6

Environnement d’exécution des Scripts

6- Environnement d'exécution des Scripts

Puisque *Windows Script Host* est un langage de script d'abord conçu pour l'administration de systèmes, cette dernière section se penche sur les éléments de l'environnement reliés à l'exécution des scripts.

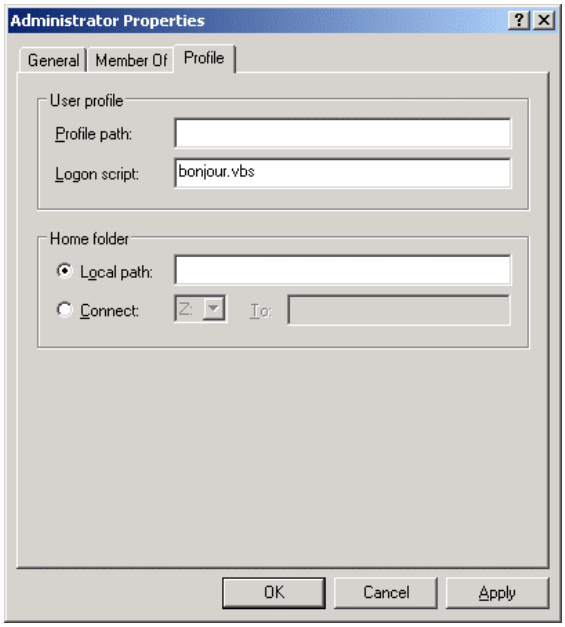
Créer des scripts de démarrage

Il peut être pratique pour un administrateur réseau de créer un script s'exécutant automatiquement à l'ouverture de session de ses utilisateurs afin de connecter les différents lecteurs réseau et imprimantes, etc. Pour ce faire, vous devez d'abord créer le script et le déposer dans un répertoire précis.

Sous un poste de travail NT 4 et 2000, le fichier de script doit être déposé dans :

```
\winnt\system32\repl\imports\scripts
```

Démarrez ensuite l'outil d'administration du système et localisez l'utilisateur ou le groupe concerné avant d'en afficher les propriétés. Sélectionnez ensuite l'onglet `Profil` et spécifiez le nom de ce fichier de script à exécuter à l'ouverture de la session.



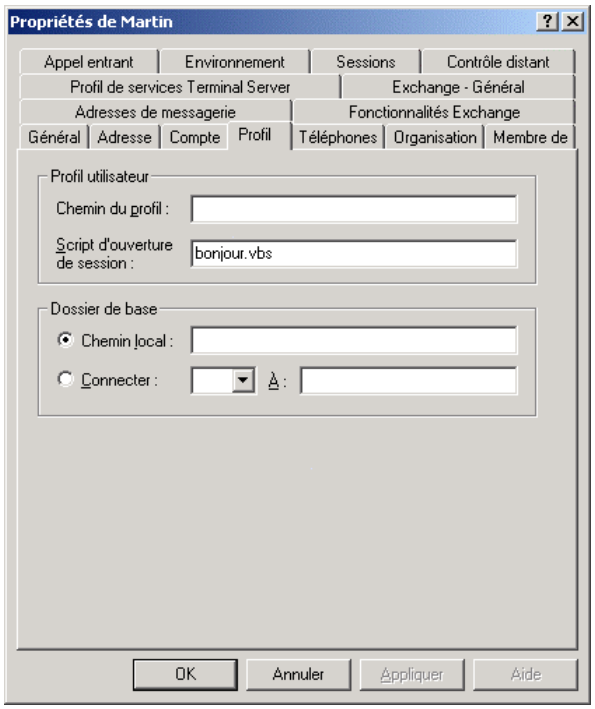
Sous un contrôleur de domaine NT 4, le fichier de script doit être déposé dans :

```
\winnt\system32\repl\imports\scripts
```

Sous un contrôleur de domaine 2000, le fichier de script doit être déposé dans :

```
\winnt\sysvol\domain\scripts\
```

Localisez ensuite l'utilisateur ou le groupe concerné et en afficher les propriétés. Sélectionnez ensuite l'onglet `Profil` et spécifiez le nom de ce fichier de script à exécuter à l'ouverture de la session.

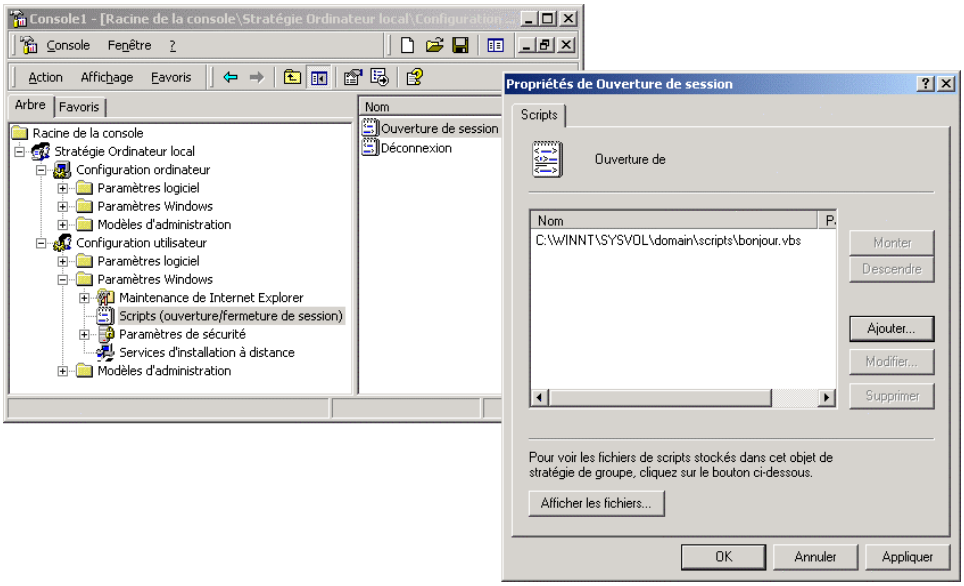


Sous Windows 2000, il est également possible de configurer les stratégies de groupe afin d'activer l'exécution d'un script au démarrage d'une session.

1. Démarrez une console MMC vierge. Pour ce faire, tapez `MMC` à l'invite de commande ou dans le menu *Démarrer → Exécuter*. Ajoutez le composant enfichable `Stratégie de groupe`.

2. Sélectionnez *Ouverture de session* ou *Déconnexion* sous *Configuration utilisateur → Paramètres Windows → Scripts (ouverture/fermeture de session)*

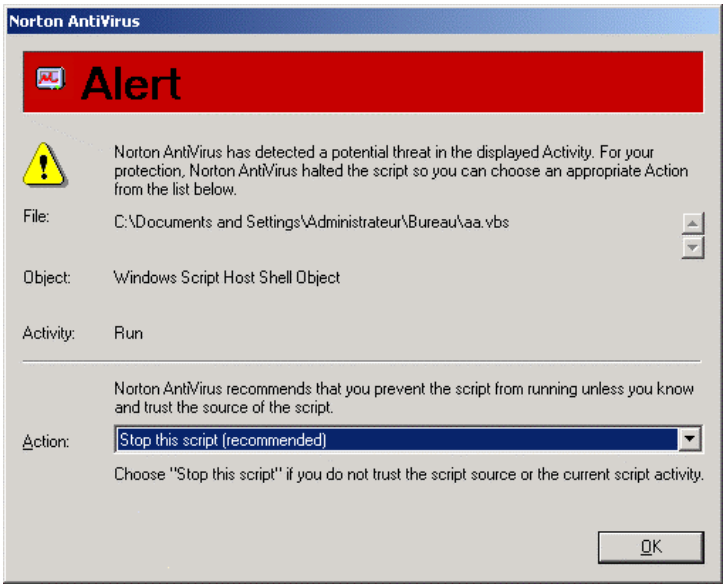
3. Ensuite, ajoutez le chemin du fichier de script dont l'exécution doit s'effectuer automatiquement.



Sécuriser l'exécution des scripts

Le *Windows Script Host* a été conçu à la base en tant qu'outil d'administration des systèmes. Cependant, on devinera rapidement que les fonctionnalités d'accès à la base de registre et aux fichiers prévus par *Windows Script Host* peuvent en faire un outil de destruction des systèmes, c'est-à-dire le transformer en virus. Puisqu'un script peut contenir du code malicieux, il peut s'avérer vital à un administrateur réseau d'encadrer l'exécution des scripts au sein d'un environnement multi-utilisateurs.

La technique la plus simple demeure l'**installation d'un antivirus** sur les postes concernés. Par exemple, *Norton Antivirus* peut bloquer l'exécution de certaines instructions de *Windows Script Host* jugées à risque. Ainsi, l'exécution d'une instruction `WScript.Run` provoque l'intervention de *Norton Antivirus* comme le démontre l'illustration ci-contre.



Norton Antivirus offre ensuite la possibilité à l'utilisateur d'arrêter le script, d'exécuter l'instruction en cours, d'exécuter l'ensemble du script ou de toujours permettre l'exécution d'une telle instruction.

Désactivation de l'exécution automatique des scripts

Par défaut, *Windows* associe les fichiers de script **.vbs* mais également **.vbe*, **.js*, **.jse* et **.wsf* aux hôtes `CScript.exe` et `WScript.exe` ce qui leur permet d'être automatiquement exécutés lorsqu'un fichier de script est activé. Bien que ce comportement semble correct, il peut s'avérer néfaste au sein d'un environnement multi-utilisateurs puisqu'un script pourrait contenir du code malicieux. Ainsi, ce type de virus pourrait automatiquement être exécuté lorsqu'activé par l'utilisateur ou par un logiciel de messagerie électronique. Il peut donc s'avérer important de protéger les systèmes de l'exécution automatique de scripts malintentionnés.

Une technique de prévention classique demeurait de renommer les applications `CScript.exe` et `WScript.exe` par quelque chose comme `_CScript.exe` et `_WScript.exe` afin de corrompre l'association effectuée par *Windows* entre les fichiers script et les applications correspondantes. L'exécution des scripts pouvait alors s'effectuer explicitement comme suit :

```
_CScript.exe c:\chemin\monScript.vbs
```

Sous les systèmes d'exploitation Windows 2000 et plus, cette technique est déconseillée puisque les applications `CScript.exe` et `WScript.exe` sont stockées dans le cache DLL de *Windows* et sont automatiquement régénérés lors du redémarrage de *Windows*.

L'association entre les fichiers de scripts et les applications peut également être interrompue à l'aide d'une simple **modification de la base de registre**. En effet, l'association est inscrite dans

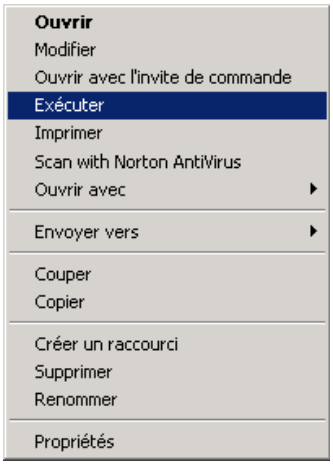
la clé `HKEY_CLASSES_ROOT\VBSFile\Shell\Open\Command` comme le démontre l'illustration suivante indiquant que l'application `WScript.exe` est utilisée pour ouvrir les fichiers *VBSFile* :

Le fait d'exécuter un fichier **.reg* comme le suivant afin de modifier la base de registre pourrait avoir l'effet d'ouvrir automatiquement *Notepad.exe* lorsque le fichier de script est activé.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\VBSFile\Shell\Open\Command]
@="Notepad.exe \"%1\" %*"

[HKEY_CLASSES_ROOT\VBSFile\Shell\Open3]
@="E&xécuter"

[HKEY_CLASSES_ROOT\VBSFile\Shell\Open3\Command]
@="C:\\WINNT\\System32\\WScript.exe \"%1\" %*"
```

CH06\Scripts Sécurisés.reg

La commande `Open` est désormais associée avec *Notepad.exe* et une troisième action *(Open3)* a été définie pour lancer `WScript.exe`. Ainsi, l'exécution des fichiers de scripts devrait se faire explicitement à l'aide du menu contextuel comme le démontre l'illustration ci-contre.



Il reste à répéter l'opération sur les fichiers *WSFFile*, *VBEFiles*, *JSFile* et *JSEFile*.

Désactivation de l'autorisation d'exécuter des scripts

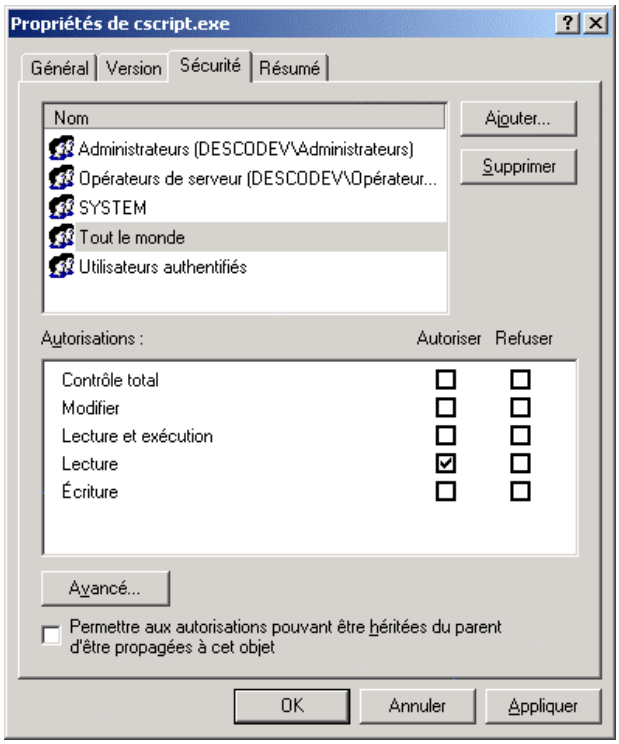
Un administrateur réseau peut désirer s'accaparer le privilège d'exécuter des scripts sur les différents postes constituant son réseau afin de s'assurer que l'action des utilisateurs ne provoquera pas de résultats indésirables sur leur poste respectif.

Il est possible dans un environnement Windows NT4, 2000 et XP de définir les permissions d'exécuter un fichier à des utilisateurs et des groupes spécifiques. Ainsi, il suffit de **limiter la permission d'exécuter les fichiers `CScript.exe` et `WScript.exe`** à des groupes restreints pour éviter qu'un utilisateur non-autorisé n'active par inadvertance un script quelconque.

1. Connectez-vous en rôle d'administrateur sur le poste local et repérez les fichiers `CScript.exe` et `WScript.exe`. Vous trouverez ceux-ci dans le répertoire système (*\winnt\system32* sous *Windows NT4* et *Windows 2000*; *\winnt\system* sous *Windows XP*).

2. À l'aide du bouton droit de la souris sur le fichier, activez le menu contextuel et sélectionnez le sous-menu Propriétés.

3. Sélectionnez l'onglet `Sécurité` puis ajoutez et supprimez les groupes et utilisateurs possédant un accès au fichier.



Notez que cette technique empêche les utilisateurs exclus des permissions d'exécuter tout script puisqu'il ne possède d'accès à l'hôte de script nécessaire à l'exécution des scripts sous *Windows*.

Une autre solution demeure d'**utiliser les stratégies de groupe pour limiter l'accès aux fichiers `CScript.exe` et `WScript.exe`**.

4. Démarrez une console MMC vierge. Pour ce faire, tapez `MMC` à l'invite de commande ou dans le menu *Démarrer → Exécuter*. Ajoutez le composant enfichable `Stratégie de groupe`.

5. Sélectionnez *N'exécutez pas les applications Windows spécifiées* sous *Configuration utilisateur → Modèles d'administration → Système*

6. Ensuite, activez la stratégie et ajoutez le nom des deux applications `CScript.exe` et `WScript.exe` à la liste d'applications dont l'exécution n'est pas permise.