LogParser

Un petit post sur un outil bien pratique pour tous ceux qui rament pour écrire des scripts sous Windows.

Un des outils indispensables dont toute production doive se doter est un analyseur de journaux d’erreur.

Logparser est un petit exécutable fourni gratuitement par Microsoft et qui permet de lire des fichiers structurés

propriétaires tels que les eventlogs \*.EVT, mais aussi les fichiers CVS, ETW, REG, etc…

Tout d’abord il s’agit de le télécharger et de l’installer en trois ou quatre clics.

Je passe rapidement sur l’install, il faudra juste bien penser à ajouter le chemin de logparser.exe dans votre PATH.

Pour le télécharger:

http://www.microsoft.com/en-us/download/details.aspx?id=24659

L’avantage principal est qu’il utilise un pseudo langage proche du SQL pour effectuer des recherches.

-i: Donne le type d’entrée du fichier. exemple, -i:EVT indique que l’on souhaite lire un fichier \*.evt.

S’il n’est pas indiqué, logparser le trouve tout seul en fonction de l’entrée.

-o: Donne le format de sortie. Par exemple -o:XML pour écrire au format XML.

S’il n’est pas indiqué, logparser le trouve tout seul en fonction du fichier indiqué dans la clause ‘into‘.

-stats: ON/OFF: si les stats sont indiquées, alors logparser renvoie le nombre de lignes traitées et le temps passé.

-q: ON/OFF: mode quiet, par exemple pour éliminer les entêtes