

# Principe de moindre privilège

Le principe de moindre privilège est, comme son nom l'indique, un principe qui consiste à lancer chaque tâche avec un compte utilisateur qui a exactement les permissions nécessaires à l'accomplissement de cette tâche.

Dans la pratique cela n'est bien sûr pas toujours réalisable mais il convient de toujours faire au mieux afin d'être le plus proche du besoin tout en laissant une surface d'attaque la plus réduite possible. Si un utilisateur n'a pas besoin de droits spécifiques pourquoi les lui fournir ? Et comment s'assurer que l'utilisateur n'a pas plus de droits qu'il ne lui en faut ?

Différentes notions techniques sont à connaître afin de pouvoir faire les meilleurs choix.

## 1. Les différents types de compte

Sous Windows, il existe différents types de comptes utilisateur. Chacun d'eux définit un ensemble de droits tel que l'accès aux fichiers, les modifications que vous êtes autorisées à effectuer sur le système d'exploitation, etc. D'une façon générale, suivant le type de compte choisi, l'utilisateur aura un niveau d'accès plus ou moins important sur le système d'exploitation.

Il existe trois principaux types de comptes :

- Invité ;
- Standard ;
- Administrateur.

### Compte utilisateur invité

Un compte utilisateur ayant des droits de type « invité » autorise l'accès aux ressources d'un ordinateur sans authentification de ce dernier. Ce type de compte n'est que très rarement utilisé en entreprise car il présente des risques non négligeables en termes de sécurité. Par défaut ce type de compte est désactivé.

### Compte utilisateur standard

Un compte utilisateur standard permet d'utiliser la plupart des fonctionnalités du système d'exploitation tant que celles-ci ne touchent pas à la sécurité de l'ordinateur ou à des paramètres communs à tous les utilisateurs.

La principale différence entre un compte utilisateur standard et un compte administrateur est le niveau d'accès de l'utilisateur aux endroits définis comme protégés par le système d'exploitation.

### Compte administrateur

Un compte utilisateur ayant les droits Administrateurs (et donc faisant partie d'une façon indirecte ou non au groupe Builtin\Administrateurs de l'ordinateur) est autorisé à agir sur la totalité du système d'exploitation et ainsi de pouvoir définir des paramètres communs à tous les utilisateurs (Installation de logiciels, définition de la sécurité de l'ordinateur, etc.).

Dans la mesure où les droits de ce compte sont très étendus, il est fortement déconseillé d'utiliser celui-ci pour vos tâches courantes. Vous verrez un peu plus loin dans ce chapitre comment Microsoft a répondu au besoin de sécurisation de ces accès Administrateurs grâce à l'UAC (*User Account Control*).

Par exemple, un utilisateur standard ne peut pas, par défaut, écrire au niveau du dossier système (c:\windows) ou dans la plupart de la base de registre, tandis qu'un administrateur peut le faire. Un administrateur peut également activer/désactiver le pare-feu, configurer les politiques de sécurité, installer un service ou un pilote pour tous les utilisateurs, etc.

Dans Windows Vista, Windows 7 et Windows 2008/2008 R2, les comptes utilisateur standard peuvent effectuer des tâches qui nécessitaient autrefois les privilèges administrateur comme :

- Afficher l'horloge système, le calendrier et modifier le fuseau horaire.
- Modifier les paramètres d'affichage et les polices installées.
- Modifier les options d'alimentation.
- Ajouter des imprimantes et autres périphériques.

- Ajouter et configurer des connexions VPN.
- Définir une clé WEP/WPA à un réseau sans fil.

Des tâches planifiées supplémentaires permettent désormais de définir une tâche de défragmentation ou de sauvegarde automatique. Auparavant, ces fonctionnalités ne pouvaient pas être réalisées aisément et nécessitaient la plupart du temps des privilèges administrateur.

Voici une liste non exhaustive des différents droits pour un utilisateur standard et un administrateur. Celle-ci vous permettra de vous rendre un peu mieux compte des autorisations de chacun.

Utilisateurs standard	Administrateurs
Établir une connexion réseau.	Installer/désinstaller des applications.
Établir une connexion réseau sans fil.	Installer le pilote d'un périphérique.
Modifier les paramètres d'affichages.	Installer les mises à jour Windows.
Défragmenter le disque dur (par l'intermédiaire d'un service).	Configurer le contrôle parental.
Lire un CD/DVD.	Installer un contrôle ActiveX.
Graver un CD/DVD.	Configurer le pare-feu.
Modifier le fond d'écran.	Modifier le type de compte d'un utilisateur.
Accéder à la date et l'horloge système et modifier le fuseau horaire.	Modifier les paramètres UAC.
Utiliser le bureau à distance pour se connecter à des ordinateurs distant.	Configurer l'accès au bureau à distance.
Configurer les options d'alimentation de la batterie.	Créer ou supprimer un compte utilisateur.
Configurer les options d'accessibilités.	Copier ou déplacer des fichiers dans les dossiers Program Files ou Windows.
Restaurer les fichiers sauvegardés de l'utilisateur.	Définir des tâches planifiées.
Définir une synchronisation entre un périphérique mobile et l'ordinateur (Smartphone, ordinateur portable, Personal Digital Assistant (PDA)).	Restaurer la sauvegarde de fichiers systèmes.
Connecter et configure un périphérique bluetooth.	Configurer le service de mise à jour automatique.

 Un quatrième type de compte était fortement utilisé sous des environnements comme Windows 2000/XP. Il s'agissait des comptes étant membre du groupe « Utilisateurs avec pouvoir ». Ce groupe était à mi-chemin entre Utilisateur Standard et Administrateurs. Il permettait en effet d'effectuer certaines tâches comme la possibilité d'écrire à certains endroits de la base de registre et du système de fichiers, sans nécessairement avoir des droits d'administrateurs. Ce type de groupe ne permettant pas de répondre à tous les besoins des applications, il a été supprimé par défaut sous Windows Vista et Windows 7. Il faut tout de même savoir que ce groupe reste utilisable afin de permettre une compatibilité descendante pour les applications le nécessitant. Pour cela, il faut charger un modèle de sécurité particulier (compatws.inf) dans Windows Vista et Windows 7 afin de modifier les droits sur certains fichiers et clés de la base de registre pour permettre au groupe « Utilisateurs avec pouvoir » d'y avoir accès.

## 2. Le contrôle d'accès utilisateur

Le contrôle d'accès utilisateur ou User Account Control (UAC) est une des principales avancées de la nouvelle gamme de système d'exploitation Microsoft Windows Vista, Windows 7 et Windows Server 2008/2008 R2.

Cette nouvelle fonctionnalité (activée par défaut sous Windows Server 2008/2008 R2) permet de vous informer de toute action nécessitant des privilèges systèmes. Un jeton d'accès complet est alors créé avec les droits les plus importants de l'utilisateur puis est passé à l'application. Cela s'appelle une élévation des privilèges. L'UAC se caractérise par une élévation des privilèges automatisée, un message d'avertissement lors de cette élévation, ainsi qu'un bureau sécurisé dédié à ce message d'avertissement.

Il sera ainsi beaucoup plus compliqué à un logiciel espion de s'installer sur le système ou de venir se greffer à un processus sans que vous en soyez informé.

Il est désormais plus simple d'identifier les tâches qui nécessiteront des droits plus importants. L'icône en forme de bouclier accolé à certaines applications et assistants de configuration indique que ces tâches vont se lancer avec des permissions d'administrateurs de l'ordinateur.



Pour les autres applications, un message d'élévation de privilège apparaîtra si besoin.

 Notez que l'affichage de la fenêtre d'élévation de privilège apparaît moins souvent sous Windows 7/2008 R2, notamment lors de tâches "sûres" comme l'installation de mises à jour ou de drivers téléchargés depuis Windows Update, l'affichage des paramètres Windows ou bien encore les outils de diagnostic de la carte réseau.

Avant que l'élévation des privilèges ne soit effectuée, Windows Server 2008/2008 R2 basculent par défaut la fenêtre de confirmation demandant cette élévation de droits vers un bureau virtuel isolé (appelé aussi "Bureau estompé" depuis Windows 7/2008 R2) et sécurisé tandis que le reste des applications continuent de s'exécuter au niveau du bureau interactif de l'utilisateur. Cela permet ainsi d'empêcher à un processus utilisateur (comme un logiciel espion) d'interagir avec la demande d'élévation de privilège et ainsi d'accepter automatiquement l'élévation.

La fenêtre de demande d'élévation pour le processus en question se trouve donc dans un environnement hermétique. Ainsi, si un attaquant choisissait de créer un exécutable permettant de reproduire avec exactitude la fenêtre d'élévation de privilège, vous n'irez pas exécuter celle-ci car son affichage ne se ferait pas dans le bureau virtuel. De même, le bureau sécurisé empêche les attaques qui consistent à truquer l'affichage du pointeur de la souris. L'attaquant peut en effet modifier l'affichage de la souris de sorte que lorsque l'utilisateur choisit de cliquer sur **Annuler**, l'action du clic de souris est effectuée sur le **Continuer** ; permettant ainsi d'exécuter l'application dangereuse. Le bureau virtuel permet ainsi de bloquer ce type d'attaque.

Par ailleurs, sous Windows Server 2008 un mode particulier nommé **Mode d'approbation d'administrateur** est activé pour tous les membres du groupe Administrateurs (hormis le compte Administrateur intégré). Ce mode montre l'élévation de privilèges lorsqu'une application nécessitant des droits d'administrateurs est lancée.

Sous Windows Server 2008 R2, une granularité plus fine de l'UAC est possible afin de limiter la demande de mot de passe. Cela est détaillé ci-après.

Il est possible de configurer ces différents paramètres via le panneau de configuration (pour Windows Server 2008 R2 uniquement) ou via une stratégie de groupe (aussi bien locale que de domaine). Pour cela, ouvrez votre éditeur de stratégie, puis rendez-vous au niveau de **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Options de sécurité**.

Les stratégies relatives à la gestion de l'UAC sont les suivantes :

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

Description : permet de définir si le compte Administrateur intégré est soumis au Mode d'approbation administrateur ou pas.

Valeur par défaut : Désactivé

#### **Contrôle de compte d'utilisateur : passer au bureau sécurisé lors d'une demande d'élévation**

Description : indique si la demande d'élévation doit se faire sur le bureau des utilisateurs interactifs ou sur le bureau virtuel sécurisé.

Valeur par défaut : Activé

#### **Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utiliser le bureau sécurisé**

Description : les programmes UIAccess comme l'assistance à distance peuvent demander l'utilisation de cette option.

Valeur par défaut : Désactivé

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

Description : définit si un utilisateur connecté avec un compte administrateur obtient une invite d'élévation de privilèges lors de l'exécution d'applications nécessitant des privilèges administrateur.

Trois choix possibles sous Windows Server 2008 :

- **Aucune invitation** (pour 2008) ou **Elever les privilèges sans invite utilisateur** (pour 2008 R2) : l'élévation se produit automatiquement et en silence (Inutile de vous préciser que cette option n'est pas recommandée).
- **Demande de consentement** : requiert une intervention de l'utilisateur pour Continuer ou Annuler l'opération d'élévation des privilèges.
- **Demande d'information d'identification** : un nom d'utilisateur et mot de passe est demandé lors de la demande d'élévation des privilèges.

Valeur par défaut : Demande de consentement.

Windows Server 2008 R2 possède des paramètres supplémentaires :

- **Demande de consentement sur le bureau sécurisé** : requiert une intervention de l'utilisateur sur le bureau sécurisé pour Continuer ou Annuler l'opération d'élévation des privilèges.
- **Demande d'information d'identification sur le bureau sécurisé** : un nom d'utilisateur et un mot de passe sont demandés sur le bureau sécurisé lors de la demande d'élévation des privilèges.
- **Demande de consentement pour les binaires non Windows** : requiert une intervention de l'utilisateur pour Continuer ou Annuler l'opération d'élévation des privilèges pour une application non signée par un certificat Microsoft.

Valeur par défaut : Demande de consentement pour les binaires non Windows.

#### **Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard**

Description : définit si un utilisateur connecté avec un compte standard obtient une invite d'élévation de privilèges lors de l'exécution d'applications nécessitant des privilèges administrateur.

Par défaut, un utilisateur standard aura la possibilité d'indiquer le mot de passe d'un compte administrateur. Il est également possible de désactiver cette option bien que cela n'empêchera pas l'utilisateur de faire un clic avec le bouton droit de la souris sur un exécutable et de choisir **Exécuter en tant qu'administrateur**.

Valeur par défaut : Demande d'informations d'identification (pour Windows Server 2008).

Demande d'informations d'identification sur le bureau sécurisé (pour Windows Server 2008 R2).

#### **Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation**

Description : lorsque ce paramètre est activé, l'utilisateur doit fournir son consentement lorsque Windows détecte un programme d'installation. Il n'est pas conseillé d'appliquer ce paramètre en environnement d'entreprise si l'utilisateur n'a pas les droits d'administrateur ou si un logiciel de télédistribution est déjà en place.

Valeur par défaut : Activé.

#### **Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des emplacements sécurisés**

Description : indique que seules les applications nécessitant un niveau d'intégrité UIAccess (c'est-à-dire lors la spécification UIAccess=true dans leur manifeste d'application) doivent se trouver à un emplacement sécurisé sur le système de fichiers. Les emplacements sécurisés sont :

- \Program Files\ (et sous-répertoires)
- \Program Files (x86)\ (et sous-répertoires)
- \Windows\System32

Valeur par défaut : Activé.

#### **Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés**

Description : seuls les exécutables signés et validés à l'aide d'un certificat auront l'autorisation d'élever leurs privilèges. La liste des applications d'administration peut donc être contrôlée par ce moyen.

Valeur par défaut : Désactivé.

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

Description : permet d'activer ou désactiver le contrôle utilisateur pour les utilisateurs qui seront Administrateurs.

Valeur par défaut : Activé

### **Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans des emplacements définis par utilisateur**

Description : cette option assure une compatibilité avec les anciennes applications qui s'exécutaient en tant qu'administrateur et écrivaient des données d'exécution de l'application dans %Program Files%, %Windir%, %Windir%\System32 ou HKLM\Software.

Valeur par défaut : Activé



Si vous utilisez une authentification biométrique, sachez que Windows Server 2008 R2 permet de simplifier l'élévation de privilèges demandée par l'UAC rendant ainsi l'expérience utilisateur meilleure.



Votre périphérique biométrique est d'ailleurs mieux géré sous Windows Server 2008 R2 que dans les versions précédentes et vous pourrez utiliser ce moyen d'authentification sans nécessairement avoir un logiciel tiers installé à partir du moment où le driver récupéré via Windows Update aura été installé.

Très souvent controversé car il modifie nos (mauvaises ?) habitudes, l'UAC permet néanmoins d'assurer un niveau de sécurité bien supérieur comparé aux versions précédentes de Windows. Ses améliorations notables sous Windows 7 et Windows Server 2008 R2 devraient néanmoins vous décider à très vite l'adopter.

## **3. Gérer vos groupes à l'aide des groupes restreints**

Les groupes restreints vous permettent de gérer les membres de groupes de sécurité afin de vous assurer du contenu de ces groupes.

Les groupes restreints sont uniquement paramétrables au niveau de stratégies de domaine. Vous ne trouverez donc pas ce paramètre au niveau d'une stratégie locale. Ce paramétrage se trouve au niveau de **Configuration Ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Groupes restreints**.

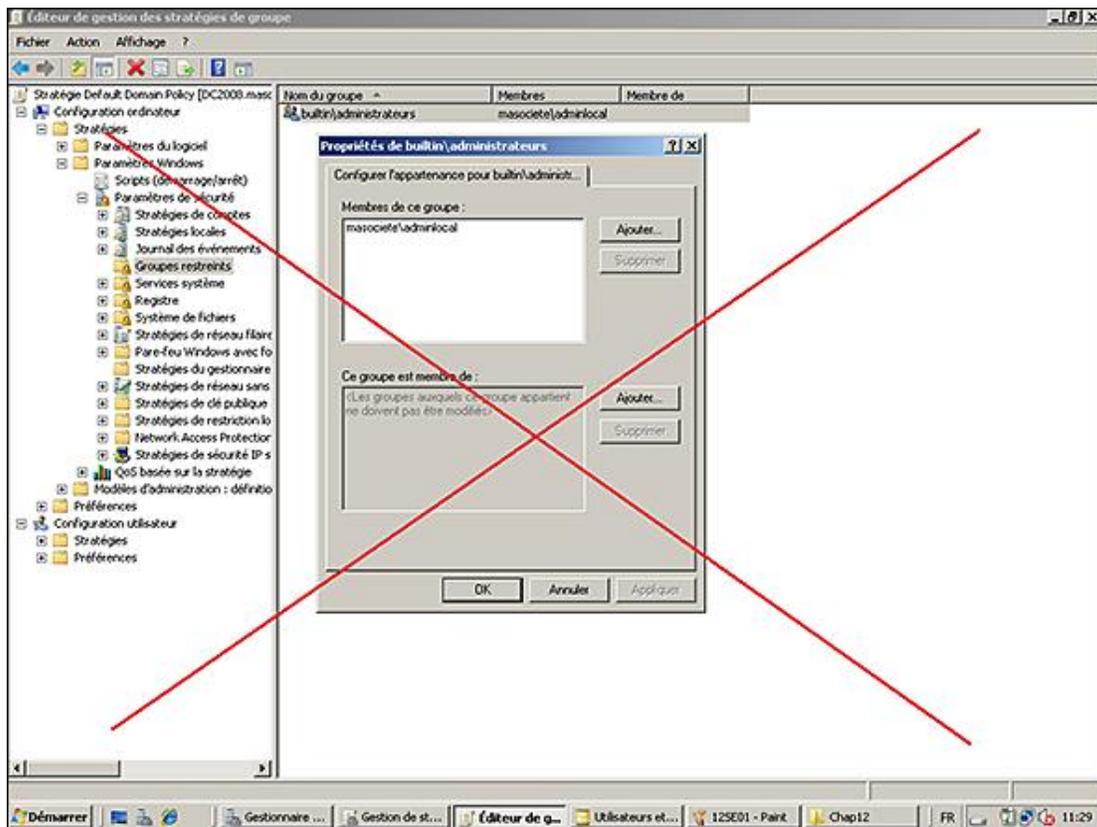
L'avantage principal, vous l'aurez compris, est de figer les membres définis au niveau de **Membre** et **Membres de...** du groupe défini comme groupe restreint. Ainsi, si par exemple l'utilisateur se voit retirer manuellement d'un groupe défini en tant que groupe restreint, il sera automatiquement ajouté à celui-ci lors de l'application de la stratégie de groupe (soit toutes les 90 minutes environ).

Avant de se lancer dans la configuration d'un groupe restreint, il convient de bien comprendre la différence entre le paramètre **Membres de ce groupe** et **Ce groupe est membre de**.

En configurant par exemple, depuis la stratégie de groupe, un groupe restreint comme le groupe local des ordinateurs nommé BUILTIN\Administrateurs (via un clic droit depuis la stratégie de groupes restreints puis **Ajouter un groupe/BuiltIn\Administrators**) et en lui indiquant un groupe de domaine nommé par exemple **MaSociete\AdminLocal** au niveau de **Membres de ce groupe**, alors tous les utilisateurs du groupe **MaSociete\AdminLocal** seront Administrateurs des ordinateurs se trouvant dans le conteneur lié à la stratégie de groupe définie.

Parfait ! Me direz-vous ? Et bien pas tant que cela...

Imaginez que ce groupe restreint soit défini au niveau des ordinateurs de votre Active Directory et qu'un utilisateur ait besoin d'être membre du groupe Administrateurs de son ordinateur (il n'est pas rare que les utilisateurs d'ordinateurs portables aient ce genre de besoin). En le rajoutant au groupe **MaSociete\AdminLocal**, l'utilisateur sera en effet membre du groupe BUILTIN\Administrateurs de son ordinateur mais également administrateur de tous les autres ordinateurs !

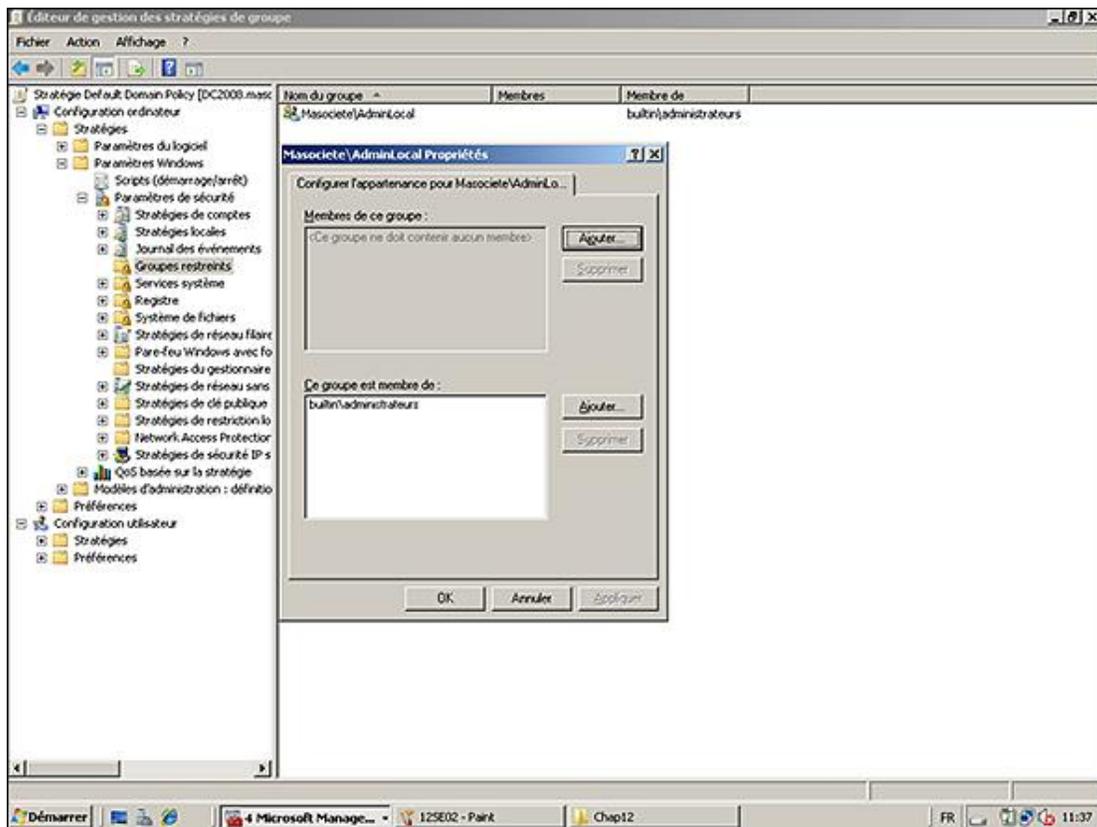


De même, si vous tentez de rajouter ce même utilisateur localement au groupe BUILTIN\Administrateurs de son ordinateur, l'application de la stratégie de groupe aura pour effet de nettoyer les membres des groupes locaux et par conséquent l'utilisateur se verra retirer les droits administrateurs.

Vous l'aurez compris, ce type de configuration n'est que peu adapté à la définition des membres des groupes au niveau des postes de travail mais il peut être très intéressant pour contrôler les membres des groupes des serveurs et contrôleurs de domaine afin de figer ces derniers.

Pour en revenir à notre utilisateur souhaitant être administrateur de son ordinateur en utilisant les groupes restreints et sans que cela n'impacte la sécurité des autres ordinateurs, il convient de définir les groupes restreints de façon un peu différente.

Il faut en effet définir un groupe restreint à partir du groupe de domaine choisi (dans notre exemple le groupe **MaSociete\AdminLocal**) et définir le paramètre **Ce groupe est membre de :** afin d'y rajouter le groupe **BUILTIN\Administrateurs** (ou BUILTIN\Administrators selon que cette stratégie de groupe est définie depuis un ordinateur français ou anglais).



Ainsi, le groupe **MaSociete\AdminLocal** a son attribut **IsMemberOf** figé et les utilisateurs faisant partie de ce groupe sont effectivement membres du groupe Administrateurs de tous les ordinateurs mais sans que cela n'empêche un utilisateur lambda d'être administrateur de son ordinateur.

La gestion des groupes représentant toujours un véritable défi pour nos systèmes d'information et la sécurité qui en découle, les groupes restreints répondent fortement à cette attente.

#### 4. Applocker ou le contrôle de l'application (Windows Server 2008 R2 uniquement)

Applocker est une fonctionnalité qui a fait son apparition sous Windows 7 (en version Enterprise et Ultimate) et Windows Server 2008 R2 afin de remplacer les stratégies de restriction logicielle des versions précédentes de Windows.

Tout comme les stratégies de restriction logicielle, Applocker permet de définir les applications autorisées à être exécutées par vos utilisateurs standards au sein de votre domaine en déployant vos paramètres via des stratégies de groupe.

L'intérêt principal est donc de limiter l'installation de malwares sur les postes de travail mais également d'empêcher l'installation de logiciels non-normés ou nécessitant une licence que vous ne possédez pas, etc.

Cette fonctionnalité concerne donc principalement les postes clients sous Windows 7 mais il peut également être intéressant d'auditer et limiter les exécutables lancés sur Windows Server 2008 R2.

Applocker présente plusieurs avantages comparés aux stratégies de restriction logicielle :

- La définition de règles plus fines basées sur l'éditeur (via la signature numérique du fichier et de ses attributs étendus tels que l'éditeur, le nom du Produit et/ou le nom du Fichier). Il est ainsi possible par exemple de n'autoriser qu'un logiciel provenant d'un éditeur spécifique et qu'à partir d'une version spécifique (comme n'autoriser que l'utilisation d'Office 2003 (Version 11.0.0.0) ou version suivante).
- La possibilité de définir des règles pour des utilisateurs ou des groupes spécifiques.
- La possibilité d'importer et d'exporter des règles.
- La possibilité d'identifier les effets de bord d'une règle en activant le mode d'audit.

Sachez également que si une stratégie de groupe possède à la fois une stratégie de restriction logicielle et une

stratégie de contrôle de l'application (Applocker), seule la stratégie Applocker sera appliquée sur le poste Windows 7/2008 R2.

Tachons de configurer ensemble Applocker.

Avant de commencer il faut savoir qu'il existe trois types de règles possibles pour juger si une application est autorisée à être exécutée ou pas.

- **Chemin d'accès** : cette règle permet d'identifier un exécutable en se basant sur un chemin. Vous pouvez par exemple définir une règle afin d'autoriser l'exécutable C:\Windows\calc.exe. Cependant cette solution n'est pas la plus efficace car si un utilisateur renomme un exécutable interdit en calc.exe dans le dossier C:\Windows, il sera alors capable d'exécuter le fichier.
- **Hachage du fichier** : cette règle permet d'identifier un exécutable en se basant sur la valeur de hachage calculée. Chaque fichier possédant une valeur de hachage unique, Windows calcule la valeur de hachage d'un fichier et la compare aux valeurs de hachage définies dans les règles Applocker afin de savoir si la règle doit s'appliquer ou pas. L'inconvénient de cette solution est que la règle doit être mise à jour à chaque nouvelle version de fichier à autoriser.
- **Editeur** : cette règle permet d'identifier un exécutable en fonction de l'éditeur (tout comme c'était le cas avec les règles de certificats des anciennes restrictions logicielles) mais en y ajoutant également des conditions plus fines comme la version du produit, etc.

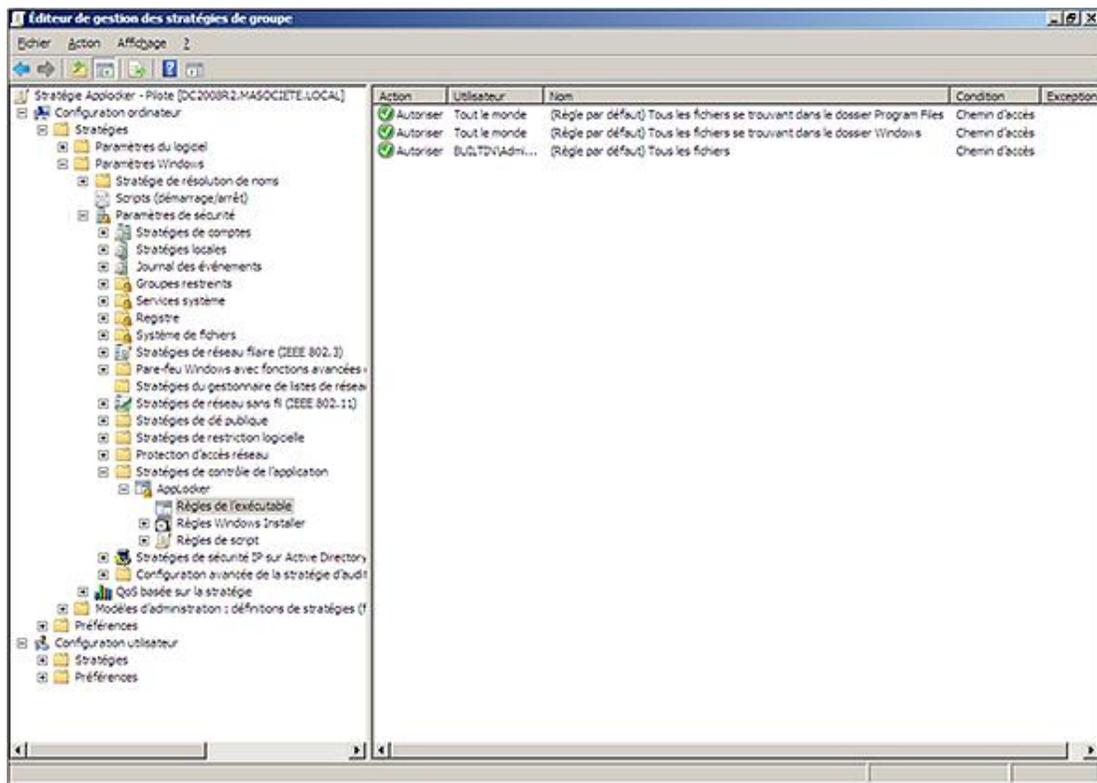
Avant de créer vos propres règles personnalisées, il faudra commencer par créer les règles par défaut. En effet, Applocker fonctionne un peu comme un pare-feu et tout ce qui n'est pas explicitement autorisé est alors refusé.

Voici donc les principales étapes à suivre afin de mettre en place Applocker au sein de votre entreprise.

- Générer les règles par défaut : afin d'éviter des effets de bord considérables, il vous faut donc générer les règles par défaut autorisant tout le monde à lancer tous les exécutables se trouvant dans le dossier Program Files ou Windows.
- Générer les règles automatiques : vous n'aurez alors plus qu'à définir des règles pour bloquer ce que vous souhaitez. Cette façon de procéder vous évitera de vous "auto-bloquer" dans certaines situations à cause de règles mal définies.
- Auditer les règles Applocker avant le déploiement massif en production.

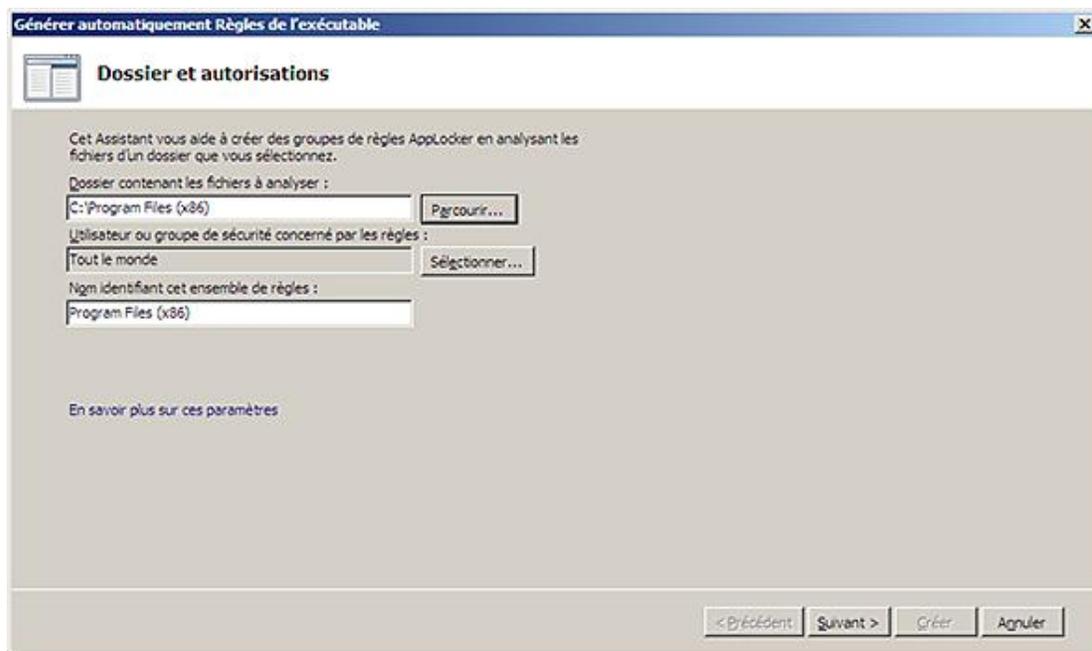
### Générer les règles par défaut

- Afin de définir vos règles pour la première fois, utilisez un poste témoin (donc sous Windows 7 ou 2008 R2) qui sera le seul poste présent dans l'unité d'organisation attaché à la stratégie de groupe que vous allez configurer. Installez les applications normées ou celles que vous souhaitez autoriser. Installez également les outils RSAT afin de créer la stratégie et les règles Applocker directement depuis ce poste (vous verrez par la suite pour quelle raison).
- Toujours depuis ce poste témoin, rendez-vous alors au niveau du paramètre **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle de l'application - Applocker**. Remarquez alors qu'il y a trois sous-catégories : Règles de l'exécutable, Règles Windows Installer et Règles de script. Faites un clic droit sur chacune de ces sous-catégories pour créer la règle par défaut en choisissant **Créer des règles par défaut**.
- Ceci aura pour effet de créer des règles par défaut autorisant "Tout le monde" à exécuter les programmes se trouvant dans le dossier **%PROGRAMFILES%** et **%WINDIR%**. Il faudra garder cela à l'esprit au moment où vous établirez vos premiers essais en production. L'interdiction l'emportant sur l'autorisation, vous pourrez alors Refuser l'accès à un programme spécifique se trouvant dans l'un de ces dossiers.



## Générer les règles automatiques

- La façon la plus simple de définir des règles pour des applications existantes est d'utiliser l'assistant. Il permet de générer les règles selon les spécificités de chaque binaire se trouvant dans le dossier que vous lui indiquez de scanner. Pour cela, faites un clic droit sur la catégorie **Règles de l'exécutable** et choisissez **Générer automatiquement les règles...**

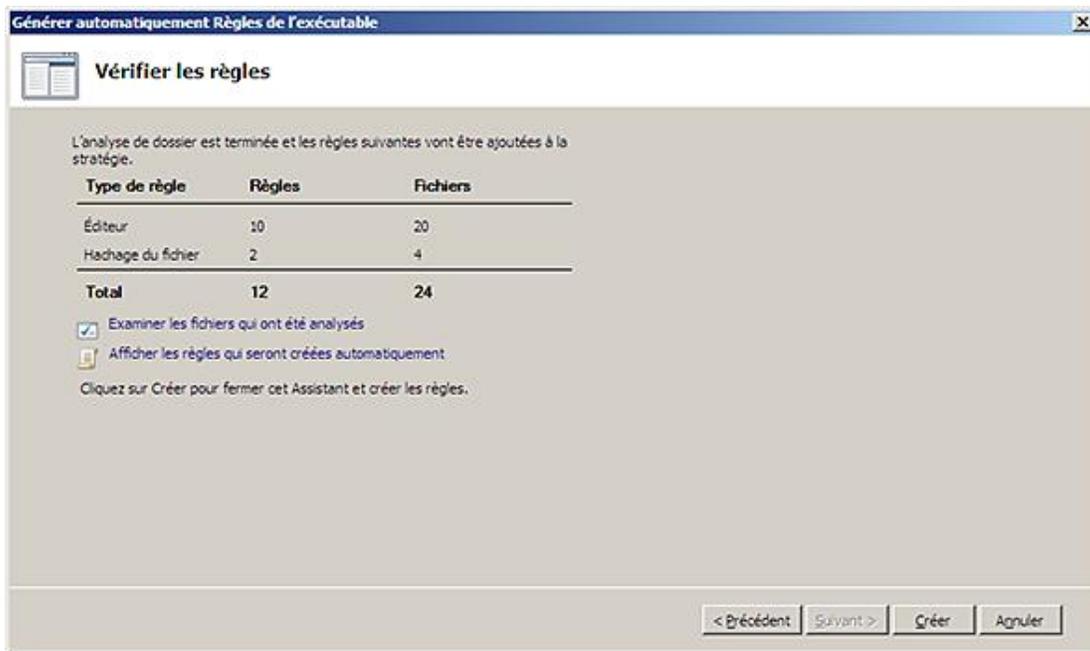


- Un assistant s'ouvre alors afin que vous lui indiquiez le répertoire à scanner, les utilisateurs concernés par cette règle, ainsi que le nom de la règle.



- L'étape suivante permet de définir les **Préférences de règles**. Les règles d'éditeur sont à préférer aux règles de hachage lors d'une première mise en place. Vous pouvez donc passer à l'étape suivante.

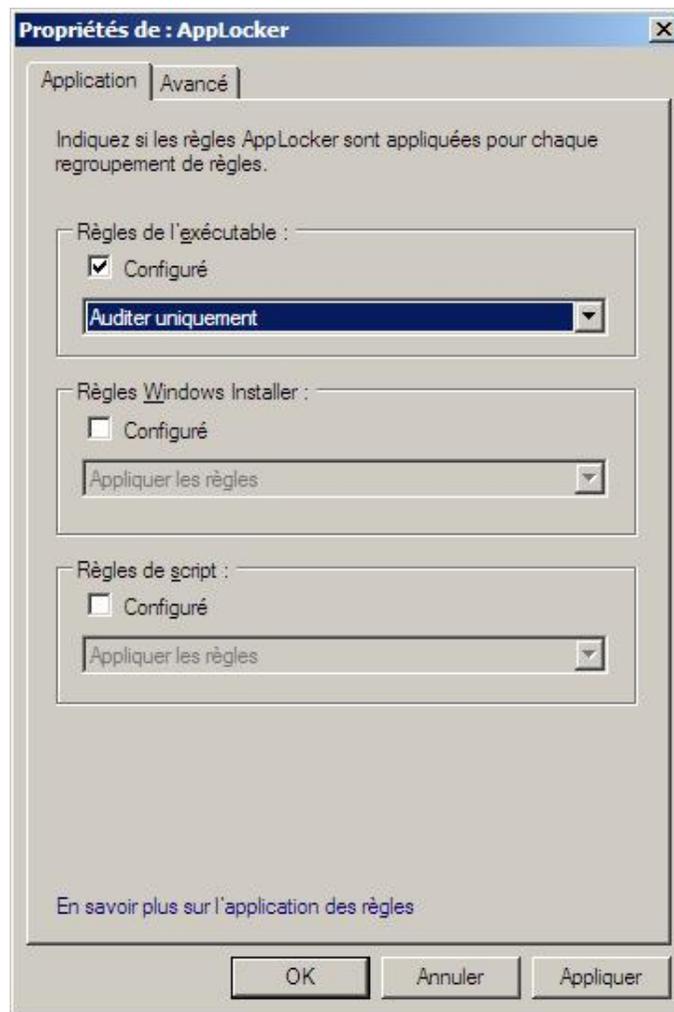
Le scan débute alors et affiche le nombre de règles identifiées ainsi que le type de règle associé. Vous aurez la possibilité d'examiner les fichiers analysés afin de supprimer tout ou partie des règles proposées.



- Cliquez sur **Créer** pour créer les règles choisies.

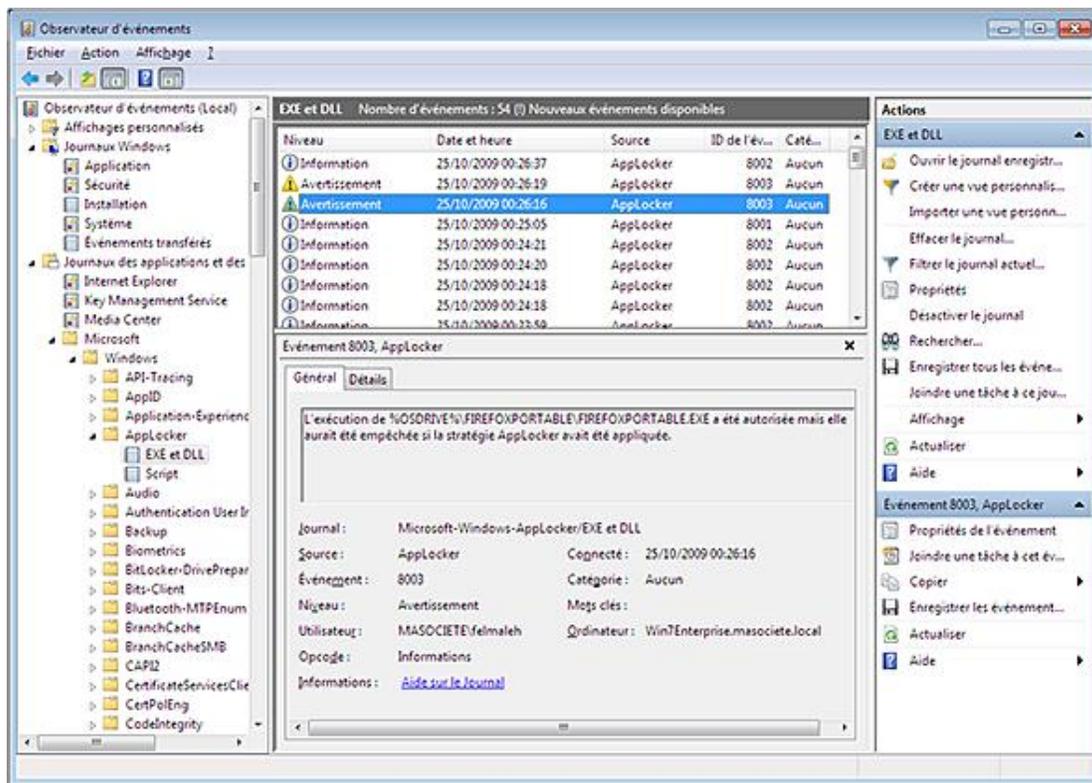
Celles-ci sont alors immédiatement ajoutées à la règle de l'exécutable.





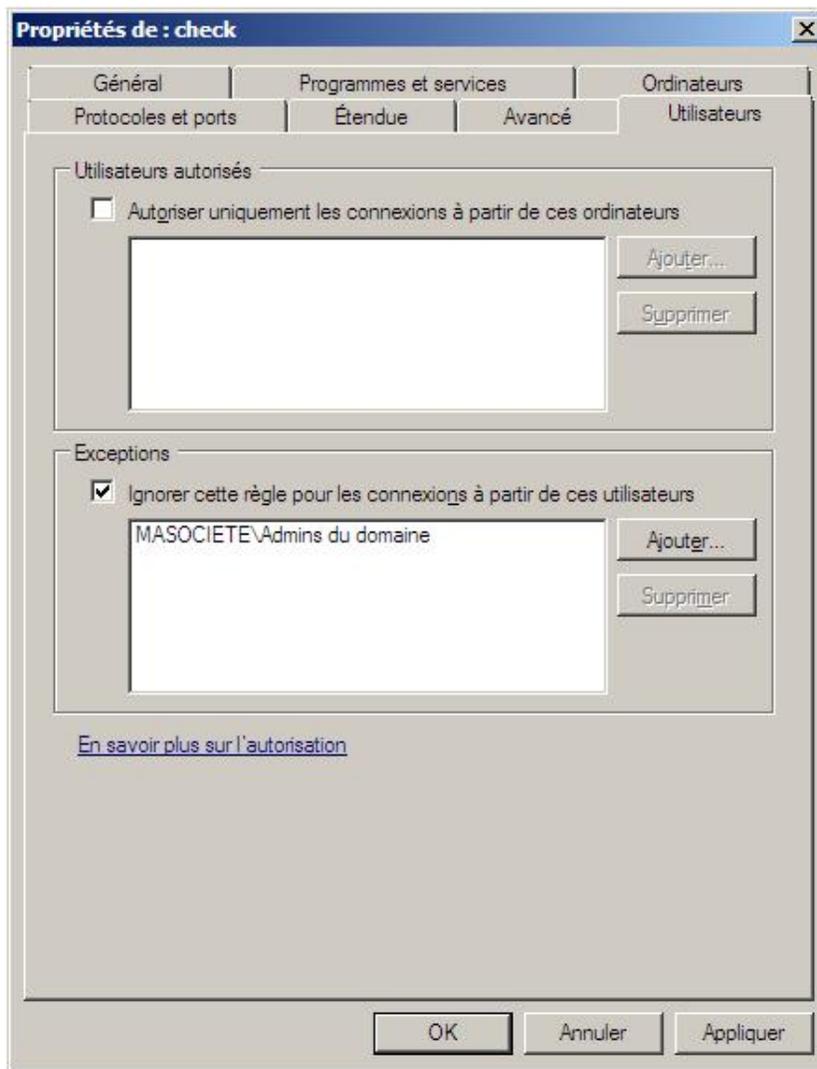
Validez en cliquant sur **OK**.

- Afin que ces paramètres puissent être appliqués sur vos postes cibles, il faut modifier le type de démarrage du service **Identité de l'application**. Celui-ci est en effet défini par défaut en démarrage Manuel et non Automatique. Vous pouvez donc configurer celui-ci directement depuis le poste client ou via cette même stratégie de groupe au niveau de **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Services système**. Sélectionnez alors le service **Identité de l'application** et définissez-le pour un démarrage automatique.
- Redémarrez votre poste client ou forcez l'actualisation de la stratégie via un **gpupdate /force** pour pouvoir tester immédiatement cette fonctionnalité. Vous pouvez alors identifier si les règles Applocker définies bloquent des applications normalement autorisées. À cette étape, l'application ne sera néanmoins pas bloquée. Afin de vérifier la liste des applications qui auraient été bloquées, lancez le journal des événements puis rendez-vous au journal se trouvant dans **Journaux des applications et des services - Microsoft - Windows - Applocker**. Recherchez alors les événements ayant l'ID 8002 (indiquant l'exécution autorisée d'une DLL ou d'un exécutable) ou 8003 (indiquant que le fichier exécuté aurait normalement été bloqué si le mode audit n'avait pas été activé).



### Appliquer les règles Applocker sur les postes de production

- Une fois vos règles correctement définies, vous pourrez les appliquer en éditant votre stratégie de groupe créée précédemment en vous rendant au niveau de **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle de l'application - Applocker** puis **Propriétés**. Dans la liste déroulante correspondant au groupement de règles que vous souhaitez réellement appliquer, choisissez **Appliquer les règles**. Validez en cliquant sur **OK**.
- Si vous le souhaitez, vous pourrez optionnellement ajouter l'adresse vers un site web de votre choix lorsqu'une application sera bloquée pour vos utilisateurs. Vous pourrez ainsi les diriger vers une page spécifique de votre site intranet afin de les informer sur ce blocage. Pour cela, éditez la stratégie **Configuration ordinateur - Stratégies - Modèles d'administration - Composants Windows - Explorateur Windows - Définir le lien d'une page web de support**.



Il est possible d'administrer la solution Applocker au travers de PowerShell. Vous trouverez les commandes PowerShell de référence à cette adresse : [http://technet.microsoft.com/en-us/library/ee424349\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee424349(WS.10).aspx)

Vous venez donc de découvrir comment mettre en place une stratégie Applocker. La solution technique n'est pas particulièrement compliquée mais il faudra surtout bien réfléchir aux différents processus à mettre en place pour que cette solution évolue en même temps que les applications de votre entreprise et sans que cela ne pénalise les utilisateurs.