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".

Revision #6
Created 2025-01-25 18:40:03 UTC by Alexandre Arsenault-Jetté
Updated 2026-02-05 20:26:41 UTC by Alexandre Arsenault-Jetté