AbulÉdu - Task - Tâche #925

Proposer ClamWin+Sentinel comme antivirus windows via webadmin (était : MoonSecure)

26/11/2010 23:32 - Eric Seigne

Statut:	Fixed - Corrigé - Implémenté	**Début:**	26/11/2010
Priorité:	Paquets	**Echéance:**	
Assigné à:	Stéphane Hays	**% réalisé:**	100%
Catégorie:	Clients windows	**Temps estimé:**	8.00 heures
Version cible:	AbulÉdu - Serveur - 11.08		

Description

Il serait intéressant (sur proposition de F.A) d'avoir cet antivirus libre dans la liste des applications complémentaires disponibles sur webadmin. Je ne propose pas de l'installer d'office pour éviter les conflits qui existent dès que plusieurs anti-virus sont installés sur un windows.

Source: http://www.moonsecure.com/index.php?option=com_content&task=view&id=30&Itemid=66

Historique

#1 - 12/12/2010 17:10 - Eric Seigne

- Statut changé de Assigned - En cours à Pending - En attente

- Priorité changé de Normale à Paquets

- % réalisé changé de 10 à 90

Bonjour,
le paquet est disponible (enfin, il est en cours d'upload) ... il reste à le tester / valider.

Frédéric (et les autres) si vous voulez le tester il suffit de (sur un serveur de test bien entendu):

- abuledu-upgrade (pour mettre à jour la base + avoir les accréditations de mise à jour etc.)
- dans les 20 minutes qui suivent le lancement de abuledu-upgrade lancer un "apt-get install ryxeo-winapps-moonsecure"
- rebooter un poste windows ou forcer la mise à jour d'un poste windows via abuladmin / forcer la mise à jour

Et ensuite nous indiquer ici même si tout marche bien ?

#2 - 12/12/2010 19:17 - Adamczak Frédéric

- Fichier moonsecure.jpg ajouté

(Fred. A) : je viens de tester et malheureusement, ça ne marche pas chez moi.
Lorsque je lance le script de mise à jour, la console affiche un message (d'erreur ?) : cf pj.

Si je fais un tail /tmp/wpkg-.....log je ne vois aucune trace de moonsecure

J'espère que ça pourra t'aider.

#3 - 12/12/2010 19:25 - Eric Seigne

- Fichier moonsecure.xml ajouté

Arg !

es-ce que tu peux essayer de mettre le fichier xml ci-joint à la place de l'autre, dans /home/appli/wpkg/packages/ ?

et me dire ensuite ce que ça donne ...

Merci
Éric

#4 - 12/12/2010 19:51 - Eric Seigne

- Fichier moonsecure.xml supprimé

#5 - 12/12/2010 19:52 - Eric Seigne

- Fichier moonsecure.xml ajouté

Je me suis planté de fichier !!! pardon !

#6 - 12/12/2010 20:35 - Adamczak Frédéric

Snif. Ça fait toujours la même chose.
Ne devrait-on pas retrouver des traces de moonsecure dans le fichier system32\wpkg.xml ?

#7 - 12/12/2010 21:06 - Eric Seigne

- Fichier moonsecure.xml supprimé

#8 - 12/12/2010 21:07 - Eric Seigne

Re,

entre temps j'ai validé la configuration automatique du proxy ... donc essaye de faire une nouvelle mise à jour, le nouveau paquet ryxeo-winapps-moonsecure devrait tomber tout seul et au boot suivant du windows tout devrait rouler, en tout cas c'est ainsi ici :)

Éric

#9 - 12/12/2010 22:34 - Adamczak Frédéric

C'est bon. Ça roule maintenant.
Merci.

#10 - 19/12/2010 21:12 - Eric Seigne

- Assigné à Eric Seigne supprimé

#11 - 21/12/2010 14:15 - Stéphane Hays

install moonsecure winapps 9.08.03 serveur ok.
Je m'attendais à son apparition dans webadmin/installapps mais non, perso j'aurais préféré choisir mon anti-virus :)
Test avec le compte AbulAdmin : Icone en barre des tâche Windows ok. Moonsécure non actif (ne sert à rien). Interface en Anglais. Lancement manuel à l'aide de l'interface, message d'erreur "timeouted starting msav".
Tests avec un compte utilisateur : popup automatique lors de l'insertion d'une clefs très pratique... mais se conclue par un message de bug " : exception message : Cannot create file "C:\Program Files\Moon Secure Antivirus\1857437.1.mss". Accès refusé.
Mise à jour base de virus impossible, (main.cvd error receiving header/lenght) base à la date du 02 juin 2008.

#12 - 21/12/2010 20:35 - Adamczak Frédéric

Je viens de rencontrer les mêmes difficultés que Stéphane.
1/ J'ai réussi à remédier à la première (moonsecure non actif, message d'erreur "timeout") en démarrant (une fois) manuellement moonsecure (c:\program Files\Moon Secure Antivirus\msavcore.exe). Depuis l'antivirus se lance à chaque démarrage d'un poste. Je suppose qu'il y doit y avoir une modification dans la base de registre qui ne s'est pas faite lors de l'installation et qui se fait après avoir lancé manuellement msavcor.exe

2/ Même bug lors de l'insertion de clé (accès refusé) lorsque je suis identifié comme utilisateur. Là visiblement c'est un problème de permissions : http://www.moonsecure.com/index.php?option=com_mamboboard&Itemid=56&func=view&catid=7&id=200#200. Le scan se fait bien lorsque je suis loggué en administrateur.

3/ Idem pour la mise à jour. Impossible, même message d'erreur, précédé d'un WARN : might be network outage. J'ai essayé de bidouiller dans les 'settings' du logiciel mais rien n'y fait.

#13 - 28/12/2010 15:32 - Adamczak Frédéric

Lors de son installation, MoonSecure crée 2 clés dans la base de registre. Toutes deux dans HKEY_LOCAL_MACHINE/Software/Microsoft/windows/Run.
La première est correctement initialisée et renvoie vers c:\Program Files\Moon Secure Antivirus\MonnTray.exe
La seconde est vide. Je la modifie manuellement et l'initialise avec c:\Program Files\Moon Secure Antivirus\msavcore.exe. Je redémarre et là ça roule, MoonSecure se lance au démarrage, le scan de clé usb se fait, etc. (en revanche, toujours pas de mise à jour).
A priori, c'est bien une histoire de clé de registre. Je ne sais pas si ça peut faire avancer le schmilblick...

#14 - 21/01/2011 14:56 - Stéphane Hays

Je test "ClamV by immunet" http://www.immunet.com/free/index.html peut être plus récent que MoonSecure ?
Immunet, pas de résident => scan "online" pas d'internet = pas d'antivirus + déploiement automatique difficile + inscription utilisateur en ligne obligatoire :(

Ou bien ClamWin beaucoup plus "libre" et efficace à déployer http://www.clamwin.com

#15 - 28/01/2011 18:36 - Adamczak Frédéric

J'ai vu qu'il existait clamsentinel http://www.framasoft.net/article5019.html qui se base sur clamWin en offrant une protection en continu.
Peut-être creuser de ce côté là.

#16 - 28/01/2011 22:30 - Stéphane Hays

Bonjour,

C'est justement l'info que je recherchais :) merci.
Du coup peut être quelques "bonnes" nouvelles d'ici peu...

Cordialement,
Stéphane.

#17 - 01/02/2011 10:18 - Stéphane Hays

- Sujet changé de Proposer MoonSecure comme antivirus windows via webadmin à Proposer ClamWin+Sentinel comme antivirus windows via webadmin (était : MoonSecure)

#18 - 01/02/2011 11:56 - Stéphane Hays

Création d'un dossier dans le "home" des utilisateurs (P:\) (Mes Documents) nommé "antivirus".
ClamWin ne sait pas désinfecter un fichier, seulement le supprimer ou le mettre en quarantaine. Donc j'ai choisi de les déplacer dans le répertoire "P:\antivirus"
La version (future) de Clamav coté serveur purgera ce répertoire régulièrement.

Configuration de ClamWin pour déploiement automatique via Wpkg.
- Création du répertoire /home/appli/wpkg/paquets/ClamWin (avec les fichiers "clamsentinel.reg, ClamSentinel.ini, ClamSentinel1.15.exe, clamwin-0.96.5-setup.exe, Clamwin.conf)

Fichier clamsentinel.reg : ajoute la clef de registre

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Clam Sentinel"="C:\\Program Files\\ClamSentinel\\ClamSentinel.exe"
```

pour le démarrage automatique au boot du système. ClamSentinel ajoute cette clef dans la brabche "User", j'ai préféré la mettre dans Local_Machine. Seul hic, c'est que dans le logiciel la coche "démarrer avec le système" est décochée... et que si l'utilisateur l'active c'est 2 ClamSentinel qui démarrent :(

Fichier ClamSentinel.ini : pas grand chose à modifier seul les volumes à scanner "DirToScan=C:\,P:\" Ce fichier est injecté dans "%PROGRAMFILES%\ClamSentinel\"

ClamWin.conf : Ce fichier est injecté AVANT l'installation de ClamWin dans le répertoire "C:\Program Files\ClamWin\bin\". Modification des chemins et ajout du proxy "servecole:3128".

Déploiement opérationnel derniers règlages et tests en cours.

#19 - 01/02/2011 15:45 - Stéphane Hays

A la première connexion d'un utilisateur, ClamSentinel n'arrive pas à écrire dans le fichier P:\antivirus\log\fichier.log puisque ce fichier n'existe pas. Il le créé donc et au second démarrage de ClamSentinel ce message n'est plus présent.

#20 - 10/02/2011 14:14 - Stéphane Hays

- Fichier clamwin.xml ajouté

- Assigné à mis à Gilles Seban

- % réalisé changé de 90 à 100

Déploiement WPKG Clamav et clamsentinel opérationnel.

#21 - 26/04/2011 17:17 - Stéphane Hays

- Assigné à changé de Gilles Seban à Eric Seigne

#22 - 01/06/2011 10:54 - Stéphane Hays

- Fichier clamwin.tar.gz ajouté

- Assigné à changé de Eric Seigne à Stéphane Hays

- Version cible mis à AbulÉdu - Serveur - 11.08

Mises à jour des version de
Clamwin 0.96.5 => 0.97
ClamSentinel 1.15 => 1.16

#23 - 01/06/2011 10:57 - Stéphane Hays

- Fichier clamwin.xml supprimé

#24 - 27/10/2011 16:15 - Stéphane Hays

- Statut changé de Pending - En attente à Testé - validé

#25 - 11/11/2011 15:14 - Eric Seigne

- Statut changé de Testé - validé à Fixed - Corrigé - Implémenté

Fichiers

moonsecure.jpg	116 ko	12/12/2010	Adamczak Frédéric
clamwin.tar.gz	36,7 Mo	01/06/2011	Stéphane Hays