Les stratégies de restrictions Logicielles

Guillaume DESFARGES
Laboratoire Supinfo des Technologies Microsoft
The Moderator

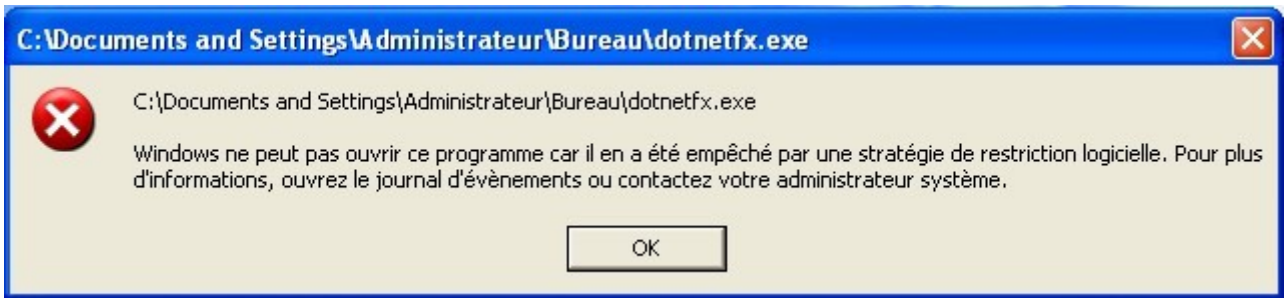
Présentation

Dans un environnement d'entreprise, les utilisateurs sont rarement simples utilisateurs de leur postes. Soit parce qu'ils ont besoin de droits étendus pour faire fonctionner certaines applications, soit pour des raisons politiques.
Le plus gros problème dans ce cas est que le support augmente son activité du fait du nombre d'appels croissant dû à des mauvaises manipulations utilisateurs (Virus/cheval de Troie, installation d'application/drivers non certifié etc.).
Il n'est d'ailleurs même pas nécessaire que l'utilisateur ait des droits étendus pour qu'il installe certains logiciel et puisse les exécuter, beaucoup de logiciels ludiques ne nécessitent que la copie de fichiers sur un répertoire.
Microsoft a donc mis en place, à partir de Windows XP, les stratégies de restrictions logicielles qui vous permettent de restreindre l'exécution de fichiers sur le poste utilisateur.

Comment ça marche ?

Les stratégies de restrictions logicielles sont un nouveau paramètre à l'intérieur des stratégies de groupes de Windows. Elles vous permettent d'empêcher l'exécution de fichiers qui n'auront pas été au préalable approuvé par l'administrateur ou, à l'inverse, d'empêcher l'exécution de fichiers qui auront été expressément interdit par l'administrateur.

Lorsque vous avez configuré une stratégie de restriction logicielle l'utilisateur tentant d'exécuter un fichier interdit recevra ce message d'erreur :



Ce qui vous permet ainsi de limiter certaines mauvaises manipulations, ou même quelque fois l'exécution de code malicieux à l'insu de l'utilisateur.

1. Installation

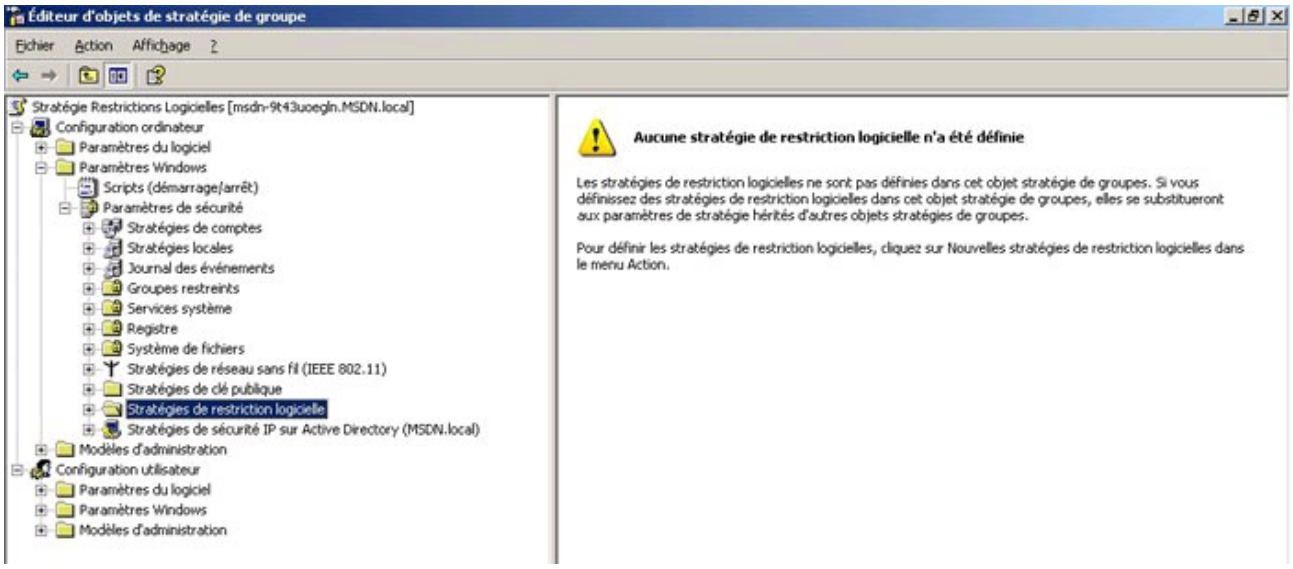
1.1 Activation

Pour pouvoir utiliser les stratégies de restrictions logicielles, il faut que Windows XP soit installé sur les postes utilisateur. Il n'est pas nécessaire d'être dans un domaine, mais dans ce cas les restrictions s'appliqueront à tous les utilisateurs du poste.
Vous pouvez limiter l'application de cette stratégie au simple utilisateur dans le cadre d'un groupe de travail (voir http://support.microsoft.com/default.aspx?scid=kb;fr;293655). Nous nous intéresserons plutôt à leur application dans un domaine Active Directory.

En revanche, vos contrôleurs de domaine peuvent parfaitement être sous 2000, mais dans ce cas, les stratégies de groupes créées dans l'optique de restrictions logicielles ne pourront être créées et éditées que sous Windows XP via le package d'administration (adminpak.msi) de Windows 2003.

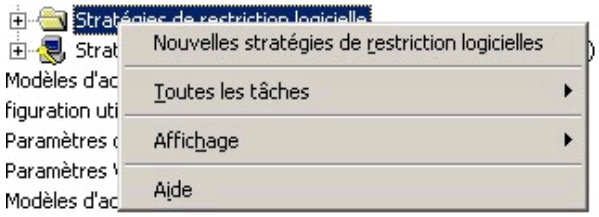
Pour créer une stratégie de restriction logicielle il faut passer par les stratégies de groupes. Dans votre interface d'édition de stratégie développez

Configuration ordinateur->Paramètres de Windows->Paramètres de sécurité.

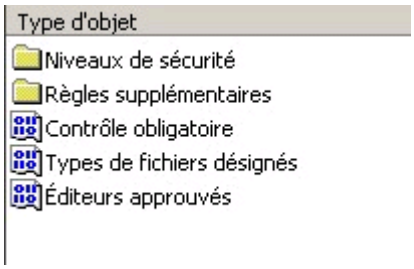


Comme vous pouvez le voir les stratégies ne sont pas activées par défaut, ceci est nécessaire pour limiter la place occupée par votre stratégie de groupe (GPO). En effet l'activation d'une stratégie de restriction logicielle (comme les autres stratégies telles wi-fi, clé publique etc.) augmente considérablement la taille de celle ci.

Comme indiqué, il suffit de cliquer bouton droit sur stratégies de restriction logicielle et de sélectionner nouvelles stratégies de restriction logicielles.

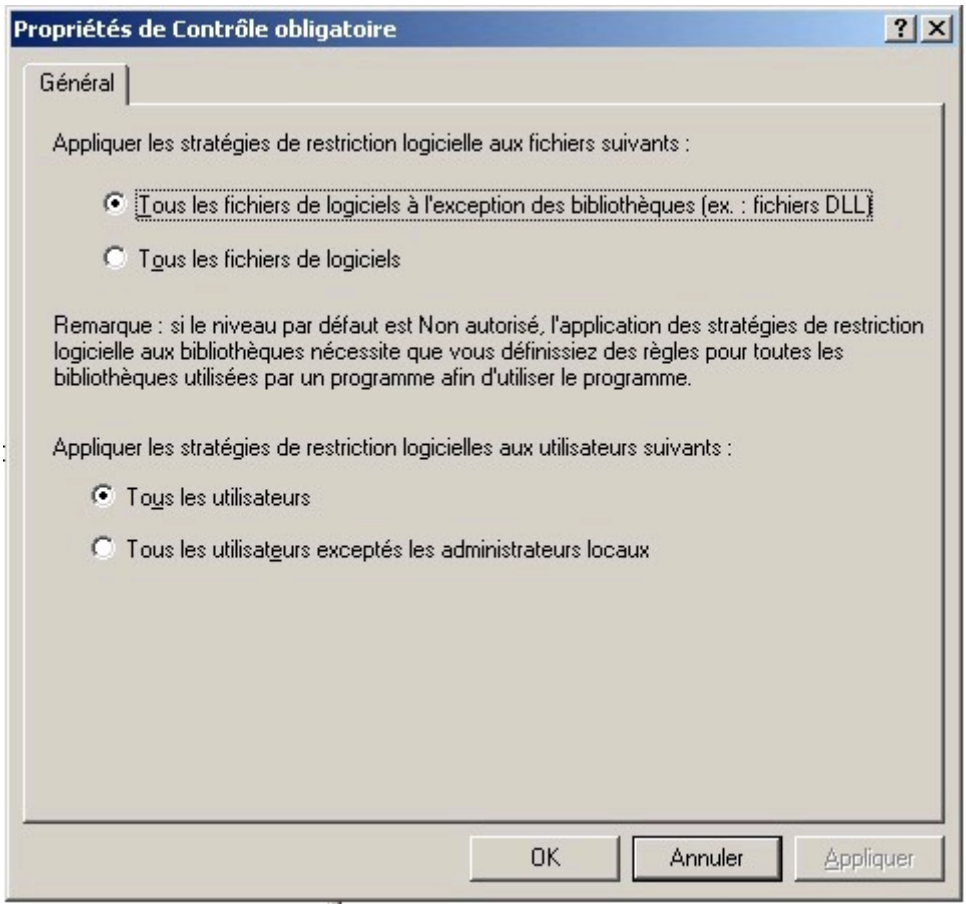


Immédiatement la partie droite se retrouve peuplée de ces éléments :



1.2 Premiers paramétrages

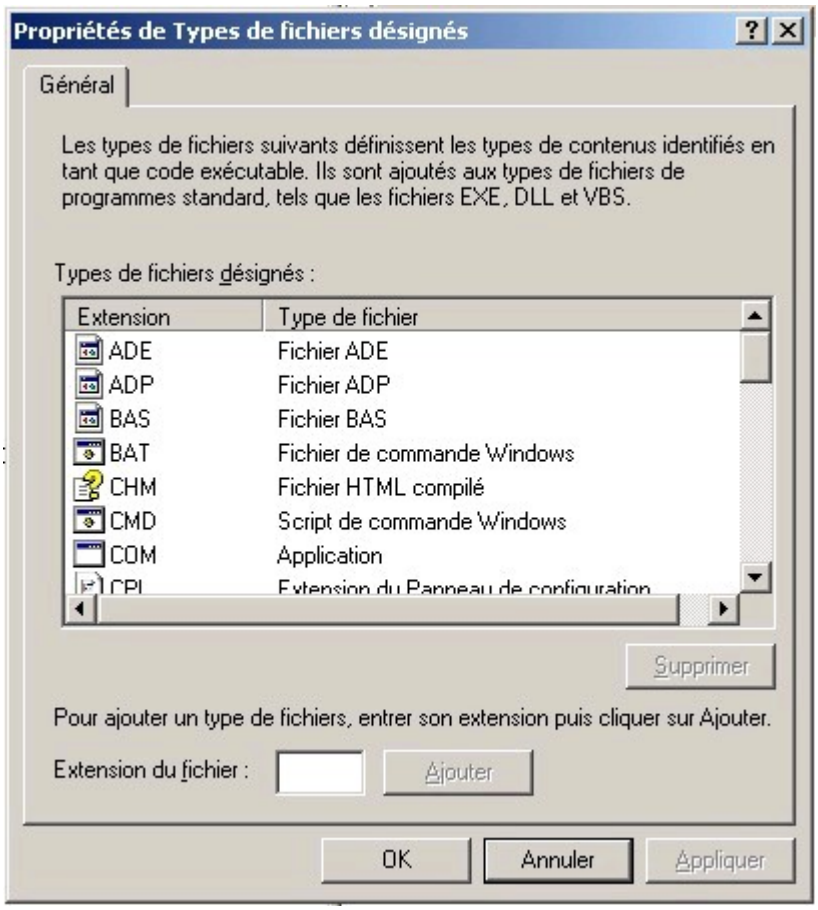
- Le **contrôle obligatoire** vous permet d'activer ou non le contrôle sur vos DLL. Par défaut le contrôle des DLL n'est pas activé pour éviter un ralentissement du système car sinon, la stratégie sera testée systématiquement à chaque appel de DLL, ce qui nuiras largement au temps de réponse de votre système.



De plus sur cette partie vous pouvez indiquer si les restrictions s'appliquent ou non aux administrateurs locaux. En effet, comme cette stratégie est une stratégie ordinateur elle s'appliquera à l'ordinateur quels que soient les utilisateurs connectés.

Les groupes restreints (voir un autre article) vous permettront de peupler le groupe local administrateurs de manière centralisée.

- Les **types de fichiers désignés** vous permettent de définir les différents types de fichiers impacté par ces restrictions logicielles en plus des fichiers par défaut (EXE, VBS, VBE, DLL si vous avez activer l'option précédente). Par défaut, la plupart des extensions d'exécutables sont implémentées.

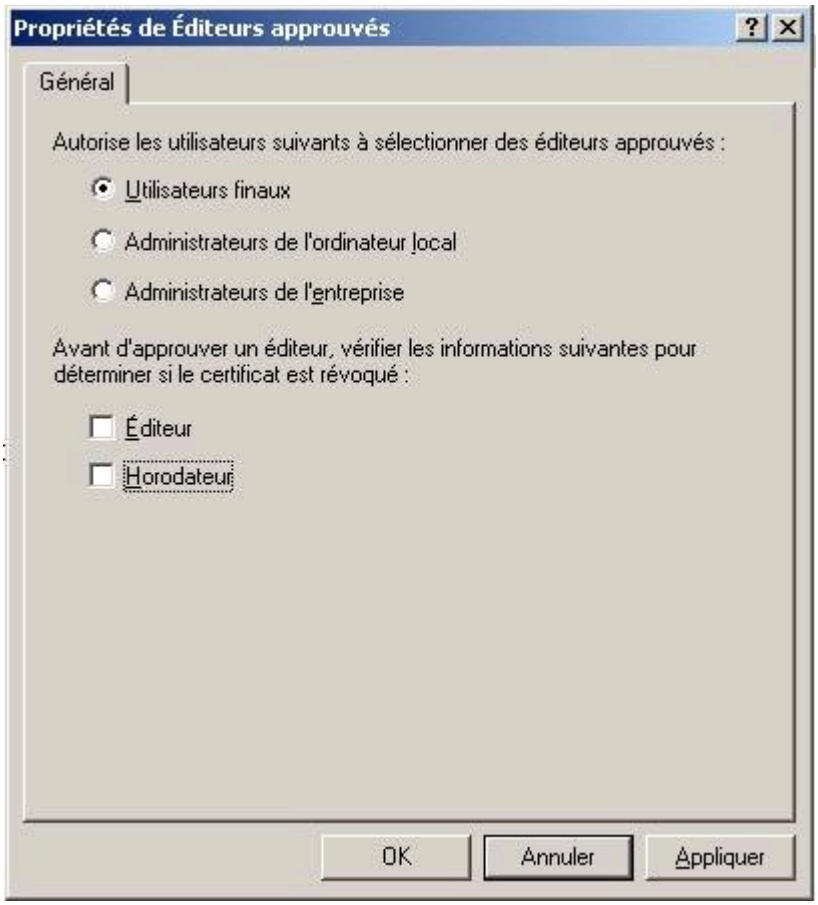


Vous pouvez ainsi ajouter des extensions supplémentaires (qui a dit mp3/avi/mpg ?), il est à noter que les fichiers lnk (Raccourci) sont inclus dans cette liste ainsi si vous mettez en place comme niveaux de sécurité restreints (voir plus loin) le menu démarrer de l'utilisateur, il deviendra inutilisable à moins de rajouter des niveaux supplémentaires.

Cette liste est liée à votre stratégie de groupe ce qui signifie que si vous la modifiez, la liste personnalisée ne sera pas copiée sur d'autres stratégies de restrictions logicielles.

De plus toutes les extensions Windows Installer (MSI, MST, MSP) sont incluses dans la liste par défaut. Ce qui signifie que, comme pour les LNK, vous pouvez fortement impacter le fonctionnement de votre poste pour l'installation de logiciels.

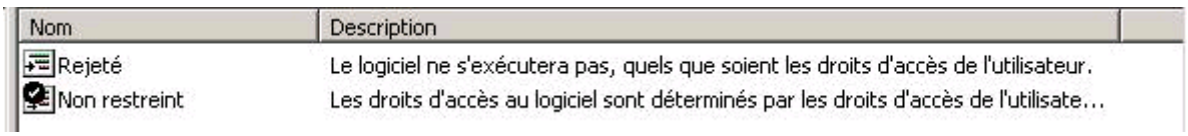
- Les **éditeurs approuvés** sont exclusivement liés aux règles de certificat (voir plus loin), elles vous permettent d'indiquer si d'autres utilisateurs sont autorisés à accepter des certificats d'éditeur de logiciel (pour des contrôles activeX par exemple). Il est conseillé de garder cette configuration telle quelle si vous n'avez pas une connaissance avancée de votre infrastructure de certificats.



1.3 Configuration

1.3.1 Les niveaux de sécurité

Les niveaux de sécurité sont au nombre de deux : Rejeté ou non restreint.



Par défaut la configuration est **Non restreint**, c'est à dire que tant que cela n'est pas expressément indiqué, les fichiers n'ont pas de restrictions logicielles et donc seules les permissions NTFS s'appliquent. C'est un niveau par lequel commencer à se familiariser avec les restrictions logicielles car cela évite de totalement bloquer le poste.

L'autre option **Rejeté** est très dangereuse si vous n'avez pas prévu à l'avance ce que vous allez faire, car à ce moment la totalité des fichiers considérés (Voir *types de fichiers désignés*) qui ne sont pas placé dans le répertoire système ou Program Files seront restreints, il est donc nécessaire d'étudier

réellement l'impact de se paramétrage, sachant qu'il est celui le plus intéressant pour verrouiller votre poste de travail utilisateur.

Pour désigner le niveaux de sécurité que vous désirez, il suffit juste de double cliquer dessus et de cliquer sur le bouton Par Défaut, ainsi la coche se déplace sur le paramètre que vous avez désigné.

1.3.2 Règles Supplémentaires

1.3.2.1 Ordre d'application

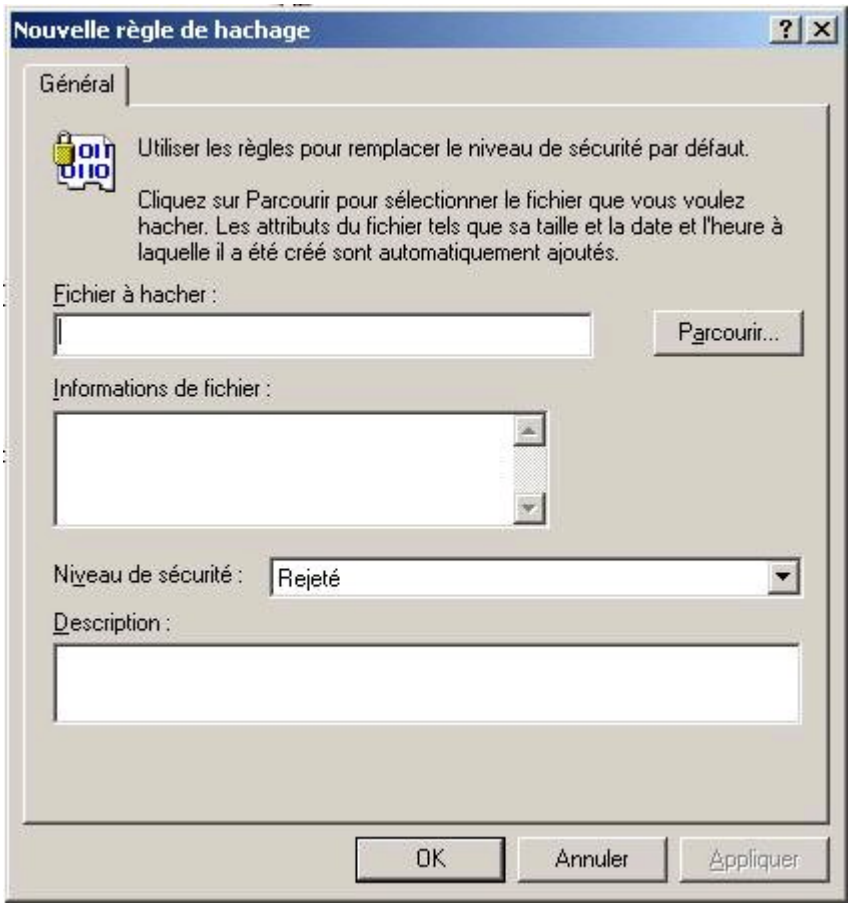
Les règles sont utilisées en conjonction du niveau de sécurité par défaut définit précédemment et elle s'applique suivant cette priorité

1. Règles de Hachage
2. Règles de Certificat
3. Règles de Chemin d'Accès
4. Règles de Zone Internet

Ainsi si deux règles s'appliquent sur le même élément ce sera la plus prioritaire qui prendra le pas sur l'autre. En revanche, si deux règles s'appliquent sur deux éléments différents mais que l'un est l'enfant de l'autre (par exemple un sur C:\Windows et l'autre sur C:\Windows\system) il n'y aura pas écrasement de la restrictions « parente » sur « l'enfant » ainsi une règle sur le répertoire C:\Program Files s'appliquera sur tout ce répertoire et les sous dossiers mais pas sur un sous dossier (par exemple c:\program Files\Microsoft Office) si une autre règle a été définie sur celui ci.

1.3.2.2 Règles de Hachage

Les règles de Hachage, comme son nom l'indique, d'autoriser au d'interdire l'accès aux fichiers au fichiers ayant un Hash définit. Le Hash est une formule mathématique s'appliquant sur le contenant d'un fichier pour générer un chiffre le plus unique possible pour identifier le fichier.



La fonction de Hash est très rapide, ce qui a comme effet de ne pas trop impacter les performances de votre poste de travail et c'est d'ailleurs pour cela que c'est la règle la plus prioritaire.

Une des applications en mode *non restreint* peut être l'interdiction de certaines applications non autorisées par l'entreprise mais l'inconvénient implique que l'administrateur de cette restrictions logicielles doit suivre l'évolution des logiciels non autorisé car lors de la sortie d'une nouvelle version le fichier applicatifs est modifié et donc son Hash aussi. Il faut alors le générer à nouveau, ce qui veux qu'avec le temps et la liste des applications interdites augmentant, l'application de ce scénario deviendra de plus en plus incommode.

Dans l'autre sens dans un mode *rejeté*, il est possible de définir le Hash des applicatifs autorisé sur votre domaine, ce qui vous permet en premier d'interdire l'utilisation de tout applicatif non autorisé ainsi que les mise à jour des applicatifs autorisé. Ce qui vous permet de contrôler totalement votre parc applicatif à l'intérieur de votre infrastructure.

Du fait qu'un Hash n'est pas un chiffre unique (statistiquement il est presque impossible que deux fichiers ait le même Hash) il est possible à un utilisateur malveillant de créer un fichier exécutable à sa guise qui aura le même fichier de Hash (ce qui est quand même long et difficile) c'est pour cela que si vous voulez avoir un poste de travail sécurisé au maximum il est intéressant par exemple de l'utiliser en conjonction avec une des autre règle voir avec des règles de permissions sur le système de fichier NTFS.

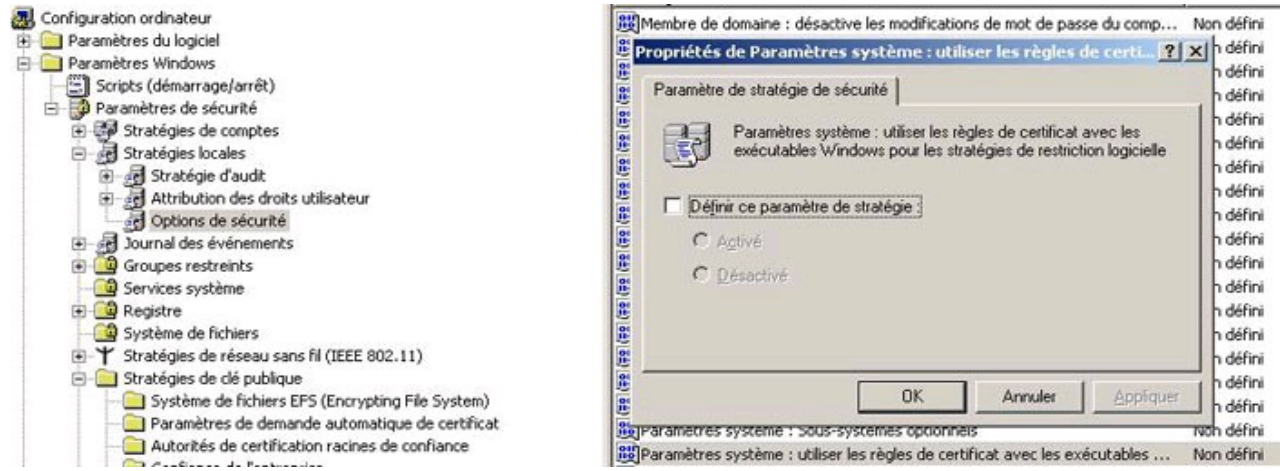
1.3.2.3 Règles de certificats

Les règles de certificats vous permettent de restreindre ou non l'accès à des fichiers suivants l'éditeur de ceux ci. En effet depuis Windows XP tout applicatif peut être livré avec un certificat pour pouvoir identifier le fournisseur. Cela correspond au message que vous recevez quand vous tentez d'ouvrir un fichier directement depuis Internet, Internet Explorer vous indique l'éditeur de l'applicatif.

Avant tout, pour appliquer vos règles de certificats, il faut activer la gestion des certificats pour les application sur les postes de travail. Pour cela par exemple sur votre Gpo de restriction logicielle il faut activer se paramètre système local, vous devez vous rendre sur

- *Configuration ordinateur>Paramètres Windows>Stratégies locales>Option de sécurité*

Et activer le Paramètre système : utiliser règles de certificats avec les exécutables Windows pour les stratégies de restrictions logicielles

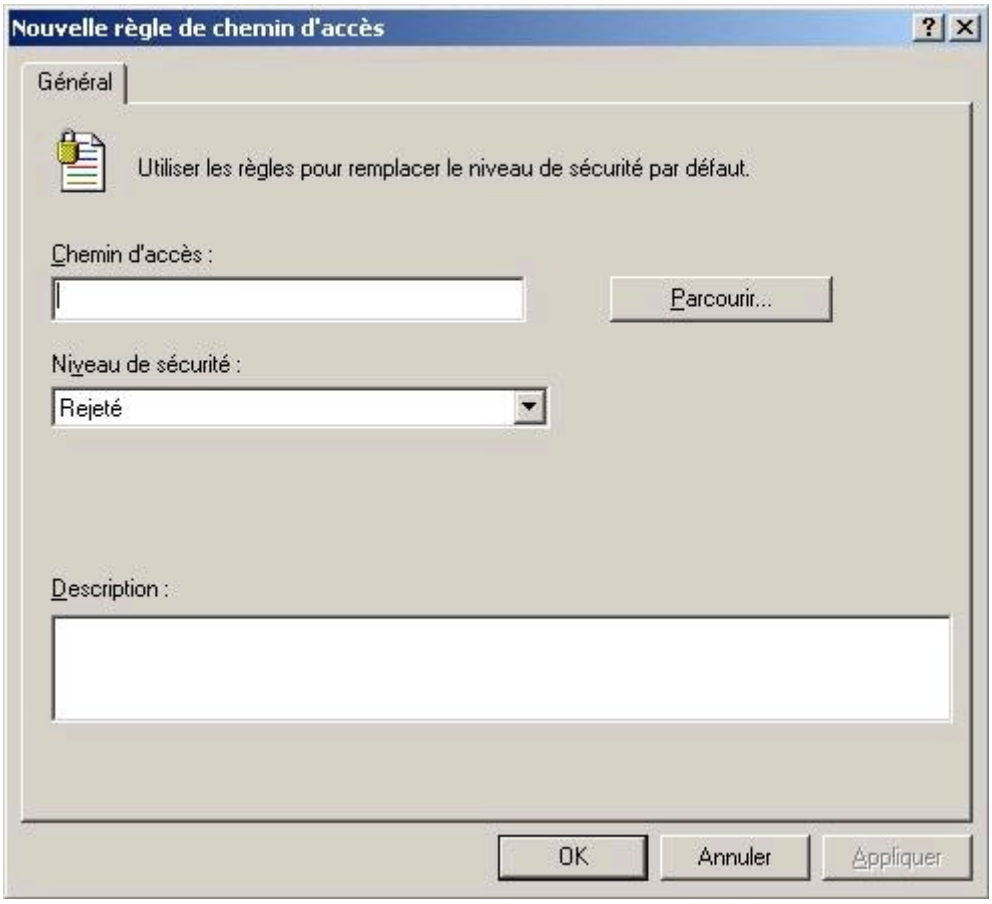


Après l'activation de ce paramètre, les Règles de certificats peuvent être utilisées dans le cadre des restrictions logicielles.

Si vous l'utilisez dans le cadre d'un environnement *non restreints* vous pouvez interdire certains programmes non autorisés mais le problème est que pour les virus vous ne pouvez compter sur la présence d'un certificats sur celui ci, l'utilisation de cette règle dans un cadre non restreints n'est vraiment pas utile.

En revanche dans un cadre de configuration *rejeté* cette règle a toute son importance, car elle vous permet par exemple de vous décharger de toutes les définitions d'application autorisé. En effet vous pouvez parfaitement autoriser Microsoft comme éditeur pour vos applications mais aussi vous pouvez fournir des certificats aux différents développeurs de votre entreprise et ainsi ils signeront les différents exécutables qu'ils créerons. Ainsi, à la différence d'une règle de hachage, il sera moins nécessaire de mettre à jour vos restrictions logicielles vu que les nouvelle version des applications internes seront toujours autorisée car utilisant un certificat défini.

1.3.2.4 Règles de Chemins d'Accès



Pour continuer dans les différentes règles supplémentaire, abordons les règles les plus simple à mettre en place, les règles de chemins d'accès. En effet elles sont plus simple car il suffit juste d'implémenter vos chemins, mais attention si vous mettez des répertoires (par exemple c:\metier\) cette règle (Rejeté/restreint) s'applique au répertoire et à tout les sous répertoires inclus.

Il faut savoir que par défaut vous avez quatre règles de chemin d'accès qui sont implémentés :

Nom	Type	Niveau de sécu...
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Chemin d'...	Non restreint
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*.exe	Chemin d'...	Non restreint
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32*.exe	Chemin d'...	Non restreint
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Chemin d'...	Non restreint

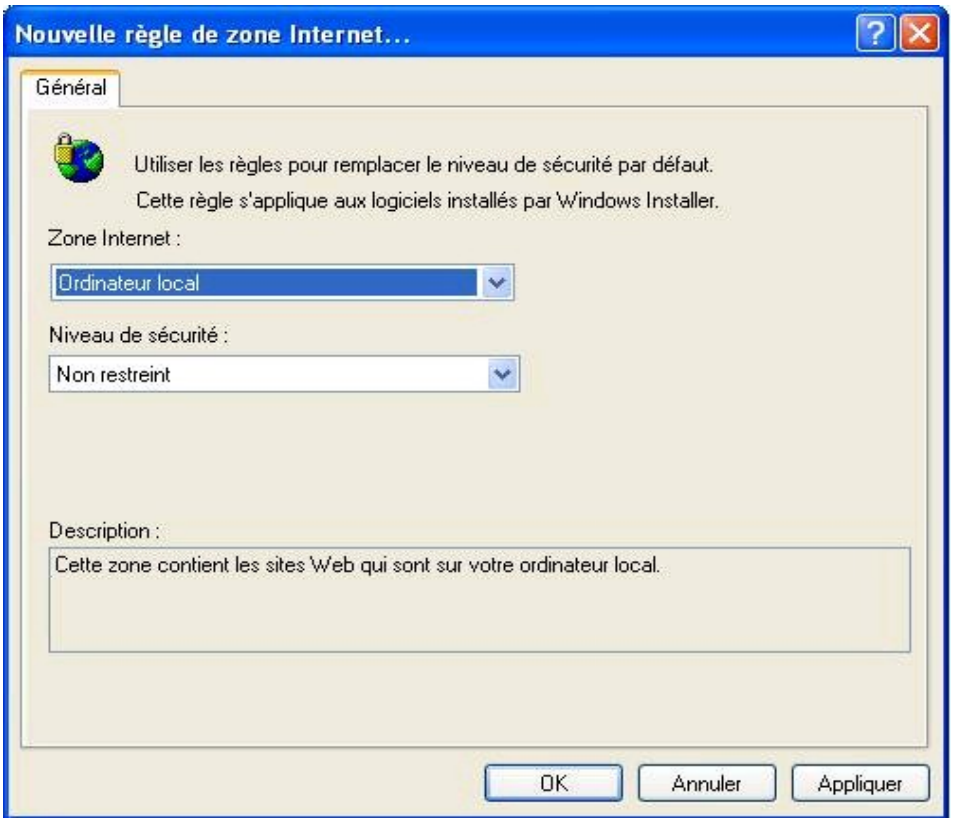
Ces règles sont nécessaires pour le bons fonctionnement de votre système d'exploitation, modifiez les à vos risques et périls.

L'application de ces règles dans un environnement non restreints peux être utile pour bloquer l'exécution d'application pour l'utilisateur sur tous les répertoires où il a un accès en écriture (documents personnels, répertoire ouvert par une application) pour ainsi bloquer un trou de sécurité apparent.

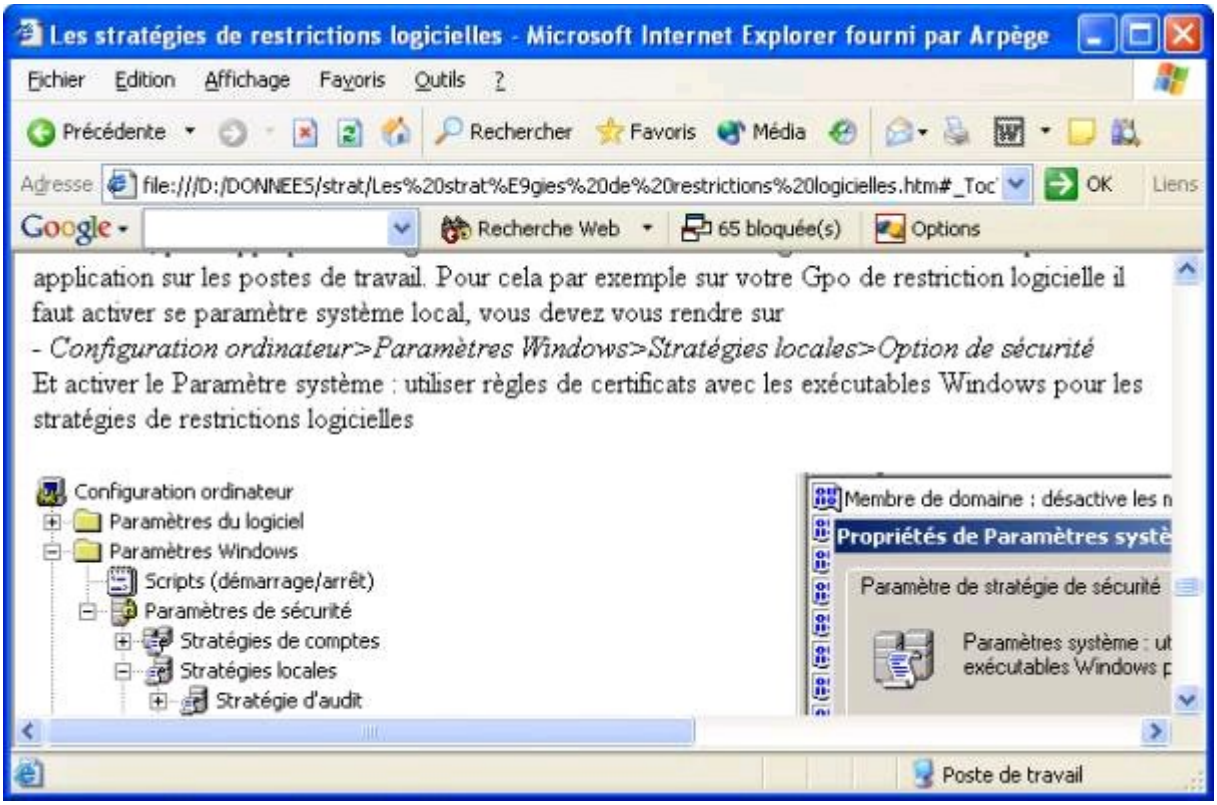
L'application de ces règles dans un environnement Rejeté vous permet d'exécuter les script de connexion en indiquant le chemin vers le répertoire de script, d'exécuter des applicatifs métier qui sont installéw dans un répertoire désigné (c:\metier par exemple), de plus comme l'exécution dans program files est autorisée par défaut (voir plus haut) vous pouvez interdire comme dans un environnement non restreints, l'exécution dans le répertoire où l'utilisateur a des droits en écriture tout en indiquant que l'exécutable de l'application de ce répertoire est autorisé, mais dans ce cas particulier le couplage à une règle de hachage (ou encore certificat) serait plus intéressant (grâce au système de priorité).

1.3.2.5 Règles de Zone Internet

La dernière règle supplémentaire est la règle de zone Internet, la première chose qui vient à l'esprit est la possibilité de bloquer l'exécution de code venant d'Internet.



Le première chose à faire est de bien se rappeler qu'Internet Explorer est intégré à Windows donc toutes vos zones Internet (Internet, Intranet, Sites de confiance, sites sensibles et Ordinateur local) sont utilisés lors de tout vos accès réseau. Preuve en est que lorsque que vous activez la barre d'état dans votre explorateur vous voyez en bas à droite le nom d'une de vos zone internet.



Il faut savoir que ces zones Internet peuvent être configurées via les GPO aussi (ceci ne sera pas couvert par cet article) et que par défaut si elles ne le sont pas tous les accès réseaux seront considéré comme des accès Internet, ce qui risque de poser un problème si vous avez configuré des restrictions pour l'accès par exemple aux scripts de démarrage ainsi qu'à l'installation d'applications à distance

Ces zones Internet peuvent être configurées indépendamment du mode de restrictions car comme il n'y a que 5 zones Internet, vous pouvez facilement définir des restrictions de bases qui s'appliquent à chacune des possibilités à l'intérieur de votre infrastructure.

Pour intégrer une granularité supplémentaire vous pouvez positionner ces règles de zone Internet et ensuite ajouter des règles de plus grande priorité (voir plus haut) pour calquer le plus possible aux spécificités de votre infrastructure.

2. Conclusion

2.1 A ne pas faire

- Ne pas appliquer de restrictions logicielles sur les stratégies par défaut (du domaine, des contrôleurs de domaine, de site) car la moindre mauvaise manipulation peut entraîner le blocage de toute votre infrastructure. Il faut savoir que le démarrage en mode sans échec empêche l'application des restrictions.
- Passer en niveau par défaut Rejeté sans prendre garde car comme précédemment cela peux provoquer le blocage de tous vos postes. Une étude préalable est nécessaire ou l'utilisation d'une OU de test contenant quelques postes pilotes
- N'activez pas les restrictions logicielles sur toutes vos GPO car l'activation augmentera la taille de vos fichier de configuration de vos stratégies de groupes et donc augmentera le trafic de démarrage des postes, c'est d'ailleurs pour cela que certaines stratégies ne sont pas activées par défaut pour alléger la taille de vos GPO. De même ne répartissez pas vos GPO à tout va (GPO activation Excel, GPO activation Word) car si vous faites des stratégie liées à l'activation de chacune de vos applications métier vous risquez de tomber dans un casse tête de gestion dont vous ne pourrez pas sortir.
- N'éditez pas de GPO de restrictions logicielles sous Windows 2000. A l'heure actuelle (SP4), l'ouverture de ces GPO provoque un message d'erreur et peut les corrompre. Préférez l'édition sur un serveur 2003 ou bien si vous êtes sur un domaine avec des serveurs 2000, l'édition depuis une station XP qui a les outils d'administration de Windows 2003.

2.2 Conclusion

Planification, Planification, Planification, je pourrais conclure juste avec ces mots car les restrictions logicielles ne peuvent pas être appliquées à la légère mais les possibilités offertes ne peuvent être ignorées quand on sait que 80% des infections virales viennent de l'utilisateur, que 75% (estimation personnelle) des problèmes utilisateur viennent d'une mauvaise manipulation lors de l'installation d'un logiciel non autorisé ou bien d'un mail infecté.

Dans l'option de renforcement de la sécurité de votre infrastructure le renforcement des restrictions logicielles doit être pris en compte et encore plus si vous ne pouvez diminuer les permissions utilisateurs si ceux ci sont administrateurs de leur postes.