Le contrôle de compte d'utilisateur

Windows Vista a introduit un nouveau concept de sécurité appelé UAP ou *User Account Protection* (en français, contrôle de compte d'utilisateur). D'autres termes sont utilisés : *Least-Privilege User Accounts* ou *Limited User Accounts* (LUA). Ce concept, désormais appelé UAC (*User Account Control*), a été conservé et amélioré dans Windows 7 puis dans Windows 8 et finalement dans Windows 10, pour qu'il apparaisse moins contraignant pour l'utilisateur. Cette fonctionnalité permet de limiter le champ d'action des logiciels malveillants.

Les utilisateurs créés par Windows ont le statut d'administrateur protégé, c'est-à-dire que la fonctionnalité UAC est activée pour ces comptes. Ce n'est pas le cas du compte Administrateur qui désigne le compte intégré au système d'exploitation mais qui, par défaut, est désactivé.

Quand un utilisateur a le droit d'interagir sans restriction avec le système, il peut installer une application, écrire dans la branche du registre HKEY_LOCAL_MACHINE, installer des périphériques, démarrer des services, etc.

En mode protégé, tous les processus initiés par un administrateur sont lancés avec un minimum de privilèges. Si, par exemple, vous ouvrez un programme à partir du menu **Démarrer**, l'application va s'exécuter dans un contexte restreint avec les mêmes privilèges que ceux qui vous ont déjà été accordés.

Si l'application requiert pour pouvoir s'exécuter convenablement, des privilèges élevés, il faudra, dans ce cas, que le compte d'administrateur puisse exécuter le processus de manière non restrictive. Le processus hérite alors des nombreux avantages accordés par cette élévation de privilèges (*Over The Shoulder* (OTS) *elevation*). Quand un programme nécessite de s'exécuter en mode d'élévation de privilèges, une boîte de dialogue vous en avertit. Il n'y a donc pas, par défaut, de possibilité d'élever les privilèges accordés à une application sans le consentement éclairé de l'utilisateur. Nous allons voir dans la suite de cette section qu'il est désormais possible, dans Windows, de désactiver la demande de confirmation du processus d'élévation de privilèges.

Notez toutefois que le service reste actif même lorsque vous sélectionnez le paramètre le moins sécurisé pour cette fonction.

1. Les comptes d'utilisateurs

À chaque fois que vous ouvrez une session d'utilisateur, un jeton d'accès (*token*) vous est attribué. Ce jeton d'accès dresse la liste des privilèges dont vous disposez et énumère les ressources auxquelles vous accédez ou tentez d'accéder. Chaque ressource disponible sur le système possède une liste de contrôle d'accès (DACL) qui tient la liste des utilisateurs et des services pouvant l'atteindre, ainsi que le niveau de permission qu'ils possèdent.

Par défaut, les administrateurs reçoivent deux jetons d'accès :

- Un jeton en tant qu'administrateur.
- Un jeton en tant qu'utilisateur standard et c'est ce dernier qui est attribué par défaut.

Lors de l'élévation d'un processus, un utilisateur reçoit les mêmes privilèges que ceux de l'administrateur. En d'autres termes, il obtient le même jeton d'accès. Le mécanisme qui vous permet de passer d'une identité à l'autre est appelé *Admin Approval Mode* (AAM).

2. Les niveaux d'intégrité

Le contrôle d'intégrité (MIC ou *Mandatory Integrity Control*) est un autre mécanisme apparu sous Vista. Il est contrôlé par une liste de contrôle d'accès ACE dans la liste système de contrôle d'accès (SACL) de tout objet "sécurisable" (clé du Registre, fichier, processus, etc.).

Chaque processus possède un niveau d'intégrité mais aussi le processus enfant qui hérite du niveau d'intégrité du processus l'ayant "enfanté". Ces niveaux d'intégrité sont appelés *Integrity access Levels* ou IL.

Signalons que le niveau d'intégrité est associé à la SACL et non à la DACL.

Un processus ne peut interagir avec un niveau d'intégrité possédant des privilèges plus élevés. Les API (*Application Programming Interface*) échoueront à partir d'un processus possédant un niveau d'intégrité faible quand il sera utilisé contre un processus d'un niveau d'intégrité plus élevé. Ceci étant fait pour éviter les risques d'attaques ou d'intrusions malveillantes.

Les entrées du Registre peuvent seulement être écrites à partir d'un processus possédant un fort niveau d'intégrité. C'est pourquoi Internet Explorer (processus d'intégrité faible) ne vous permet d'écrire que dans des portions congrues de l'Explorateur ou du Registre Windows.

Les niveaux d'intégrité sont les suivants :

- **High (haut)** : correspond aux privilèges système d'administrateur. Ce niveau de privilèges vous donne le droit d'écrire dans le répertoire \Program Files et la branche du Registre HKEY_LOCAL_MACHINE.
- **Medium (moyen)** : correspond au niveau Utilisateur. Ce niveau de privilèges vous donne le droit d'écrire dans votre répertoire d'utilisateur et la branche du Registre HKEY_CURRENT_USER.
- **Low (faible)** : ce niveau ne vous permet que d'écrire dans les zones sans niveau de privilèges comme la clé HKEY_CURRENT_USER\Software\LowRegistry ou les répertoires nommés LOW et qui sont présents dans l'Explorateur Windows. Par ailleurs, une fonctionnalité appelée "Interface utilisateur d'isolation des privilèges" (*User Interface Privilege Isolation* ou UIPI) vient renforcer ce dispositif et ce afin de prévenir les attaques de type "Escalade des privilèges".

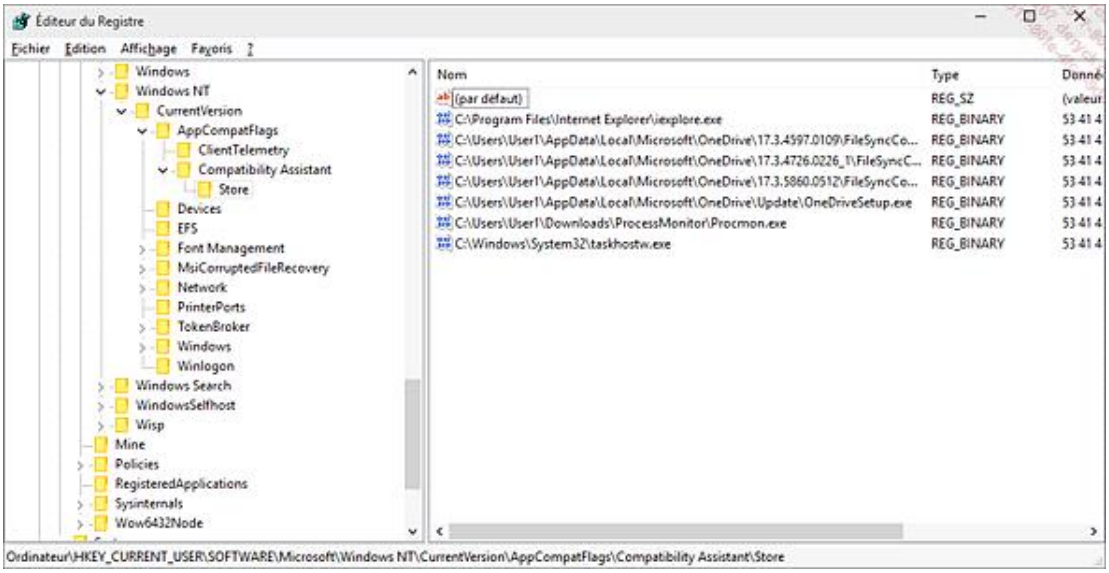
Windows 8 a ajouté aux niveaux d'intégrité précédents le niveau d'isolation **AppContainer**, également présent dans Windows 10. Ce niveau d'isolation est celui utilisé par défaut pour l'exécution des applications Windows Store.

3. L'élévation de privilèges

Certaines opérations ne sont pas adaptées à l'utilisation des listes de contrôle d'accès. Imaginons qu'un utilisateur ait besoin de sauvegarder un ensemble de fichiers, il est beaucoup plus simple de lui accorder le privilège de sauvegarde quelles que soient les permissions NTFS attachées aux fichiers plutôt que de modifier un à un le masque des permissions de chacune des ressources auxquelles il peut accéder. Un processus peut recevoir une élévation de privilèges dans les circonstances suivantes :

- Si l'application est une plate-forme d'installation comme Windows Installer ou Install Shield.
- Si l'application possède une entrée dans la couche de compatibilité des applications ou la base de données de compatibilité des applications.

Dans le premier cas, une entrée sera présente dans cette arborescence du Registre : HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store.



Dans le second cas, un fichier portant l'extension *.sdb* aura été créé par l'exécutable CompatAdmin.exe.

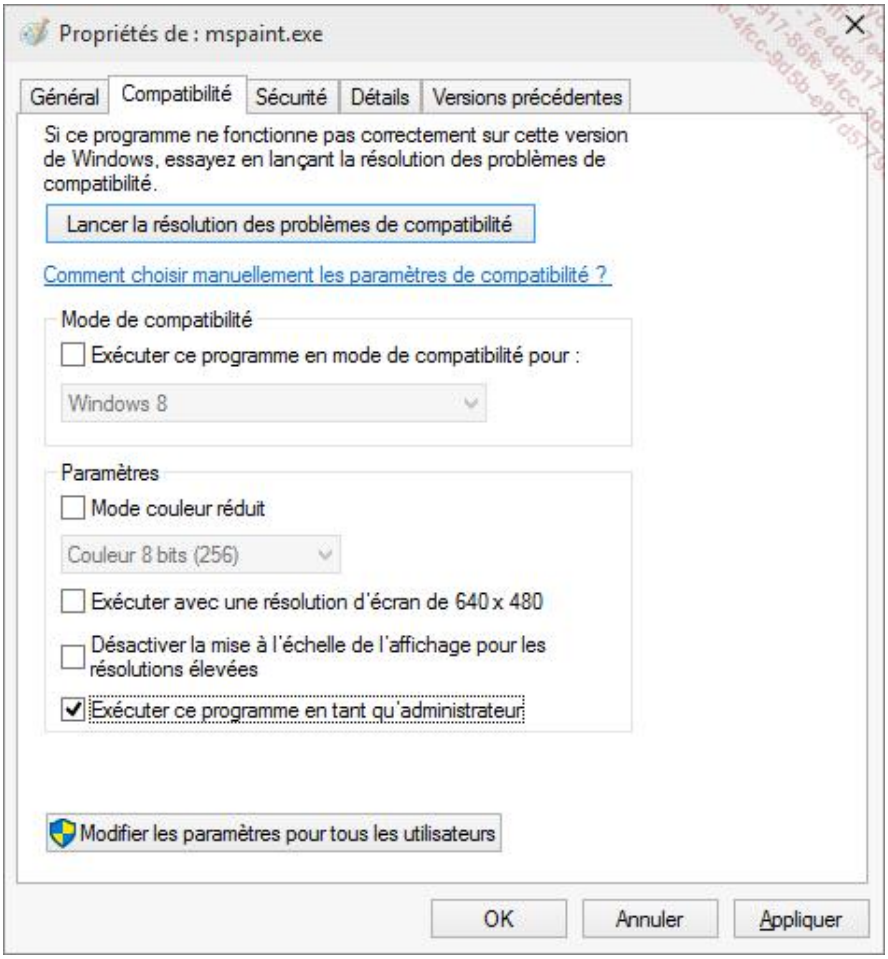
- Si le fichier manifeste de l'application contient une requête de niveau d'exécution précisant que l'application requiert un niveau de privilèges élevés.

Vous pouvez aussi invoquer cette élévation de privilèges en cochant la case **Exécuter en tant qu'administrateur** dans le menu contextuel de l'application ou du raccourci. Voyons comment procéder :

- Avec le bouton droit de la souris cliquez sur un des programmes présents à partir du menu **Démarrer**.
- Sélectionnez la commande **Exécuter en tant qu'administrateur**.

Afin d'automatiser ce processus, suivez cette procédure :

- Recherchez sur le disque le répertoire d'installation du programme à exécuter. Une fois le fichier exécutable localisé, effectuez un clic droit puis cliquez sur le sous-menu **Propriétés**.
- Cliquez sur l'onglet **Compatibilité** puis cochez la case **Exécuter ce programme en tant qu'administrateur**.



À partir d'un raccourci, la procédure est un peu différente :

- Effectuez un clic droit sur le raccourci puis cliquez sur le sous-menu **Propriétés**.
- Cliquez sur l'onglet **Raccourci** puis sur le bouton **Avancé...**.
- Cochez la case **Exécuter en tant qu'administrateur**.

Voici une autre possibilité :

- Dans la zone de texte **Rechercher** placée au-dessus du menu **Démarrer**, saisissez : **cmd**.
- Effectuez un clic droit sur la mention **cmd.exe** puis cliquez sur la commande **Exécuter en tant qu'administrateur**.

À partir de là, toutes les commandes que vous exécuterez à partir de l'invite de commandes seront lancées avec des autorisations d'administrateur.

Il y a deux autres scénarios permettant une élévation de privilèges :

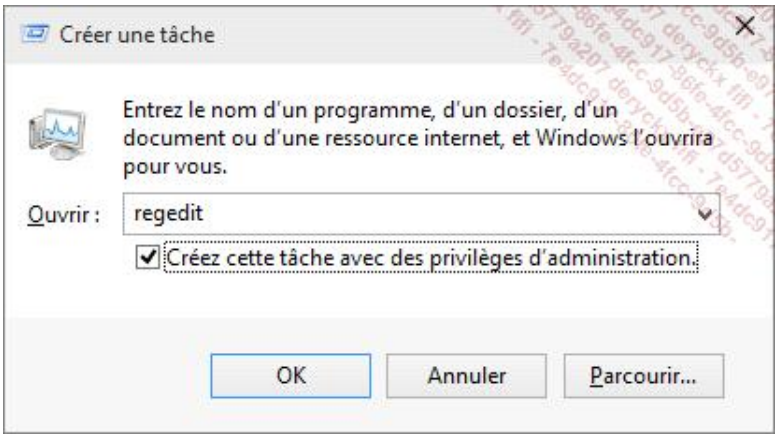
- Quand un programme est initié à partir d'un processus ayant déjà reçu cette élévation de privilèges. Un bon exemple est le fait que beaucoup d'outils doivent être lancés à partir d'une fenêtre d'invite de commandes exécutée en tant qu'administrateur.
- Quand un programme est lancé à partir du Gestionnaire des tâches :

- Depuis la zone de recherche à droite du menu **Démarrer**, saisissez : `taskmgr`.
- Cliquez sur le lien **Plus de détails**.

- Cliquez sur **Fichier - Exécuter une nouvelle tâche**.

Notez que vous pouvez aussi cliquer avec le bouton droit de la souris sur la barre des tâches puis sur la commande correspondante.

- Activez la case à cocher **Créez cette tâche avec des privilèges d'administration**.



Dans ce cas, le Gestionnaire des tâches lance les processus en utilisant l'API CreateProcess et non CreateRestrictedProcess.

4. Le processus de virtualisation

Un processus initié par un compte d'utilisateur standard ne peut écrire dans la branche du Registre HKEY_LOCAL_MACHINE. Cette particularité va, bien évidemment, provoquer des problèmes puisque, dans beaucoup de cas, l'application ne pourra fonctionner normalement. Afin de contourner cette difficulté, depuis Vista a été mis en place un mécanisme appelé Virtualisation. Quand un processus possédant des privilèges faibles doit écrire dans une zone protégée du Registre ou de l'Explorateur, les données sont instantanément transférées dans une zone dédiée à l'utilisateur. Ces zones "Utilisateur" prennent alors le pas sur les zones "Ordinateur".

Quand un processus ne peut écrire dans la branche HKEY_LOCAL_MACHINE\Software, les écritures manquées sont inscrites dans : HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\Software

Le processus de virtualisation des fichiers opère, quant à lui, ce type de substitution : %Profil_d'utilisateur%\AppData\Local\VirtualStore\Program Files pour %Program Files%, %Profil_d'utilisateur%\AppData\Local\VirtualStore\Windows pour %Windir%, etc.

Les processus sont virtualisés, sauf dans les cas suivants :

- Ils sont initiés avec des privilèges d'administrateur.
- Le fichier exécutable contient un manifeste appelé requestedExecutionLevel.
- Ils concernent des opérations qui ne sont pas initialisées à partir d'une session interactive.

5. Le contrôle de compte d'utilisateur en action

Quand une application ne vous propose pas automatiquement d'être initiée en tant qu'administrateur il est possible :

- D'accéder au menu contextuel du raccourci ou du fichier exécutable puis de cliquer sur la commande **Exécuter en tant qu'administrateur**.
- De lancer l'application à partir d'une autre application qui, elle, a été exécutée en tant qu'administrateur.

Quand à partir d'un compte d'administrateur vous lancez une application nécessitant une élévation de privilèges, vous obtenez ce type de boîte de dialogue : "Voulez-vous autoriser cette application à apporter des modifications à votre appareil".

À partir d'un compte d'utilisateur standard il vous sera demandé, pour continuer, le mot de passe d'un compte possédant des privilèges d'administrateur.

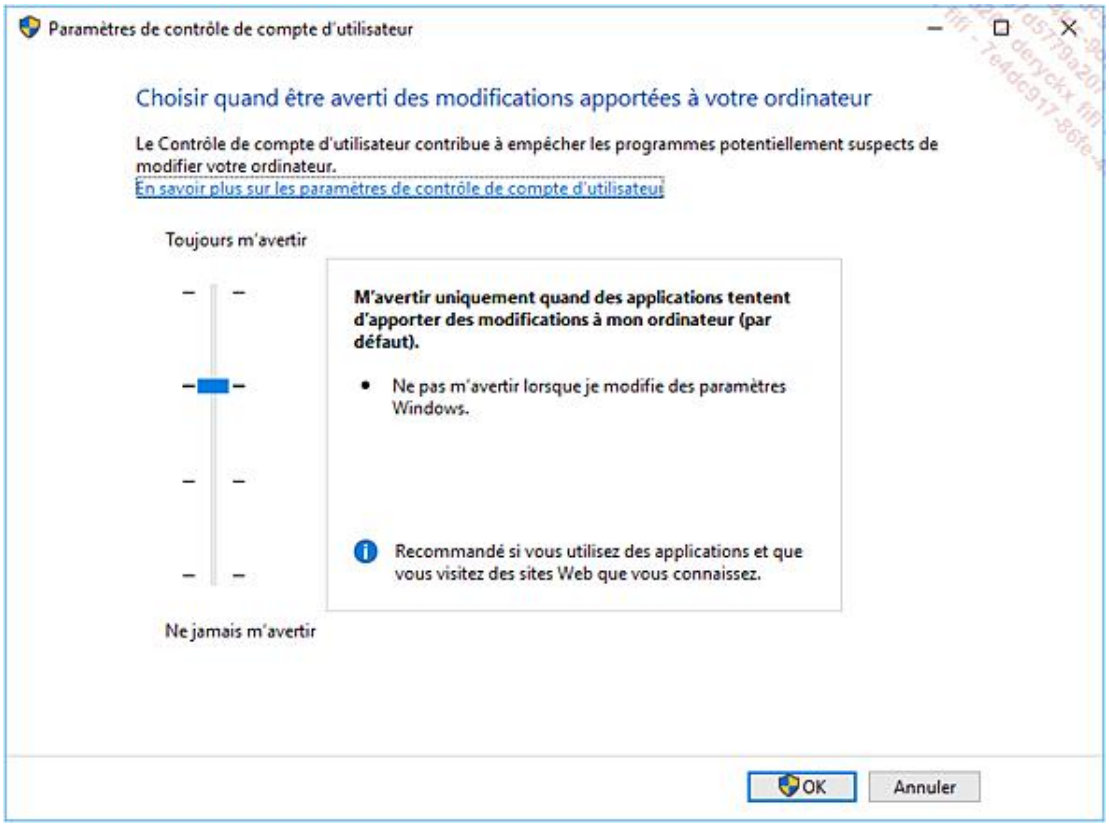
Le schéma suivant :

- L'application est analysée par le système d'exploitation.
- Si l'éditeur est Microsoft ou si l'application a été signée numériquement, il vous sera signifié que Windows a besoin de votre autorisation pour continuer (bandeau bleu).
- Si l'application n'a pas été signée numériquement, il vous sera signalé qu'un programme non identifié veut accéder à votre ordinateur (bandeau orange).
- Si l'application est interdite, il vous sera notifié que le programme a été bloqué. Dans ce cas :
  - Tentez de débloquer le programme en localisant son emplacement : Faites un clic droit et dans le premier onglet, cochez **Débloquer**.
  - Vérifiez également les paramètres de l'UAC. Il est peut-être réglé de manière trop élevée.

De plus, il existe dans l'interface graphique un certain nombre d'indications signalant qu'une action nécessite une élévation de privilèges :

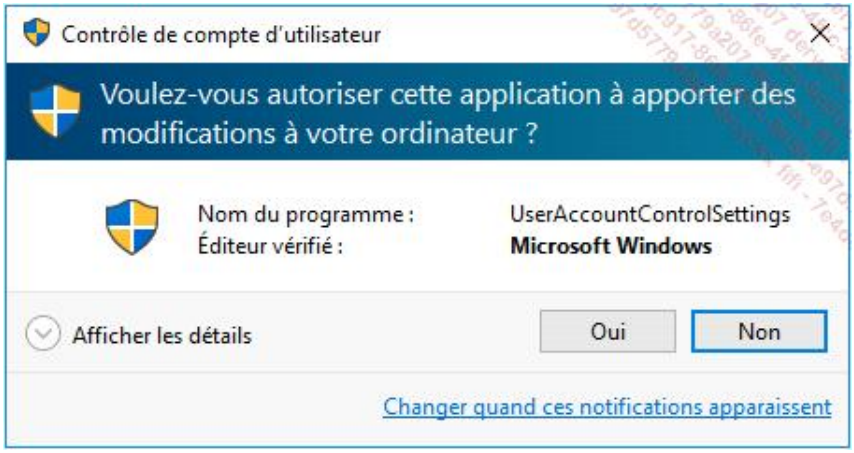
1. Rendez-vous dans le **Panneau de configuration**, section **Comptes d'utilisateurs**, puis **Comptes d'utilisateurs**.
2. Sélectionnez l'option **Modifier les paramètres de contrôle du compte d'utilisateur**.

Le bouton **OK** est rehaussé du blason représentant le bouclier du Centre de sécurité.



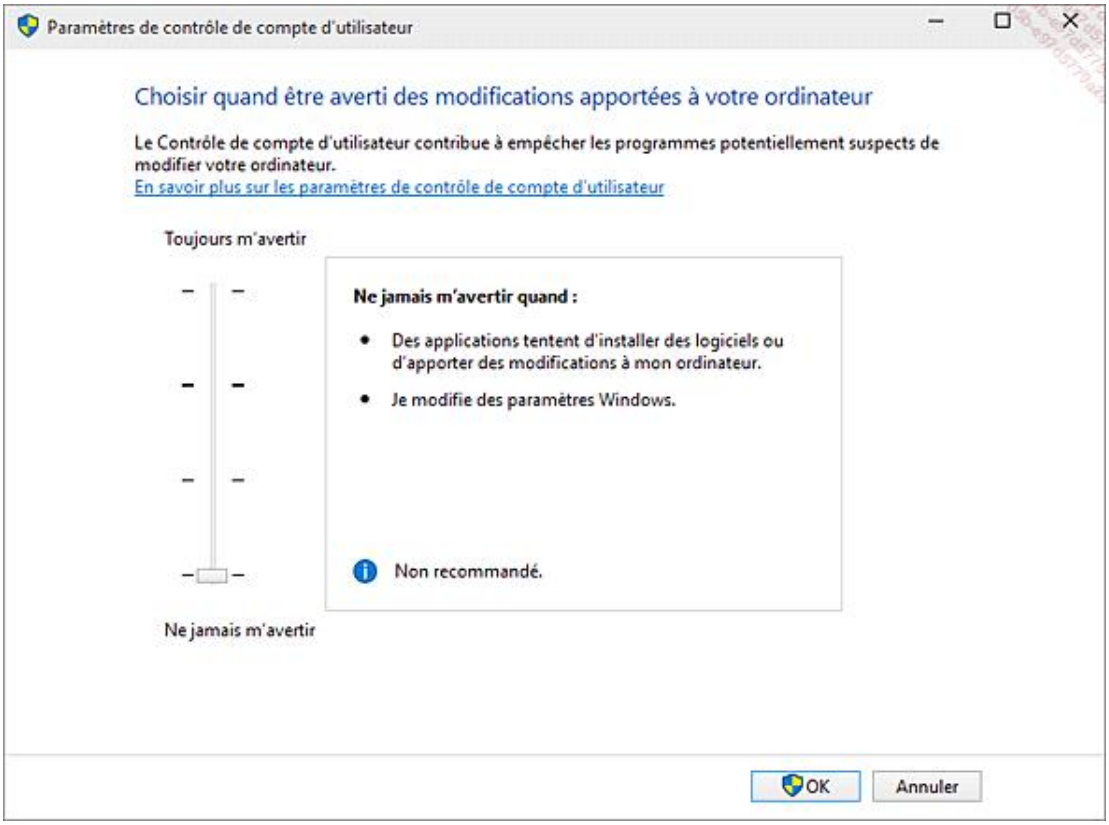
- Cliquez sur ce bouton.

Vous pouvez cliquer sur le bouton **Afficher les détails** afin de savoir quels sont les fichiers système qui seront exécutés.



6. Désactiver le contrôle de compte d'utilisateur

- À partir du **Panneau de configuration**, dans la section **Comptes d'utilisateurs - Comptes d'utilisateurs**, sélectionnez l'option **Modifier les paramètres de contrôle du compte d'utilisateur**.
- Configurez la fonctionnalité en déplaçant le curseur sur l'option **Ne jamais m'avertir**. Cliquez sur le bouton **OK** pour valider le nouveau paramétrage.



Vous pouvez aussi utiliser l'utilitaire de configuration système :

- Dans la zone de texte **Rechercher** placée à droite du menu **Démarrer**, saisissez : `msconfig`.
- Cliquez sur l'onglet **Outils**.
- Sélectionnez **Modifier les paramètres du contrôle des comptes d'utilisateurs** puis cliquez sur le bouton **Lancer**.

Attention, le contrôle de compte utilisateur n'est pas totalement désactivé, même si vous sélectionnez l'option **Ne jamais m'avertir**. Si vous désirez toutefois le désactiver totalement, vous devrez configurer la valeur EnableLUA à 0 dans la clé de registre : **HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows - CurrentVersion - Policies - System**.

Attention toutefois, la désactivation complète du contrôle de compte utilisateur impacte le fonctionnement des applications Windows Store puisque dans ce cas aucune application ne pourra être lancée.

7. Paramétrer le contrôle de compte d'utilisateur

Examinons maintenant les différents paramètres qui sont à notre disposition en utilisant l'Éditeur d'objets de stratégie de groupe.

- Pour cela, saisissez `gpedit.msc` dans la zone de recherche.
- Vous devez ouvrir cette arborescence : **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Options de sécurité**.

Nous avons indiqué à chaque fois les manipulations correspondantes dans le Registre puisque l'Éditeur d'objets de stratégie de groupe n'est pas installé dans beaucoup de versions de Windows.

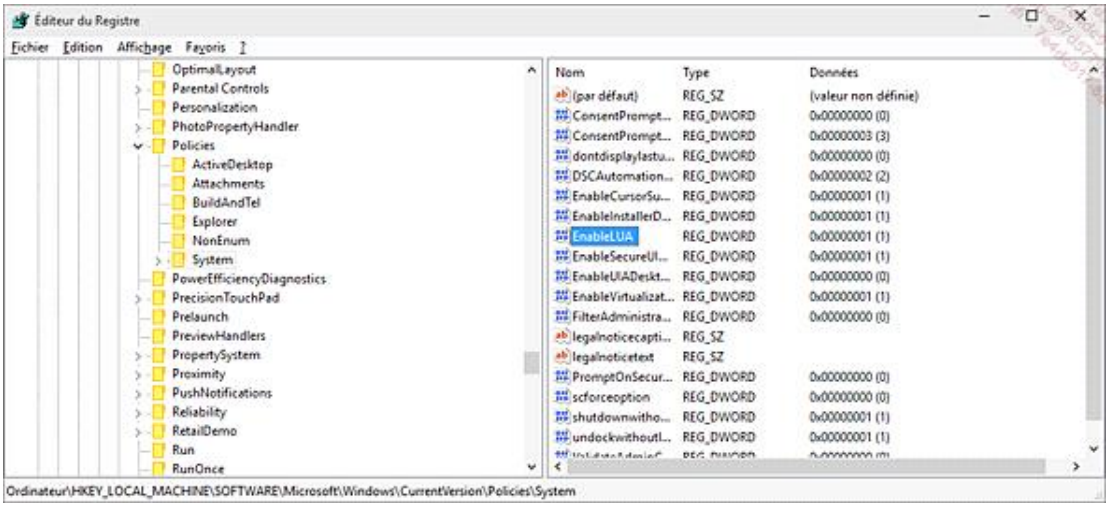
Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur

Si cette stratégie est désactivée, le type d'utilisateur du mode Approbation administrateur et toutes les autres stratégies UAC relatives seront désactivés. En clair, cela revient à supprimer le contrôle du compte d'utilisateur. Une fois que vous avez désactivé cette stratégie, redémarrez votre machine.

- Si vous utilisez la commande `Exécuter`, une mention va vous prévenir que cette tâche sera créée avec les autorisations d'administrateur.
- Si vous ouvrez le Centre de sécurité de Windows, une mention vous avertira que le contrôle du compte utilisateur est désactivé.

Cela correspond à cette manipulation dans le Registre Windows :

- Clé : **HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows - CurrentVersion - Policies - System**
- Valeur DWORD : EnableLUA
- Données de la valeur : 0.



Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur

Cette stratégie vous permet de paramétrer le comportement de la boîte de dialogue lors d'une demande d'élévation de privilèges initiée à partir d'un compte possédant des privilèges d'administrateur. Il y a six choix possibles :

- **Demande d'informations d'identification sur le bureau sécurisé** : l'administrateur sera invité sur le bureau sécurisé (environnement de bureau estompé ou obscurci) à renseigner un nom d'utilisateur privilégié et un mot de passe.
- **Demande de consentement sur le bureau sécurisé** : l'administrateur sera invité sur le bureau sécurisé (environnement de bureau estompé ou obscurci) à sélectionner l'action Autoriser ou Refuser.
- **Demande d'informations d'identification** : l'administrateur sera invité à renseigner un nom d'utilisateur privilégié et un mot de passe directement sur le bureau actif.
- **Demande de consentement** : l'administrateur sera invité à sélectionner l'action Autoriser ou Refuser sur le bureau actif.
- **Demande de consentement pour les binaires non Windows** : pour les applications externes à Microsoft, l'administrateur sera invité sur le bureau sécurisé (environnement de estompé ou obscurci) à sélectionner l'action

Autoriser ou **Refuser**.

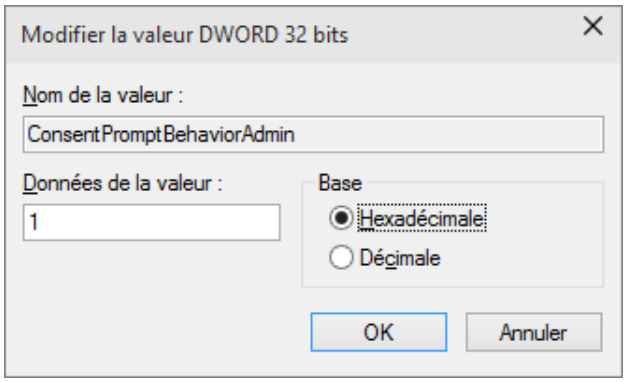
- **Élever les privilèges sans invite utilisateur** : il n'y aura pas de demande de consentement transmise à l'administrateur.

Dans ce dernier cas, le contrôle de compte d'utilisateur reste actif mais aucune boîte de dialogue ne vient interrompre vos tâches de maintenance.

- Clé : **HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows - CurrentVersion - Policies - System**
- Valeur DWORD : ConsentPromptBehaviorAdmin

Les valeurs possibles sont :

- 0 : Élever les privilèges sans invite utilisateur
- 1 : Demande d'informations d'identification sur le bureau sécurisé
- 2 : Demande de consentement sur le bureau sécurisé
- 3 : Demande d'informations d'identification
- 4 : Demande de consentement
- 5 : Demande de consentement pour les binaires non Windows



Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation

Cette stratégie détermine si la demande d'élévation effectuera la demande sur le Bureau des utilisateurs interactifs ou sur le Bureau sécurisé. Ce paramètre évite l'effet d'estompement ou d'obscurcissement dès qu'une élévation de privilèges est demandée.

- Clé : **HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows - CurrentVersion - Policies\System**
- Valeur DWORD : PromptOnSecureDesktop
- Données de la valeur : 0.

Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

Cette stratégie détermine le comportement du mode Approbation administrateur pour le compte Administrateur intégré. L'Administrateur intégré ouvrira une session en mode Approbation administrateur et devra donner son approbation pour toutes les opérations qui requièrent une élévation de privilège. Si cette stratégie est désactivée, l'Administrateur pourra exécuter toutes les applications avec des privilèges d'administration complets. Si vous

utilisez souvent le compte Administrateur, cette stratégie est intéressante à utiliser.

- Clé : **HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows - CurrentVersion - Policies - System**
- Valeur DWORD : FilterAdministratorToken
- Données de la valeur : 0.