RunAsLoggedOnUser

Soumis par Gilles LAURENT
14-08-2007
Dernière mise à jour : 06-06-2017

Exécution d'un processus distant sous l'autorité de l'utilisateur connecté localement

L'idée de créer cet outil est tout d'abord née de plusieurs sollicitations privées. L'évènement déclencheur à été la conversation avec Nicolas et Jacques sur le forum windows.server portant sur le même sujet. Bon ! retour de congés, j'ai donc retroussé les manches histoire de me mettre en jambes et également pour faire chauffer le compilateur tout poussiéreux avant la reprise :-)

Tout d'abord, il est bon de savoir que cet outil n'a d'intérêt que s'il s'exécute sous une autorité différente de celle de l'utilisateur courant (i.e l'utilisateur ayant ouvert une session localement sur son poste de travail). Son application principale consiste donc à être lancé sur une machine distante à l'aide d'un outil permettant l'exécution à distance d'un processus tel que l'outil PSExec de Windows sysinternals.

Quelle est donc l'utilité d'un tel outil vous demandez-vous? Et bien actuellement, l'outil PSExec ne permet d'exécuter un processus sur une machine distante que sous l'autorité :

- de l'utilisateur connecté sur la machine exécutant PSExec (moyennant droits)
- de l'utilisateur spécifié avec les arguments -u et -p
- du compte LocalSystem avec l'argument -s

RunAsLoggedOnUser ouvre une nouvelle possibilité ! Celle d'interagir de manière dynamique avec la session de l'utilisateur de la machine distante. Les commandes fournis s'exécutant dans le contexte de l'utilisateur, il est donc désormais possible de connecter un lecteur réseau à distance, de connecter une imprimante réseau à la volée, de démarrer des applications graphiques à distance et cela dans le contexte de l'utilisateur, de modifier le profil de l'utilisateur connecté (registre HKCU, système de fichiers propre à l'utilisateur, variables d'environnement ...), ... et pour les commandes de type console (i.e CUI), celles-ci pourront même s'exécuter en toute transparence du point de vue de l'usager du poste de travail.

RunAsLoggedOnUser s'intègre réellement dans la session de l'utilisateur connecté (primary token Vs impersonated token) : Le profil utilisateur est disponible, les variables d'environnement propres à l'utilisateur sont définies et l'accès au réseau de l'entreprise est totalement accessible au même titre et avec les mêmes droits (ACL) que l'utilisateur connecté localement sur le poste distant. Bien sûr, il est nécessaire de disposer d'un compte privilégié pour exécuter cet outil à distance, sécurité NT oblige bien évidemment ! Le compte exécutant la commande RunAsLoggedOnUser doit tout d'abord être en mesure de se connecter à la machine distante, puis avoir les droits et la possibilité de s'élever en tant que service NT (LocalSystem ou LocalService). Cela tombe bien ! L'outil PSExec permet déjà de réaliser les tâches requises ;-)

Une autre application possible concerne les tâches planifiées. Par exemple, exécuter une tâche planifiée sous l'autorité LocalSystem (Commande AT ou le planificateur de tâches) du poste de travail et donner la possibilité à la tâche planifiée d'exécuter des actions sous l'autorité de l'utilisateur connecté permettant ainsi d'interagir avec la session et les droits de l'utilisateur connecté localement.

Historique:

Version 1.0.0.5

- release x86 crt
- release x86 / x64 msvcrt12 (Visual C++ 2013 Redistribuable)
- compatibilité Vista/7/8/10 64 bits
- nouveau paramètre -debug permettant de rediriger les traces dans un fichier
- mise à jour de l'aide en ligne

Version 1.0.0.4

- nouveau paramètre -sid permettant de spécifier l'identificateur de session
- mise à jour de l'aide en ligne

Note : Le paramètre -sid permet de spécifier l'identificateur de session (session Id) dans laquelle la commande distante s'exécutera. L'identificateur de session peut être déterminé soit par le gestionnaire des services Terminal Server ou

par le gestionnaire des tâches après avoir ajouté la colonne "Identificateur de session" et coché l'option "Afficher les processus de tous les utilisateurs".

Version 1.0.0.3
- redirection automatique des flux stdin, stdout, stderr
- nouveau paramètre -wait permettant d'attendre la fin du processus distant
- possibilité d'ouvrir une console interactive sous l'autorité de l'utilisateur distant
- support de l'expansion retardée des variables d'environnement
- mise à jour de l'aide en ligne

Note : L'interpréteur de commandes cmd.exe (%comspec%) tente de résoudre automatiquement les variables d'environnement présentes sur la ligne de commandes avant l'exécution. Pour que les variables d'environnement soient résolues non pas sur le système local mais sur le système distant, il suffit d'encadrer les variables d'environnement avec des accolades. Par exemple, pour que la variable d'environnement système %computername% soit résolue sur le système distant, il suffit de spécifier la variable en utilisant la syntaxe {computername}.

Version 1.0.0.2
- tentative d'activation des privilèges avant la recherche du processus shell
- message "accès refusé" si le compte ne dispose pas des droits requis
- ajout du pré requis LocalSystem dans l'écran d'aide (Usage)

Version 1.0.0.1
- première release publique

Plateformes supportées:
Windows 2000/XP/2003/Vista/7/8/10 (32bits / 64bits)

Usage:
RunAsLoggedOnUser [-debug] [-hide] [-wait [timeout (s)]] [-sid sid] -cmd [path\]program [arguments]

Aide en ligne:
RunAsLoggedOnUser v1.0.0.5 (c) 2008-2017 Gilles LAURENT
Runs the specified executable file under the logged on user's authority
Usage : RunAsLoggedOnUser [-hide] [-wait [timeout (s)]] [-sid sid] -cmd [path\]program [arguments]
Commands :

-cmd <program> Name of application to execute
<arguments> Arguments to pass to the specified program
-debug Enables debug mode. Log file will be created in %TEMP%
-hide Runs the CUI (i.e console) program hidden on remote host
-sid <sid> Executes the program in the specified user session id
-wait [timeout (s)] Waits until the running process terminates or timeout

Examples:

:: Needs to run under the LocalSystem account or the current user !!
RunAsLoggedOnUser -cmd "notepad.exe %systemroot%\system32\eula.txt"

PSExec \\host -s -c RunAsLoggedOnUser.exe -wait -hide -cmd {comspec}
PSExec \\host -s -c RunAsLoggedOnUser.exe -hide -cmd "net use H: /d"
PSExec \\host -s -c RunAsLoggedOnUser.exe -cmd "cmd /c echo {computername}"

Téléchargement:
Guide PDF: -
Archive: RunAsLoggedOnUser.zip