EMPÊCHER L'INTERRUPTION DES SCRIPTS DE CONNEXION

(*R. DARGEIN – 29 NOV. 2005*)

Cette documentation a été rédigée à partir de différentes solutions présentées sur les listes de diffusion, en particulier par Jean-François Bados, Jean–Michel Coste, Christian Draux et Alain Fournier.
Je tiens donc à les remercier pour leurs recherches et leurs essais.

PROBLÉMATIQUE

Les scripts de connexion à un serveur Windows NT/2000/2003, comme ceux générés par GUNT, sont souvent des fichiers batch (extension .BAT) stockés dans le partage NETLOGON. Lors de la connexion d'un utilisateur, l'exécution du script se fait dans une fenêtre de type “DOS” qui peut être interrompue par un simple clic. Afin de réduire ce risque d'interruption une solution consiste à masquer cette fenêtre,
La méthode est différente selon la version du système d'exploitation de la machine cliente.

Une autre solution consiste à bloquer le clavier et la souris de l'utilisateur pendant la durée d'exécution du script.

Toutes les solutions présentées ci-dessous ont été testées.

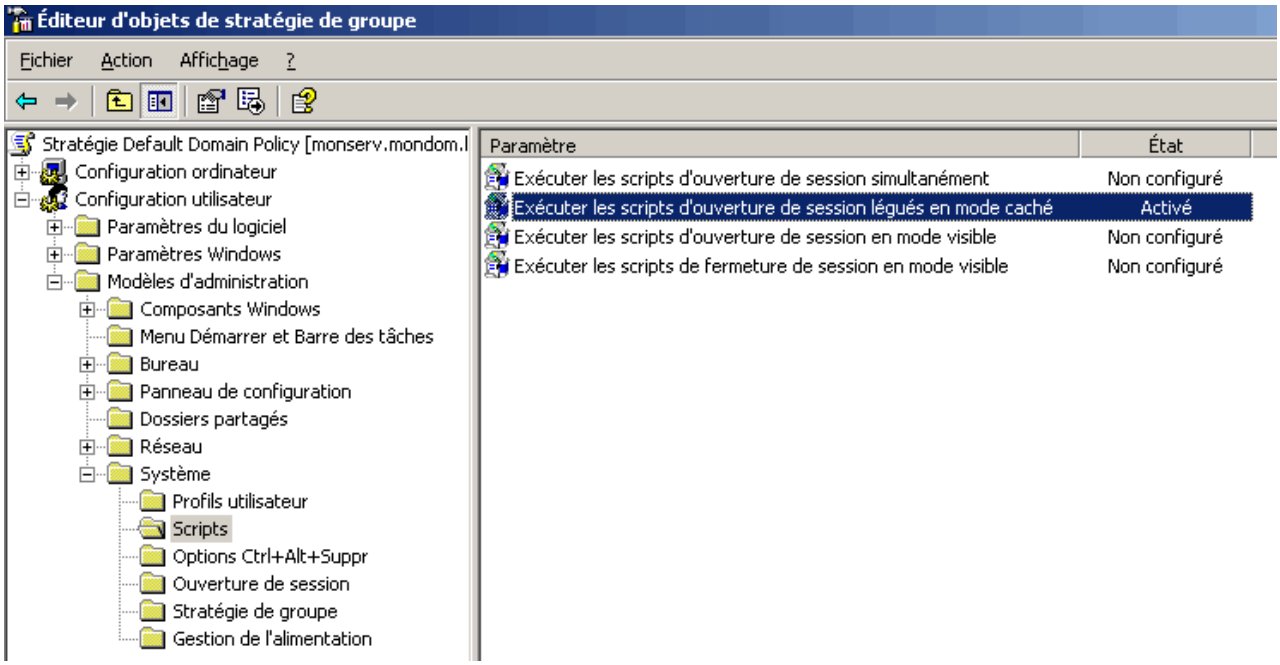
PARC CONSTITUÉ UNIQUEMENT DE STATIONS WINDOWS 2000 ET/OU WINDOWS XP

Dans le cas d'un parc où tous les ordinateurs ont un OS Windows 2000 ou Windows XP, le plus simple est d'utiliser les stratégies de groupe pour demander que les scripts de connexion se déroulent en mode caché.

1. Sur le serveur, lancer "*Utilisateurs et ordinateurs Active Directory*"
2. dans l'arborescence à gauche faire un clic droit sur le domaine puis choisir "Propriétés".
3. Dans l'onglet "Stratégie de groupe", cliquer sur "Nouveau" pour créer une nouvelle stratégie et lui donner un nom (on évite de travailler sur la stratégie "Default Domain Policy").
4. Sélectionner ensuite cette nouvelle stratégie et cliquer sur "Monter" pour la placer avant "Default Domain Policy"
5. Cliquer ensuite sur "Modifier" pour ouvrir l'éditeur de stratégie.
6. Développer l'arborescence dans la partie gauche de la fenêtre pour pointer sur "Scripts" : Configuration utilisateur → Modèles d'administration → Système → Scripts.

7. Dans la partie droite choisir la stratégie "Exécuter les scripts d'ouverture de session légués en mode caché" et la mettre sur "Activé".

8. Fermer l'éditeur de stratégies et l'utilitaire "*Utilisateurs et ordinateurs Active Directory*"



PARC CONSTITUÉ UNIQUEMENT DE STATIONS WINDOWS 98

Dans ce cas l'utilisation des GPO n'est pas possible. Il faut avoir recours à un utilitaire (hidewndw.exe) gratuit et téléchargeable.

Cet outil est considéré par certains antivirus comme un programme espion, il faudra donc avant de le télécharger et l'utiliser l'exclure de la liste des programmes espions au niveau de la console d'administration de l'antivirus ainsi qu'exclure le dossier où il sera installé des paramètres de scan.

Les étapes de la mise en œuvre de hidewndw sont donc :

1. Exclusion de hidewndw de la liste des spywares

2. Exclusion de son dossier d'installation des paramètres de scan

3. Téléchargement de l'utilitaire

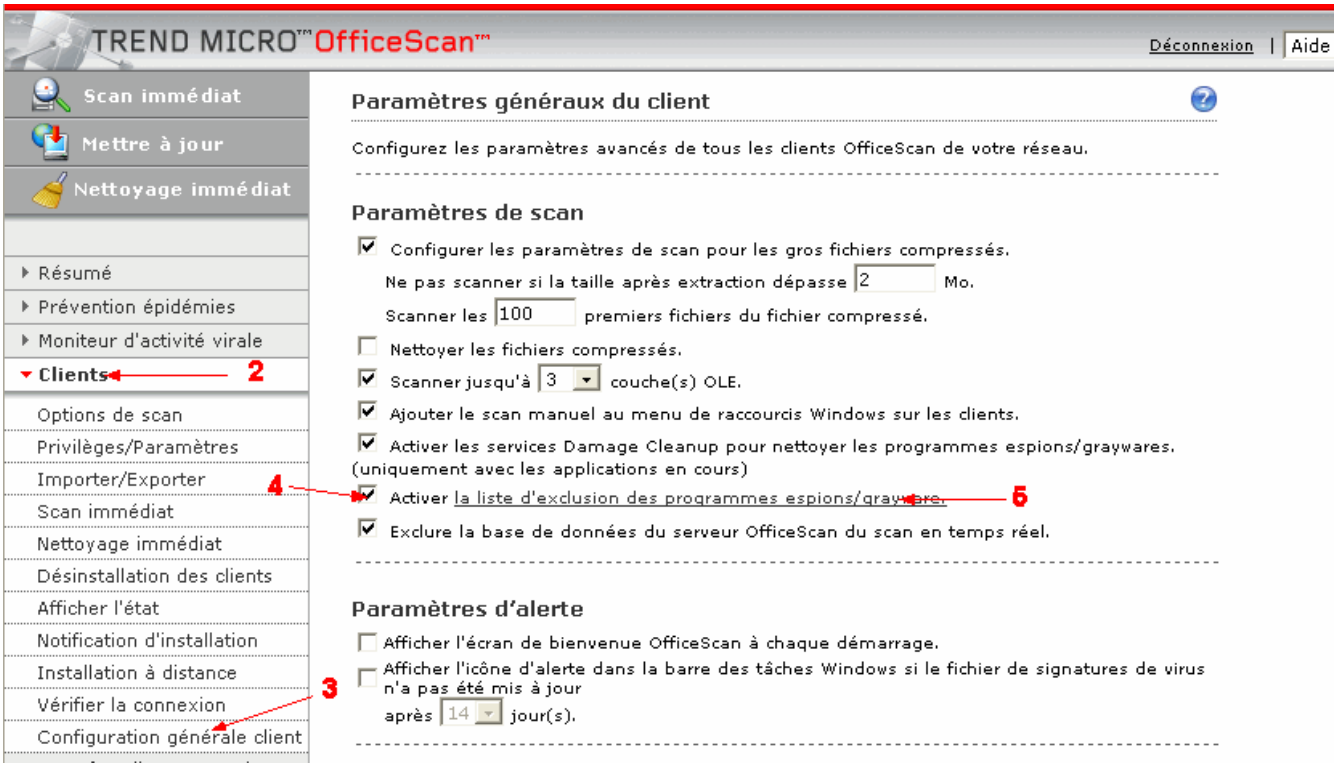
4. Décompression et installation

5. Modification des scripts de connexion.

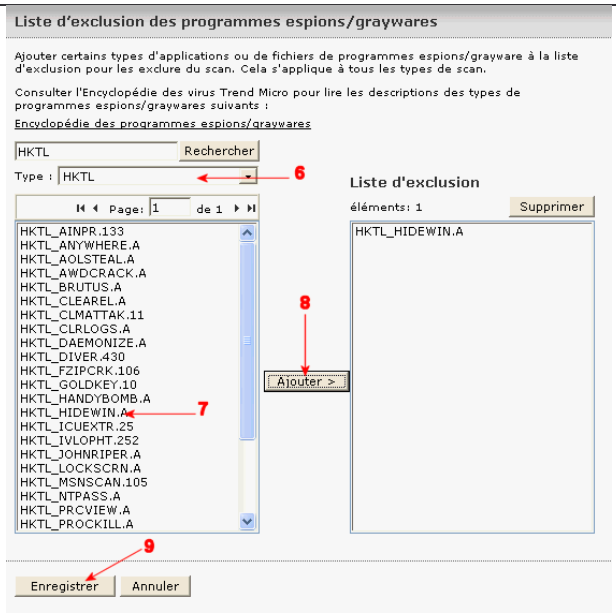
1. Exclusion de hidewndw de la liste des spywares

La procédure n'est donnée que pour la solution antivirale OfficeScan de Trend Micro retenue par l'académie de Créteil. Pour les autres solutions antivirales, reportez vous leur documentation.

1. lancer la console d'administration d'OfficeScan et connectez-vous
2. à gauche, dérouler le menu "*Clients*".
3. sélectionner la rubrique "*Configuration générale client*"
4. sur la page cocher la case "*Activer la liste d'exclusion des programmes espions/graywares*".
5. cliquer sur le lien "la liste d'exclusion des programmes espions/graywares", une fenêtre s'affiche.



6. dans cette fenêtre, dérouler la liste "Type" et sélectionner "HKTL"
7. dans la liste de gauche, sélectionner "HKTL_HIDEWIN.A"
8. cliquer sur "Ajouter"
9. cliquer sur "Enregistrer" puis "Fermer"

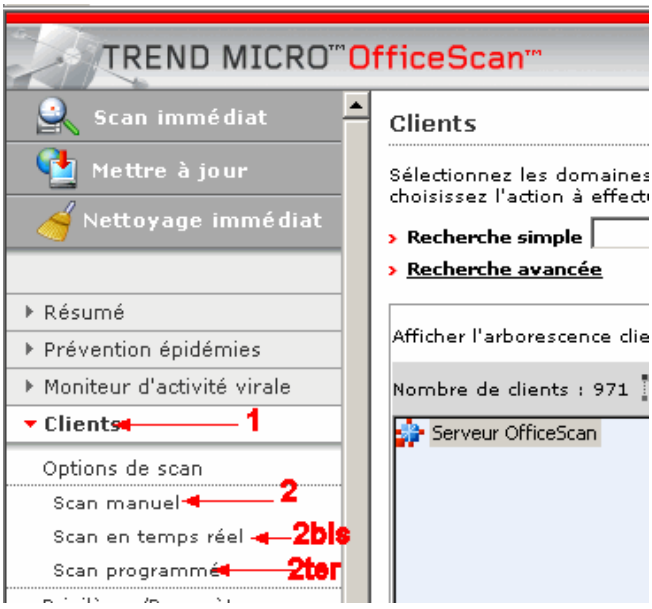


10. de retour dans la partie configuration générale des clients, faire défiler la page vers le bas et cliquer sur "Enregistrer".

2. Exclusion du dossier d'installation de hidewndw des paramètres de scan d'Officescan

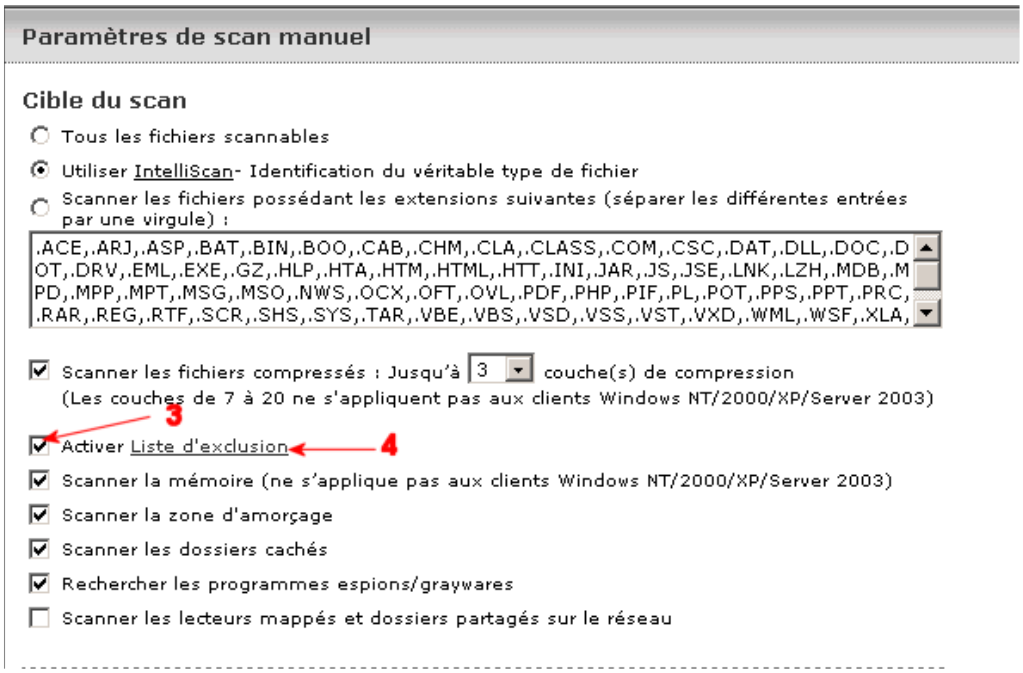
Dans la console d'Officescan :

1. Dérouler le menu "Clients" puis "Options de scan"
2. Cliquer sur "Scan manuel"



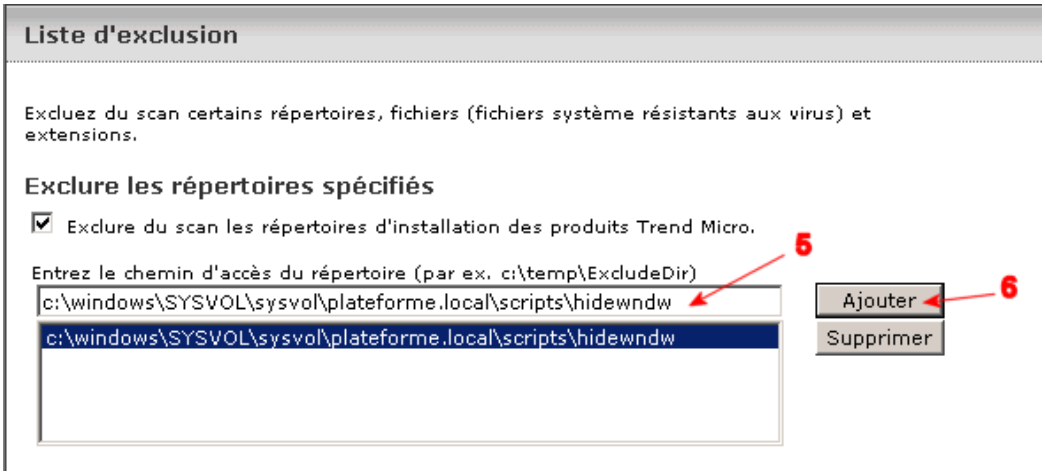
3. Dans la fenêtre des paramètres de scan manuel, cocher la case "Activer la liste" d'exclusion

4. Puis cliquer sur le lien "Liste d'exclusion"



5. Dans la fenêtre d'exclusion, entrer le chemin complet du dossier où hidewndw sera installé
   Dans cet exemple, l'utilitaire sera installé dans le sous-dossier *hidewndw* du partage NETLOGON dont le chemin absolu sur le serveur est :
   c:\windows\SYSVOL\sysvol*Nom de domaine*\scripts

6. cliquer sur "Ajouter" pour compléter la liste des répertoires exclus.



7. Cliquer en bas de page sur "Appliquer à tous" (faire de même pour la fenêtre *Paramètres de scan manuel*)

8. Recommencer à partir du point 2 pour les scan en temps réel et scan programmé (2bis, 2ter)

3. Téléchargement de l'utilitaire hidewndw

Le programme hidewndw.exe est disponible avec son aide sous forme compressée à l'adresse suivante :

http://netdial.caribe.net/~adrian2/creations.html

et sur le site de diffusion de l'académie (menu "Serveurs", rubrique "Gunt/Esu") :

http://diff.ac-creteil.fr/di

4. Décompression et installation

Décompressez le fichier zip et copier le fichier hidewndw.exe dans le partage NETLOGON (ou dans un sous-dossier de ce partage).

Si vous souhaitez diminuer un peu le trafic réseau au moment de la connexion, il vaut mieux alors copier hidewndw.exe dans un dossier sur chacune des machines windows 98. Ce déploiement peut être fait manuellement ou par script. Dans ce dernier cas la syntaxe sera :

IF NOT EXIST c:\windows\hidewndw.exe xcopy \\NomServeur\netlogon\hidewndw.exe c:\windows /r/h/y/Q

Dans cette documentation nous considérerons que hidewndw.exe est unique placé dans le dossier hidewndw du partage NETLOGON.

5. Modification des scripts de connexion

La commande permettant de masquer la fenêtre du scripts sur une station Windows 98 est :

\\NomServeur\netlogon\hidewndw\hidewndw.exe /fh /c "tty"

Placer cette ligne en début de script de connexion à l'aide de GUNT.

(voir le document " *Modification des scripts de connexion avec GUNT*" téléchargeable sur le forum de l'académie http://forum.ac-creteil.fr/info sous-forum "GUNT, ESU et DISTRIB" ou sur le site de diffusion http://diff.ac-creteil.fr/di menu "*Serveurs*", rubrique "*Gunt/Esu*")

PARC CONSTITUÉ DE STATIONS WINDOWS 98 ET WINDOWS 2000/XP

Cette situation est la plus fréquente dans nos établissements.

Il serait possible de faire une combinaison des 2 solutions précédentes (GPO + hidewndw.exe) mais le plus simple est de tout réaliser avec hidewndw.exe.

Les étapes 1 à 3 du point précédent restent les mêmes.
Seule la modification du script de connexion diffère car il faudra tenir compte de la version de l'OS du client.

Dans le cas d'une station **Windows 98** la syntaxe est :

\\NomServeur\netlogon\hidewndw\hidewndw.exe /fh /c "tty"

Dans le cas d'une station **Windows 2000/XP** la syntaxe est :

\\NomServeur\netlogon\hidewndw\hidewndw.exe /fh /c "ConsoleWindowClass"

Le script doit donc tester la version de l'OS de la machine cliente (en cherchant par exemple l'existence du fichier command.com à la racine de C:).
Le morceau de script à ajouter dans le fichier BAT est donc :

```
if EXIST c:\command.com goto w9x
:winxp
\\MONSERV\NETLOGON\hidewndw\hidewndw /fh /c "ConsoleWindowClass"
goto suite
:w9x
\\MONSERV\NETLOGON\hidewndw\hidewndw /fh /c "tty"
:suite
```

Ainsi le script complet doit ressembler à ceui-ci :

```
@ECHO OFF
if EXIST c:\command.com goto w9x
:winxp
\\MONSERV\NETLOGON\hidewndw\hidewndw /fh /c "ConsoleWindowClass"
goto suite
:w9x
\\MONSERV\NETLOGON\hidewndw\hidewndw /fh /c "tty"
:suite
ECHO Script généré par GUNT Version 3.0.1.9
REM La ligne suivante permet de lancer UNCONN (déconnexion des lecteurs)
\\MONSERV\NETLOGON\UNCONN.EXE /keep=z
NET USE P: /Home /Yes
NET USE Q: "\\MONSERV\11L$" /Yes
REM La ligne suivante permet de lancer le client ESU
REM  \\MONSERV\NETLOGON\ESU\ESUCLNT.EXE
```

BLOCAGE DU CLAVIER ET DE LA SOURIS

Une autre approche pour empêcher l'interruption volontaire du script de connexion par l'utilisateur consiste à bloquer temporairement, le temps d'exécution du script, le clavier et la souris.

Ceci est possible grâce à un utilitaire dénommé *bloque.exe* écrit par Yannick Lanchec développeur de GUNT.

L'utilisation en est extrêmement simple et est identique pour toutes les versions de Windows des stations clientes.

Ce programme est à placer dans le partage NETLOGON et doit être appelé en début de script pour bloquer clavier et souris, et en fin de script pour les débloquer.

Le programme bloque.exe et la documentation rédigée par son auteur sont disponibles en téléchargement, avec l'autorisation de Yannick Lanchec, sur les site et forum de l'académie de Créteil.

Site : http://diff.ac-creteil.fr/di menu "Serveurs", rubrique "Gunt/Esu"

Forum : http://forum.ac-creteil.fr/info forum "GUNT, ESU et DISTRIB"