

- Ouvrir le gestionnaire des tâches (Ctrl+Alt+Suppr),
- Terminer le processus **explorer.exe,**
- En passant par le menu **Fichier | Nouvelle tâche (Exécuter...)**, relancer **explorer**.

Méthode 3

- Lancer la commande :
  - RUNDLL32.EXE USER32.DLL,UpdatePerUserSystemParameters ,1 ,True

Méthode 4

- En dernier recours, fermer puis ouvrir à nouveau la session.

Utiliser le Registre

Sauvegarder le registre

Pas de fonction « annuler » dans le Registre = il faut **sauvegarder !**

Ouvrir l'arborescence que vous voulez enregistrer. Puis :

- **Fichier** | **Exporter** ou clic droit **Exporter**

Enregistrer avec une extension .reg

Observation de cette structure de fichier…

Utiliser le Registre

Syntaxe des fichiers REG : exemple

Fichier .reg

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\test]
@="données de la valeur"
"Chaîne"="Test"
"DWORD"=dword:0000000b
"Binaire"=hex:01,02,03,aa
"Chaîne multiple"=hex(7):4c,00,69,00,67,00,6e,00,65,00,\
20,00,31,00,00,00,4c,00,69,00,67,00,6e,00,65,00,20,00,\
32,00,00,00,4c,00,69,00,67,00,6e,00,65,00,20,00,33,00,\
00,00,00,00
"Chaîne extensible"=hex(2):25,00,53,00,79,00,73,00,74,\
00,65,00,6d,00,52,00,6f,00,6f,00,74,00,25,00,00,00
```

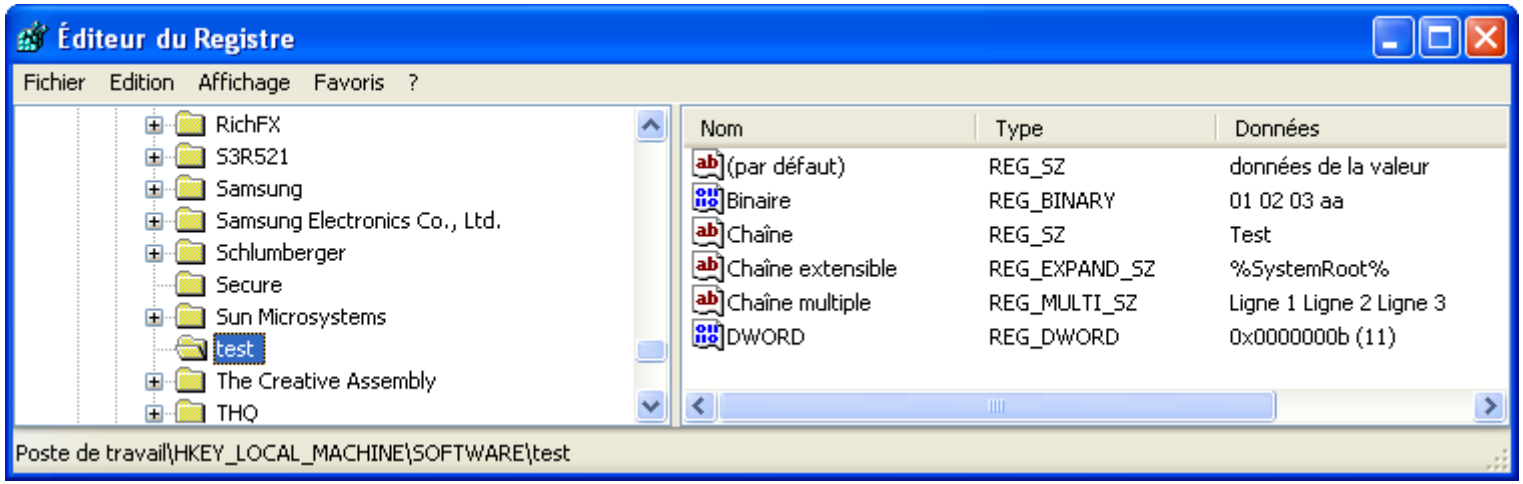
Version regedit

Ajout clé

Données valeur par défaut

Valeur | type | données

Résultat fusion



Utiliser le Registre

Syntaxe des fichiers REG : grandes lignes

Grandes lignes des fichiers REG

- Type valeur chaîne non précisé;
- Données de type DWORD en hexadécimale;
- Valeurs binaires indiquées en utilisant la notation : hex:
- Valeurs de chaîne multiple indiquées en utilisant la notation : hex(7):
- Valeurs de chaîne extensible indiquées en utilisant la notation : hex(2):
- lignes en notation hexadécimale sont continuées en utilisant le signe \
- Valeurs de chaîne multiple : retour à la ligne = 00
- Toutes les lignes sont codées avec code ASCII en hexadécimale : 25,53,79,73,74,65,6d,52,6f,6f,74,25,00 = % S y s t e m R o o t % avec particularité : caractères codés sur deux octets, il faut donc redoubler chaque valeur : 25 devient donc : 25,00; 00 devient donc : 00,00.

Utiliser le Registre

Syntaxe des fichiers REG : suppression

Supprimer une clé = une arborescence

- [-HKEY_LOCAL_MACHINE\SOFTWARE\test]

Supprimer une entrée

- "nom_de_la_valeur"=-

Utiliser le Registre

Un mot sur les fichiers INF

Quelles différences entre les fichiers REG et fichiers INF ?

- Fichier REG permet de modifier, ajouter ou supprimer des clés de la base de registre;
- Fichier INF permet en plus l'ajout ou la copie de fichiers depuis un répertoire source vers un répertoire destination.

Fichiers INF

- organisés en plusieurs sections associées à des fonctions particulières allant de la gestion des fichiers jusqu'à la modification de la base de registres.
- Respectent les règles suivantes :
  - Les sections commencent avec un nom de section entouré de crochets.
  - La section [Version] identifie la compatibilité
  - L'utilisation de variable est possible en utilisant la syntaxe %nom_de_la_variable%. Les variables sont définies dans la section [Strings]. Pour utiliser le caractère % dans une chaîne, il faut utiliser la syntaxe suivante : %%

Utiliser le Registre

Fichiers INF : applications

Installation d'un driver (Détection d'un nouveau périphérique), ou d'un module Windows.

Installation automatique d'un programme (notamment pour installer un programme à l'insu d'un utilisateur).

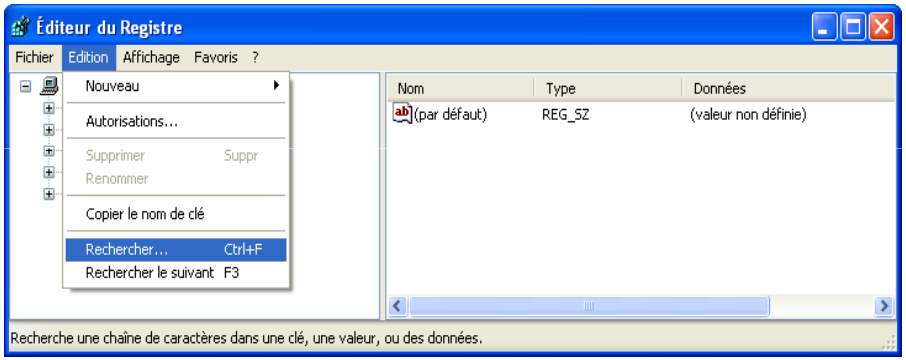
Modification d'une entrée dans la base de registre lors du script de connexion.

Utiliser le Registre

Lancer une recherche dans le Registre

La fonction de recherche de clefs, de valeurs et de données, se fait par le menu :

- **Edition** | **Rechercher** (ou Ctrl + F)



F3 permet de chercher l'occurrence suivante.

Regedit n'est pas capable de rechercher une donnée par son type (par ex REG_DWORD ou REG_BINARY). Pour contourner cette limitation :

- Exporter la base de registre ou la branche de la base de registre dans un fichier REG.
- Recherche sur ce fichier grâce à un simple éditeur de texte.

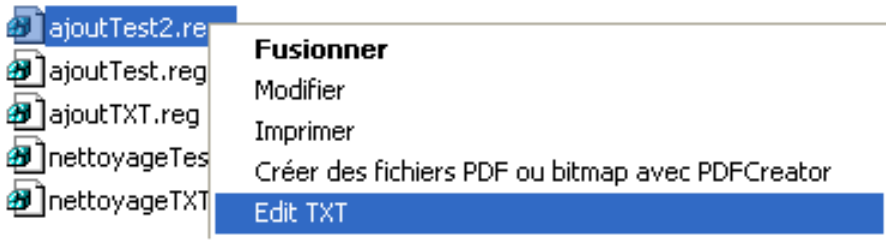
Utiliser le Registre

Exercice 1

Énoncé

- Lorsqu'un fichier n'est pas associé à un programme il est difficile de le consulter, il faut passer par "ouvrir avec", puis parcourir tous les programmes, en choisir un, confirmer ...
- Nous vous proposons d'écrire un fichier REG qui va ajouter "Edit TXT" pour tous les fichiers dans le menu contextuel de l'explorateur Windows simplement en cliquant droit sur le fichier

Objectif :



Utiliser le Registre

Exercice 1 : solution

Proposer une solution

- Dans quelle partie de la base de registre allez-vous travailler ?
- Pour quel type de fichiers souhaitez-vous offrir cette possibilités ?
- Que s'agit-il de faire ?
- Que devez-vous faire ?

Utiliser le Registre

Exercice 1 : solution

Proposer une solution

- Dans quelle partie de la base de registre allez-vous travailler ? HKCR
- Pour quel type de fichiers souhaitez-vous offrir cette possibilités ? TOUS => *
- Que s'agit-il de faire ? Proposez une nouvelle possibilité d'exécution du fichier à l'aide d'une commande => SHELL
- Que devez-vous faire ? Exécuter notepad sur le fichier (%1 paramètre) pour l'ouvrir

Utiliser le Registre

Exercice 1 : solution

Proposer une solution

- Dans quelle partie de la base de registre allez-vous travailler ? HKCR
- Pour quel type de fichiers souhaitez-vous offrir cette possibilités ? TOUS => *
- Que s'agit-il de faire ? Proposez une nouvelle possibilité d'exécution du fichier à l'aide d'une commande => SHELL
- Que devez-vous faire ? Exécuter notepad sur le fichier (%1 paramètre) pour l'ouvrir

Fichier .reg

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\*\shell]
[HKEY_CLASSES_ROOT\*\shell\EditeurTXT]
@="Edit TXT"
[HKEY_CLASSES_ROOT\*\shell\EditeurTXT\command]
@="notepad %1"
```

Utiliser le Registre

Exercice 1 : exemple de nettoyage solution

Fichier .reg

```
Windows Registry Editor Version 5.00
[-HKEY_CLASSES_ROOT\*\shell\EditeurTXT]
```

Utiliser le Registre

Exercice 2 : Lancer une application que vous avez créé

Énoncé

- Créer un fichier REG, qui lance le programme GetFileName (programme que vous avez créé et qui copie le chemin absolu du fichier dans le presse-papier), permettant ainsi la création de la fonction « Récupérer le nom » dans le menu contextuel de l'explorateur Windows en cliquant droit sur un fichier.

Solution

- À trouver

Utiliser le Registre

Exercice 3 (à faire en TP) : Installation d'un logiciel

Énoncé

- Installer Paint Shop Pro 7 sur le client pour un utilisateur;
- Modifier le Registre du client pour que cela fonctionne pour tous les utilisateurs.
- L'installer sur le serveur, sur D:\Volume\logiciels\ et l'exécuter depuis le client.
- Automatiser la mise à jour de la clé registre utilisateur à l'ouverture de session

Utiliser le Registre

Exercice 3 (à faire en TP) : Installation d'un logiciel

Énoncé

- Installer Paint Shop Pro 7 sur le client pour un utilisateur;
- Modifier le Registre du client pour que cela fonctionne pour tous les utilisateurs. Regarder les fichiers modifiés par l'installation et faire la même chose pour « All Users ».
- L'installer sur le serveur, sur D:\Volume\logiciels\ et l'exécuter depuis le client. Créer un fichier REG modifiant chemin dans la base de registre
- Automatiser la mise à jour de la clé registre utilisateur à l'ouverture de session. Script

Utiliser le Registre

Restaurer le registre

En sens inverse, fonction Importer = fusion du contenu d'un fichier .reg avec le Registre.

Si le système ne démarre pas :

- Il faut accéder au 'DOS', soit avec une disquette de boot, soit au démarrage du système, ou appuyer sur [F8] pour avoir accès au 'DOS'.
- A l'invite système c: , Tapez : scanreg /restore.
- Une fenêtre s'ouvre et vous demande quelle sauvegarde vous souhaitez restaurer. Sélectionnez votre sauvegarde et validez.
- Rebootez la machine, afin de prendre en compte la mise à jour.

Windows XP possède aussi des points de restauration

Utiliser le Registre

Points de restauration Windows XP

Vérifier le service

- Le service suivant doit être démarré automatiquement.
- **Démarrer** | **Exécuter** | **services.msc**

Créer un point de restauration :

- **Démarrer** | **Programmes** | **Accessoires** | **Outils système** | **Restauration du système**
- Sélectionner Créer un point de restauration

Restaurer un point de restauration :

- **Démarrer** | **Programmes** | **Accessoires** | **Outils système** | **Restauration du système**
- Sélectionner Restaurer mon ordinateur à une heure antérieure,
- Choisir dans le calendrier affiché la date du point de restauration (à gauche),
- Choisir dans la liste de droite (si un choix est possible) le point de restauration précis
- Le système va redémarrer pour restaurer les fichiers systèmes modifiés.

Attention : création des points de restauration = place sur le disque dur

Plan

- Accès au Registre
- Structure du Registre
- Utiliser le Registre
- Programmes facilitant la gestion du Registre

Quelques Programmes

Regmon.exe

- Permet d'afficher en temps réel l'activité du Registre.

RegCleaner.exe

- Permet de nettoyer le Registre de façon automatique ou avancée.

RegShot.exe

- Permet de prendre deux clichés du Registre afin de pouvoir les comparer.
- Bon complément à Regmon quand certains logiciels refusent de fonctionner avec Regmon en arrière-plan.

D'autres programmes sont présentés sur votre feuille de TD

Bibliographie

Comment en savoir plus ?

Le Registre de Windows XP, J. Anderruthy, micro application, 2005.

Le Registre de Windows XP, Webastuces sarl, Micro Application, 2002.

http://leregistre-fr.net/ http://www.secretswindows.com

http://www.pctools.com/guides/registry/

Fin

Merci de votre attention,

Résumé BDR

Le **Registre Windows (BDR)** est une base de données utilisée par le système d'exploitation Windows, contenant :

- les données de configuration de Windows,
- les données de configuration des autres logiciels installés sur la machine,
- les données de gestion du matériel
  - exemple : le pilotage des périphériques (processeur, BIOS, cartes PCI),
- les profils et préférences des utilisateurs,
- et plein d'autres choses… (des données de sécurité, etc…)

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

Historique

La BDR est apparue véritablement avec Windows 95, bien qu'un peu présente sous Windows 3.x.

Par rapport à Windows 3.x, la BDR présente l'immense avantage de pouvoir se débarrasser des fameux fichiers «***.ini** »

⟹ Besoin de « rangement », de mettre en ordre les fichiers de configuration du système.

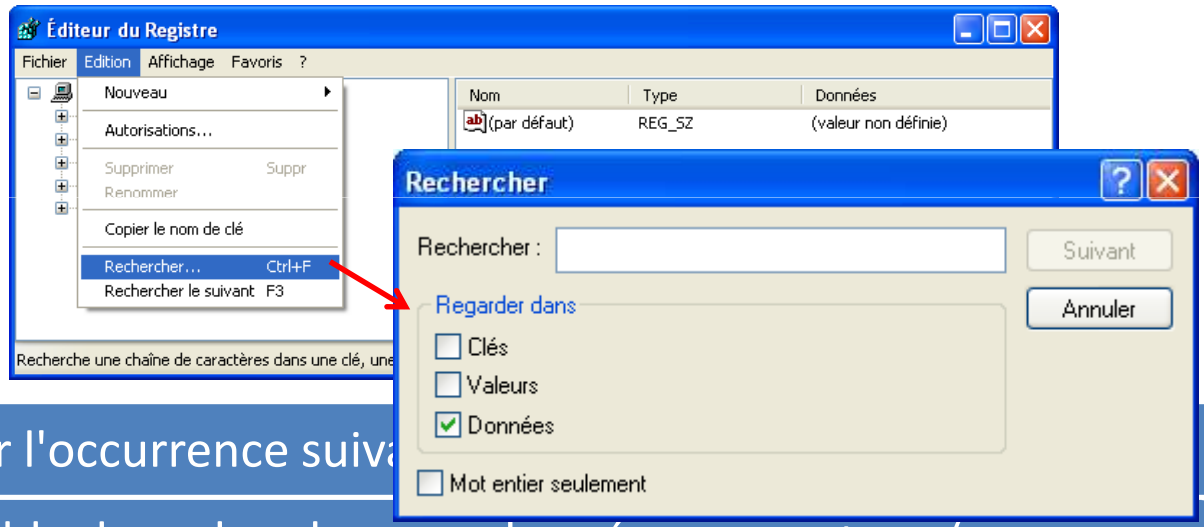
Remarque : pour des raisons de compatibilité descendante avec les anciennes applications, quelques fichiers .ini demeurent, néanmoins les programmes spécifiquement écrits pour Windows 9x/XP n'y ont en principe plus recours.

Utiliser le Registre

Lancer une recherche dans le Registre

La fonction de recherche de clefs, de valeurs et de données, se fait par le menu :

- **Edition** | **Rechercher** (ou Ctrl + F)



F3 permet de chercher l'occurrence suiva

Regedit n'est pas capable de rechercher une donnée par son type (par ex REG_DWORD ou REG_BINARY). Pour contourner cette limitation :

- Exporter la base de registre ou la branche de la base de registre dans un fichier REG.
- Recherche sur ce fichier grâce à un simple éditeur de texte.