Distribution EOLE - Tâche #21062

Scénario # 21299 (Terminé (Sprint)): Assistance aux utilisateurs (40-42)

client scribe et gestion du firewall windows

20/07/2017 10:11 - équipe eole Academie d'Orléans-Tours

Statut:	Fermé	**Début:**	20/07/2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Fabrice Barconnière	**% réalisé:**	100%
Version cible:	sprint 2017 40-42 Equipe MENSR	**Temps estimé:**	3.00 heures
		Temps passé:	4.00 heures

Description

Bonjour,

Nous avons dans le cadre d'un déploiement en partenariat avec une collectivité le besoin d'autoriser dans le FW windows des postes du domaines le lancement d'un exe qui est sur le réseau (partage dédié via lecteur réseau ou dossier dans "script" de netlogon , peut importe).

Hors de ce que j'ai pu testé sur ma maquette 2.5, et avec des PC en W7 et W10, que l'on lance cet exe depuis le netogon ou depuis un lecteur réseau, le FW windows voit toujours le chemin de l'appli à autoriser en "\\scribe\mon\chemin\prog.exe"

Je n'ai donc pas le choix de créer une règle dans liste_fwregles.eol du type :

```
Vista:: "test" ;; proto = "udp" ;; program="\\scribe\mon\chemin\prog.exe" ;; action = "allow"
```

Cette ligne ne fait aucune création dans le FW windows.

Alors que celle-ci est ok :

```
Vista:: "test" ;; proto = "udp" ;; program="P:\mon\chemin\prog.exe" ;; action = "allow"
```

Mais elle ne sert a rien car windows ne voit pas ce chemin la comme dit ci-dessus. On peut créer à la main sans soucis la règle dont j'ai besoin, mais pas via le client scribe. Du coup je suppose qu'il y a un bug avec les chemin commençant par "\\" ?

Par ailleurs http://eole.ac-dijon.fr/documentations/2.5/completes/beta/ModuleScribe/co/06-Parefeu_config.html ne parle pas de l'option program ?

L'échéance de notre déploiement est courant septembre, donc si vous pouvez nous donner des pistes de solution fin d'été, ça serait idéal :-)

Merci,

Nicolas

Historique

#1 - 01/09/2017 17:52 - Emmanuel GARETTE

- Tracker changé de Demande à Tâche

- Statut changé de Nouveau à En cours

- Assigné à mis à Emmanuel GARETTE

- % réalisé changé de 0 à 20

- Temps estimé mis à 3.00 h

- Tâche parente mis à #21131

- Restant à faire (heures) mis à 3.0

En parcourant le code j'ai l'impression que le problème vient de l'utilisation de "strip" :

```
>>> i="\\scribe\mon\chemin\prog.exe"
>>> print i.strip()
\scribe\mon\chemin\prog.exe
```

pourriez-vous tester avec \\\scribe\mon\chemin\prog.exe ?

En effet :

```
>>> i="\\\scribe\mon\chemin\prog.exe"
>>> print i.strip()
\\scribe\mon\chemin\prog.exe
```

Pourriez-vous décrire plus les tests que vous réalisez pour que je puisse reproduire ?

#2 - 05/09/2017 16:45 - équipe eole Academie d'Orléans-Tours

- Fichier Capture.JPG ajouté

J'ai testé ta proposition et ai actuellement :

gen_patch
CreoleCat -t liste_fwregles.eol
root@scribemaq118:~# tail /home/client_scribe/liste_fwregles.eol

```
Vista:: "Utilisateur" ;; proto = "any" ;; program="%EOLEPATH%\cliscribe\utilisateur.exe" ;; ip_src = me ;; ip_
dst = any ;; action = "allow"
Vista:: "NuWinC" ;; proto = "any" ;; program="%EOLEPATH%\NuWINc\nuwinc.exe" ;; action = "allow"
Vista:: "GestionPostes" ;; proto = "any" ;; program="P:\gestion-postes\gestion-postes.exe" ;; action = "allow"


# NuWINc
WinNT|Win2K|WinXP|Vista:: "NuWINc" ;; proto = "tcp" ;; ip_src = "me" ;; ip_dst = "any" ;; port_dst = "4129" ;;
 action = "allow"

#Alarme du CD45 : il faut autoriser le programme a utiliser le reseau
Vista:: "alarmeCD45" ;; proto = "udp" ;; program="\\\scribe\professeurs\alarme\cgalarme.exe" ;; action = "allo
w"
```

root@scribemaq118:~# md5sum /home/client_scribe/liste_fwregles.eol > /home/client_scribe/liste_fwregles.eol.MD5SUM
more /home/netlogon/adminVista.txt

```
cmd,\\10.118.99.187\netlogon\scripts\trend.bat,HIDDEN,NOWAIT
cmd,\\10.118.99.187\netlogon\scripts\ocs-windows.bat,HIDDEN,NOWAIT
cmd,\\10.118.99.187\netlogon\infosquota\infosquota.exe
lecteur,P:,\\scribe\professeurs
lecteur,R:,\\scribe\icones$
lecteur,S:,\\scribe\groupes
lecteur,T:,\\scribe\commun
lecteur,I:,\\scribe\scan
cmd,P:\alarme\cgalarme.exe,NOWAIT
```

Et pourtant, mon poste me demande toujours (en PJ) l'autorisation du programme.
La règle apparait bien dans le FW windows si j'ai un truc du genre "P:\mon progr" mais ne sert à rien (CF l'explication de départ et la PJ qui montre le chemin que windows voit)

Pour le contexte, la collectivité c'est engagée à déployer une solution "d'alarme silencieuse" pour les risques d'attentat. Ils sont partit sur une solution via les postes prof et administratif.

Dispo sur l'irc (nicobzh) si besoin.

Nicolas

#3 - 11/09/2017 10:06 - Emmanuel GARETTE

Si vous placer la commande à la main : netsh advfirewall firewall add rule name="alarmeCD45" action=allow proto="udp" program="\\scribe\professeurs\alarme\cgalarme.exe"

Est-ce que cela fonctionne ?

#4 - 11/09/2017 10:17 - Scrum Master

- Tâche parente changé de #21131 à #21164

#5 - 11/09/2017 11:12 - équipe eole Academie d'Orléans-Tours

Il manque "dir=in" ;-)

mais sinon

```
netsh advfirewall firewall add rule name="alarmeCD45" action=allow proto="udp" program="\\scribe\professeurs\a
larme\cgalarme.exe" dir=in
```

Fonctionne sur mon W7.

La proposition de Joël sur IRC

```
jojo2024: gnunux, nrobin : pour https://dev-eole.ac-dijon.fr/issues/21062 vous avez fait des essais avec 4 bar
res obliques invers?es ?
```

Ne change rien (idem avec 3), cela ne créer pas la règle.

#6 - 28/09/2017 17:27 - Joël Cuissinat

- Statut changé de En cours à Nouveau

- Assigné à Emmanuel GARETTE supprimé

- Tâche parente changé de #21164 à #21299

<gnunux> jojo2024, moi je ne sais pas reproduire ...
<gnunux> si quelqu'un sait me dire comment reproduire je veux bien regarder
<jojo2024> Je reporte la demande sur le prochain sprint mais ce sera la dernière fois !

#7 - 28/09/2017 18:06 - équipe eole Academie d'Orléans-Tours

Bonjour,

Le problème étant dans la création de la règle, il n'y a besoin que d'un PC W7 pour tester, sur n'importe quelle url bidon. Qu'il n'y ait pas d'exe en face ne change rien et n'empeche pas la reproduction du problème...

La règle dans le FW windows n'est pas créé à l'heure actuelle dès lors qu'elle commence par "\\" dans /home/client_scribe/liste_fwregles.eol
Ce qui ne gêne en rien la commande "standard" nesh.

Merci de votre aide, et je reste dispo sur l'irc si besoin.

Nicolas

#8 - 16/10/2017 08:39 - Fabrice Barconnière

- % réalisé changé de 20 à 100

- Restant à faire (heures) changé de 3.0 à 0.5

Testé sur Scribe 2.5.2 : la règle est bien créée.
Avec la commande netsh, la règle est créée immédiatement.
Avec le client Scribe, il faut que ce service soit relancé le le PC pour que la création de la règle se fasse. Une fermeture de session ne suffit pas.

Il faut soit un reboot, soit relancer le service **Service Scribe** via la console **services.msc** du PC.

#9 - 16/10/2017 08:39 - Fabrice Barconnière

- Statut changé de Nouveau à En cours

- Assigné à mis à Fabrice Barconnière

#10 - 16/10/2017 16:49 - équipe eole Academie d'Orléans-Tours

Ah...En effet, avec relance, ça fonctionne sans problème de "\"...
Je n'y avait pas du tout pensé, et les VM de tests ne sont jamais éteintes.

Du coup signalement inutile, à fermer !

Merci Fabrice.

#11 - 17/10/2017 08:17 - Fabrice Barconnière

- Projet changé de eole-client à Distribution EOLE

- Statut changé de En cours à Fermé

- Restant à faire (heures) changé de 0.5 à 0.0

#12 - 18/10/2017 10:00 - Fabrice Barconnière

Modification de la documentation :

- /2_5/modules/Scribe/50-Scribe/02_clients_Windows/02_clients_scribe_administration/06_Administration_avancee/06-Parefeu_config.scen
- /2_6/modules/Scribe/50-Scribe/02_clients_Windows/02_clients_scribe_administration/06_Administration_avancee/06-Parefeu_config.scen

Fichiers

Capture.JPG	97,4 ko	05/09/2017	équipe eole Academie d'Orléans-Tours