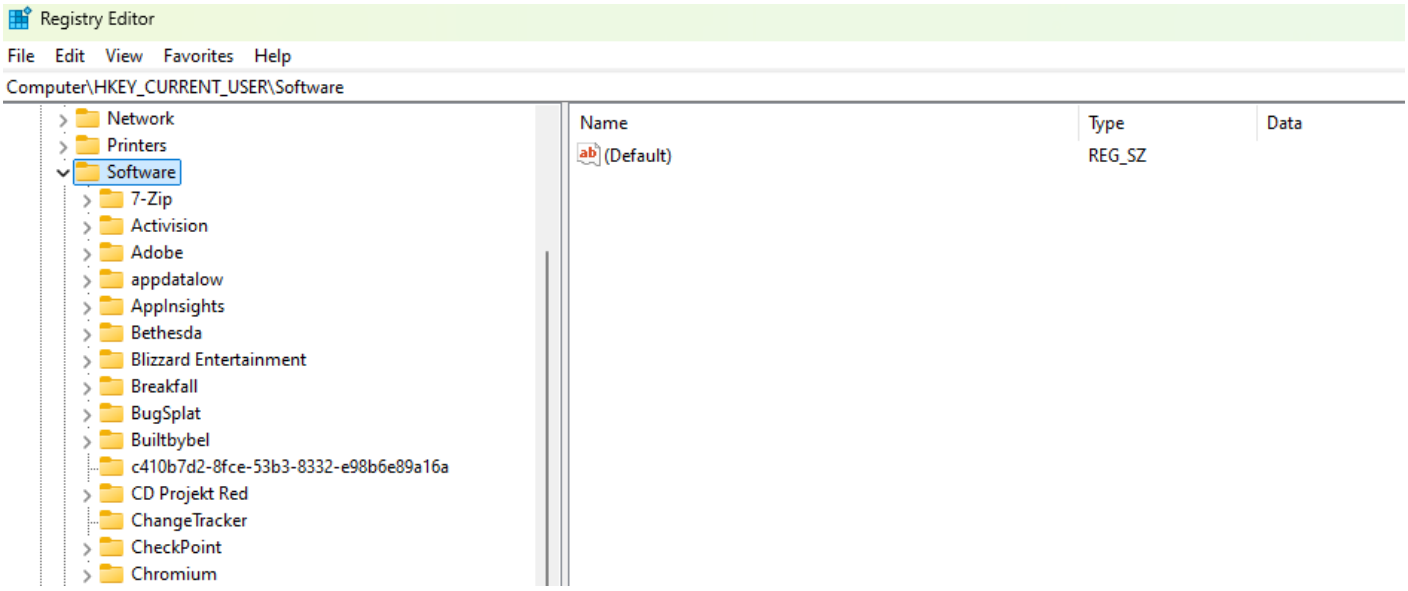
Emplacements d'intérêt

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

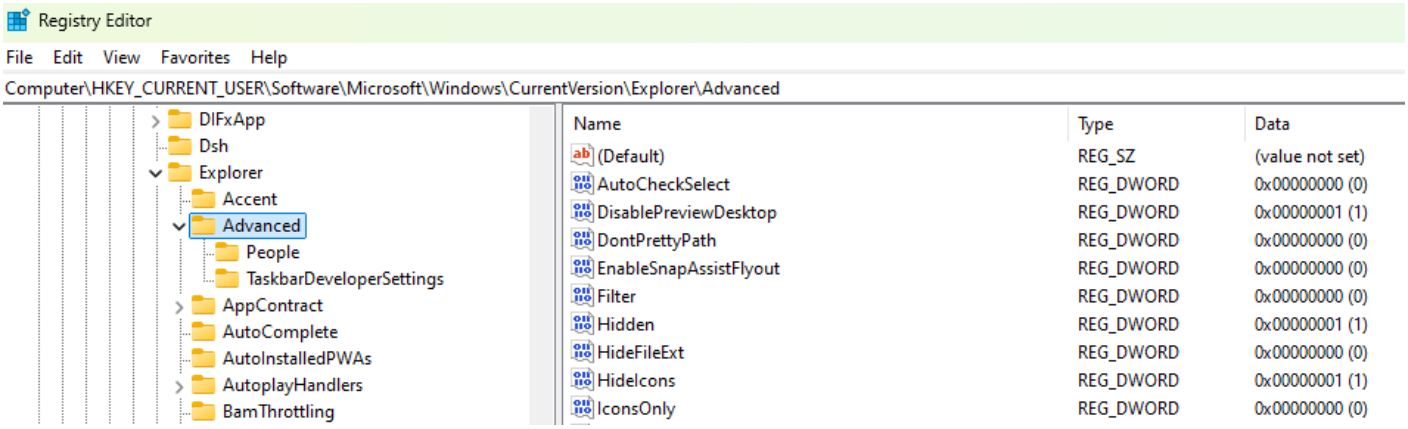
[HKEY_CURRENT_USER\Software] et [HKEY_CURRENT_USER\Software\WOW6432Node]

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]

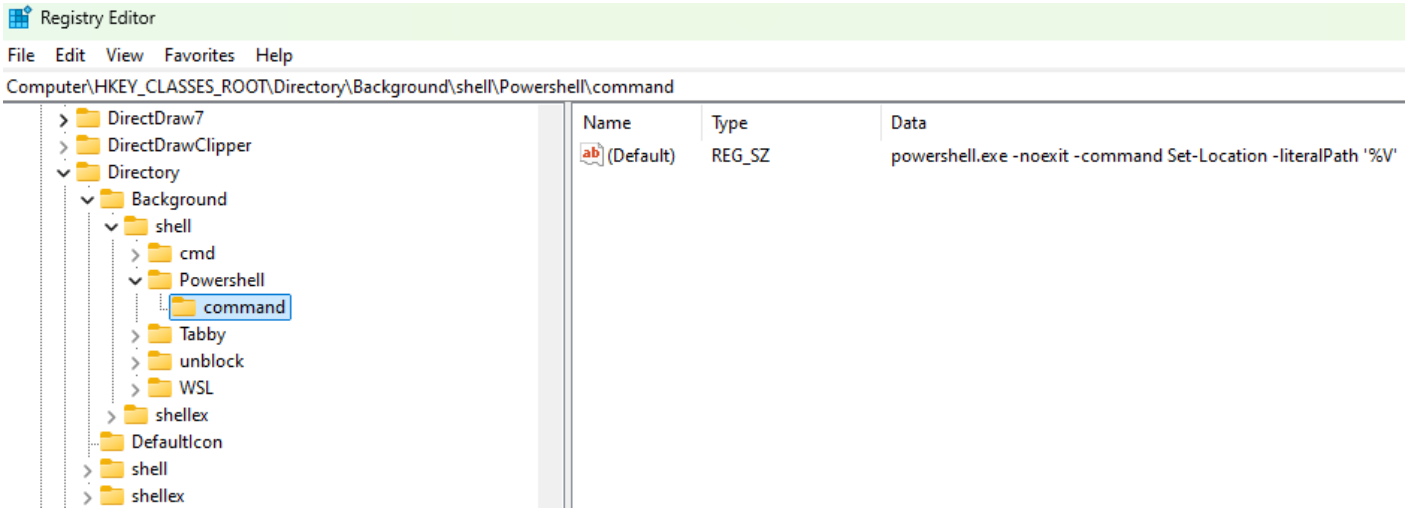
Les politiques de groupes et stratégies de sécurité locales appliquées à un utilisateur se trouvent à cet endroit. Il est possible d'y ajouter manuellement les entrées correspondant à des paramètres de GPO (adm/admx) pour paramétrer une machine même si elle n'est pas jointe à un domaine. Le site suivant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

Revision #11
Created 2025-01-25 17:26:45 UTC by Alexandre Arsenault-Jetté
Updated 2026-02-05 20:36:12 UTC by Alexandre Arsenault-Jetté