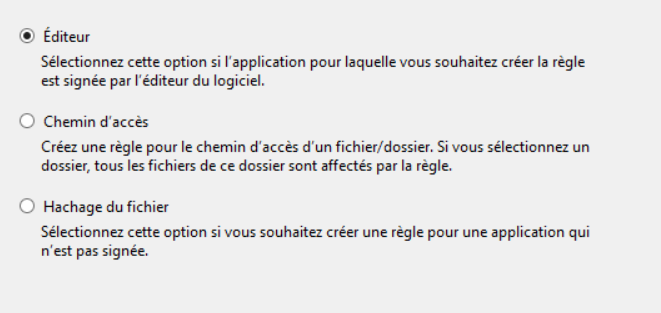
Mise en place par GPO de contrôle d’applications (restrictions / autorisations)

# Présentation

Applocker est intégré à Windows serveur 2012R2 et permet à la fois d’empêcher le lancement d’applications et d’empêcher leur installation.

Applocker permet de verrouiller en fonction de plusieurs critères :



Le critère par éditeur, permet de bloquer des applications en fonction de l’éditeur du logiciel.

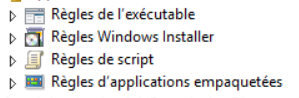
Le critère chemin d’accès, permet de bloquer en fonction d’un emplacement, exemple : je veux interdire tout exécution de logiciels dans c:\users

Le hachage de fichier permet de bloquer des logiciels non signés numériquement

<https://fr.wikipedia.org/wiki/Fonction_de_hachage>

La mise en place d’AppLocker nécessite d’avoir l’exécutable sur le serveur sur lequel on effectue la manipulation.

AppLocker permet de bloquer des exécutables, des packages MSI (Windows Installer), des scripts et des packages APPX (Applications Windows Store – extension des GPO par ADMX Windows 10 obligatoire)



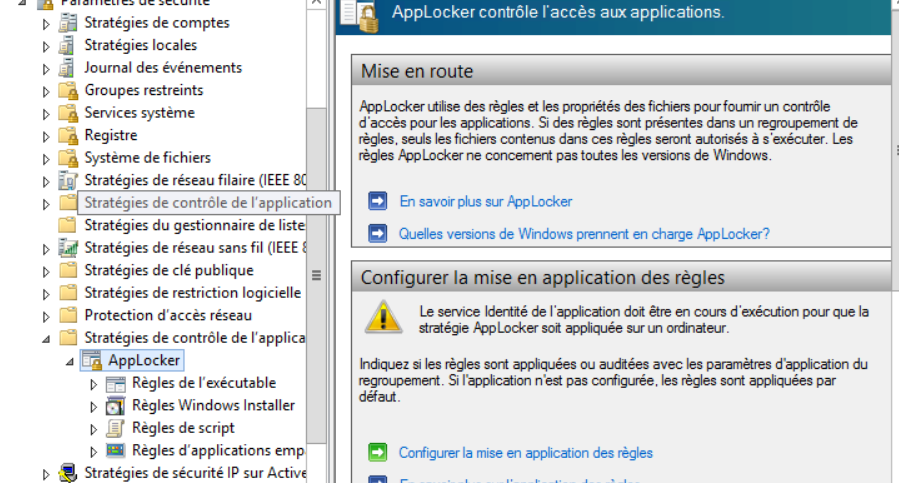
# Mise en place – blocage de toutes les applications Google sur un domaine AD

## Pré-requis

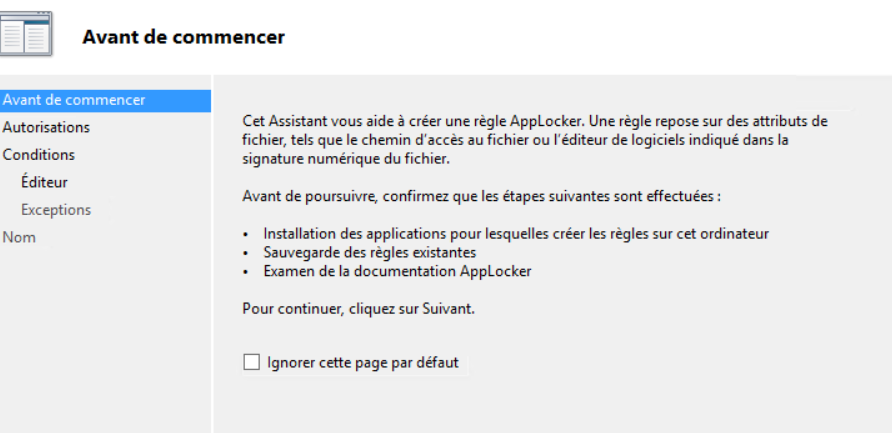
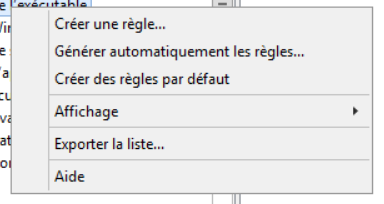
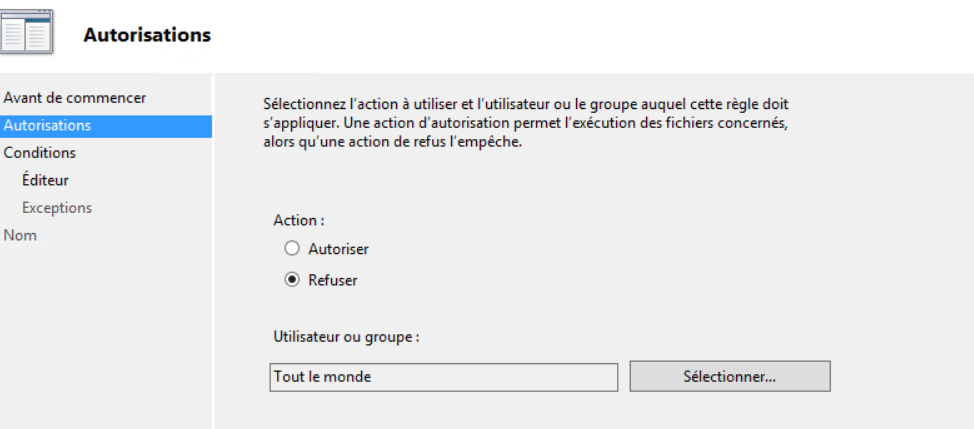
Serveur avec domaine AD, chrome.exe copié sur le serveur

## Installation

Créer une GPO sur l’ensemble du domaine et l’éditer

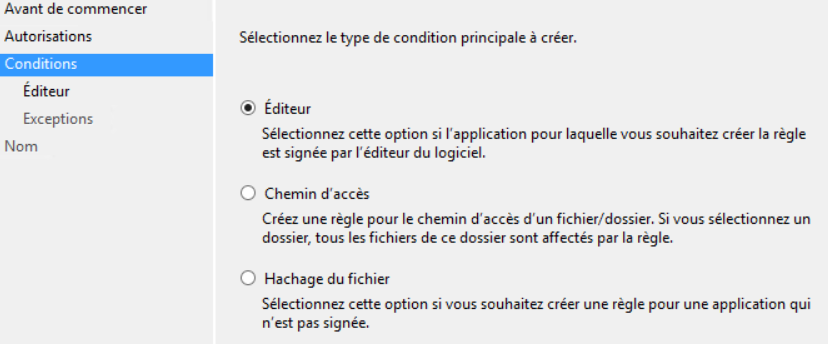


J’ajoute une règle d’éxécutable

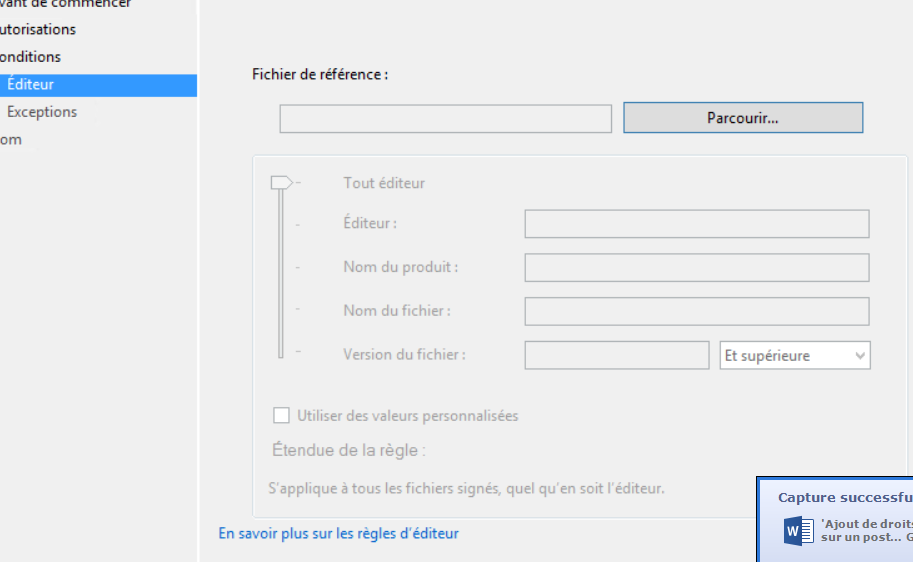
Je crée une règle de type refuser pour tout le monde

Je peux éventuellement préciser le ou les groupes de sécurité refuser ou autoriser

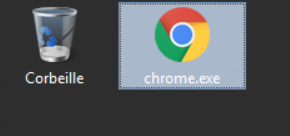
Attention, le refus à tout le monde est supérieur même si certains sont autorisés

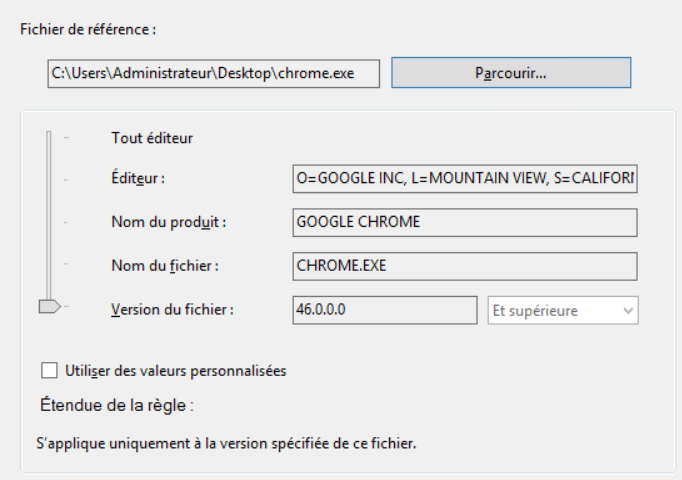
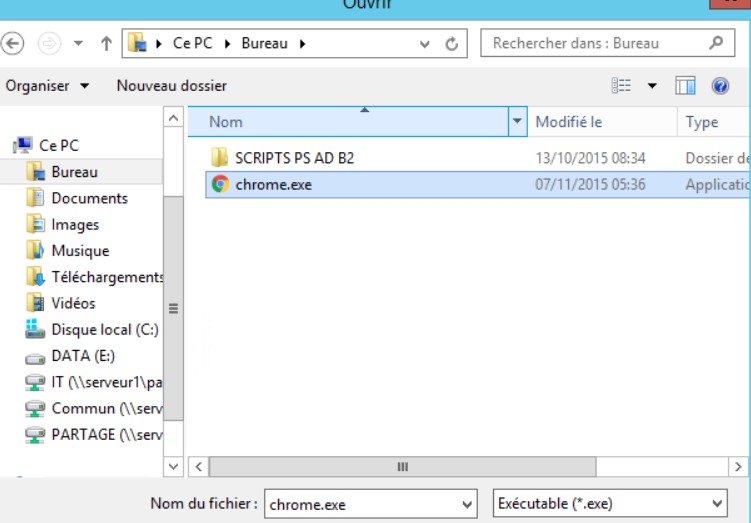


Je choisi ensuite le type d’interdiction que je souhaite, ici Editeur

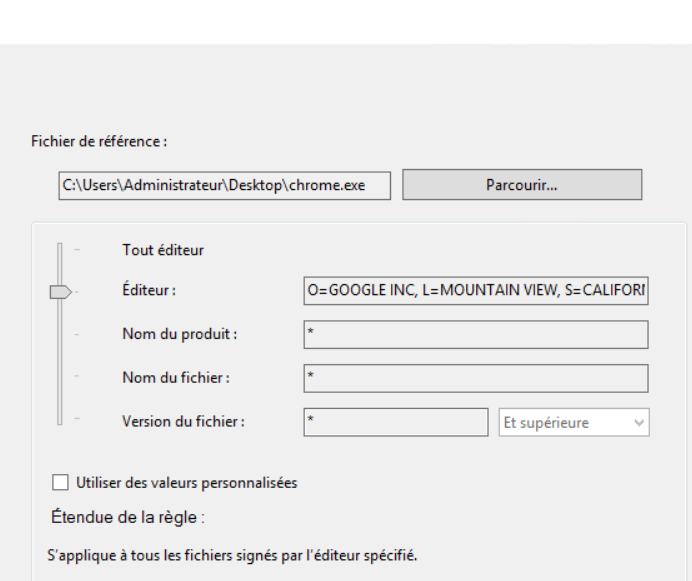


J’ai besoin de fournir l’exécutable à prendre en compte et de choisir le degré d’interdiction.

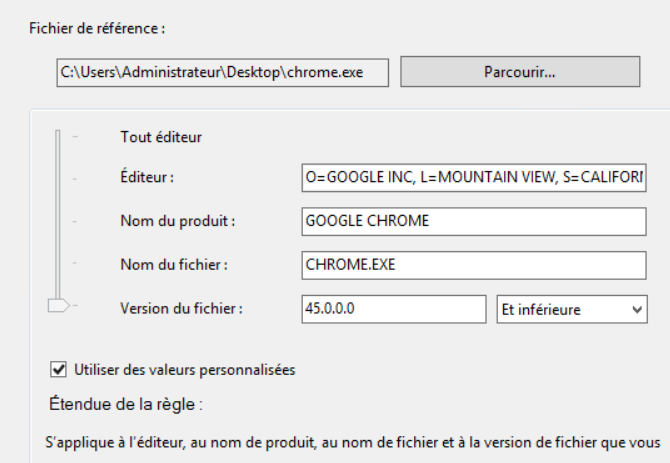




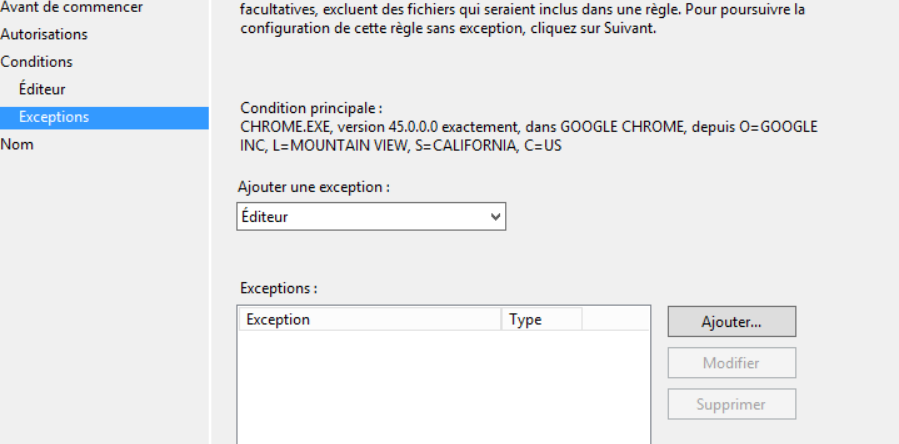
J’interdis tout utilisation de produit Google



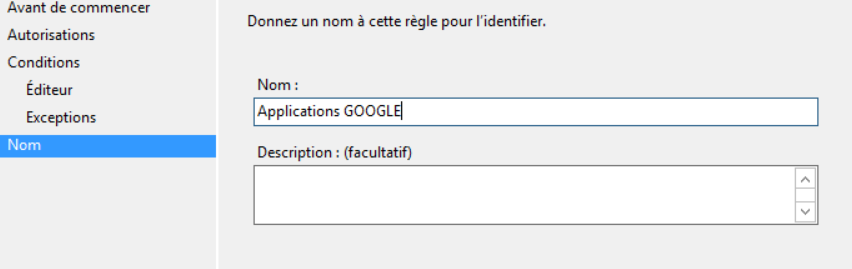
J’interdis ici toute utilisation d’un Google chrome d’une version inférieure à la version 45



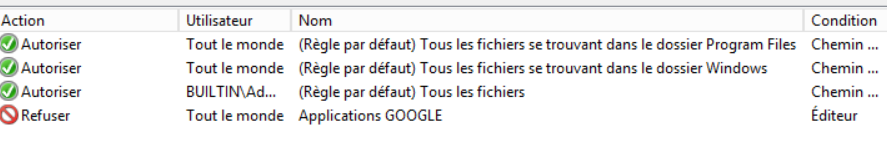
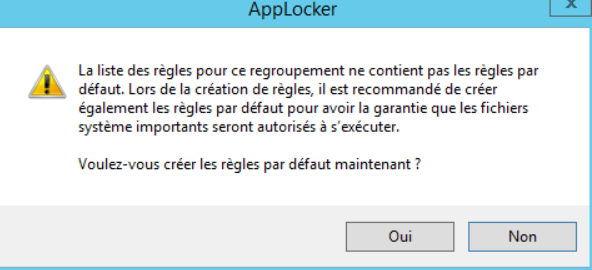
Je peux éventuellement ajouter des exceptions.



Je nomme la règle Google



Je crée les règles par défaut qui vont autoriser certains chemins du système



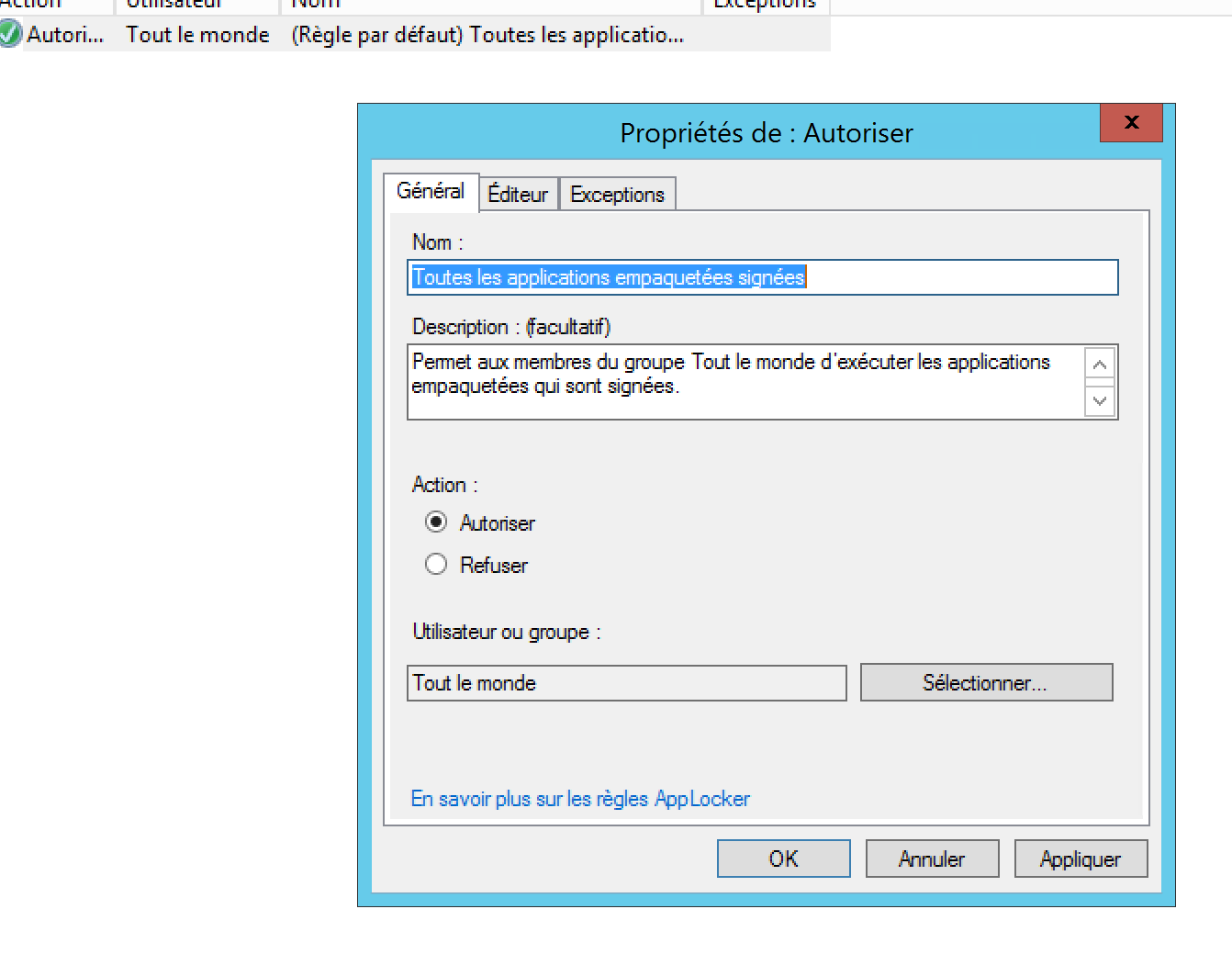
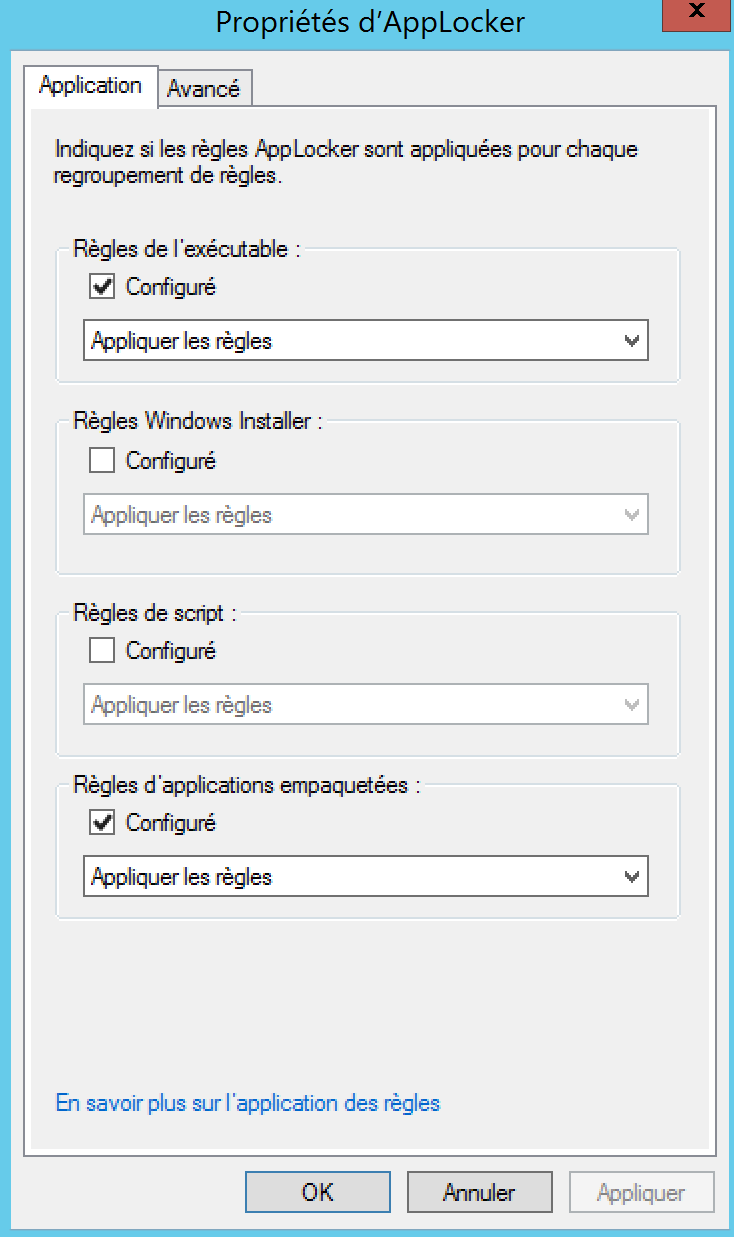
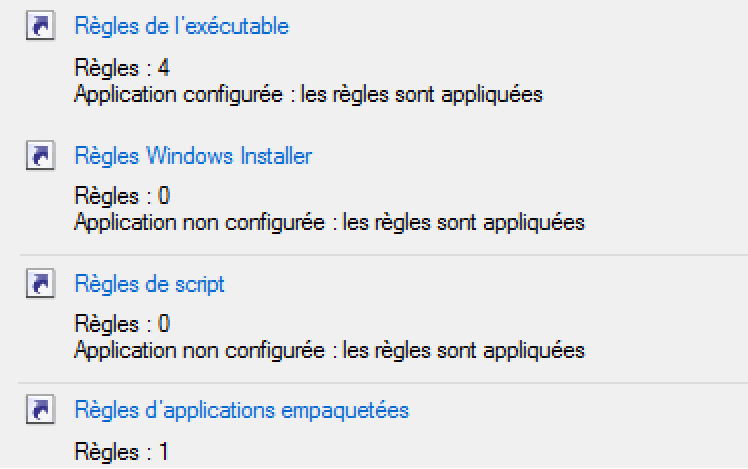
Attention, avec Windows 10 il faut modifier la règle Tous les fichiers en les autorisant pour tout le monde.

Attention le menu de Windows 10 ne fonctionne pas avec APPLOCKER si on ne paramètre pas les règles par défaut pour les applications Windows Store

<https://technet.microsoft.com/fr-fr/library/mt592642(v=vs.85).aspx>

<https://technet.microsoft.com/en-us/library/jj582992(v=ws.10).aspx>

Il faut donc appliquer des règles de base pour les applications empaquetées

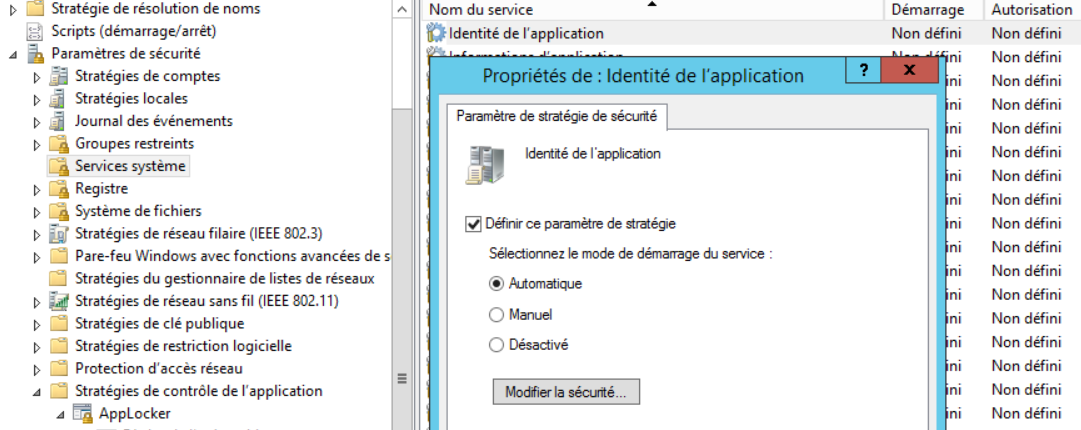


J’active le lancement automatique du service identité de l’application

Applocker utilise un service local, pour que applocker fonctionne je dois faire en sorte que le service démarre automatiquement lors du démarrage de la machine.

Je dois définir ce service en démarrage auto car il est désactivé par défaut.

Je vais activer ce service par GPO



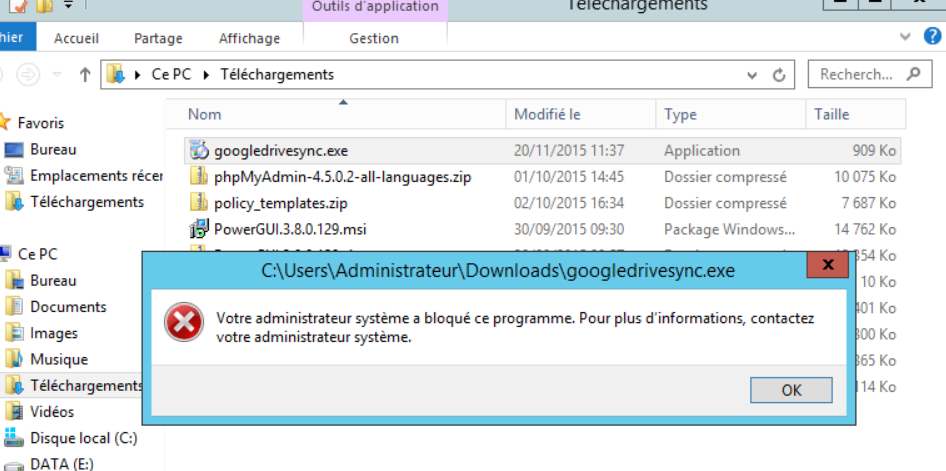
Attention, il s’agit ici du service IDENTITE DE L’APPLICATION et pas PROTECTION LOGICIELLE

J’applique ensuite ma GPO et je tente d’installer Google Chrome ou Google Drive



Si le service identité de l’application a démarré alors la gpo a bien été appliquée.

Je télécharge Google Drive et je tente une installation en exécutant en tant qu’admin, même en renommant cela ne fonctionnera pas car mon verrouillage est basé sur la signature de l’éditeur.



Si j’essaye de contourner l’interdiction en arrêtant et en désactivant le service, l’interdiction va rester et même en désactivant le service et en redémarrant le service va se réactiver à l’application de la GPO au démarrage.

# Procédure de déploiement

Gestion des stratégies de groupe : créer une GPO sur l’ensemble du domaine

Créer une nouvelle GPO et la nommer « APP LOCKER »

Editeur de gestion de stratégie de groupe : configuration ordinateur -> paramètre Windows -> paramètre de sécurité -> stratégie de contrôle de l’application -> APP LOCKER

Service système pour le démarrage automatique de la GPO « APP LOCKER » -> identité de l’application

Appliquer la GPO : « gpupdate /force » dans CMD pour mettre la jour la GPO