Structure du registre

Ruches

Définition d'une ruche

Le registre de Windows est composé de "ruches" ou "hives". Ces ruches contiennent des clés en lien avec leur rôle. Chaque ruche a un rôle spécifique. Quoi qu'il soit possible de créer des ruches personnalisées, 5 ruches sont dédiées au système d'exploitation, chaque utilisateur a une ruche pour ses paramètres individuels et une ruche par défaut défini le squelette d'une ruche pour un nouvel utilisateur.

Ruches système

Les ruches systèmes sont situées dans le dossier "%SystemRoot%\System32\Config" (%SystemRoot% fait généralement référence à C:\Windows). Les fichiers sans extension sont les fichiers activement chargés dans le système. Les fichiers .log sont les historiques de transactions et sont individuels à chaque ruche. Les fichiers .sav sont des copies de sauvegarde qui peuvent être restaurés en cas de mauvaise manipulation ou de restauration de point d'état de système.

HKEY_CURRENT_CONFIG

La ruche "HKEY_CURRENT_CONFIG" ou HKCC est le fichier "System" qui est regénérée à chaque démarrage contient certaines informations récupérées lors du démarrage de la machine en lien avec certains périphériques et services.

HKEY_CLASSES_ROOT

La ruche "HKEY_CLASSES_ROOT" ou "HKCR" est le fichier contient l'information au sujet des applications enregistrées telles que l'association des extensions de fichier aux applications, les actions par défaut pour certains périphériques etc. Cette ruche est imbriquée dans la ruche "HKEY_LOCAL_MACHINE\SOFTWARE"

HKEY_LOCAL_MACHINE

La ruche "HKEY_LOCAL_MACHINE" ou "HKLM" est la ruche principale pour la configuration du système. Elle est divisée en quatre sections et les noms de fichier corresopndent aux noms des clés à la racine de HKLM. Ces ruches s'appliquent à l'ensemble du système d'exploitation et affectent donc tous les utilisateurs.

HKLM\SAM

La ruche "HKLM\SAM" contient les informations de sécurité relatives aux groupes et utilisateurs du système. L'accès à cette ruche est bloquée par défaut. Pour y accéder, on doit s'accorder les permissions.

HKLM\Security

La ruche "HKLM\Security" est liée à la base de données de sécurité du domaine Active Directory auquel l'ordinateur serait joint. L'accès à cette ruche est bloquée par défaut. Pour y accéder, on doit s'accorder les permissions.

HKLM\Software

La ruche "HKLM\Software" est la ruche qui sera le plus souvent consulté et modifiée par les administrateurs. C'est généralement à cet endroit que les paramètres d'applications installées appliquées à tout le système se situeront. On pourrait penser ici à la langue d'affichage d'une application, au chemin complet de son répertoire d'installation, à la version du logiciel, aux logiciels enfichables (plug-ins) pour vos navigateurs web ou pour votre éditeur de texte favori.

Les paramètres mentionnés directement sous la clé HKLM\Software s'appliquent aux logiciels 64 bits tandis que les paramètres mentionnés sous la clé HKLM\Software\WOW6432Node s'appliquent aux applications 32 bits de votre PC.

HKLM\System

La clé "HKLM\System" contient les paramètres systèmes liés par exemple aux composants du systèmes d'exploitation, aux pilotes installés pour les périphériques du système etc. Sa section "ControlSet" ou "CurrentControlSet" et sa sous-section "Control" contient les paramètres liés à l'état et l'identité du système.

Ruches d'utilisateur

HKEY_USERS et HKEY_CURRENT_USER

Chaque utilisateur possède une ruche qui lui est unique. Il s'agit du fichier "ntuser.dat" situé à la racine de son dossier d'utilisateur. Toutes ces ruches sont listées sous "HKEY_USERS" mais la ruche "HKEY_CURRENT_USER" est la ruche ouverte pour l'utilisateur consultant le registre. Cette ruche contient les paramètres systèmes et paramètres des logiciels uniques à chaque utilisateur. On peut ici penser aux paramètres de l'explorateur de fichiers tels que l'affichage des extensions de fichier, le dossier d'ouverture par défaut de l'explorateur de fichiers ou encore au thème sombre ou clair du système. Certains logiciels peuvent être configurés seulement par utilisateurs tels que 7-Zip, Steam, vos navigateurs web, etc.

C:\Users\Default\ntusers.dat

Quoi que non chargé par défaut, ce fichier est le gabarit de ruche pour tous les nouveaux utilisateurs qui seront créés. À titre d'exemple, si on modifie le thème, la position de la barre des tâches et la page d'accueil d'un navigateur web, ces paramètres seront appliqués par défaut à tous les nouveaux utilisateurs. Cette ruche est parmis les plus intéressantes lors de la personnalisation d'une image d'installation de Windows.

Il peut être chargé avec la commande "reg load HKLM\TempDefault C:\Users\Default\NTUSER.DAT" et ensuite modifié avec PowerShell ou "regedit". Il peut être déchargé une fois modifié avec la commande "reg unload HKLM\TempDefault".

Clés et valeurs

Clés

Une clé peut être considérée comme un dossier dans une ruche. Dans certain cas, une clé sera une ruche imbriquée ou liée à une autre. On peut penser à HKLM\Software qui est en soit une ruche mais est manipulée comme étant une clé ou les clés situés sous HKEY_USERS qui sont des ruches individuelles. Chaque clé possède une valeur par défaut nommée "(Default)" qui est une chaîne de caractère indéfinie à la création de la clé. Quoi que celle-ci puisse être modifiée, les valeurs associées à une clé seront habituellement nommées. Tout comme le chemin d'accès le plus long supporté par l'explorateur de fichiers, le chemin d'accès d'une clé ne doit pas excéder 255 caractères.

Valeurs

Une valeur est une donnée associée à un nom. On pourrait ici penser à des fichiers et leur contenu ou encore à un nom de variable et une valeur lui étant assignée. Différents types de valeurs existent avec différents objectifs. Le nom de la valeur ne doit pas excéder 16 383 caractères ou 128Kb. La donnée associée au nom historiquement ne devait pas excéder 1 MB mais peut maintenant être étendue jusqu'à en remplir la mémoire vive.

Ceci dit, toute valeur excédant 2Kb devrait être stockée dans un fichier et la clé de registre devrait correspondre au chemin d'accès du fichier. On pourrait penser ici à l'arrière-plan d'une application où la méthode logique serait de pointer vers le fichier d'image plutôt que de stocker l'image dans le registre.

REG_SZ

Les valeurs de type REG_SZ contiennent une chaîne de caractère de longueur fixe.

REG_MULTI_SZ

Les valeurs de type REG_MULTI_SZ contiennent plusieurs chaînes de caractères uniques (une par ligne).

REG_EXPAND_SZ

Les valeurs de type REG_EXPAND_SZ représentent une chaîne de caractère comprenant des variables d'environnement. On pourrait ici imaginer que la valeur contienne %username%. Lorsque cette valeur serait consultée, la variable serait étendue et remplacée par sa valeur.

REG_BINARY

Les valeurs de type REG_BINARY sont une valeur binaire simple.

REG_DWORD

Le type de données "DWORD" ou "double word" est un nombre entier de longueur fixe de 32 bits. Il peut être représenté de façon binaire ou hexadécimale.

REG_QWORD

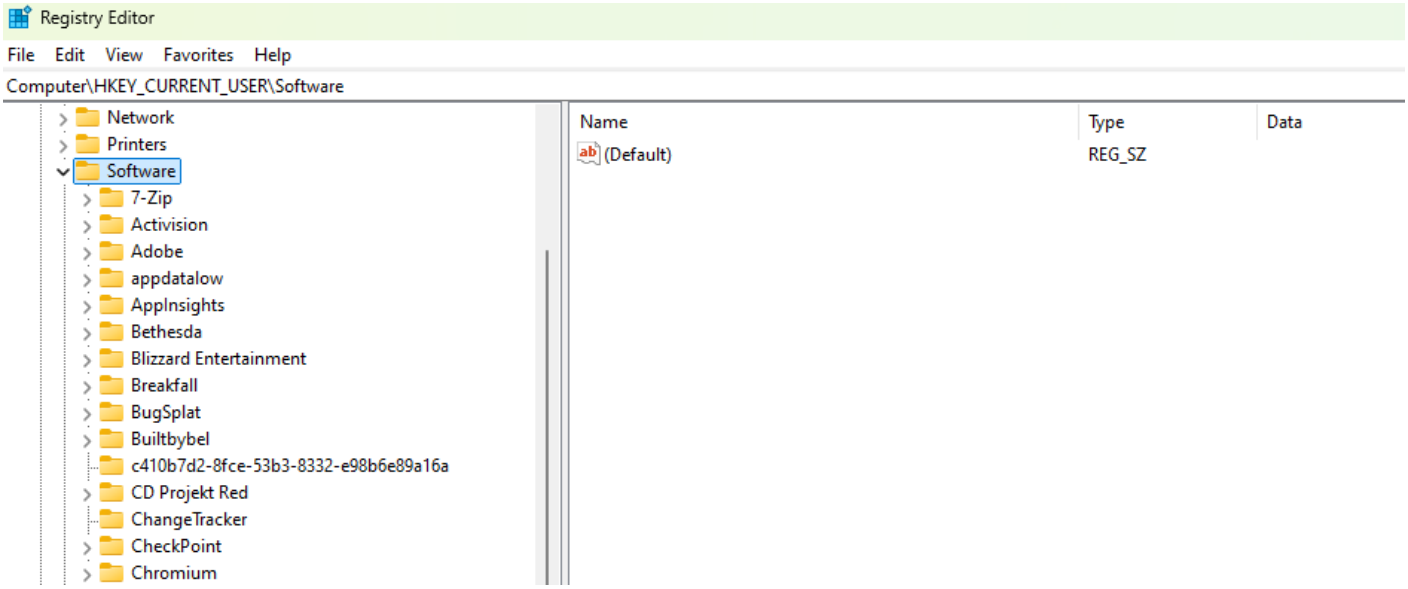
Le type de données "QWORD" ou "quad word" est un nombre entier de longueur fixe de 64 bits. Il peut être représenté de façon binaire ou hexadécimale.

Emplacements d'intérêt

[HKEY_CURRENT_USER] et [HKEY_USER] (*et C:\Users\Default\ntuser.dat*)

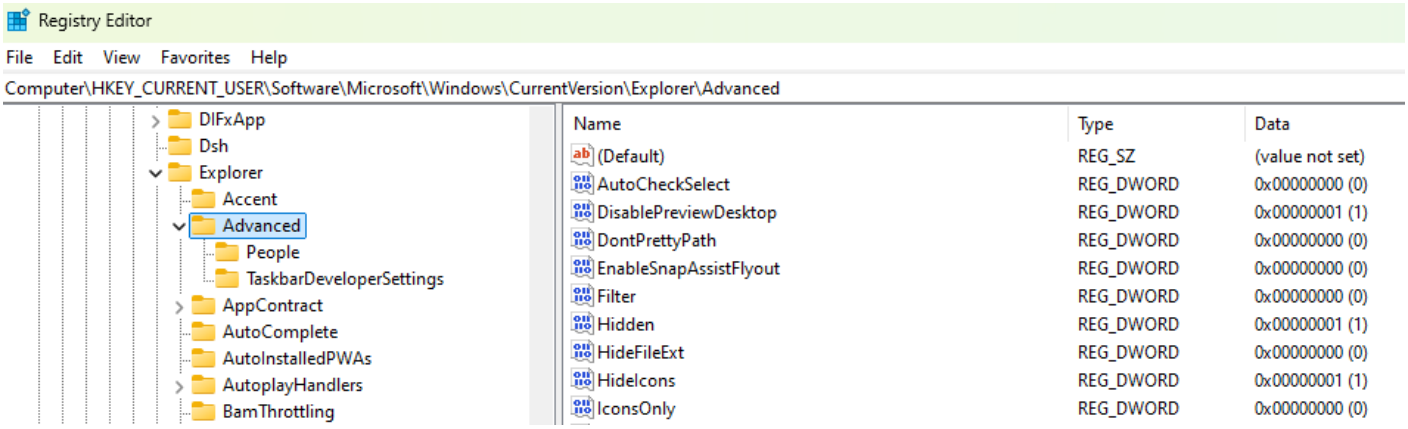
[HKEY_CURRENT_USER\Software] et [HKEY_CURRENT_USER\Software\WOW6432Node]

Ces emplacements contiennent les paramètres par utilisateur pour la majorité des applications installées. Le squelette de profil (*C:\Users\Default\ntuser.dat*) peut être accédé en le chargeant dans le registre à l'aide de la commande "reg load HKU\DefaultUser C:\Users\Default\ntuser.dat"



[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]

Cette clé et ses sous-clés contiennent l'ensemble de la configuration de l'explorateur Windows. La vaste majorité des paramètres d'affichage et comportement de l'interface Windows pour un utilisateur se situent à cet endroit. On peut ici penser à l'alignement de la barre des tâches, les paramètres d'affichage pour les fichiers masqués,



[HKCU\Software\Policies]

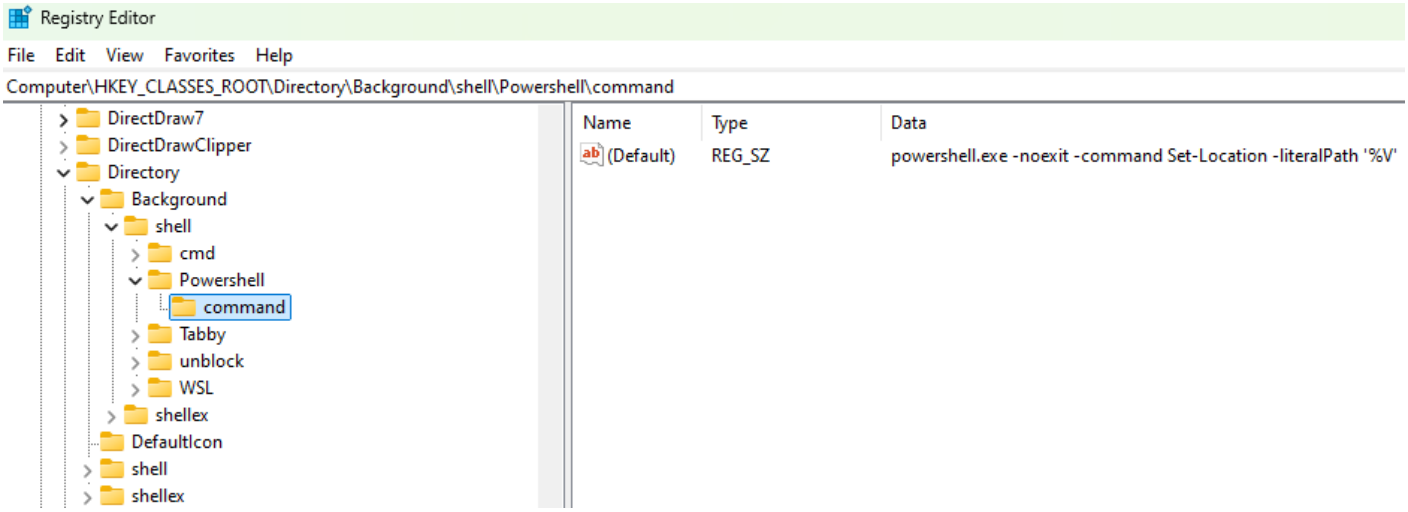
Les politiques de groupes et stratégies de sécurité locales appliquées à un utilisateur se trouvent à cet endroit. Il est possible d'y ajouter manuellement les entrées correspondant à des paramètres de GPO (adm/admx) pour paramétrer une machine même si elle n'est pas jointe à un domaine. Le site suivant est une excellente librairie de ces "hacks" de registre.

https://admx.help/

[HKCR]

[HKEY_CLASSES_ROOT\Directory\Background\shell]

Il est possible ici d'ajouter des actions personnalisées au menu contextuel de Windows (clic droit).



[HKLM]

[HKLM\Software\Policies]

Les politiques de groupes et stratégies de sécurité locales appliquées au système sont stockées à cet endroit. Il est possible d'y ajouter manuellement les entrées correspondant à des paramètres

de GPO (adm/admx) pour paramétrer une machine même si elle n'est pas jointe à un domaine. Le site suivant est une excellente librairie de ces "hacks" de registre.

https://admx.help/ (down)

https://gpedit.tplant.com.au/

https://gpsearch.azurewebsites.net/

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]

On trouve à cet endroit une tonne de paramètres appliqués au système tels que les profils et options d'alimentation, l'identité du système, les paramètres de certains services comme OpenSSH et SNMP, etc.