GUIDE

STORMSHIELD ENDPOINT SECURITY

# GUIDE DE PRISE EN MAIN

Version 7.2

Dernière mise à jour du document : 10 août 2020

Référence : ses-fr-guide_de_prise_en_main-v7.2

# Table des matières

Dans la documentation, Stormshield Endpoint Security est désigné sous la forme abrégée : SES.

# 1. Avant de commencer

L'objectif de ce document est de vous aider dans la mise en œuvre initiale de SES. Il est complémentaire au *Guide d'administration* de la solution qui décrit de manière exhaustive ses fonctionnalités.

Chaque entreprise ayant des besoins différents et des particularités dans son système d'information, ce document ne donne que des recommandations et certaines règles de sécurité ne s'appliquent pas à tous les contextes.

Nos recommandations de configuration de la solution SES s'appliquent à la version 7.2 de SES.

# 2. Protéger et configurer le serveur SES

La première étape du déploiement de la solution consiste à sécuriser le serveur SES. Nous vous recommandons d'appliquer les mesures suivantes :

- Mettre à jour Windows update
- Installer un antivirus sur le serveur
- Activer le firewall Windows du serveur
- Mettre en place une sauvegarde du serveur
- Superviser le serveur (avec un outil comme Nagios)

Les ports à ouvrir sur le firewall Windows du serveur sont les suivants :

- Communications entrantes :
  - TCP 80 (personnalisable) : Agent SES vers Serveur SES (Téléchargement fichier MSI + mise à jour antivirus)
  - TCP 443 (personnalisable) : Agent SES vers Serveur SES (téléchargement certificat)
  - TCP 16004 : Agent SES vers Serveur SES (logs)
  - TCP 16005 : Agent SES vers Serveur SES
  - TCP 16006 : Agent SES vers Serveur SES
  - TCP 16007 : Console SES vers Serveur SES (synchronisation)
- Communications sortantes :
  - TCP 1433 (personnalisable) : Serveur SES vers Serveur SQL (accès bases de données)
  - UDP 1434 (personnalisable) : Serveur SES vers Serveur SQL (accès bases de données)

**AVERTISSEMENT**
Si le serveur SQL utilise des ports dynamiques (cas de l'installation par défaut avec SQL express), vous avez deux solutions :

- Modifier la configuration de SQL pour avoir des ports fixes,
- Ouvrir d'autres ports dans le firewall du serveur Windows.

# 3. Protéger l'accès à la console SES

Si vous administrez SES pour un client, vous devez créer des comptes d'administration différents pour chaque administrateur. La solution permet de tracer chaque action.

La partie **Audit** permet de retrouver les modifications qui ont été effectuées et par qui. Cela peut par exemple être utile lorsqu'il y a un problème avec une configuration ou une politique de sécurité.

# 4. Configurer les agents SES

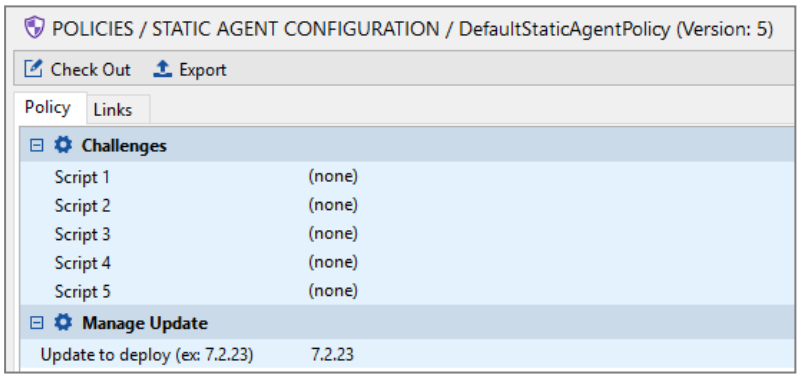
## 4.1 Configuration dynamique

Nous vous recommandons d'utiliser les configurations dynamiques des agents suivantes :

- Mode Warning + pas de notification + autoriser l'arrêt de l'agent : pendant la première phase d'installation,
- Mode Normal + notification + interdire l'arrêt de l'agent : pour les personnes ayant une bonne maîtrise de l'informatique,
- Mode Normal + pas de notification + interdire l'arrêt de l'agent : pour les utilisateurs finaux.

## 4.2 Configuration statique

Dès l'installation de la solution, nous vous recommandons de spécifier la version de l'agent. Par exemple si vous installez SES version 7.223, vous devez configurer la mise à jour des agents en version 7.223 :



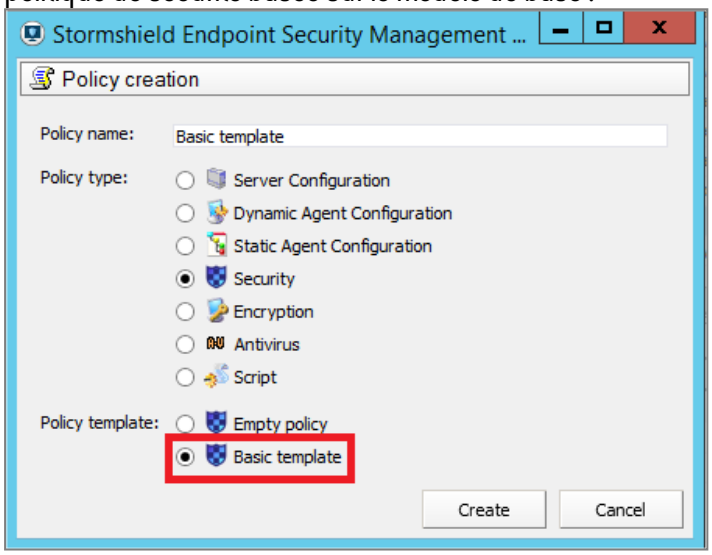

Ainsi lorsque vous migrerez en 7.2.24, vous créerez une autre configuration statique que vous appliquerez uniquement aux ordinateurs qui serviront à tester la migration.

# 5. Créer une politique de sécurité de base

Le niveau de sécurité informatique dans une entreprise dépend essentiellement du temps alloué à la sécurité. Ci-dessous nous donnons deux exemples de configuration. La première politique de sécurité bloque 95% des vulnérabilités, la deuxième apportant une meilleure sécurité en bloque 99,9% (ces chiffres sont une estimation et peuvent varier en fonction des menaces).

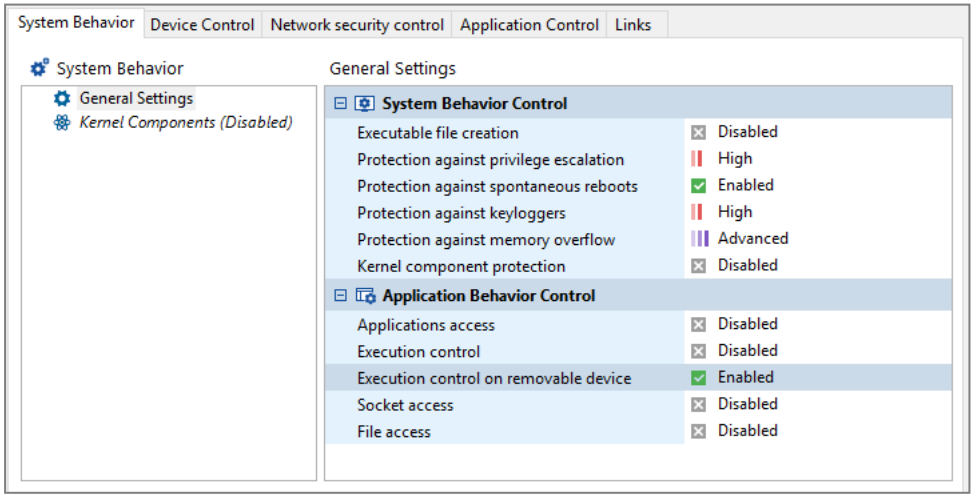
## 5.1 Configurer SES en une journée

Si vous souhaitez effectuer votre première configuration en une seule journée, créez une politique de sécurité basée sur le modèle de base :




## 5.2 Configurer SES en deux jours minimum

Choisissez un modèle de politique de base et ajoutez quelques paramètres généraux :




Le contrôle applicatif peut être utilisé en mode liste noire ou liste blanche. Nous vous recommandons de l'utiliser en mode liste noire pour la plupart des terminaux à protéger. Le mode liste blanche peut être utilisé dans des environnements qui subissent très peu de modifications (systèmes embarqués, postes isolés avec une application précise, terminaux de points de vente, etc.).

L'utilisation des logs détaillés ou l'utilisation du mode liste blanche peut avoir un impact sur les performances des machines, car le contrôle est très important sur les processus qui peuvent être exécutés sur le poste. La phase de démarrage de l'ordinateur peut être ralentie.

## 5.3 Configurer le contrôle du comportement système

Pour plus de détails sur ces protections, consultez le *Guide d'administration* de SES.

### 5.3.1 Autoriser la création de fichiers exécutables

- **Désactivé** : sécurité basse,
- **Haut/Critique** : sécurité haute avec les contraintes suivantes :
  - Il faut désactiver SES à chaque installation/mise à jour d'un logiciel,
  - Une infrastructure de pré-production doit être utilisée pour créer les règles sur les applications de confiance nécessaire.

Cette protection peut facilement être activée sur les serveurs, par exemple les serveurs RDS 2016.

### 5.3.2 Protection contre l'élévation de privilèges

- **Désactivé** : sécurité basse,
- **Haut** : ce niveau est déconseillé car le mode critique protège mieux,
- **Critique** : sécurité haute avec les contraintes suivantes :
  - SES devra peut-être être désactivé pour installation/mise à jour d'un logiciel,
  - Une infrastructure de pré-production devra être utilisée pour créer les règles sur les applications de confiance nécessaire.

Le blocage des attaques de type pass-the-hash (par exemple via le logiciel mimikatz) nécessite le niveau critique pour cette protection.

### 5.3.3 Protection contre les redémarrages forcés

Cette protection est conseillée pour les serveurs uniquement. Dans le cas où cette protection est utilisée, il faut faire confiance aux applications de déploiement du type SCCM, Ninite, LANDesk, etc.

### 5.3.4 Protection contre les keyloggers

- **Désactivé** : sécurité basse,
- **Haut** : sécurité haute avec la contrainte suivante :
  - Des règles sur les applications de confiance devront être créées pour autoriser quelques logiciels. Pour plus d'informations, reportez-vous à la section Configurer la protection contre les keyloggers.
- **Critique** : déconseillé, car génère des faux positifs.

### 5.3.5 Protection contre les débordements mémoire

C'est la protection qui protège le mieux le poste de travail. Nous vous recommandons de l'activer lorsque c'est possible. Il sera peut-être nécessaire de créer plusieurs règles sur les applications

de confiance. Pour plus d'informations, reportez-vous à la section Configurer la protection contre le débordement de mémoire.

### 5.3.6 Contrôle des événements kernel

Cette protection n'est possible que si les ordinateurs ont tous les mêmes pilotes (même hardware), et elle ne fonctionne que sur des systèmes Microsoft Windows 32 bits.

## 5.4 Configurer le contrôle du comportement des applications

### 5.4.1 Accès aux applications et Contrôle des exécutions

Ces protections nécessitent de créer un certain nombre de règles sur les applications de confiance (~300), elles sont donc déconseillées, sauf cas de très haute sécurité.

### 5.4.2 Contrôle des exécutions sur périphérique amovible

Cette protection est vivement conseillée si vous ne bloquez pas les clés USB.

L'utilisateur doit confirmer qu'un fichier exécutable peut être exécuté depuis un périphérique amovible et un log est alors généré. Il est ainsi possible de générer un rapport indiquant quelle application a été exécutée depuis un périphérique amovible et par quel utilisateur.

Les actions suivantes, par exemple, pourraient aussi déclencher des notifications :

- Si une clé USB en ReadyBoost est connectée, les Windows Update pourront lancer des *.exe* sur la clé,
- Les projecteurs Barco en USB demandent de lancer l'exécutable : *d:\clickshare for windows.exe*.

### 5.4.3 Accès au réseau et Accès aux fichiers

Ces protections nécessitent de créer un certain nombre de règles sur les applications de confiance, elles sont donc déconseillées, sauf cas de très haute sécurité.

# 6. Configurer la protection contre l'élévation de privilèges

Un grand nombre d'applications nécessitent une élévation de privilèges. C'est le cas de la majorité des programmes d'installation.

> **AVERTISSEMENT**
> L'application PowerShell n'a normalement pas besoin de l'élévation de privilèges pour fonctionner (cela dépend du script utilisé). Le fait d'autoriser l'élévation de privilèges à PowerShell permet à un grand nombre de logiciels malveillants de s'exécuter.

- Interdisez PowerShell ,
- Ou limitez PowerShell aux scripts signés par GPO,
- Ou limitez PowerShell aux scripts dans un répertoire spécial ou sur un serveur de fichiers.

# 7. Configurer la protection contre le débordement de mémoire

Les applications suivantes sont connues pour engendrer du débordement de mémoire, et il faut donc leur appliquer des règles de confiance. Pour savoir comment créer des règles de confiance dans le panneau **Contrôle applicatif**, consultez le *Guide d'administration* de SES.

- les applications Intel pour le Bluetooth :
  - c:\program files (x86)\intel\bluetooth\devmonsrv.exe
  - c:\program files (x86)\intel\bluetooth\mediasrv.exe
  - c:\program files (x86)\intel\bluetooth\obexsrv.exe
- le logiciel TeraCopy :
  - *\teracopy.exe
- la suite logicielle Cygwin :
  - c:\cygwin64*.exe
- Quelques antivirus peuvent également générer du débordement de mémoire : Symantec et Kaspersky par exemple.

Il est fortement recommandé de faire confiance à l'antivirus.

Nous vous recommandons de faire confiance aux autres applications uniquement si les applications ne fonctionnent pas avec SES en mode Normal.

Il ne faut jamais faire confiance aux navigateurs web Internet Explorer/Firefox/Chrome, ni aux applications Adobe. Si vous rencontrez un débordement de mémoire sur une de ces applications, c'est certainement qu'un virus vient d'être bloqué. Si ce n'est pas le cas, faites appel au Technical Assistance Center de SES.

# 8. Configurer la protection contre les keyloggers

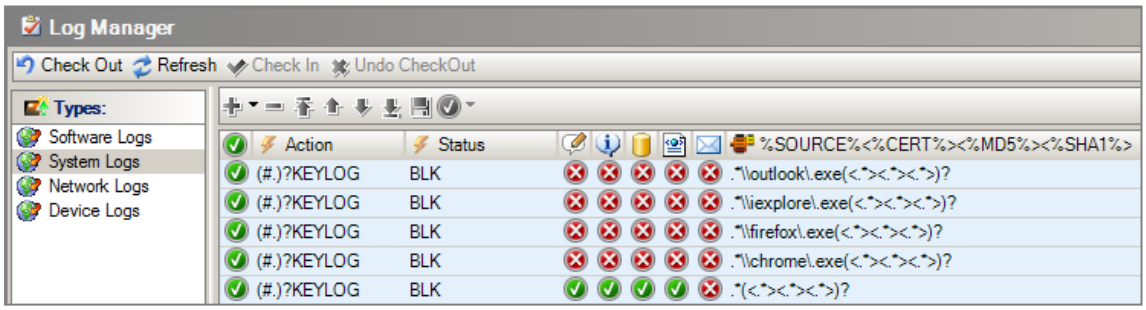
## 8.1 Supprimer les logs des faux positifs

Les applications Microsoft Office et les navigateurs web génèrent des événements de type keylogger, ce sont de faux positifs. Par exemple :

- c:\program files\microsoft office 15\root\office15\winword.exe
- c:\program files\microsoft office 15\root\office15\excel.exe
- c:\program files\microsoft office 15\root\office15\powerpnt.exe
- c:\program files\microsoft office 15\root\office15\onenote.exe
- *\clview.exe
- *\skype.exe
- *\Lync.exe
- c:\program files\internet explorer\iexplore.exe
- c:\program files (x86)\google\chrome\application\chrome.exe
- c:\program files (x86)\mozilla firefox\firefox.exe
- Windows live

Nous vous recommandons de ne pas faire confiance à ces applications. Dans le panneau **Configuration des logs**, vous pouvez masquer les logs correspondants à ces faux positifs. Ceci évitera les questions des utilisateurs car ils ne verront plus ces alertes.

Par exemple :




Nous vous recommandons de bien commenter ce type de paramétrage si plusieurs administrateurs ont accès à la console.

## 8.2 Autoriser les raccourcis clavier

Les raccourcis clavier sont les touches des ordinateurs portables qui permettent par exemple d'augmenter ou de réduire le volume sonore.

Par exemple pour des ordinateurs de la marque Dell, le programme suivant fait du keylogging :

- c:\program files\delltpad\apmsgfwd.exe

Pour les ordinateurs Hewlett Packard :

- c:\program files (x86)\hewlett-packard\hp mainstream keyboard\cnyhkey.exe
- c:\program files (x86)\hewlett-packard\hp mainstream keyboard\modledkey.exe

Nous vous recommandons de faire confiance à ces applications si vous faites confiance au fabricant du matériel. Il faut donc créer des règles de confiance dans le panneau **Contrôle applicatif**.

## 8.3 Autoriser les environnements virtuels

Les environnements virtuels (VMWare, Citrix, etc.) prennent le contrôle d'une machine virtuelle. Il est nécessaire de faire confiance à ce type d'application, par exemple :

- c:\program files (x86)\vmware\vmware workstation\x64\vmware-vmx.exe

## 8.4 Autoriser TeamViewer, DameWare, VNC, etc.

Les outils de prise de contrôle à distance font du keylogging, par exemple :

- c:\program files (x86)\teamviewer\teamviewer_desktop.exe
- c:\program files (x86)\teamviewer\tv_x64.exe
- c:\program files (x86)\teamviewer\tv_w32.exe

Il est obligatoire de faire confiance à ces applications si un utilisateur souhaite prendre le contrôle à distance d'un ordinateur. Selon la situation, ou pour certains besoins en sécurité, il peut être intéressant de bloquer ces applications.

## 8.5 Autoriser les outils de visioconférence

Les outils de visioconférence (Skype, WebEx, GoToMeeting) permettent de prendre le contrôle à distance des ordinateurs, par exemple :

- c:\program files\skype\phone\skype.exe

Nous vous recommandons de faire confiance à ces applications.

## 8.6 Autoriser Common Desktop Agent, et tous les autres logiciels

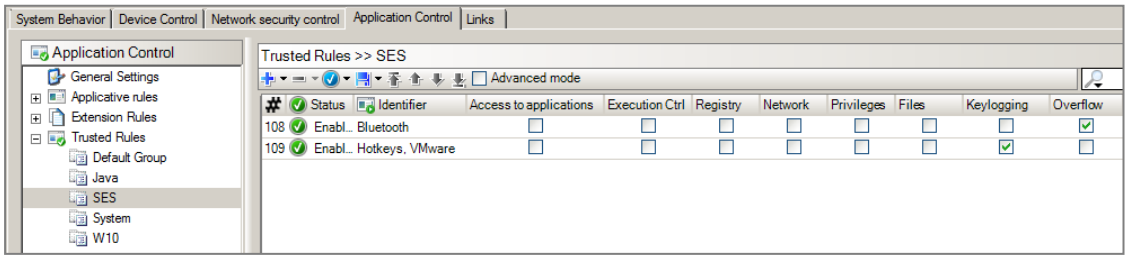
Si vous avez une imprimante Samsung par exemple, vous possédez le logiciel suivant :

- c:\program files\common files\common desktop agent\cdasrv.exe

Testez le logiciel avec SES en mode Normal. S'il ne fonctionne pas, créez une règle de confiance dans SES.

## 8.7 Résultat final attendu

La configuration de votre politique de sécurité devrait donc ressembler à la configuration suivante :



# 9. Autoriser et bloquer les extensions de fichiers

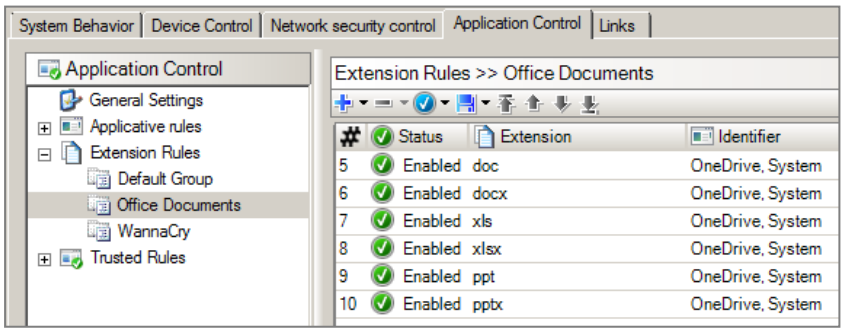
Si vous avez utilisé le modèle de base de la politique de sécurité :

- Ajoutez l'autorisation de l'antivirus pour l'extension *.pst* pour que l'antivirus puisse trouver les virus dans votre messagerie,
- Bloquez les extensions multimédia pour limiter la charge CPU des serveurs TSE.

Bloquez les extensions d'applications suivantes si possible :

| Extension | Usage |
|---|---|
| docm | Document à macros actives |
| dotm | Modèle à macros actives. Attention, utilisé par Outlook, Word, Excel, etc. Autoriser *normal.dotm* dans les règles applicatives, et bloquer **.dotm*. |
| hta | HTML Program Format |
| pif | Windows Program Information File for dos programs |
| pptm | Présentation à macros actives |
| potm | Modèle à macros actives |
| ppam | Complément à macros actives |
| ppsm | Diaporama à macros actives |
| sldm | Diapositive à macros actives |
| torrent | Fichiers torrent |
| vbe | Visual Basic Editor |
| vbs | Visual Basic Scripting. Attention, peut être utilisé par des scripts à l'ouverture de session Windows par exemple. Dans ce cas il faudra autoriser les scripts *vbs* dans les règles applicatives de *cscript.exe*, et bloquer **.vbs*. |
| xlsm | Classeur à macros actives |
| xltm | Modèle à macros actives |
| xlam | Complément à macros actives |
| wsf | Windows Script File |
| wsh | Windows Scripting Host |

Pour éviter qu'un processus anormal accède aux documents Microsoft Office, restreignez l'accès aux documents Office aux applications spécifiques, par exemple :




L'identifiant « System » correspond aux fichiers suivants :

| Type | Value | Description |
|---|---|---|
| Path / Certificate | c:\program files* | Program Files x64 |
| Path / Certificate | c:\program files (x86)* | Program Files x32 |
| Path / Certificate | c:\windows* | Windows |
| Path / Certificate | *\setup*.exe - Microsoft Corporation.cer (Microsoft Code Signing PCA) (Microsoft Code Signing PCA) (Microsoft Code (Microsoft Code Signing PCA) | Setup |

## 9.1 Résultat final attendu

La configuration de la protection des extensions dans votre politique de sécurité devrait donc ressembler à la configuration suivante :

Extension Rules >> Dangerous

| # | Status | Extension | Identifier | Log | Description |
|---|---|---|---|---|---|
| 11 | Enabled | hta | \|systemroot\|\explorer.exe | ____ | HTML Program Format |
| 12 | Enabled | vb | \|systemroot\|\explorer.exe | ____ | Visual Basic Scripting |
| 13 | Enabled | vbe | \|systemroot\|\explorer.exe | ____ | Visual Basic Editor |
| 14 | Enabled | vbs | \|systemroot\|\explorer.exe | ____ | Visual Basic Scripting |
| 15 | Enabled | wsf | \|systemroot\|\explorer.exe | ____ | Windows Script File |
| 16 | Enabled | wsh | \|systemroot\|\explorer.exe | ____ | Windows Scripting Host |
| 17 | Enabled | torrent | \|systemroot\|\explorer.exe | ____ | Torrent |
| 18 | Enabled | scr | \|systemroot\|\explorer.exe<br>\|systemroot\|\system32\rundll32.exe<br>Screensavers | ____ | Screensavers |
| 19 | Enabled | pif | \|systemroot\|\explorer.exe | ____ | Program Information File (for DOS programs) |
| 20 | Enabled | jse | \|systemroot\|\explorer.exe | ____ | JScript Encoded Script File |
| 21 | Enabled | msc | \|systemroot\|\explorer.exe<br>\|systemroot\|\system32\consent.exe<br>\|systemroot\|\system32\mmc.exe | ____ | Microsoft Management Console Snap-in Control File |

# 10. Bloquer les virus qui se propagent facilement

## 10.1 Bloquer les fichiers *exe* et *js* avec une extension trompeuse

Dans les stratégies de groupe Windows (GPO), nous vous recommandons de ne pas masquer les extensions connues.

Les virus peuvent en effet se dissimuler derrière des extensions doubles pour tromper l'utilisateur et ainsi se propager facilement. Par exemple :

- *.pdf.exe*
- *.pdf.js*
- *.pdf.rtf*

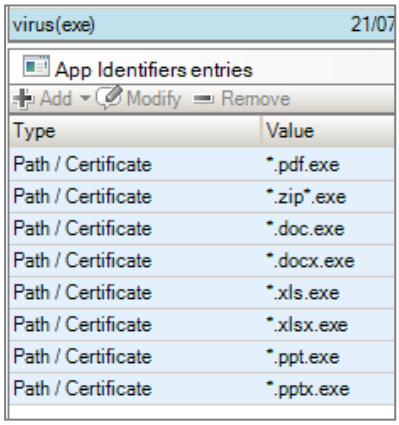
Pour bloquer cette possibilité, appliquez les recommandations suivantes.

### 10.1.1 Empêcher l'exécution de fichiers portant des extensions doubles se terminant par *.exe*

Pour empêcher l'exécution de fichiers portant une extension double *.xxx.exe* et pouvant contenir des virus, suivez la procédure suivante.

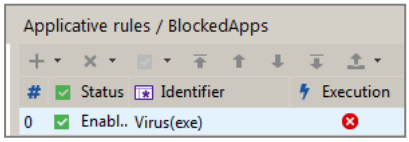
#### Identifiant d'application

Créez un identifiant d'application "Virus" regroupant les extensions trompeuses suivantes :




#### Règle applicative

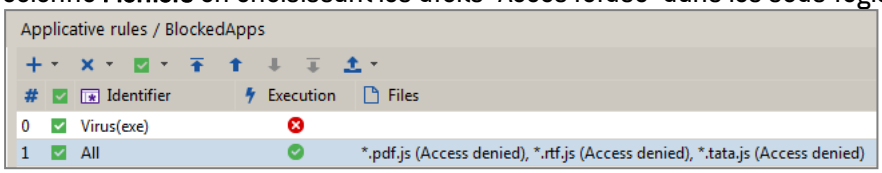
Interdisez l'exécution des identifiants précédemment créés :

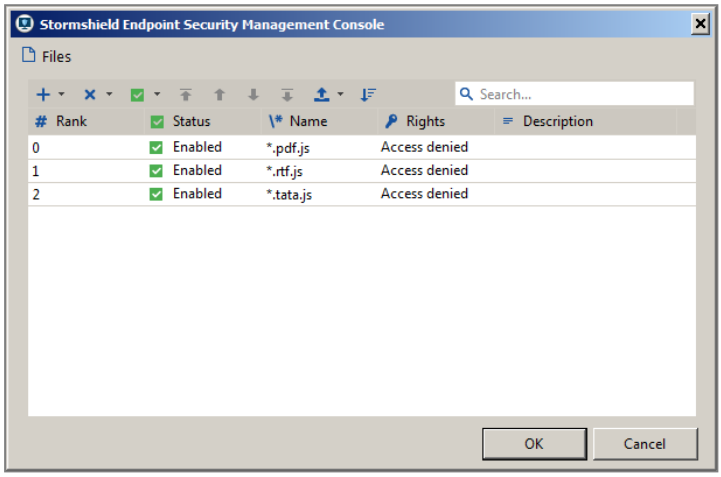



### 10.1.2 Empêcher la lecture de fichiers portant des extensions doubles se terminant par *.js*

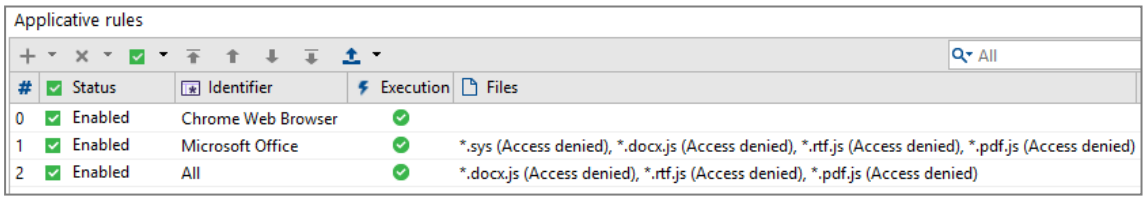
Pour empêcher la lecture ou l'activation de fichiers portant une extension double *.xxx.js* et pouvant contenir des virus, créez la règle applicative suivante :

1. Sélectionnez l'identifiant **All** et ajoutez les extensions doubles se terminant par *.js* dans la colonne **Fichiers** en choisissant les droits "Accès refusé" dans les sous-règles :




2. Si une règle précédant la règle **All** comporte déjà des sous-règles **Fichiers** spécifiques, vous devez ajouter les extensions doubles à bloquer dans cette règle également. Il ne suffit pas de spécifier ces extensions dans la règle **All** car l'agent arrête de parcourir les règles dès lors qu'il en trouve une qui correspond au processus en cours et qui possède des sous-règles **Fichiers** (qu'elles correspondent à la ressource visée ou non).




### 10.1.3 Empêcher la lecture de fichiers portant des extensions doubles se terminant par *.rtf*

Pour empêcher la lecture de fichiers portant des extensions doubles se terminant par *.rtf*, vous devez créer une règle applicative identique à la règle décrite ci-dessus pour les extensions *.js* ou compléter les sous-règles de cette même règle.

Cependant, lorsque WordPad ou toute autre application permettant la lecture de fichiers *.rtf* ne peut ouvrir un fichier de manière normale, il utilise les "noms courts" de Windows (ou noms de fichiers 8.3).

Par exemple le nom de fichier *file.pdf.rtf* devient *filepd~1.rtf*.

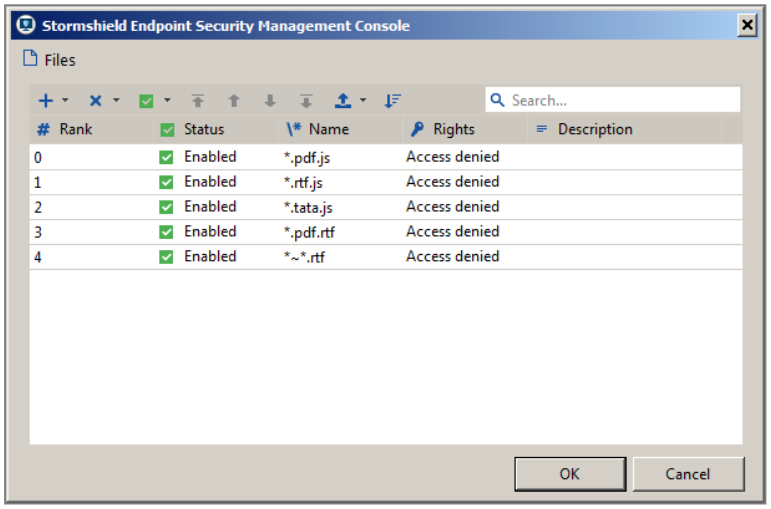
L'extension double est ainsi masquée par le nom court et la règle applicative n'est donc pas suffisante. Elle ne sera en effet pas appliquée puisque l'extension double ne sera pas reconnue.

Pour empêcher la lecture de ces types d'extensions doubles, vous devez donc :

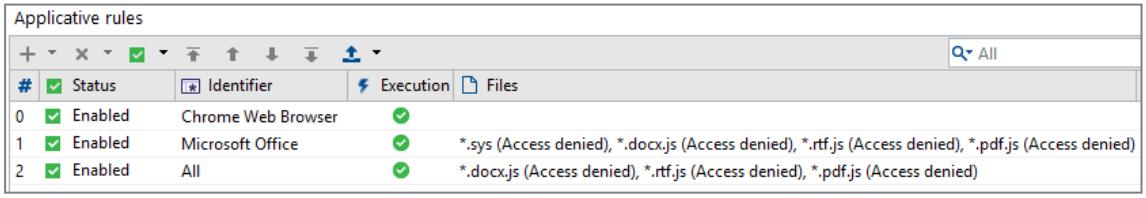
1. Créer une règle applicative identique à la règle décrite ci-dessus pour les extensions *.js*.
2. Désactiver la création de noms de fichiers 8.3 dans Windows à l'aide de la commande `fsutil.exe behavior set disable8dot3 1` à exécuter en ligne de commande en tant qu'administrateur.

Notez que cette commande désactive la création de noms 8.3 pour les nouveaux fichiers seulement. Elle n'efface pas les anciens noms et les fichiers existants ne seront donc pas bloqués.

Si vous n'avez pas la possibilité de désactiver la création de noms de fichiers 8.3 ou si vous souhaitez bloquer des fichiers qui existaient avant que la fonctionnalité ait été désactivée sur le poste de travail, vous devez ajouter une sous-règle fichier portant sur le nom *~*.rtf* dans la règle applicative :


3. Si une règle précédant la règle **All** comporte déjà des sous-règles **Fichiers** spécifiques, vous devez ajouter les extensions doubles à bloquer dans cette règle également. Il ne suffit pas de spécifier ces extensions dans la règle **All** car l'agent arrête de parcourir les règles dès lors qu'il en trouve une qui correspond au processus en cours et qui possède des sous-règles **Fichiers** (qu'elles correspondent à la ressource visée ou non).




## 10.2 Limiter les possibilités des scripts Windows

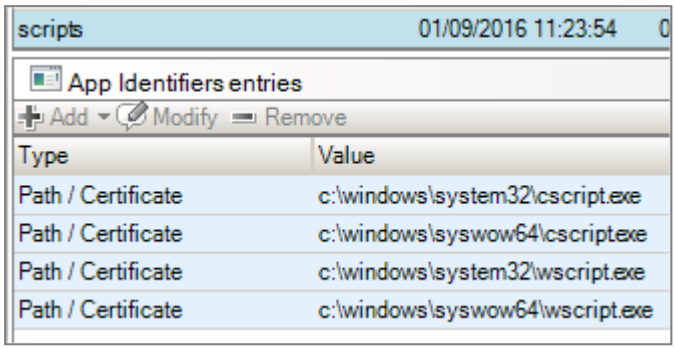
- *wscript.exe* lance les javascripts *js*, il ne doit pas créer des **.exe*.
- *cscript.exe* lance les vbscripts *vbs*, il ne doit pas créer des **.exe*.

On ne peut pas bloquer les fichiers *js* dans les extensions de fichiers, car cette extension est très largement utilisée par les sites web et donc par les navigateurs.

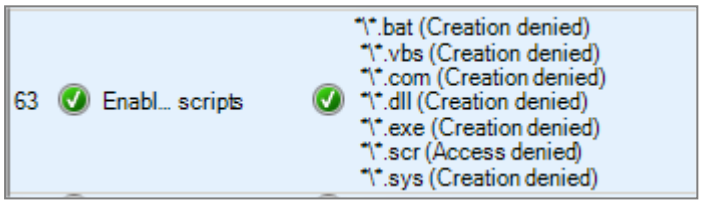
Dans un explorateur de fichiers, si on double clique sur un fichier *js*, il est ouvert par Wscript.

On peut bloquer les vbscripts avec la protection des extensions de fichier, mais le blocage de cscript permet de bloquer les scripts *vbs* qui auraient une extension autre que *vbs*.

### 10.2.1 Identifiant d'application




### 10.2.2 Règle applicative

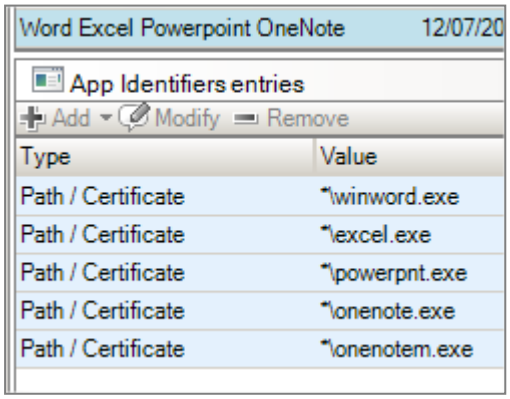


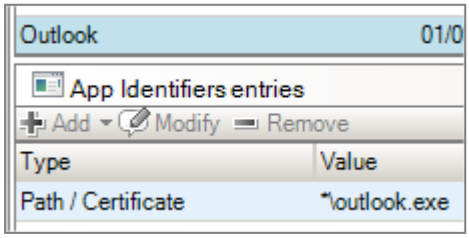

## 10.3 Limiter les possibilités des applications Microsoft Office

Les fichiers *.dotm* sont des modèles de document avec des macros. On ne peut pas bloquer les fichiers *.dotm* avec les règles d'extension car Microsoft Outlook et Word utilisent un fichier *.dotm* pour les modèles par défaut.

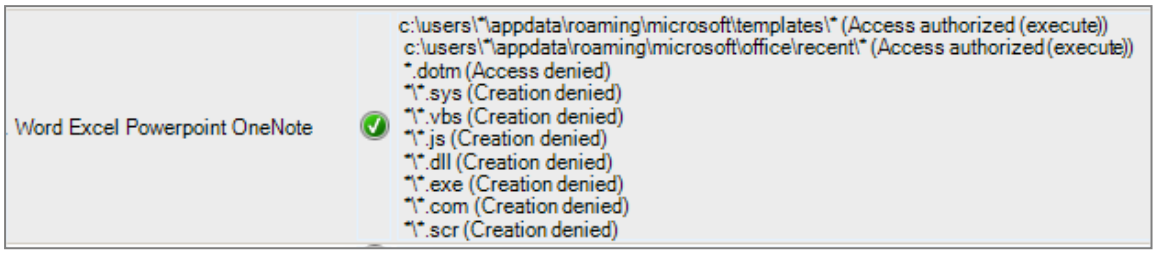
Il faut donc autoriser les fichiers *.dotm* utiles à Microsoft Outlook et Word et interdire les autres fichiers *.dotm*.

### 10.3.1 Identifiant d'application

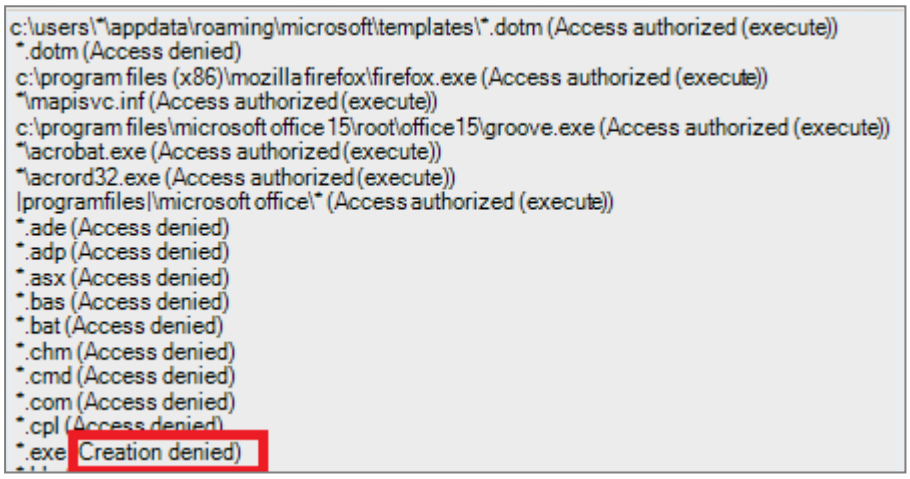


### 10.3.2 Règle applicative




Une règle applicative pour Microsoft Outlook existe déjà, mais on peut la modifier ainsi pour bloquer les fichiers *.dotm* malveillants :

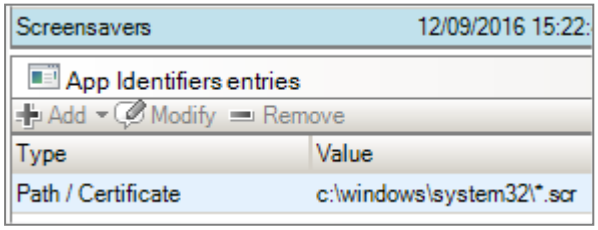



Si on sélectionne **Creation denied** pour l'extension **.exe* au lieu de **Access denied**, cela évite de créer un très grand nombre de règles.

## 10.4 Limiter les écrans de veille à ceux de Microsoft Windows

Beaucoup de virus se cachent dans les écrans de veille, nous vous recommandons donc de limiter les écrans de veille à ceux installés nativement par Microsoft.

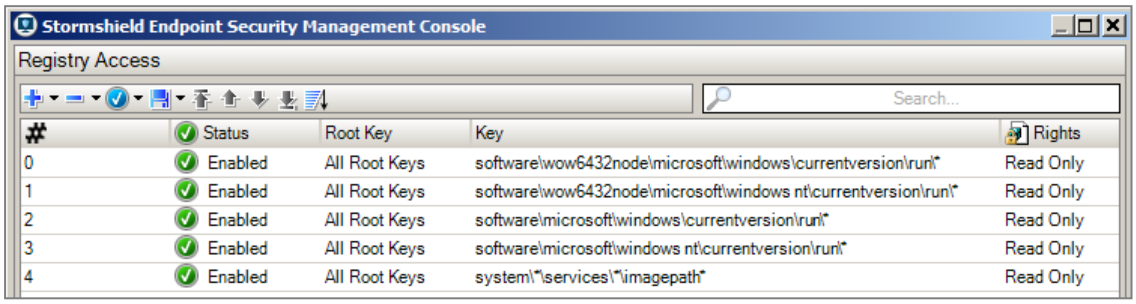
### 10.4.1 Identifiant d'application




### 10.4.2 Règle d'extension

# 11. Bloquer les malwares persistants

Les malwares s'enregistrent dans les clés de registre pour être relancés au prochain démarrage de Microsoft Windows. Pour éviter cela, vous devez interdire à tous les programmes (= « * ») d'écrire dans les clés de registre suivantes :




| # | Status | Root Key | Key | Rights |
|---|---|---|---|---|
| 0 | Enabled | All Root Keys | software\wow6432node\microsoft\windows\currentversion\run* | Read Only |
| 1 | Enabled | All Root Keys | software\wow6432node\microsoft\windows nt\currentversion\run* | Read Only |
| 2 | Enabled | All Root Keys | software\microsoft\windows\currentversion\run* | Read Only |
| 3 | Enabled | All Root Keys | software\microsoft\windows nt\currentversion\run* | Read Only |
| 4 | Enabled | All Root Keys | system*\services*\imagepath* | Read Only |

Vous devez ensuite faire confiance aux applications légitimes qui ont besoin d'être lancées au démarrage. Pour cela, il faut créer des règles de confiance pour ces applications et cocher la case correspondante dans la colonne **Registre**.

Vous pouvez par exemple faire confiance aux programmes suivants :

- c:\windows\servicing\trustedinstaller.exe
- c:\windows\system32\wermgr.exe
- c:\windows\system32\stikynot.exe
- c:\windows\system32\services.exe
- c:\program files\windows sidebar\sidebar.exe
- c:\program files (x86)\stormshield\stormshield endpoint security agent\srservice.exe
- c:\users*\appdata\local\microsoft\onedrive\onedrive.exe
- c:\program files (x86)\dropbox\client *\dropbox.exe
- c:\users*\appdata\roaming\zoom\bin\zoom.exe
- c:\program files (x86)\malwarebytes anti-malware\mbam.exe

# 12. Protéger la messagerie

Ci-dessous, une liste d'extensions utilisées par Microsoft Outlook :

Extension Rules

| # | Status | Extension | Identifier | Log | Description |
|---|---|---|---|---|---|
| 34 | Enabled | pst | "\outlook.exe<br>|systemroot|\explorer.exe | ____ | Microsoft Outlook Mail Database |
| 35 | Enabled | ost | "\outlook.exe<br>|systemroot|\explorer.exe | ____ | Microsoft Outlook Mail Database |

Des outils comme « nk2edit » permettent de collecter les adresses e-mail de vos correspondants Outlook. Cela signifie qu'un malware pourrait également le faire pour se propager à d'autres postes. Il faut donc interdire l'accès au répertoire suivant pour toutes les applications sauf Outlook :

| | | |
|---|---|---|
| Enabled | c:\users*\appdata\local\microsoft\outlook\roamcache* | Access denied |

Applicative rules >> Desktop tools

| # | Status | Identifier | Execution | Files |
|---|---|---|---|---|
| 2 | Enabled | Microsoft Office | ✓ | *.sys (Access denied)<br>*.vbs (Read only - RX (execution allowed))<br>*.js (Read only - RX (execution allowed))<br>*.dll (Read only - RX (execution allowed))<br>*.exe (Read only - RX (execution allowed))<br>*.com (Read only - RX (execution allowed))<br>*.scr (Read only - RX (execution allowed))<br>*.png (Read/write - RW (execution denied))<br>*.jpg (Read/write - RW (execution denied))<br>*.bmp (Read/write - RW (execution denied))<br>*.gif (Read/write - RW (execution denied)) |

# 13. Protéger ses mots de passe

Si vous stockez vos mots de passe dans un gestionnaire de mots de passe, vous pouvez protéger l'accès aux fichiers portant l'extension du gestionnaire avec une règle applicative. Par exemple, l'extension *kdbx* pour le logiciel KeePass.

# 14. Créer une liste blanche d'extensions

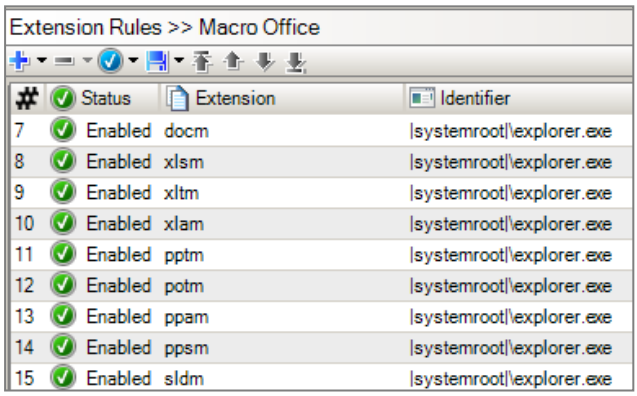
Les logiciels malveillants de type CryptoLocker fonctionnent avec les extensions de fichier. Voici une méthode pour protéger vos données.

## 14.1 Identifier les extensions utilisées

Par exemple *.doc*, *.docx*, *.xls*, *.xlsx*, *.ppt*, *.pptx*, *.dwg*, etc.

## 14.2 Créer des règles d'extensions dans les règles applicatives

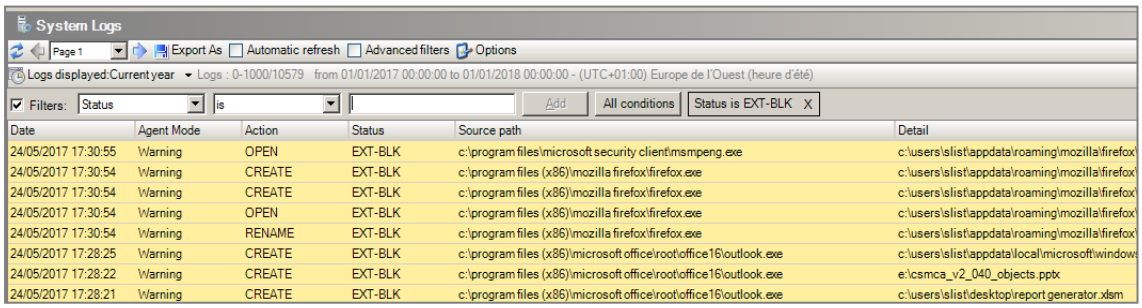
Testez les règles en mode **Warning** dans la **Configuration dynamique de l'agent** ou bien en mode **Test** sur les règles d'extensions elles-mêmes. Analysez ensuite les logs et améliorez les règles en fonction, avant de passer en mode **Normal**.




| # | Status | Extension | Identifier |
|---|---|---|---|
| 7 | Enabled | docm | |systemroot|\explorer.exe |
| 8 | Enabled | xlsm | |systemroot|\explorer.exe |
| 9 | Enabled | xltm | |systemroot|\explorer.exe |
| 10 | Enabled | xlam | |systemroot|\explorer.exe |
| 11 | Enabled | pptm | |systemroot|\explorer.exe |
| 12 | Enabled | potm | |systemroot|\explorer.exe |
| 13 | Enabled | ppam | |systemroot|\explorer.exe |
| 14 | Enabled | ppsm | |systemroot|\explorer.exe |
| 15 | Enabled | sldm | |systemroot|\explorer.exe |

## 14.3 Filtrer et exporter les logs Système

Filtrez les logs portant le status « EXT-BLK »




| Date | Agent Mode | Action | Status | Source path | Detail |
|---|---|---|---|---|---|
| 24/05/2017 17:30:55 | Warning | OPEN | EXT-BLK | c:\program files\microsoft security client\msmpeng.exe | c:\users\slist\appdata\roaming\mozilla\firefox |
| 24/05/2017 17:30:54 | Warning | CREATE | EXT-BLK | c:\program files (x86)\mozilla firefox\firefox.exe | c:\users\slist\appdata\roaming\mozilla\firefox |
| 24/05/2017 17:30:54 | Warning | CREATE | EXT-BLK | c:\program files (x86)\mozilla firefox\firefox.exe | c:\users\slist\appdata\roaming\mozilla\firefox |
| 24/05/2017 17:30:54 | Warning | OPEN | EXT-BLK | c:\program files (x86)\mozilla firefox\firefox.exe | c:\users\slist\appdata\roaming\mozilla\firefox |
| 24/05/2017 17:30:54 | Warning | RENAME | EXT-BLK | c:\program files (x86)\mozilla firefox\firefox.exe | c:\users\slist\appdata\roaming\mozilla\firefox |
| 24/05/2017 17:28:25 | Warning | CREATE | EXT-BLK | c:\program files (x86)\microsoft office\root\office16\outlook.exe | c:\users\slist\appdata\local\microsoft\windows |
| 24/05/2017 17:28:22 | Warning | CREATE | EXT-BLK | c:\program files (x86)\microsoft office\root\office16\outlook.exe | e:\csmca_v2_040_objects.pptx |
| 24/05/2017 17:28:21 | Warning | CREATE | EXT-BLK | c:\program files (x86)\microsoft office\root\office16\outlook.exe | c:\users\slist\desktop\report generator.xlsm |

Exportez les logs filtrés au format *.csv*. Pour avoir une politique plus précise, vous pouvez également effectuer l'opération extension par extension.

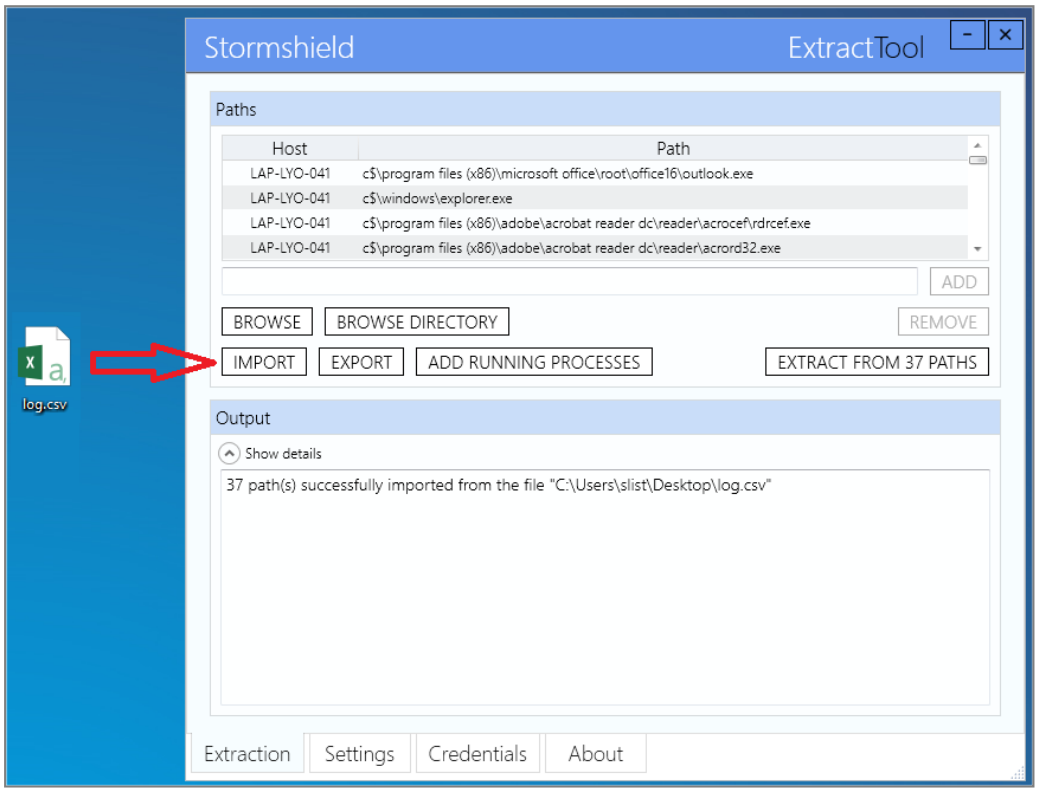
## 14.4 ExtractTool

Le logiciel ExtractTool permet de créer des hashes ou d'extraire des chemins de fichiers, ou bien d'extraire des certificats de signature de fichiers signés (signature embarquée ou provenant d'un catalogue de sécurité Microsoft). Vous pouvez ensuite importer les données extraites dans la console SES afin de créer des identifiants d'applications qui seront utilisés dans des politiques de sécurité pour protéger des applications en mode liste blanche ou liste noire.

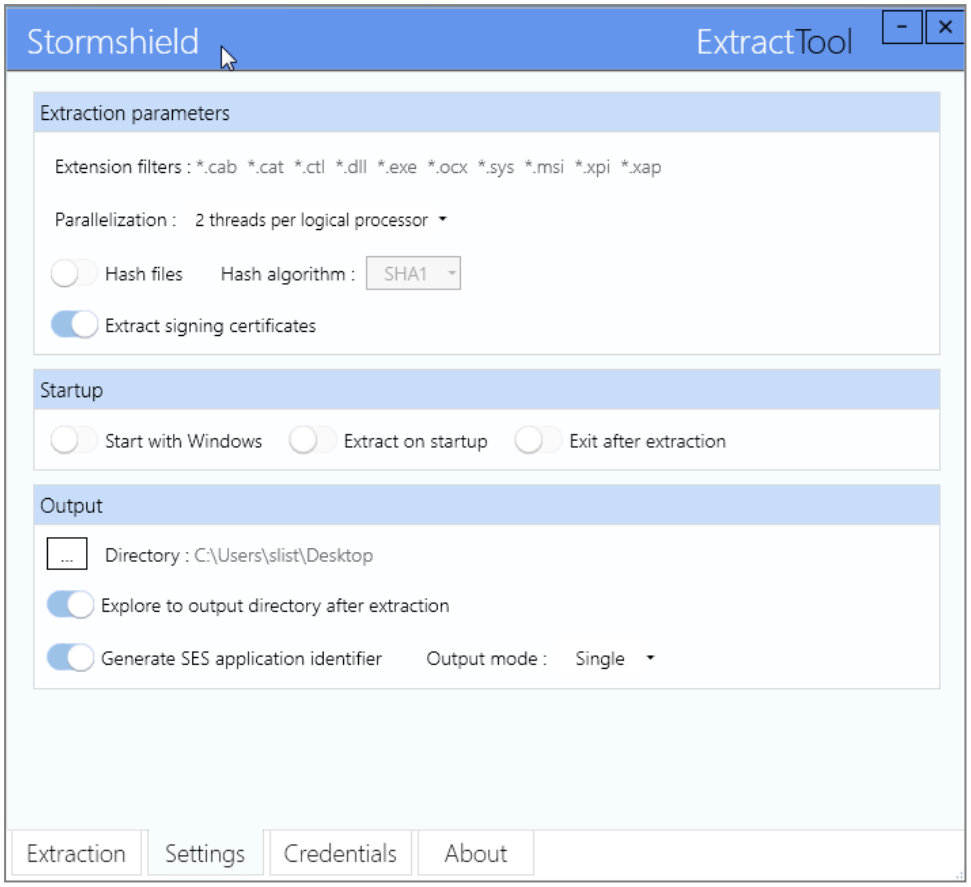
Pour obtenir le logiciel ExtractTool de Stormshield, adressez-vous à votre Ingénieur Avant-Vente Stormshield.

### 14.4.1 Importer les logs

A l'aide du logiciel ExtractTool, importez le fichier de logs au format *.csv* :




### 14.4.2 Paramétrer ExtractTool pour avoir un seul Identifiant




Lorsque la configuration est terminée, lancez l'extraction en cliquant sur **Extract from x PATHS**.

## 14.5 Importer le résultat dans la console SES

Effectuez les opérations suivantes dans l'ordre :

1. Importer les certificats dans la console SES,
2. Importer les identifiants d'application dans la console SES.

## 14.6 Autoriser les applications à accéder aux extensions

Ce nouvel identifiant doit pouvoir accéder à toutes les extensions définies dans la politique de sécurité.

# 15. Bloquer l'accès à Internet

Il est possible de bloquer l'accès Internet à toutes les applications (application = « * ») sauf quelques exceptions. Voici des exemples de ces exceptions pour les systèmes d'exploitation Windows 7, 8 et 10 64 bits :

## 15.1 Autoriser les mises à jour antivirus de Windows

- c:\program files\windows defender\mpcmdrun.exe

## 15.2 Autoriser les navigateur Web / FTP

- c:\program files (x86)\internet explorer\iexplore.exe (32 bits)
- c:\program files\internet explorer\iexplore.exe (64 bits)
- c:\program files (x86)\mozilla firefox\firefox.exe (32 bits)
- c:\program files\mozilla firefox\firefox.exe (64 bits)
- c:\program files (x86)\google\chrome\application\chrome.exe
- c:\program files\filezilla ftp client\filezilla.exe

## 15.3 Autoriser les visioconférences, prises de contrôle à distance

- c:\users*\appdata\local\citrix\gotomeeting*\g2mcomm.exe
- c:\program files (x86)\teamviewer\teamviewer.exe
- c:\programdata\webex\webex*\atmgr.exe

## 15.4 Autoriser les outils de synchronisation (si nécessaire)

- c:\program files (x86)\dropbox\client\dropbox.exe
- c:\program files (x86)\dropbox\update\dropboxupdate.exe

- c:\users*\appdata\local\microsoft\onedrive\onedrive.exe
- c:\users*\appdata\local\microsoft\onedrive*\onedrivestandaloneupdater.exe

- c:\program files (x86)\google\drive\googledrivesync.exe
- c:\program files\siber systems\goodsync\goodsync.exe

## 15.5 Bloquer si possible l'accès à Internet à la suite Microsoft Office

La suite Microsoft Office se connecte à Internet :

- Pour chercher les modèles de documents Office,
- Pour vérifier la licence,
- Pour chercher des virus avec des macros Word / Excel, etc.

Par mesure de sécurité, pour les grosses sociétés il est vivement conseillé d'installer un serveur de licence KMS (Key Management Service) Microsoft dans votre LAN, et d'interdire l'accès à Internet aux applications Microsoft Office.

- c:\program files\microsoft office 15\root\office15\winword.exe
- c:\program files\microsoft office 15\root\office15\excel.exe
- c:\program files\microsoft office 15\root\office15\powerpnt.exe
- c:\program files\microsoft office 15\root\office15\outlook.exe

## 15.6 Autoriser la solution Stormshield Data Security

Pour pouvoir télécharger les listes de révocation de certificats, la solution SDS doit pouvoir aller sur Internet :

- c:\program files\arkoon\security box\kernel\sbkrnl.exe

La solution SDS for Cloud and Mobility a également besoin d'accéder à Internet :

- c:\users*\appdata\local\stormshield\stormshield data security\datasecurity.exe

## 15.7 Autoriser les mises à jour des logiciels

Exemples :

- c:\program files\keepass password safe 2\keepass.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe

## 15.8 Interdire les dump mémoire Microsoft

L'application suivante envoie des dumps mémoire à Microsoft lorsque des applications s'arrêtent brutalement. Il ne faut pas lui autoriser l'accès à Internet :

- c:\windows\system32\wermgr.exe

# 16. Protéger le réseau

Vous devez paramétrer la sécurité de Microsoft Windows et des applications pour protéger votre réseau.

## 16.1 Ports 137/138 - NetBIOS

Un domaine Microsoft Windows avec un annuaire Active Directory en version 2008 ou supérieure peut se passer de NetBIOS. On peut donc bloquer les ports 137 et 138 pour toutes les applications « récentes ».

## 16.2 Port 1900 - Découvertes SSDP

Par défaut, sur Microsoft Windows 7, 8 et 10 le service de découvertes SSDP est actif.

Cela peut générer un grand nombre de logs réseau SES vers le port 1900.

Il est conseillé de désactiver ce service dans Microsoft Windows :

- Lancez *services.msc* et arrêtez le service **Découverte SSDP : SSDPSRV**.

Attention, sur Windows 8.1 et 10, le service Hôte de périphérique UPnP ne démarrera pas si le service de découvertes SSDP est désactivé.

## 16.3 Port 5355 - LLMNR

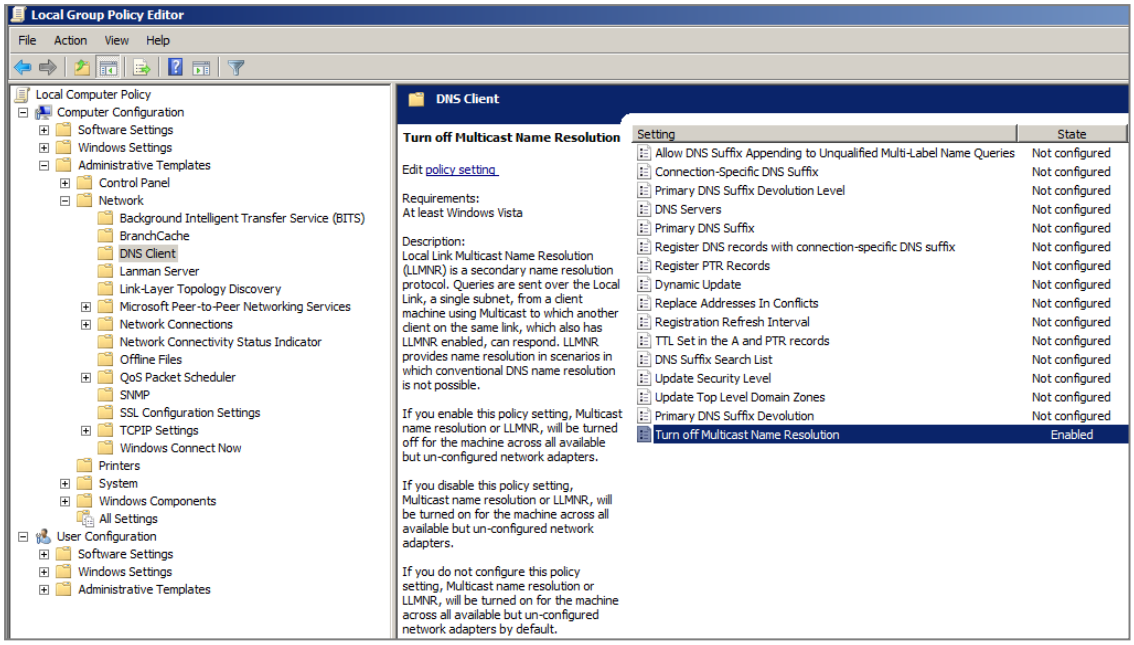
Le protocole LLMNR (Link-local Multicast Name Resolution) est basé sur le protocole DNS (Domain Name System). Il permet aux ordinateurs de résoudre des noms sur un même réseau local sans utiliser de serveur DNS central.

Sur Windows 7, 8 et 10, le service LLMNR est activé par défaut.

Cela peut générer un grand nombre de logs réseau SES vers le port 5355.

Nous vous recommandons de désactiver ce service dans Microsoft Windows :

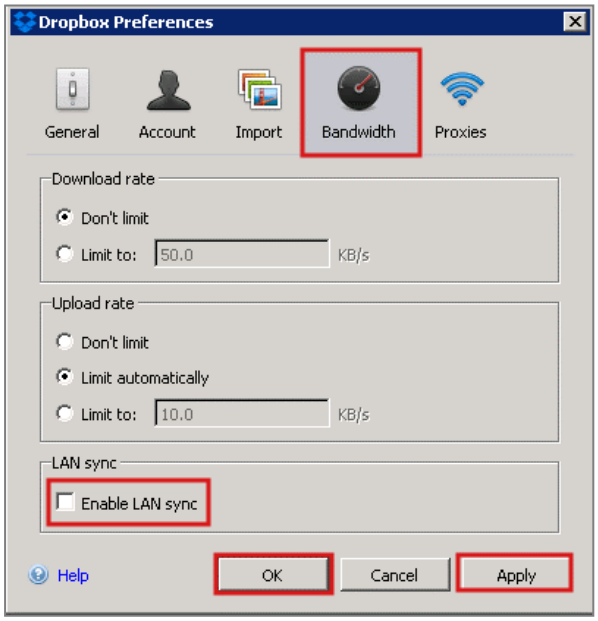
1. Entrez *gpedit.msc* dans le champ de recherche du menu **Démarrer** de Microsoft Windows pour ouvrir l'**Éditeur de stratégie de groupe locale**.
2. Dans l'arborescence, naviguez jusqu'au dossier **Configuration ordinateur** > **Modèles d'administration** > **Réseau** > **Client DNS**.
3. Dans les paramètres du dossier **Client DNS**, double-cliquez sur **Désactiver la résolution de noms multidiffusion** et sélectionnez l'option **Désactivé**.




## 16.4 Port 17500 - Dropbox LAN synchronization

Dropbox envoie des trames de synchronisation LAN sur le port 17500 vers l'adresse IP de broadcast.

Il est possible de désactiver la synchronisation dans le client Dropbox.




## 16.5 Port 5353 - Protocole Bonjour

Les systèmes et logiciels Apple (iTunes par exemple) utilisent le protocole Bonjour sur le port 5353.

Avec SES, il est possible de bloquer l'accès au réseau à l'application *mDNSResponder.exe*.

- Pour les systèmes 32 bits :

1. Ouvrez l'invite de commandes Microsoft Windows.
2. Tapez la commande `"%PROGRAMFILES%\Bonjour\mDNSResponder.exe" -remove` et validez.
3. Tapez la commande `regsvr32 /u "%PROGRAMFILES%\Bonjour\mdnsNSP.dll"` et validez.

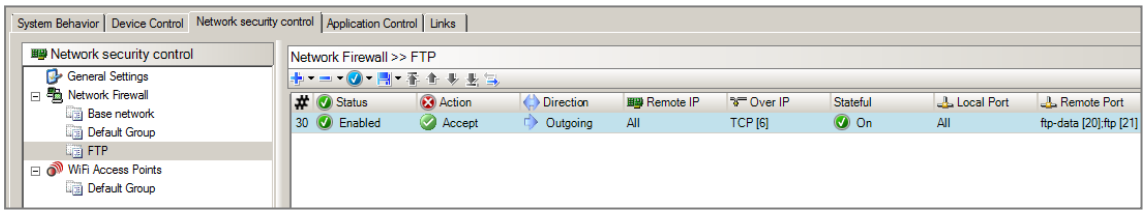
- Pour les systèmes 64 bits :

1. Ouvrez l'invite de commandes Microsoft Windows.
2. Tapez la commande `"C:\Program Files (x86)\Bonjour\mDNSResponder.exe" -remove` et validez.
3. Tapez la commande `regsvr32 /u "C:\Program Files (x86)\Bonjour\mdnsNSP.dll"` et validez.

Après avoir redémarré, vérifiez que tous vos programmes fonctionnent correctement et accèdent à Internet. Si tout fonctionne, vous pouvez renommer ou supprimer le dossier *Bonjour*.

## 16.6 Port 21 - FTP

Par défaut, le port 21 est bloqué dans les règles firewall. Il suffit de le débloquer. Attention, veillez à mettre la règle en tête des règles (#0) pour que la règle soit bien prise en compte.



# 17. Utiliser des scripts pour configurer une politique

Les scripts ci-dessous peuvent être utilisés dans SES. Ils permettent par exemple d'appliquer des politiques de sécurité différentes selon l'utilisateur local, l'heure, le fait que l'ordinateur soit portable, etc.

## 17.1 Détecter le groupe local

Ce script permet de savoir si l'utilisateur authentifié sur la session Windows fait partie d'un groupe local spécifique (passé en argument).

Voici un exemple de la commande à lancer si vous souhaitez interroger le groupe local "Administrateurs" :

```
cscript.exe c:\check_admin.vbs Administrateurs
```

```
If Wscript.Arguments.Count < 1 Then
       Wscript.Echo "Renseigner la commande et le groupe local, Ex : cscript.exe
c:\check_admin.vbs Administrateurs "
       Wscript.Quit(0) 'Quitte et renvoie la valeur "FAUX" à SES

End If

'=========================================================

GroupToMatch = Wscript.Arguments(0)
const separate    = "\"
strComputer = "."
'=========================================================

Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\"
& strComputer & "\root\cimv2")
Set colComputer   = objWMIService.ExecQuery("Select * from Win32_ComputerSystem")

Set colGroups = GetObject("WinNT://" & strComputer & "")
colGroups.Filter = Array("group")
'=========================================================

' Récupération du  CurrentUser
For   Each   objComputer   in   colComputer
       CurrentUserName   =   objComputer.UserName

Next
'=========================================================

For Each objGroup In colGroups
       For Each objUser in objGroup.Members
               If UCase (objGroup.name) = UCase (GroupToMatch)Then
                  If UCase (objUser.Name) = UCase ((Right (CurrentUserName, Len
(CurrentUserName) - Instr  (CurrentUserName, separate)))) then
               wscript.echo "L'utilisateur: " & (Right (CurrentUserName, Len
(CurrentUserName) - Instr  (CurrentUserName, separate))) & " est membre du
groupe: " & GroupToMatch
                        wscript.quit (1) 'Quitte et renvoie la valeur "VRAI" à SES
                  else

                   If UCase (objUser.Name) = UCase (CurrentUserName) then
                      wscript.echo "L'utilisateur: " & CurrentUserName & "

 fait partie du groupe: " & GroupToMatch
                        wscript.quit (1) 'Quitte et renvoie la valeur "VRAI" à SES
```

```
                        End if
                        end if
                End if
        Next

wscript.echo "L'utilisateur: " & CurrentUserName & " n'est pas membre du groupe "
& GroupToMatch & " ou ce groupe n'existe pas"
Next
wscript.quit (0) 'Quitte et renvoie la valeur "FAUX" à SES
```

## 17.2 Détecter l'heure

Ce script permet d'appliquer une politique selon les heures de travail ou de repos d'un utilisateur.

```
If  Hour  (Now ())>= 18 OR hour (Now ()) < 9 Then
    Wscript.echo hour (Now()), "Heure de repos"
    Wscript.quit (1)
Else
    Wscript.echo hour (Now ()), "Heure de travail"
    wscript.quit (0)
End If
```

## 17.3 Détecter la présence d'une batterie d'ordinateur portable

Ce script permet de savoir si SES est exécuté sur un ordinateur portable ou un ordinateur de bureau.

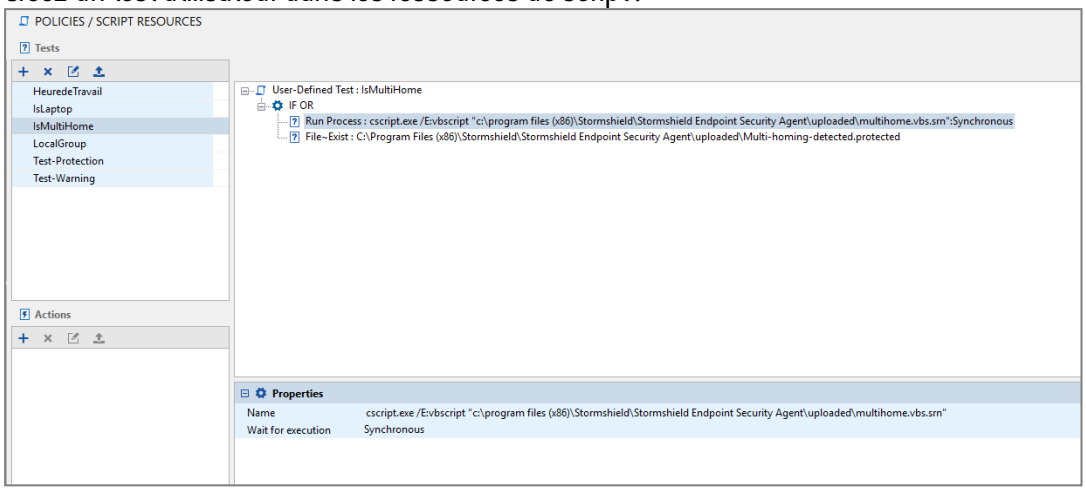
```
' Launch script with:
' wscript.exe //d //x has_a_battery.vbs

If   IsLaptop (".") Then
      WScript.Echo "Laptop"
       wscript.quit (1) 'return true to SES
Else
     WScript.Echo "Desktop or Server"
      wscript.quit (0) 'return false to SES
End   If


Function   IsLaptop (myComputer)
' This Function checks if a computer has a battery pack.
' One can assume that a computer with a battery pack is a laptop.
'
' Argument:
' myComputer [string] name of the computer to check,
       or "." for the local computer
' Return value:
' True if a battery is detected, otherwise False
   On   Error   Resume   Next
   Set   objWMIService = GetObject ("winmgmts://" & myComputer & "/root/cimv2")
   Set colItems = objWMIService.ExecQuery ("Select * from Win32_Battery" , , 48)
   IsLaptop = False
   For Each objItem in colItems
     IsLaptop = True
   Next
   If Err Then Err.Clear
   On Error Goto 0
 End Function
```

## 17.4 Détecter le multihoming

Ce script permet de savoir si l'ordinateur est connecté sur deux liens Internet simultanément. Si c'est le cas, ce script crée un fichier : *C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security Agent\uploaded\Multi-homing-detected.protected*.

Pour lancer le script déployé par SES :

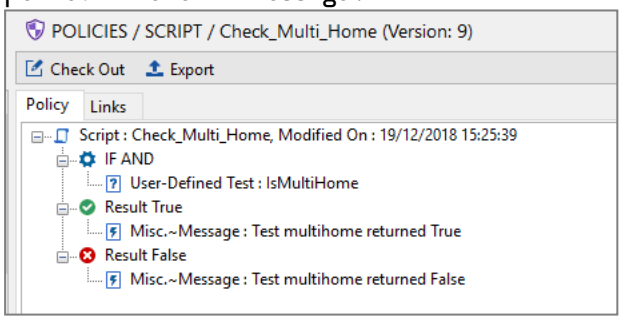
1. Créez un test utilisateur dans les ressources de script :




2. Indiquez la ligne de commande pour exécuter le script :

```
Cscript.exe /E:Vbscript "C:\Program Files (x86)\Stormshield\Stormshield Endpoint
Security Agent\uploaded\Multi-Homing-script.vbs.srn"
```

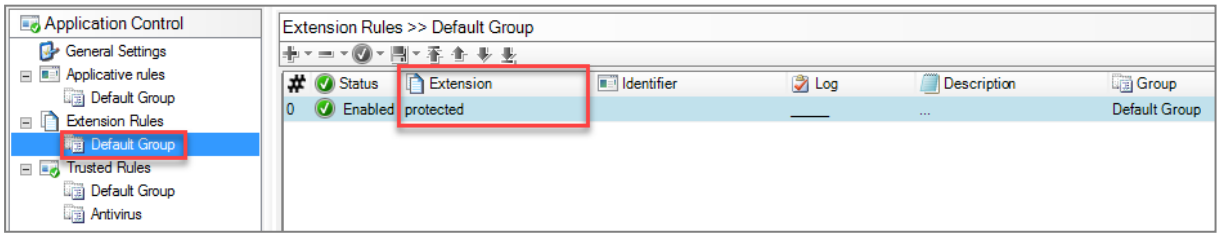
3. Si le script s'exécute sans erreur, il retournera la valeur 0=faux. Si le fichier existe, le script retournera 1=vrai. Le test **IF OR** retournera donc vrai.
4. Créez un script pour indiquer les actions à réaliser en fonction du résultat. L'exemple suivant permet d'afficher un message :



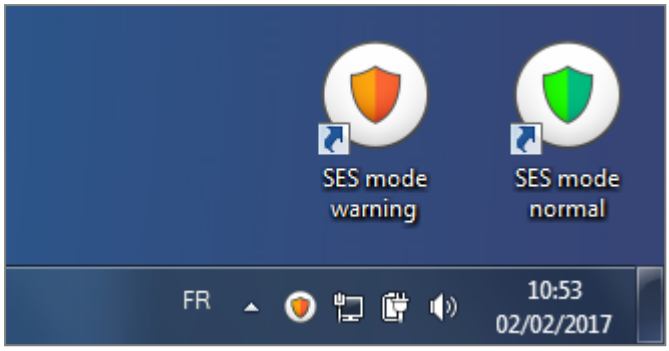

```
'Variables
'
vGatewayProtected = "C:\Program Files (x86)\Stormshield\Stormshield Endpoint
Security Agent\uploaded\Gateway.protected" 'Can be modified / adapted
vMultiHomingProtected = "C:\Program Files (x86)\Stormshield\Stormshield Endpoint
Security Agent\uploaded\Multi-Homing-Detected.protected" 'Can be modified /
adapted
'
'List default gateways
'
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\CIMV2")
Set colItems = objWMIService.ExecQuery("SELECT * FROM Win32_
NetworkAdapterConfiguration Where IPEnabled = True")
Set oFso = WScript.CreateObject("Scripting.FileSystemObject")
Set GatewayProtectedFile = oFso.CreateTextFile(vGatewayProtected, True)
'
For Each objItem In colItems
                strDefaultIPGateway = Join(objItem.DefaultIPGateway, ",")
                GatewayprotectedFile.WriteLine(strDefaultIPGateway)
Next
'
'Count the number of default gateway address in the Gateway.protected file
'
Const ForReading = 1
```

```
Set oReg = New RegExp
Set oFso = CreateObject("Scripting.FileSystemObject")
sData = oFso.OpenTextFile(vGatewayProtected, ForReading).ReadAll
 With oReg
                .Global = True
                .Pattern = "\r\n"
                lGatewayAddressNumber = .Execute(sData).Count
End With
'
GatewayprotectedFile.close
'
Set oFex = CreateObject("Scripting.FileSystemObject")
If lGatewayAddressNumber > 1 and oFex.FileExists(vMultiHomingProtected) then
                'If the file Gateway.protected already exists do nothing
Elseif lGatewayAddressNumber > 1 then
       'If the file Gateway.protected contains 2 or more default gateway addresses then
the file Multi-homing-detected.protected
       'is created. This value can be modified if a workstation needs more than 1
default gateway address
       Set MultiHomingProtectedFile = oFso.CreateTextFile(vMultiHomingProtected,True)
       Dim objShell1
       Set objShell1 = CreateObject ("WScript.Shell")
       objShell1.Run """c:\Program Files (x86)\Stormshield\Stormshield Endpoint
Security Agent\ssusrlog.exe"" -w MULTI_HOMING_ON ""multi homing
test"""
       'This command generates a log to inform the enduser and the administrator
Else
Set oFdo = CreateObject("Scripting.FileSystemObject")
If oFdo.FileExists(vMultiHomingProtected) Then
       oFdo.DeleteFile(vMultiHomingProtected)
       Dim objShell2
       Set objShell2 = CreateObject ("WScript.Shell")
       objShell2.Run """c:\Program Files (x86)\Stormshield\Stormshield Endpoint
Security Agent\ssusrlog.exe"" -i MULTI_HOMING_OFF
""multi homing test"""
       'This command generates a log to inform the enduser and the administrator
       End If
End If
'Removing the Gateway.protected file
Dim oFdo
Set oFdo = CreateObject ("Scripting.FileSystemObject")
oFdo.DeleteFile vGatewayProtected
Set oFso = Nothing
Set oFdo = Nothing
Set oReg = Nothing
WScript.Quit()
```

Le script ci-dessus utilise des fichiers portant l'extension "*protected*". On peut protéger ce type de fichier à l'aide d'une règle d'extension de fichier du type :



## 17.5 Changer de configuration en un clic




Ci-dessous, 2 scripts Autolt (https://www.autoitscript.com/site/autoit/ ) qui créent / effacent un fichier *c:\tmp\warning.txt* qui permet de changer la configuration de SES.

Il faut compiler ces scripts avec Autolt, et créer des raccourcis sur le bureau vers ces *.exe*.

### 17.5.1 Passer en mode normal

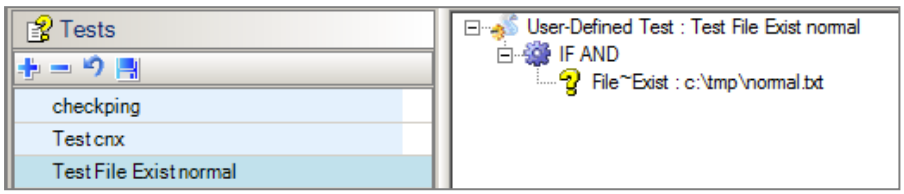
```
#include   <WinAPIFiles.au3>
#include   <MsgBoxConstants.au3>

;
; AutoIt Version: 3.0
; Language:       English
; Platform:       Win32/64
; Author:         John Doe
;

Local Const $sFilePath = "C:\tmp\normal.txt"
Local $hFileOpen = FileOpen ($sFilePath, $FO_OVERWRITE)
If   $hFileOpen = -1 Then
     MsgBox  ($MB_SYSTEMMODAL, "", "An error occurred when writing to disk.")
     Exit
EndIf
FileClose ($hFileOpen)
FileDelete ("c:\tmp\warning.txt")
Run ("C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security
Agent\ssmon.exe /reconnect")
```

### 17.5.2 Passer en mode warning

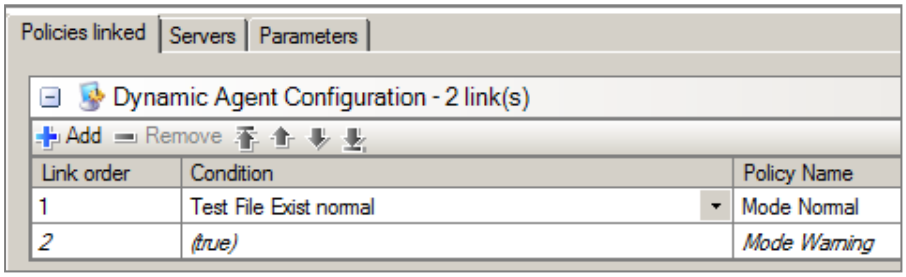
```
#include   <WinAPIFiles.au3>
#include   <MsgBoxConstants.au3>

;
; AutoIt Version: 3.0
; Language:       English
; Platform:       Win32/64
; Author:         John Doe
;

Local Const $sFilePath = "C:\tmp\warning.txt"
Local $hFileOpen = FileOpen ($sFilePath , $FO_OVERWRITE)
If $hFileOpen = -1 Then
    MsgBox  ($MB_SYSTEMMODAL, "", "An error occurred when writing to disk.")
    Exit
EndIf
FileClose  ($hFileOpen)
FileDelete ("c:\tmp\normal.txt")
```

```
Run ("C:\Program Files (x86)\Stormshield\Stormshield Endpoint Security
Agent\ssmon.exe /reconnect")
```

### 17.5.3 Créer le test de la présence du fichier




### 17.5.4 Configurer l'environnement SES

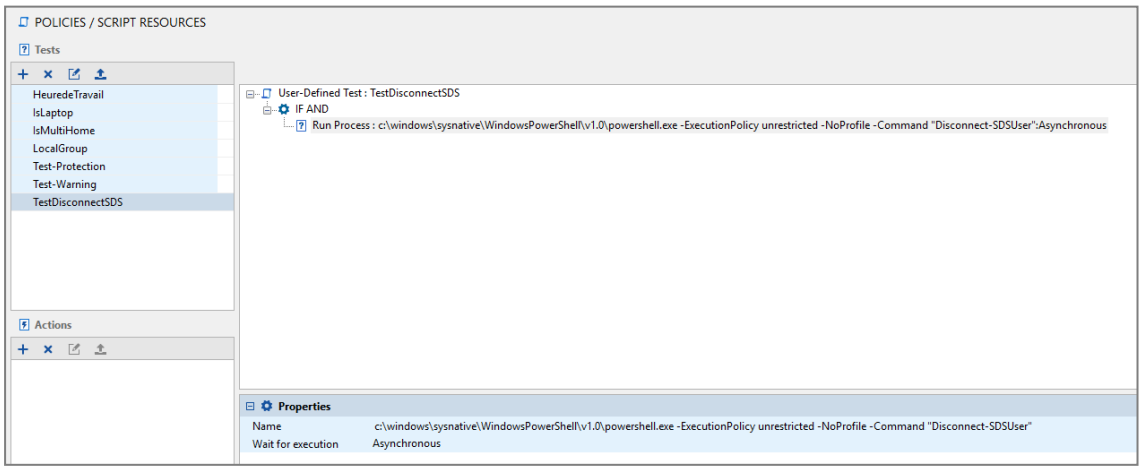



## 17.6 Déconnecter Stormshield Data Security Enterprise lors d'un événement SES de type débordement de mémoire

Si un débordement de mémoire est détecté par SES, on peut déconnecter la solution SDS Enterprise sur l'ordinateur pour éviter qu'un éventuel logiciel malveillant ne puisse accéder, par exemple, à un répertoire chiffré avec le module Stormshield Data Team de SDS. Le script se déclenche et déconnecte SDS lorsque SES détecte un débordement mémoire et génère un log.

### 17.6.1 Créer le test utilisateur qui déconnecte SDS

Ce test permet de lancer l'exécution du script.



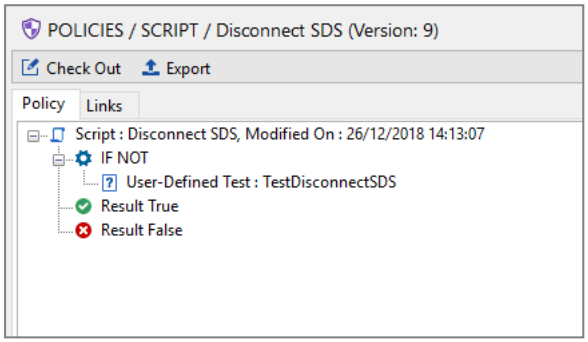

```
c:\windows\sysnative\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy
unrestricted -NoProfile -Command "Disconnect-SDSUser"
```

Indiquez le répertoire "sysnative" dans le chemin afin que le script fonctionne sur des systèmes 32 et 64 bits.

Choisissez **Asynchrone** dans le paramètre **Attente de l'exécution**.

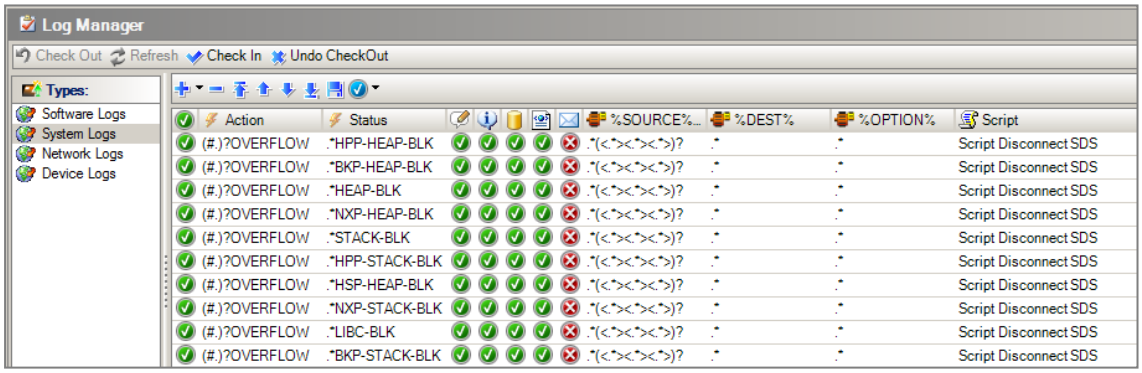
### 17.6.2 Créer le script qui déconnecte SDS

Intégrez le test utilisateur au script ci-dessous, qui sera déclenché lorsque l'événement de débordement mémoire sera détecté.




### 17.6.3 Paramétrer l'exécution du script sur événement

Dans la configuration des logs, il faut faire appel au script créé précédemment :




| Action | Status | %SOURCE%... | %DEST% | %OPTION% | Script |
|---|---|---|---|---|---|
| (#.)?OVERFLOW | .*HPP-HEAP-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*BKP-HEAP-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*HEAP-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*NXP-HEAP-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*STACK-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*HPP-STACK-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*HSP-HEAP-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*NXP-STACK-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*LIBC-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |
| (#.)?OVERFLOW | .*BKP-STACK-BLK | .*(<.*><.*><.*>)? | .* | .* | Script Disconnect SDS |

# 18. Analyser les logs

L'objectif de l'analyse des logs est de réduire le nombre de logs au maximum dans la console pour ne garder et recevoir que les logs les plus utiles.

## 18.1 Désactiver le rafraîchissement automatique

Désactivez le rafraîchissement automatique pour éviter que de nouvelles lignes viennent s'ajouter pendant le travail d'analyse des logs.

## 18.2 Choisir la période des logs à analyser

Nous vous recommandons d'analyser les logs à partir du lendemain du dernier changement de politique de sécurité. Consultez le panneau **Audit** pour connaître cette date.

## 18.3 Choisir les colonnes à afficher

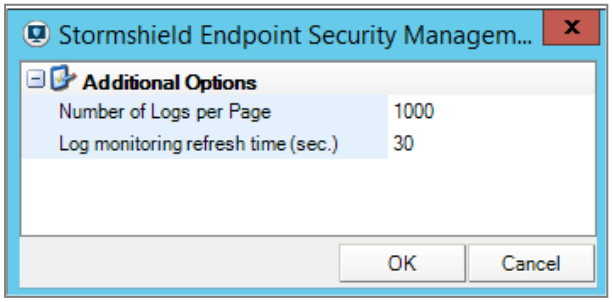
Les logs contenant beaucoup d'informations, nous vous recommandons de masquer les colonnes qui peuvent être inutiles selon les cas :

- Adresse IP
- Nom de machine
- Nom AD
- ID Agent
- Mode de l'agent (inutile si tous les ordinateurs sont dans le même mode Warning ou Normal)
- Description
- MD5 source
- SHA-1 source
- Émetteur source
- RID

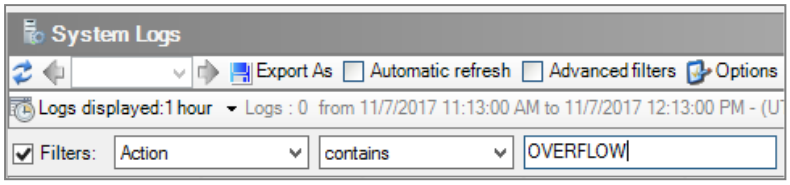
Les colonnes **Détail** et **Option** sont très importantes, elles indiquent entre autres les fichiers bloqués et les ports réseau bloqués.

## 18.4 Augmenter le nombre de logs par page dans les options

Par défaut, 100 logs s'affichent par page. Pour éviter un trop grand nombre de pages, passez ce paramètre à 1000 logs par page dans le menu **Options** des panneaux de surveillance des logs.

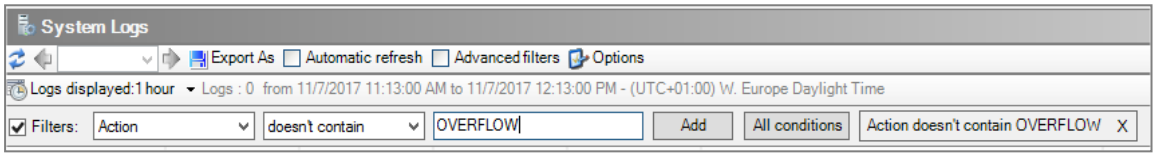


## 18.5 Analyser les logs de type Action=OVERFLOW

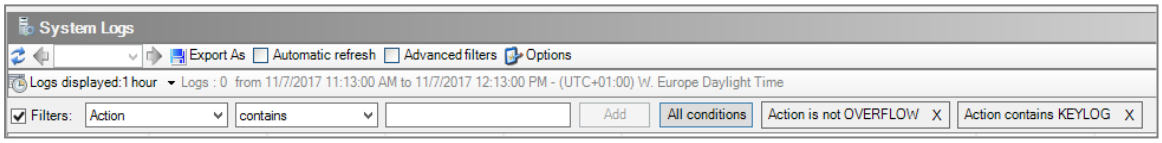



Par exemple les pilotes Intel Bluetooth sont connus pour faire du débordement de mémoire. Aucune autre application ne doit être de confiance dans SES. Si des débordements sont constatés dans les logs, ce sont des comportements qui ont été bloquées par SES.

A l'aide des filtres dans les logs, supprimez ce type de log de l'affichage.

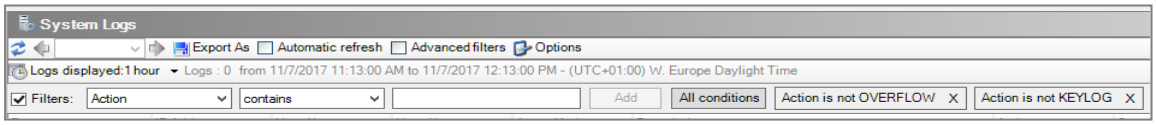



## 18.6 Analyser les logs de type Action=KEYLOG




Il peut être nécessaire d'ajouter des règles de confiance pour les raccourcis clavier, les logiciels de visioconférence, de prise de contrôle à distance Citrix/Remoteng, etc.

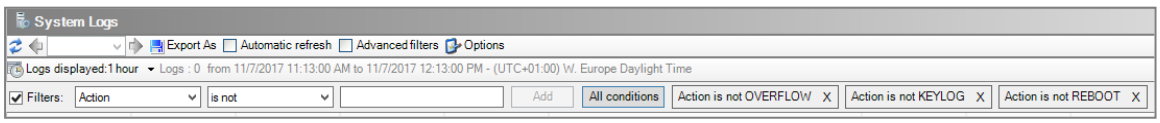
A l'aide des filtres dans les logs, supprimez ce type de log de l'affichage.




## 18.7 Analyser les logs de type Action=REBOOT

Les installeurs d'application, et les applications de déploiement de type SCCM par exemple sont des applications qui nécessitent les droits de redémarrage.

A l'aide des filtres dans les logs, supprimez ce type de log de l'affichage.




## 18.8 Analyser les logs de type Action=SU

Dans la colonne **Détail**, vous pouvez voir la nature de l'élévation de privilège, par exemple SE_LOAD_DRIVER_PRIVILEGE. Si besoin, ajoutez une règle de confiance pour l'application concernée par le log.

A l'aide des filtres dans les logs, supprimez ce type de log de l'affichage.

## 18.9 Analyser les logs de type Action=SOCK-CONNECT

Ce type de log correspond aux applications qui se connectent vers une adresse IP (connexion sortante).

Dans la colonne **Détail**, vous pouvez voir l'adresse IP de destination.

Dans le colonne **Option**, vous pouvez voir le port de destination.

Supprimez tous les logs avec les options à 137/138 qui correspondent au port NetBIOS.

A l'aide des filtres dans les logs, supprimez ce type de log de l'affichage.

## 18.10 Analyser les logs de type Action=SOCK-ACCEPT

Ce type de log correspond aux applications qui acceptent une connexion entrante.

Dans la colonne **Détail**, vous pouvez voir l'adresse IP source.

Dans le colonne **Option**, vous pouvez voir le port.

Supprimez tous les logs avec les options à 137/138 qui correspondent au port NetBIOS.

A l'aide des filtres dans les logs, supprimez ce type de log de l'affichage.

## 18.11 Analyser les logs de type Statut=EXT-BLK

Ce type de log correspond aux tentatives d'accès à des fichiers avec une extension particulière.

Supprimez les logs qui correspondent aux programmes de Windows non essentiels comme :

- c:\windows\system32\searchprotocolhost.exe
- c:\windows\syswow64\searchprotocolhost.exe
- c:\windows\system32\compattelrunner.exe

## 18.12 Analyser le reste des logs

S'il reste moins de 1000 logs, ils sont affichés à l'écran. Les dernières lignes de logs ne doivent pas être négligées, elles mettent souvent en évidence les problèmes.

**ASTUCE**
Dans les règles applicatives, les numéros de version des logiciels peuvent être remplacés par « * », ainsi les règles seront encore valables pour les versions suivantes.

# 19. Purger les logs

## 19.1 Choisir la durée de rétention des logs

La durée de rétention des logs peut être limitée par la taille du disque dur, la limite de taille de la base (10 Go pour SQL Express), mais également par la date. Dans l'exemple ci-dessous les logs de plus de 12 mois sont purgés toutes les nuits.

## 19.2 Créer un script SQL sur le serveur

```
USE Stormshield
DELETE FROM dbo.db_SoftwareLog
WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())
DELETE FROM dbo.db_SystemLog
WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())
DELETE FROM dbo.db_NetworkLog
WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())
DELETE FROM dbo.db_MediaLog
WHERE (ltimestamp + (60*60*24*30*12)) < DATEDIFF(second, CONVERT (Datetime,
'1970-01-01', 20), getUtcdate())
```

## 19.3 Créer un script bat sur le serveur qui appelle le script SQL

Attention au chemin, le répertoire peut être 90, 100, 110… selon la version de SQL.

```
@echo off
REM Utilise le compte SA pour se connecter (nécessite de mettre le mot de passe
en clair dans les batchs)
REM Méthode déconseillée.
@echo on
"C:\Program Files\Microsoft SQL Server\100\Tools\Binn\sqlcmd.exe" -S
127.0.0.1\Stormshield,1433 -U SA -P P@ssw0rd -i
c:\data\stormshield\purgelogssql.sql
@echo off
REM Utilise les droits du compte qui exécute le batch (nécessite un compte admin)
REM Méthode conseillée.
@echo on
"C:\Program Files\Microsoft SQL Server\90\Tools\Binn\sqlcmd.exe" /E -S
127.0.0.1\Stormshield,1433 -i c:\data\stormshield\purgelogssql.sql
```

## 19.4 Créer une tache planifiée

Créez une tache planifiée qui lance le script *bat* toutes les nuits. Attention à utiliser un utilisateur qui possède les droits d'accès aux bases de données SQL de SES.

STORMSHIELD

documentation@stormshield.eu