ReadEventLogFile

Soumis par Gilles LAURENT
27-01-2016

Afficher le contenu d'un fichier d’événement Windows (.evt / .evtx) dans le bloc-notes
Je réalise l'installation d'un certain nombre de correctifs sur des parcs de machines Windows 7 / 8.1 en utilisant les fichiers .msu et l'utilitaire wusa.exe inclus dans Windows. C'est une bonne idée de générer des fichiers journaux séparés pour chaque mise à jour sachant que wusa.exe supporte cette option en utilisant le paramètre /log:<nom du fichier>. Cependant, il s'avère que les fichiers journaux créés ne sont pas de simples fichiers texte. Lorsqu'ils sont ouvert dans Notepad ou Wordpad je constate qu'ils contiennent beaucoup de données binaire qui ne peuvent être lues via un simple éditeur de fichiers texte. Ces fichiers journaux se révèlent être au format .evt, format reconnu nativement par l'observateur d'événements Windows eventvwr.exe. Il me semble un peu lourd d'utiliser l'observateur d'événements à cet effet. J'ai donc développer le script PowerShell ReadEvtLogFile qui permet d'afficher en toute simplicité le contenu d'un fichier log au format .evt/.evtx dans le bloc-notes. La capture d'écran ci-dessous montre l'intégration du script au sein du menu SendTo de l'explorateur Windows.

Le contenu du fichier d'événement Windows s'affiche instantanément dans le bloc-notes. Bien qu'ici le fichier journal soit muni de l'extension .log, il est toutefois correctement décodé et affiché par le script.

Intégration du script au menu Envoyer vers ...1. Déposer le script PowerShell ReadEvtLogFile.ps1 dans un dossier quelconque2. Créer un nouveau raccourci avec les propriétés suivantes :
Dossier : %USERPROFILE%\AppData\Roaming\Microsoft\Windows\SendTo Cible : powershell.exe -NoProfile -WindowStyle Hidden -File <path>\ReadEvtLogFile.ps1 [-OpenIfFailed] Nom : Event Log File Reader
Note : Penser à modifier la stratégie d'exécution des scripts Windows PowerShell via la Cmdlet Set-ExecutionPolicy Historique :
Version 1.1 - 20160128 - Introduces -OpenIfFailed switch to open the file with notepad on failureVersion 1.0 - 20160127 - Première Release Publique

Plateformes supportées :
Windows 7 et versions supérieures

Pré requis :
Microsoft Windows Powershell 2.0+Téléchargement :
Guide PDF : -
Archive : ReadEvtLogFile.zip