République du Sénégal

***Un peuple-Un but -Une Foi***

**Ministère de l’Enseignement Supérieur de la Recherche et de l’Innovation**

****

**GROUPE ISM**

**SOUTENANCE LICENCE 1**

**PSE**

**L1B GLRS**

**MODÉRATEURS:**

**Kokou Godwin TCHAKPANA**

**MABUILA NKOUNGA Franck-Ba**

**Moutagha Abou DIA**

**Okana Gildas MANDOU**

**PROFESSEUR :**

M. **Massamba LO**

1. **La notion de PowerShell**
2. **La notion de Registre**
3. **Qu’est-ce qu’un Registre ?**

Le registre un composant incontournable, un composant à connaître, car tout informaticien a besoin de le manipuler un jour ou l'autre. La base de registre Windows est une base de données structurée où le système et les logiciels stockent de nombreuses informations, notamment sur leur configuration. Des données indispensables au bon fonctionnement du système et des logiciels que vous installez sont stockées dans la base de registre. Le Registre Windows est un composant essentiel du système d'exploitation Windows. D'ailleurs, pour parler de ce composant, on emploie différents termes : le ***registre***, la ***base de registre*** ou le ***Registre Windows***, ce dernier étant le terme officiel.

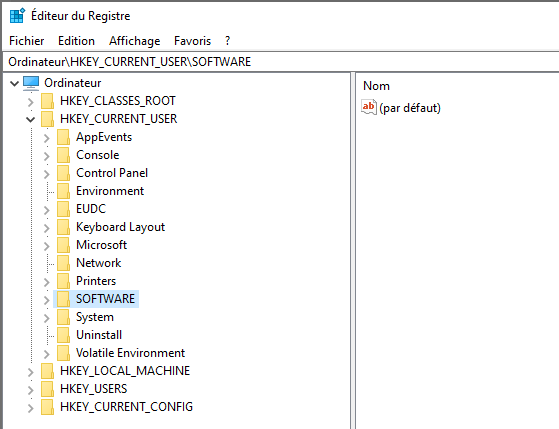
Bien souvent, on l'utilise sans s'en rendre compte à partir de l'interface graphique de Windows. Il contient les paramètres liés aux services Windows, aux associations de fichiers (par exemple, associer Microsoft Word à l'extension "docx"), la configuration et les données des logiciels, la configuration matérielle de votre machine, des informations sur les profils des utilisateurs, ou encore sur les stratégies de groupe.

1. **Structure de la base de registre**

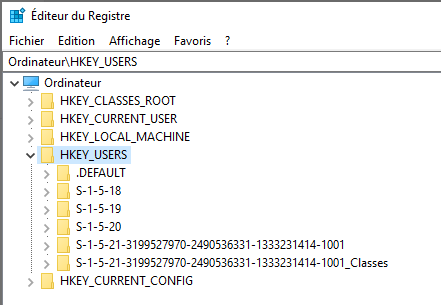
La base de données du Registre Windows est organisée en plusieurs sections que l'on appelle des **ruches**. Une machine Windows dispose de ruches par défaut avec chacune un rôle spécifique. Ci-dessous le nom et le rôle de chaque ruche principale à connaître au sein de la base de registre Windows :

1. **Les Ruches**

* **HKEY\_CLASSES\_ROOT (HKCR)** : Cette ruche contient les informations sur les associations de fichiers, ce qui fait qu'elle contient beaucoup de valeurs différentes. Elle contient également des données sur les bibliothèques DLL, COM et ActiveX.
* **HKEY\_CURRENT\_USER (HKCU) :** Cette ruche contient les paramètres correspondants à l'utilisateur actuellement connecté sur la machine. Si un logiciel stocke des données propres à l'utilisateur connecté sur la machine, il va les stocker dans cette ruche. Cette ruche se matérialise par l'existence du fichier "NTUser.dat" pour stocker les données de l'utilisateur en cours. Lorsqu'on l'explore, on remarque qu'elle se décompose en plusieurs catégories, notamment des données relatives aux logiciels installés et à Windows dans "SOFTWARE" (c'est bien souvent là-dedans que l'on fait des modifications).



* **HKEY\_LOCAL\_MACHINE (HKLM)** : Cette ruche stocke les informations liées à la machine en elle-même et ces valeurs sont prioritaires par rapport à celles définies dans la ruche HKEY\_CURRENT\_USER. Grâce à cela, l'administrateur peut garder le contrôle sur la machine plus facilement. Nous retrouvons des informations sur le matériel, mais aussi sur les paramètres des logiciels communs à tous les utilisateurs.
* **HKEY\_USERS (HKU)** : Cette ruche contient la liste des utilisateurs et offre une vue globale. En fait, HKEY\_CURRENT\_USER est une sous-ruche de HKEY\_USERS. Un utilisateur standard connecté peut modifier seulement les valeurs dans HKEY\_CURRENT\_USER alors qu'un administrateur pourra modifier l'ensemble des valeurs en passant par HKEY\_USERS.

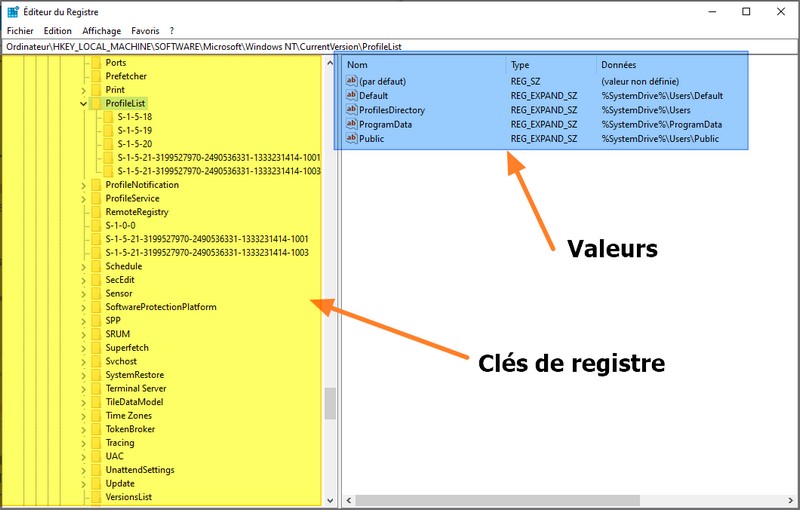


* **HKEY\_CURRENT\_CONFIG (HKCC)** : Cette ruche intègre des informations relatives à la configuration courante de Windows. Elle contient l'ensemble des paramètres liés à la configuration logicielle et matérielle courante du PC. Elle est régénérée après chaque démarrage de Windows. Il s'agit en fait d’un raccourci vers la sous-ruche HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current.

1. **Les clés et leurs valeurs**

Les ruches contiennent deux types d'éléments : les clés et les valeurs.

Les clés sont comme des dossiers : elles vont permettre d'organiser la base de registre et de créer l'arborescence. Ensuite, au sein des clés nous retrouvons des valeurs. Chaque clé dispose d'un type, d'un nom et d'une valeur associée. Les valeurs sont de différents types : tout dépend du format de la valeur à stocker à l'intérieur. Il peut s'agir tout simplement d'une valeur binaire qui aura "0" ou "1" et qui agira comme un booléen, ou alors d'une chaîne de caractères simple ou alors avec plusieurs valeurs. Les types supportés sont : *Chaîne* (string) ; *Binaire* ; *DWORD 32 bits* ; *QWORD 64 bits* ; *Chaînes multiples* ; *Chaîne extensible*.



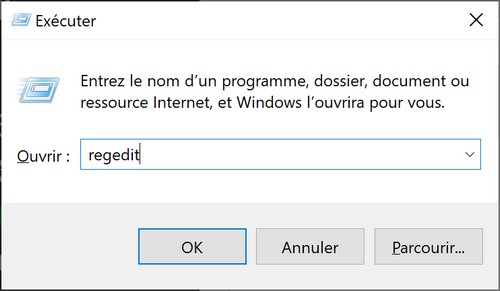
**Quelques exemples de clés**

* ***HARDWARE*** : cette sous-clé comprend notamment les informations sur la configuration matérielle, telles qu'elles sont détectées par Windows au démarrage. En la déployant, dans la sous-catégorie Description, vous pourrez par exemple y trouver les informations sur le processeur, telles qu'elles apparaissent dans le panneau de configuration système de Microsoft. On trouvera aussi dans DeviceMap et RessourceMap, des informations sur les périphériques et les ressources système. La clé est générée à chaque démarrage de Windows à partir du matériel détecté.
* ***SECURITY et SAM*** : ces deux clés contiennent des informations relatives aux comptes utilisateurs. La modification des clés est impossible, même pour un administrateur du système.
* ***SOFTWARE*** : comme son nom l'indique, la clé Software contient des paramètres relatifs aux logiciels inclus dans Windows, ainsi qu'aux logiciels tiers. On remarquera en la déployant que les clés sont organisées selon l'arborescence Editeur/Logiciel. Les paramètres présents dans la clé SOFTWARE sont des paramètres qui s'appliquent à tous les utilisateurs. D'autres paramètres spécifiques à l'utilisateur se trouveront dans les clés HKEY\_USERS ou HKEY\_CURRENT\_USER.
* ***SYSTEM*** : cette sous-clé contient des paramètres matériels ainsi que des informations sur le système, tels que les pilotes ou la mémoire système. On notera que la sous clé contient deux jeux de configuration, Windows utilisant toujours le dernier jeu de configuration n'ayant pas posé de problème.

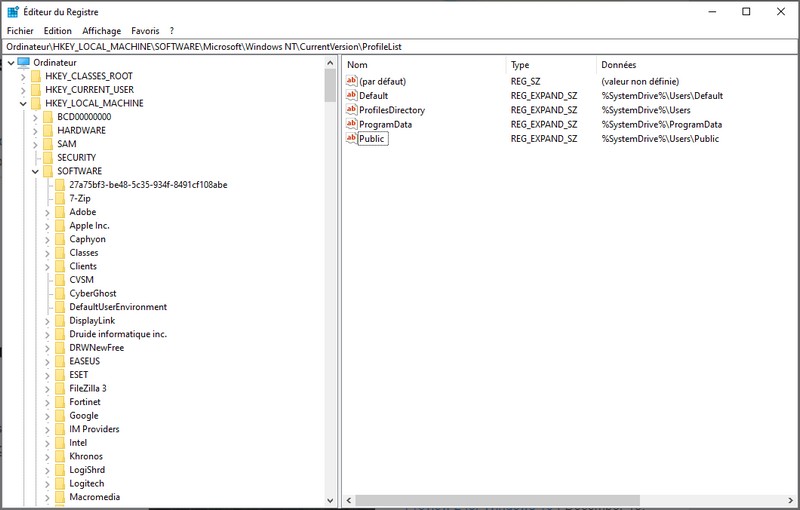
1. **Accès à la base de registre**

Que ce soit pour personnaliser son système de façon avancée ou pour réaliser un dépannage, on peut être amené à modifier la base de registre Windows. J'entends par modifier : ajouter une nouvelle valeur, modifier une valeur existante ou supprimer une valeur existante.

Windows intègre un éditeur de registre que l'on peut ouvrir facilement grâce à la commande "regedit". On peut appeler cet utilitaire dans "Exécuter", dans la zone de recherche du menu Démarrer de Windows (cela va retourner "Éditeur du Registre" ou encore dans une Invite de commande / console PowerShell).

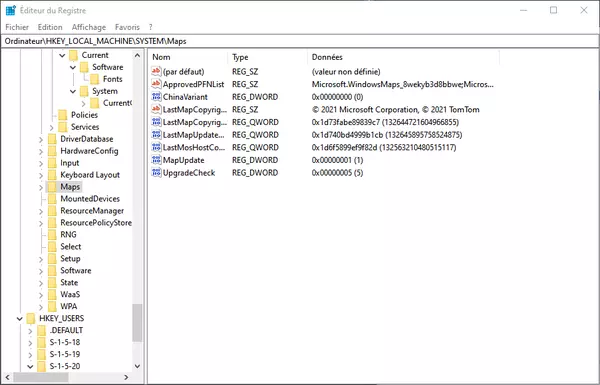


Ci-dessous l'interface de l'éditeur du registre intégré à Windows. À gauche, on va parcourir l'arborescence, et à droite on a la liste des valeurs contenues dans la clé sélectionnée. La partie supérieure qui commence par "Ordinateur" indique le chemin complet de la clé sélectionnée. On appelle ce chemin une ‘’***branche***’’.



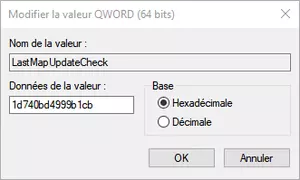
1. **Comment modifier un registre ?**

Pour voir le contenu d'une clé, faites un double clic dessus. Vous pouvez aussi faire un clic simple pour la sélectionner, puis cliquer sur le petit triangle devant. Faites de même pour "replier" une branche. Quand une clé est sélectionnée à gauche, les informations associées s'affichent automatiquement dans le volet droit de la fenêtre, avec un nom, un type et des données.



Il existe différents types de données dans le Registre. Les plus courantes sont **REG\_SZ** (valeurs textuelles standards, qui contiennent du texte facilement lisible et modifiable), **REG\_DWORD** (valeurs numériques qui contiennent un nombre entier en hexadécimal ou en binaire), **REG\_MULTI\_SZ** (valeurs textuelles multiples, qui contiennent une suite de valeurs texte séparées par un caractère particulier), **REG\_EXPAND\_SZ** (valeurs textuelles extensibles qui contiennent un texte générique que Windows modifie selon la configuration) et **REG\_BINARY** (valeurs binaires qui contiennent des données binaires pures difficiles à déchiffrer).

Pour modifier une valeur dans le volet droit, faites un double clic dessus. Une fenêtre flottante apparaît et vous pouvez alors modifier le nom et la valeur de la donnée les champs idoines.

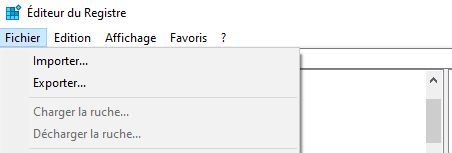


Selon le cas, modifiez des données et validez en cliquant sur le bouton OK ou en appuyant sur la touche Entrée de votre clavier, ou annulez avec le bouton Annuler ou la touche Esc. Notez que vos modifications sont automatiquement enregistrées dans le Registre.

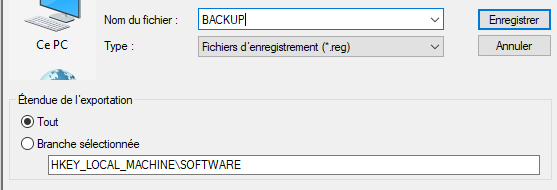
Il ne faut rien modifier dans le Registre si vous ne savez pas ce que vous faites ! Si vous devez absolument modifier des éléments, pour faire une réparation ou une amélioration, procédez avec prudence et commencez par faire une sauvegarde de la base. Et idéalement, suivez un guide pas-à-pas pour ne pas vous tromper ! Toute modification est à vos risques et périls…Au sein de la base de registre Windows, il est à noter qu'une clé peut être renommée, une valeur aussi, mais que le type d'une valeur ne peut pas être changé.

1. **La sauvegarde d’un registre**

Avant de modifier le registre, notamment lorsqu'il s'agit d'effectuer des modifications importantes, il est recommandé d'effectuer une sauvegarde. En cas de mauvaise manipulation et de crash de Windows, cette sauvegarde peut s'avérer utile. Pour sauvegarder la base de registre Windows, il faut exporter son contenu dans un fichier REG. On peut exporter tout ou partie du registre : le registre complet, une ruche complète ou simplement une clé. À l'aide de l'éditeur du registre, il faut cliquer sur "Fichier" puis "Exporter". Le bouton "Importer" permettra de faire l'opération inverse, à savoir restaurer le registre.



Il suffit de nommer le fichier, et de sélectionner l'étendue de l'exportation. Il faut sélectionner "Tout" pour sauvegarder tout le registre, sinon on peut se contenter de la branche sélectionnée.



La sauvegarde de la base de registre Windows peut s'avérer relativement longue, car il y a beaucoup de données à exporter. La sauvegarde donne lieu à un fichier REG qui fera facilement plusieurs centaines de Méga-octets. En ligne de commande, et sans passer par PowerShell, la commande ci-dessous sert à importer un fichier REG pour réaliser une restauration : « **REG IMPORT "mon-fichier.reg"** ». Ceci s'avère particulièrement utile si votre système est crashé, que vous souhaitez restaurer la base de registre Windows et que vous avez seulement accès à l'Invite de commande.