

Explications exhaustives sur UAC (User Account Control)

Par Jean-Claude BELLAMY [MVP] - <http://www.bellamyjc.org>

UAC (User Account Control) est un dispositif né avec VISTA qui gère de façon très fine (et parfois un peu trop facilitant le transit intestinal!) les PRIVILÈGES.

Alors que les "permissions" (droits de lecture, écriture, exécution, ...) concernent des "objets" tels que des fichiers, dossiers, clefs de la BDR, les "privilèges" concernent les comptes utilisateurs.

Ces privilèges sont identifiés par des noms symboliques, qui indiquent à quoi ils correspondent.

Par exemple :

"SeSecurityPrivilege"

Gérer le journal d'audit et de sécurité

"SeTakeOwnershipPrivilege"

Prendre possession de fichiers ou d'autres objets

"SeLoadDriverPrivilege"

Charger et décharger les pilotes de périphériques

"SeSystemtimePrivilege"

Modifier l'heure système

"SeCreatePagefilePrivilege"

Créer un fichier d'échange

"SeBackupPrivilege"

Sauvegarder les fichiers et les répertoires

"SeRestorePrivilege"

Restaurer les fichiers et les répertoires

"SeShutdownPrivilege"

Arrêter le système

...

Sous VISTA, on dénombre 35 privilèges différents !

Suivant le type de compte (administrateur, "lambda", invité, ...) un privilège peut être :

- refusé (inexistant)
- attribué et désactivé
- attribué et activé

La plupart du temps, les privilèges sont désactivés.

Explications exhaustives sur UAC (User Account Control)

La liste des privilèges attribués à un compte est définie dans un "jeton" (token) fourni par le système lors de l'ouverture de session. (très exactement, c'est le processus système LSA = Local Security Authentication qui se charge de cela).

Quand un utilisateur désire exécuter une tâche particulière, le système contrôle tout d'abord s'il détient le ou les privilèges nécessaires

(p.ex. pour lancer une sauvegarde complète des disques, il faut détenir "SeBackupPrivilege")

S'il n'a pas ce privilège, il se fait jeter comme un malpropre !

S'il l'a, il faut ensuite que le logiciel concerné demande l'activation du privilège (car généralement la plupart des privilèges sont désactivés).

Puis une fois que l'action est terminée, le logiciel (s'il est bien écrit) va désactiver le privilège, dans un but de sécurité.

Microsoft s'est rendu compte que ce système n'était pas suffisant, en particulier quand le compte en cours est un administrateur.

En effet, si un processus "malveillant" (= une cochonnerieware telle que virus, ver, cheval de Troie, ...) a pu se lancer sous ce compte admin, il va se dépêcher d'activer tous les privilèges possibles, et commettre tous les dégâts qu'il veut.

Afin d'empêcher cela, à partir de VISTA, quand un membre du groupe des administrateurs ouvre une session, le système ne lui donne pas de jeton correspondant à son statut d'admin (et donc avec tous les privilèges attribués), mais seulement un "jeton au rabais", quasi identique à celui d'un compte lambda.

Ainsi un processus "alien" va se retrouver coincé, puisque ne possédant que très peu de privilèges.

Quand un processus a besoin de privilèges élevés, cela va provoquer l'ouverture d'une boîte de dialogue indiquant que l'appli en cours a besoin d'une autorisation supplémentaire, réalisée différemment suivant que :

Explications exhaustives sur UAC (User Account Control)

- on appartient au groupe des admins,

Dans ce cas, il suffit d'appuyer sur un bouton de continuation
(ou d'annulation si on a des doutes sur le processus)

- on n'appartient pas au groupe des admins

Dans ce cas, il faut sélectionner un compte administrateur
et donner son mot de passe, puis appuyer sur un bouton
de continuation (ou d'annulation ...)

A ce moment là le système (LSA) va fournir un "jeton complet" du compte
administrateur concerné, qui sera alors doté de tous les privilèges prévus.

Privilèges attribués dans le jeton "lambda" :

SeChangeNotifyPrivilege

SeTimeZonePrivilege

SeIncreaseWorkingSetPrivilege

SeUndockPrivilege

SeShutdownPrivilege

Privilèges attribués EN PLUS dans le jeton "complet" (ou si UAC est désactivé) :

SeBackupPrivilege

SeCreateGlobalPrivilege

SeCreatePagefilePrivilege

SeCreateSymbolicLinkPrivilege

SeDebugPrivilege

SeImpersonatePrivilege

SeIncreaseBasePriorityPrivilege

SeIncreaseQuotaPrivilege

SeLoadDriverPrivilege

SeManageVolumePrivilege

SeProfileSingleProcessPrivilege

SeRemoteShutdownPrivilege

SeRestorePrivilege

SeSecurityPrivilege

SeSystemEnvironmentPrivilege

SeSystemProfilePrivilege

SeSystemtimePrivilege

SeTakeOwnershipPrivilege

Explications exhaustives sur UAC (User Account Control)

NB: le compte "Administrateur" (ou "Administrator" en anglais, ...), c'est à dire le compte dont le SID (Security IDentifier) se termine par "500", n'est pas soumis à cette règle des 2 jetons (un lambda et un "complet"), car il lui est attribué uniquement le jeton complet dès qu'il ouvre une session.

Donc le comportement de VISTA vis à vis de ce compte est le même que celui de XP (et précédents) vis à vis de n'importe quel compte administrateur.

Si on est masochiste, on peut paramétrer le système afin que ce compte soit soumis aux mêmes règles d'élévation de privilèges :

Il faut modifier l'entrée

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken

en lui affectant la valeur 1

Comme Microsoft a estimé que c'était risqué de l'utiliser, le compte "Administrateur" est désactivé par défaut.

A moins de l'activer (par la commande "NET USER Administrateur /ACTIVE:YES"), on ne peut pas ouvrir de session ordinaire sous ce compte, mais seulement en mode sans échec.

Pour les "vieux briscards" qui ont l'habitude de manipuler des comptes admins (sous NT, W2K, XP, W2K3), ce système est assez facilitant le transit intestinal! ;-)

On peut le désactiver totalement ou au minimum en limiter les effets.

Je décris les manip sur mon site :

<http://www.bellamyjc.org/fr/windowsvista.html#UAC>

On peut néanmoins CONSERVER UAC, MAIS masquer la boîte de dialogue d'élévation de privilèges (pour les administrateurs) en modifiant l'entrée :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin

en lui affectant la valeur 0

Il est également recommandé de désactiver le changement de bureau quand on élève les privilèges.

En effet, par défaut, la boîte de dialogue de continuation est affichée dans un AUTRE BUREAU. (pour éviter qu'un "alien" puisse simuler un "sendkey" sur le bouton "continuer")

Explications exhaustives sur UAC (User Account Control)

Si bien que si on est en train d'effectuer un dépannage à distance, et bien on ne verra JAMAIS ce dialogue (seul le bureau principal est transmis)!!!

Il faut donc modifier l'entrée

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop

en lui affectant la valeur 0

En ce qui concerne "VirtualStore", cela a été conçu pour éviter des plantages trop violents dans le cas où l'utilisateur n'a pas les privilèges nécessaires pour effectuer certaines tâches de CONFIGURATION de logiciels.

Cela concerne des ÉCRITURES dans :

- l'arborescence de la BDR HKLM\Software
- l'arborescence de dossiers %PROGRAMFILES%
- l'arborescence de dossiers %SYSTEMROOT%

Seuls les admins avec leur jeton complet ont le droit d'écrire dedans (sauf modif volontaire par un admin)

Dans les autres cas, l'écriture est redirigée (de façon transparente) dans le dossier %LOCALAPPDATA%\VirtualStore, dans lequel on trouve des sous-répertoires :

Program Files

ProgramData

Windows

et en ce qui concerne HKLM, la redirection est faite dans

HKCU\Software\Classes\VirtualStore\Machine\Software

Dans l'explorateur, si on sélectionne un dossier protégé tel que %PROGRAMFILES% ou %SYSTEMROOT%, on voit apparaître un bouton "Fichiers de compatibilité" qui redirige automatiquement vers le dossier de virtualisation associé.

NB: SEULS les fichiers de configuration (.ini, .xml, ...) sont redirigés.

Les autres fichiers (binaires p.ex.) seront refusés.

La virtualisation peut être désactivée en mettant à 0 l'entrée

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization

Explications exhaustives sur UAC (User Account Control)

En ce qui concerne VirtualStore, si on désactive l'UAC, on désactive par la même occasion la virtualisation.

Donc, si "EnableLUA" est à 0 (= UAC totalement désactivé), la virtualisation l'est aussi, quelle que soit la valeur de "EnableVirtualization".

--

May the Force be with You!

La Connaissance s'accroît quand on la partage

Jean-Claude BELLAMY [MVP] - <http://www.bellamyjc.org>