La base de Registre

Le Registre joue un rôle clé dans la configuration de votre système d'exploitation. C'est non seulement un ensemble de données statiques présent sur le disque dur mais aussi, au travers d'une architecture complexe d'informations dynamiques, une fenêtre ouverte sur le cœur de votre système.

L'**Éditeur du registre** est un outil permettant de visualiser et d'éditer l'ensemble des informations contenues dans les fichiers de ruche. Les fichiers de ruche sont les fichiers qui contiennent les paramètres de votre système d'exploitation et de vos applications. Ils constituent ce que l'on appelle le Registre.

Avec Windows 10 (1909), la base de Registre se dote d'une barre d'adresse que l'on peut masquer, de l'auto-complétion de raccourcis-clavier et d'abréviations facilitant la navigation et la recherche.

1. Lancer le Registre

- Dans la zone de recherche placée à droite du menu **Démarrer**, saisissez : `regedit`. Afin de lancer plusieurs instances du Registre, servez-vous du commutateur `-m` : `regedit -m`. Vous pouvez le faire autant de fois que vous voulez. Rappelez-vous simplement que les modifications apportées dans une des instances ne seront pas répercutées dans l'autre, à moins de donner le focus à la fenêtre et d'actualiser l'affichage en appuyant sur la touche [F5].

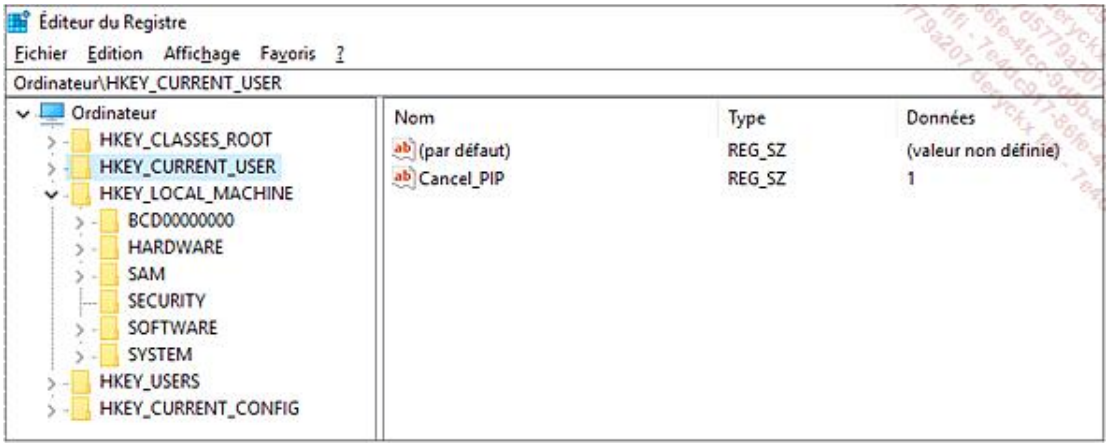
2. Actualiser le Registre

Sous Windows 10, que vous procédiez à une modification dans le Registre ou dans l'Éditeur d'objets de stratégie de groupe, les modifications sont immédiatement répercutées (à quelques exceptions près).

3. Les valeurs et les données de la valeur

Il y a cinq branches visibles que vous pouvez développer de différentes façons :

- En cliquant sur la petite flèche placée sur la gauche.
- En double cliquant sur une des branches.
- En cliquant avec le bouton droit de la souris sur une des branches puis en sélectionnant l'option **Développer**.



Vous allez voir qu'à l'intérieur de chacune des branches, il y a une arborescence de clés et de sous-clés. Les clés sont une manière d'organiser les données présentes en les classant par thématique.

Si vous sélectionnez une des clés, un certain nombre de données apparaît dans le volet de droite. Ce sont les valeurs. Une valeur est constituée de trois informations :

- nom de la valeur
- type de la valeur
- données inscrites dans la valeur appelées "Données de la valeur"

Chacune des clés peut contenir une ou plusieurs valeurs.

S'il n'est pas possible de modifier les branches principales, vous pouvez effectuer toutes sortes d'opérations dans les clés, les valeurs et les données de la valeur.

4. Structure du Registre

Les clés racine visibles sont au nombre de cinq.

- **HKEY_CLASSES_ROOT** : contient principalement les informations d'association de fichiers, les composants COM et les informations d'enregistrement des objets.
- **HKEY_CURRENT_USER** : contient les données concernant l'utilisateur actuellement connecté.
- **HKEY_LOCAL_MACHINE** : contient les données relatives au système.
- **HKEY_USERS** : contient les données concernant l'ensemble des utilisateurs de votre machine.
- **HKEY_CURRENT_CONFIG** : contient les informations concernant le profil matériel actuel.

Il est courant de noter certaines clés en utilisant les abréviations suivantes :

- HKEY_CLASSES_ROOT : HKCR
- HKEY_CURRENT_USER : HKCU
- HKEY_LOCAL_MACHINE : HKLM
- HKEY_USERS : HKU
- HKEY_CURRENT_CONFIG : HKCC

La lettre H représente le Handle Windows vers les clés (KEY).

Certaines clés fonctionnent comme des liens miroir pointant vers d'autres arborescences :

- La clé HKEY_CURRENT_CONFIG est le miroir de cette branche : **HKEY_LOCAL_MACHINE - SYSTEM - CurrentControlSet - Hardware Profiles - Current**
- La clé HKEY_CLASSES_ROOT est le miroir de celle-ci : **HKEY_LOCAL_ MACHINE - SOFTWARE - Classes**
- La clé HKEY_CURRENT_USER correspond à celle-ci : **HKEY_USERS - <Utilisateur actuellement connecté>**

En conclusion, seules les clés HKEY_USERS et HKEY_LOCAL_MACHINE possèdent une existence propre.

5. Les fichiers de ruche

Toutes ces informations sont directement extraites des fichiers de ruche qui sont principalement placés dans *\Windows\system32\config*. Voici la liste des correspondances :

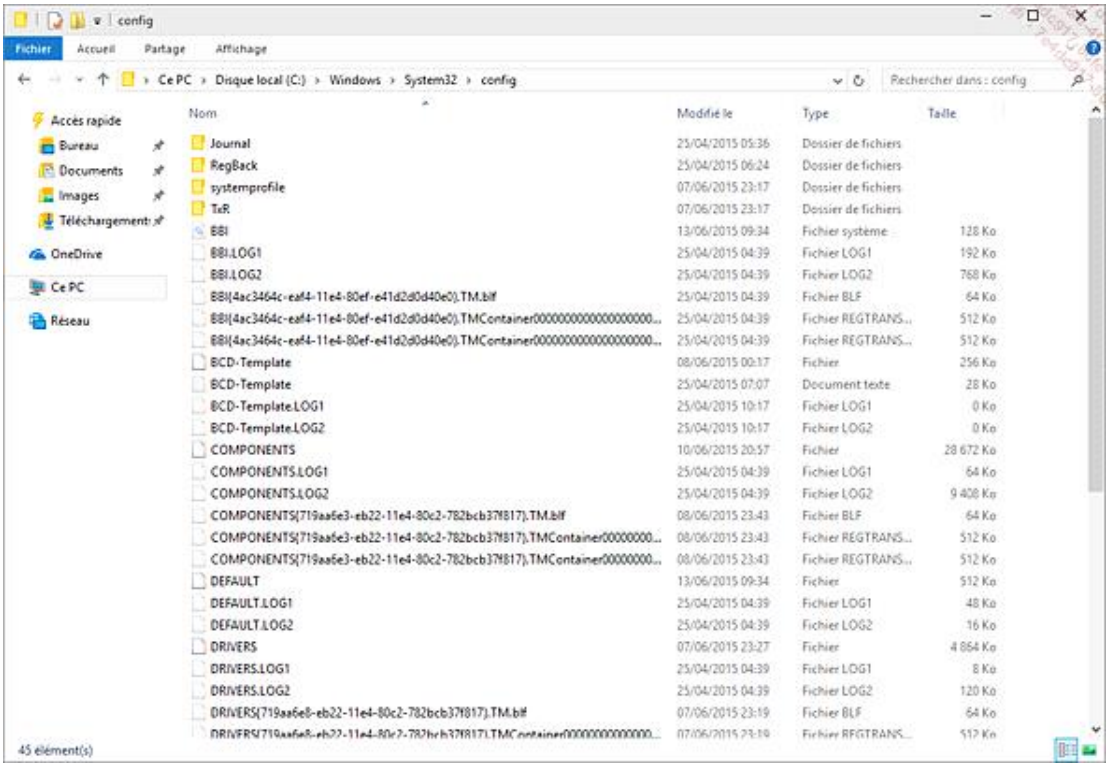
- HKEY_LOCAL_MACHINE\BCD00000000 : *\Boot\BCD*
- HKEY_LOCAL_MACHINE\COMPONENTS : *\Windows\system32\config\COMPONENTS*. Les nouvelles versions de Windows n'incluent pas cette ruche. Par exemple, si votre installation de Windows 10 est neuve (pas mise à jour depuis Windows 7), cette clé n'apparaît pas.
- HKEY_LOCAL_MACHINE\DRIVERS : \Windows\system32\config\DRIVERS. Cette ruche est créée pour le démarrage du système et est effacée peu après.
- HKEY_LOCAL_MACHINE\HARDWARE : Cette ruche volatile est entièrement placée en mémoire et ne correspond donc pas à un emplacement précis de l'Explorateur Windows.
- HKEY_LOCAL_MACHINE\SAM : \windows\system32\config\SAM
- HKEY_LOCAL_MACHINE\SECURITY : *\Windows\system32\config\SECURITY*
- HKEY_LOCAL_MACHINE\SOFTWARE : *\Windows\system32\config\SOFTWARE*
- HKEY_LOCAL_MACHINE\SYSTEM : *\Windows\system32\config\SYSTEM*
- HKEY_USERS\.DEFAULT : \Windows\system32\config\DEFAULT
- HKEY_USERS\SID : *\Users\"Nom_Utilisateur"\ntuser.dat*
- HKEY_USERS\SID de l'utilisateur_Classes : \Users\"Nom_Utilisateur"\AppData\Local\Microsoft\ Windows\UsrClass.dat

Il y a deux fichiers de ruches un peu particuliers créés par NTDETECT.COM à chaque démarrage :

- HKEY_USERS\S-1-5-19 : \Windows\ServiceProfiles\LocalService\NTUSER.DAT. Service local.
- HKEY_USERS\S-1-5-20 : \Windows\ServiceProfiles\NetworkService\NTUSER.DAT. Service réseau.

Il y a différents types de fichiers :

- Regtrans-ms : ces fichiers sont des journaux de transactions utilisés pour stocker les changements en bases de registre afin d'éviter la corruption des fichiers de ruche.
- Blf : ces fichiers journaux sont utilisés au même titre que les fichiers regtrans-ms par le composant CLFS (*Common Log File System*) pour stocker les changements en bases de registre afin d'éviter la corruption des fichiers de ruche.
- LOG : ces fichiers sont des fichiers journaux retraçant les modifications intervenues dans telle clé ou telle valeur.



Des versions de sauvegarde des fichiers de ruche sont disponibles dans le répertoire C:\Windows\System32\config\RegBack. C'est a priori le meilleur choix si vous désirez restaurer manuellement un fichier de ruche de type Machine par une autre version.

La liste des fichiers de ruche peut s'obtenir en affichant le contenu de cette clé du Registre : **HKEY_LOCAL_MACHINE - SYSTEM - CurrentControlSet - Control - hivelist**.

6. Manipuler le Registre

Il existe plusieurs manières de créer une nouvelle clé. Vous pouvez par exemple :

- Sélectionner la clé parente.
- Cliquer sur **Édition - Nouveau - Clé**.

Une mention *Nouvelle clé #1* va apparaître.

Puisque vous êtes par défaut en mode Édition, vous pouvez directement saisir le nom de votre clé.

Afin de passer une nouvelle fois en mode Édition, appuyez sur la touche [F2].

Vous pouvez également vous servir du menu contextuel accessible à partir de la clé qui jouera le rôle de conteneur ou, tout en ayant pris soin que cette dernière soit sélectionnée, vous servir du menu contextuel accessible dans le volet de droite.

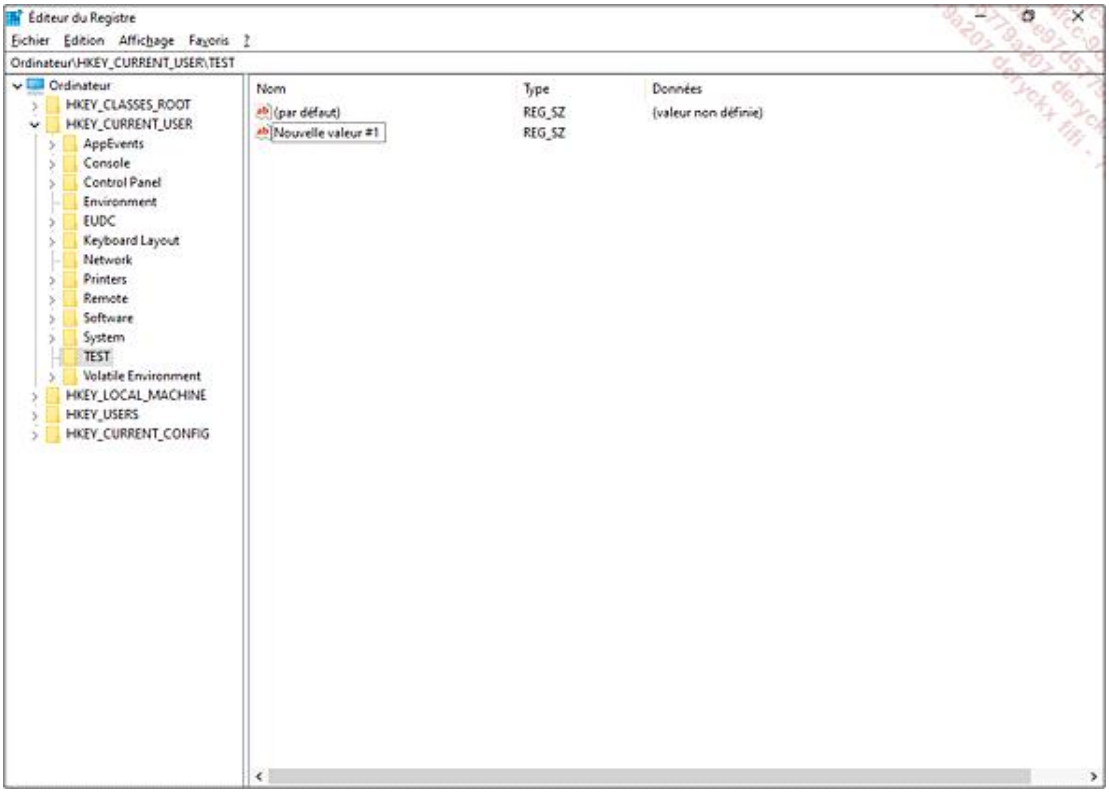
Il est possible de la même manière de supprimer ([Suppr]) ou de renommer une clé.

Vous ne pouvez pas supprimer ou sélectionner différentes clés en gardant la touche [Ctrl] ou [Shift] enfoncée. Ce n'est pas le cas pour les valeurs.

Notez qu'à chaque fois que vous allez créer une clé, une valeur (par défaut) sera automatiquement créée.

7. Modifier les valeurs

De la même manière que précédemment, vous pouvez créer de nouvelles valeurs DWORD, chaîne, binaire, etc. Le nom par défaut sera celui-ci : Nouvelle valeur #1.



Afin d'inscrire des données dans l'entrée que vous venez de créer, double cliquez dessus puis saisissez votre chaîne de caractères dans la zone de texte **Données de la valeur**.

Vous pouvez aussi cliquer avec le bouton droit de la souris sur cette entrée puis cliquez sur la commande **Modifier**. La même commande est accessible à partir du menu **Édition**.

Il existe deux commandes : **Modifier** et **Modifier données binaires**. Cette dernière vous permet d'afficher les données dans leur représentation hexadécimale.

Vous pouvez directement afficher ce type de données si vous avez sélectionné une valeur DWORD ou binaire en cliquant sur **Affichage - Affichage des données binaires**.

Par ailleurs, quand vous saisissez les données de valeur dans une entrée DWORD, vous avez le choix entre utiliser la base décimale ou hexadécimale. Il vous suffit, dans le premier cas, de cocher le bouton radio **Décimale**. De toute façon, le chiffre ou le nombre que vous aurez saisi s'affichera en base hexadécimale.

Quand vous créez une nouvelle valeur chaîne, les données de la valeur sont vides.

Dans le cas d'une valeur DWORD ou binaire, les données seront automatiquement égales à zéro ou la valeur binaire sera de longueur zéro.

Quand vous créez une nouvelle clé, la valeur (par défaut) indique que les données ne sont pas définies (valeur non

définie).

8. Rechercher dans le Registre

- Afin de lancer une recherche, sélectionnez l'arborescence de départ puis cliquez sur **Édition - Rechercher** (ou [Ctrl][F]). Il est désormais possible de lancer une recherche sur toutes les ruches en sélectionnant **Ordinateur**.
- Dans la zone de texte **Rechercher**, saisissez l'expression recherchée.
- Dans la rubrique **Regarder dans**, indiquez si votre recherche portera sur les :
  - **Clés**
  - **Valeurs**
  - **Données**

Vous pouvez cocher la case **Mot entier seulement** si vous préférez ne retrouver que les occurrences qui correspondent exactement à l'expression recherchée (et non partiellement).

Afin de relancer une recherche, cliquez sur **Édition - Rechercher le suivant** ou appuyez sur la touche [F3].

À chaque fois, l'entrée ou la clé correspondante sera mise en surbrillance.

Par ailleurs, une recherche démarre toujours à partir de la clé sélectionnée. Afin de réinitialiser rapidement votre point de départ de la recherche appuyez sur la touche [Home] ou [Début]. La branche Ordinateur sera automatiquement mise en surbrillance.

9. Importer ou exporter une clé

Cette opération vous permet de copier l'ensemble des valeurs contenues dans une clé ainsi que la clé elle-même. Son intérêt est que vous pouvez exporter une portion du Registre en provenance d'un ordinateur "sain" puis l'importer sur le système "malade". C'est une manière rapide et sûre de réparer un problème dû à des entrées défectueuses dans le Registre.

- Sélectionnez une des clés du registre.
- Cliquez sur **Fichier - Exporter**.

Vous pouvez aussi bien vous servir de la commande **Exporter** présente dans le menu contextuel de la clé.

- Dans la liste déroulante **Enregistrer dans**, sélectionnez le répertoire de destination.
- Dans la zone de texte **Nom du fichier**, saisissez un nom pour le fichier.

Souvenez-vous que le nom que vous choisissez n'a strictement aucune importance !

- Dans la liste déroulante **Type**, sélectionnez le format que portera votre fichier d'enregistrement.

Vous avez le choix entre :

- **Fichiers d'enregistrement(*.reg)** : le fichier aura une extension en REG et comportera comme en-tête ceci : Windows Registry Editor Version 5.00. Ce format est compatible avec les versions Windows XP et ultérieur.
- **Fichiers ruche du Registre (*.*)** : ce fichier ne portera pas d'extension visible. Nous verrons un peu plus loin son utilité pratique.
- **Fichiers texte (*.txt)** : le fichier portera une extension TXT. Vous remarquerez qu'il affiche le nom de la classe ainsi que l'heure de dernière écriture pour chaque clé ou valeur listée.
- **Fichiers d'enregistrement Win9x/NT4 (*.reg)** : ce format d'enregistrement est compatible avec les anciennes versions de Regedit que l'on peut trouver dans Windows 9X, ME et Windows NT. L'en-tête du fichier sera celui-ci : REGEDIT4. Vous pouvez aussi utiliser ce format d'enregistrement sur les systèmes plus récents de Windows.
- **Tous les fichiers** : cette possibilité permet simplement de changer l'extension de votre fichier d'enregistrement.

Cette option mérite quelques éclaircissements : il n'est pas nécessaire qu'un fichier d'enregistrement comporte une extension REG. Cela fonctionne aussi bien avec un fichier sans extension portant une extension que vous avez inventée.

- Dans la rubrique **Étendue de l'exportation**, précisez si vous souhaitez exporter le Registre complet (**Tout**) ou simplement l'arborescence que vous avez sélectionnée. (**Branche sélectionnée**) Cette dernière possibilité est beaucoup plus raisonnable !
- Cliquez sur le bouton **Enregistrer**.

Édition

Afin d'éditer un fichier d'enregistrement REG ou au format Texte, effectuez un clic droit sur le fichier puis sélectionnez la commande **Modifier**.

Le fichier d'enregistrement s'ouvrira dans le Bloc-notes Windows.

Vous pouvez aussi définir un autre programme en cliquant sur le sous-menu **Ouvrir avec**.

Concernant les fichiers de ruche, voici la procédure :

- Effectuez un clic droit sur le fichier puis sélectionnez la commande **Ouvrir avec**.

- Dans la fenêtre sui s'affiche, choisissez une application pour ouvrir le fichier, par exemple le Bloc-notes Windows.

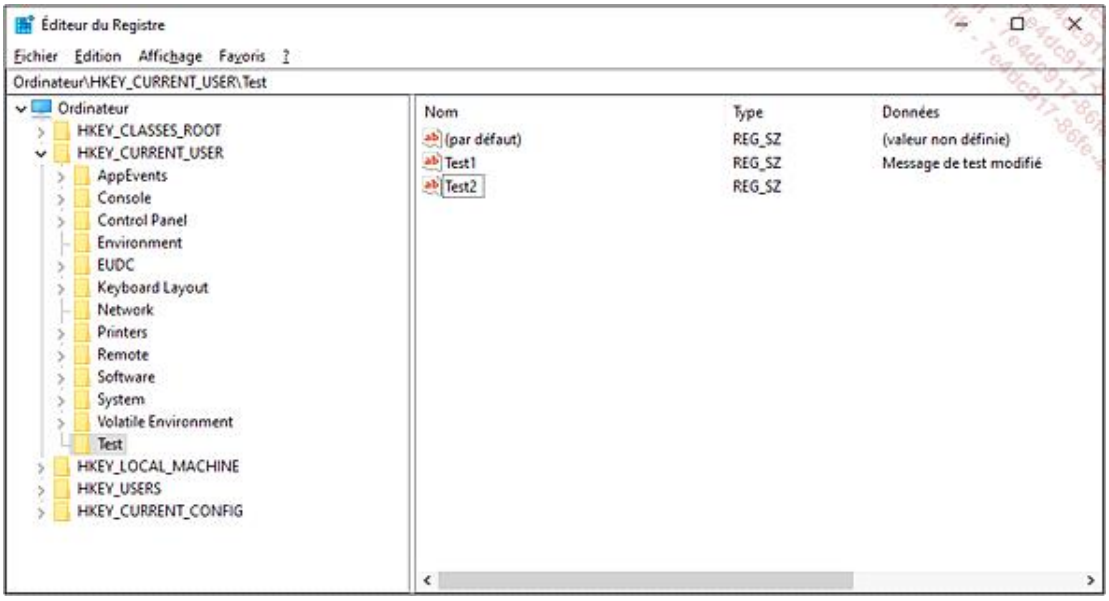
Comme vous pourrez le constater, c'est illisible !

Comparaison des formats de sauvegarde

Voyons maintenant les avantages et les inconvénients des deux formats de sauvegarde :

Un fichier de ruche fera le double de la taille d'un fichier *.reg*. C'est une image au format binaire de l'arborescence que vous avez sauvegardée. Vous ne pouvez pas importer un tel fichier en vous servant de la commande Regedit ou en double cliquant sur le fichier de ruche. Vous devez cliquer sur **Fichier - Importer** puis sélectionner le fichier de ruche. À l'inverse d'un fichier *.reg*, l'arborescence existante sera écrasée et son contenu entièrement remplacé par celui du fichier *.hiv*. Dans le cas d'un fichier *.reg*, les anciennes valeurs sont conservées. Si deux valeurs portent le même nom, seules les données de la valeur sont éventuellement modifiées. Examinons un exemple d'application pratique :

- Dans le Registre, ouvrez cette branche : HKEY_CURRENT_USER.
- Créez une nouvelle clé nommée *Test*.
- Sélectionnez cette dernière clé puis créez une valeur chaîne nommée *Test1*.
- Éditez cette valeur puis saisissez un texte quelconque : C'est juste un test.
- Exportez la clé *Test* comme un fichier de ruche puis au format REG.
- Éditez de nouveau la valeur *Test1* puis modifiez son contenu.
- Créez alors une seconde valeur chaîne nommée *Test2*.



- Ouvrez l'Explorateur Windows dans l'emplacement où vous avez sauvegardé vos fichiers REG et de ruche.
- Effectuez un clic droit sur le fichier REG puis sur la commande **Fusionner**.

Notez que vous pouvez aussi double cliquer sur le fichier d'enregistrement.

- Confirmez la fusion des données avec le Registre Windows.

Après avoir actualisé l'affichage du Registre en appuyant sur la touche [F5], vous pourrez constater que :

- Les données de la valeur *test1* ont bien été modifiées.
- La valeur *test2* est toujours présente.

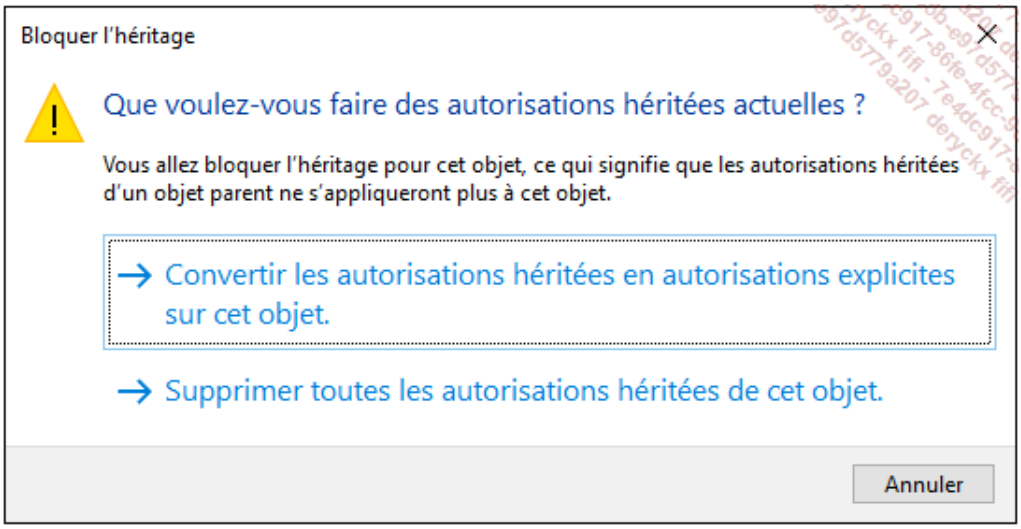
- Dans le Registre, cliquez sur **Fichier - Importer** puis sélectionnez le dossier contenant le fichier de ruche sauvegardé.
- Dans la liste déroulante placée en bas de la fenêtre, sélectionnez l'option **Fichiers ruche du Registre (*.*)** puis sélectionnez le fichier de ruche.
- Cliquez sur le bouton **Ouvrir**.
- Confirmez le remplacement de la clé.

Le Registre Windows s'actualise immédiatement et la clé *Test2* a bien été supprimée.

Tout ceci pour dire que, si vous devez sauvegarder des clés du Registre avant de faire une opération qui vous semble périlleuse, il vaut mieux les exporter au format de ruche et non au format REG.

Il y a une autre question qui vient à l'esprit : si j'opère une modification dans les autorisations d'une clé du Registre, est-ce qu'il est possible de restaurer le jeu des permissions NTFS ? Là encore, nous allons refaire le même type de manipulation :

- Sélectionnez la clé nommée *Test* puis dans le menu **Édition** cliquez sur le sous-menu **Autorisations**...
- Cliquez sur le bouton **Avancé**, puis sur le bouton **Désactiver l'héritage**.
- Cliquez sur le lien **Convertir les autorisations héritées en autorisations explicites sur cet objet**.



- Sélectionnez votre nom d'utilisateur qui apparaît dans la rubrique **Groupe ou noms d'utilisateur** puis cliquez sur les boutons **Supprimer** et **OK**.

Nous avons donc :

- Désactivé le mécanisme d'héritage des permissions NTFS.
- Supprimé votre compte d'utilisateur de la liste des utilisateurs pour lesquels une ACE a été définie.

- Avec le bouton droit de la souris, cliquez sur votre fichier d'enregistrement puis sur la commande **Fusionner**.

Si vous accédez de nouveau au jeu des permissions NTFS de la clé Test, vous verrez que la situation est toujours la même.

- Procédez à la même manipulation mais en important cette fois-ci le fichier de ruche.
- Ouvrez de nouveau la fenêtre des autorisations de la clé *Test*. Le mécanisme d'héritage et le jeu des permissions ont cette fois-ci été rétablis.

La conclusion est là encore sans appel : si vous devez procéder à des modifications dans le jeu des permissions d'une clé, choisissez comme système de sauvegarde un fichier de ruche.

10. Réparer un service en utilisant les fonctionnalités WinRE

Nous allons utiliser la même astuce afin d'éditer le Registre Windows. Cela suppose que la commande **Dernière bonne configuration connue** n'a pas fonctionné et que vous ne pouvez pas restaurer votre ordinateur dans un état antérieur.

- Ouvrez une fenêtre d'invite de commandes.
- Saisissez ces deux commandes en validant à chaque fois par la touche [Entrée] :
  - `cd \windows\inf\`
  - `notepad setupapi.setup.log`

Chaque service et pilote de périphérique est classé par date.

- Identifiez donc le dernier pilote ou service qui a été installé.
- Saisissez ensuite cette commande : `regedit`.
- Chargez la ruche SYSTEM qui est accessible à cet emplacement : **Windows - System32 - Config**
- Attribuez-lui un nom temporaire puis ouvrez cette arborescence : **Current - ControlSetxxx_Services**
- Localisez ensuite la clé qui a été installée par le service ou le pilote.
- Éditez une valeur DWORD nommée **Start** puis saisissez comme données de la valeur le chiffre 4.

Ceci afin de le désactiver.

- Déchargez la ruche temporaire puis redémarrez votre ordinateur.