horizon-default-settings - Feature - Fonctionnalité #989

horizon-clamav-default-settings: paquet pour installation automatique de l'antivirus serveur

12/12/2010 12:21 - Eric Seigne

Statut:	Fixed - Corrigé - Implémenté	**Début:**	12/12/2010
Priorité:	Paquets	**Echéance:**	
Assigné à:	Eric Seigne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	8.00 heures
Version cible:	version-9.08		

Description

Pour que l'antivirus serveur se déploie automatiquement il faut préconfigurer le système:

- https://secure.ryxeo.com/doku.php/exploitation/commandes_utiles
- ajouter un administrateur adminvirus
- créer un sous répertoire quarantaine chez cet utilisateur
- à chaque scan on créé un répertoire 20101208 dans quarantaine et un fichier de log
- il faut que aesd ait le droit d'aller lire ce fichier de log

connexion avec le ticket #120 pour la partie webadmin

Demandes liées:

Lié à horizon-webadmin - Feature - Fonctionnalité #120: webadmin: rapports de...	**Fixed - Corrigé - Implémenté**	**25/02/2010**

Révisions associées

Révision 534d38c5 - 12/12/2010 13:56 - Eric Seigne

fix #989

Historique

#1 - 12/12/2010 15:00 - Eric Seigne

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

- Assigné à changé de Eric Seigne à Stéphane Hays

Stéphane,
ce paquet est poussé sur le serveur de mise à jour officiel mais aucune école ne l'a encore (c'est un nouveau paquet), il faudrait donc que tu prenne une ou deux écoles dans le pool pour tester ce "truc".

Installation classique:

- apt-get update
- apt-get install horizon-clamav-default-settings
- /etc/init.d/firewall restart

Et ensuite il faut laisser tourner tout seul pour voir au bout de 2 ou 3 jours si:

- /var/log/aesd/antivirus/ se remplit doucement de logs
- /home/administrateurs/adminvirus/quarantaine/ également

Merci d'avance pour les retours d'infos ... Je viens de l'installer à l'école **aristide-briand (pessac)**, tu peux essayer partout où tu veux sauf chez eux :)

#2 - 13/12/2010 10:14 - Eric Seigne

Attention, a creuser, à aristide briand le 1er scan n'est pas terminé que le 2° démarre !

Améliorer pour éviter que ça ne dure trop longtemps (custom de la config pour ne pas extraire les compressés par ex. ou le cache de firefox ou ...)

#3 - 15/12/2010 09:50 - Eric Seigne

Améliorer le cron pour qu'il démarre le soit à 19h au lieu de daily qui est lancé à 6h25 du mat'

Améliorer le exclude pour ne pas scanner:

- firefox cache
- .xsession-errors
- ... à trouver / noter / réfléchir

#4 - 15/12/2010 12:40 - Eric Seigne

Et j'ai droit à cette erreur: *libclamav JIT: *** JITed code intercepted runtime error* qui semble être un "bug" classique mais peut-être uniquement quand on est en ssh (?)

#5 - 19/12/2010 12:48 - Eric Seigne

Seconde installation (stéphane, je n'ai pas vu où t'a fait une installation de test), je teste au **cafésol de saintes** avec les améliorations de ce matin: impossible d'avoir deux clamav en même temps et améliorations diverses (exclusion etc.).

#6 - 19/12/2010 12:48 - Eric Seigne

- % réalisé changé de 0 à 80

#7 - 19/12/2010 14:21 - Eric Seigne

Retours de tests:

- **cafésol de saintes**: le scan complet a pris 30 minutes et a dégagé quelques virus (cf mail privé)
- **aristidebriand**: ça roule mais le répertoire /home/classes/recuperation est un handicap certain avec ses milliers de fichiers ...
- **i-kbane la teste**: en cours

#8 - 20/12/2010 09:08 - Eric Seigne

Ecole Aristide Briand; 2770 minutes soit plus de 46 heures pour tout scanner ... je pense qu'il faut trouver une solution !

```
----------- SCAN SUMMARY -----------
Known viruses: 856324
Engine version: 0.96.3
Scanned directories: 243977
Scanned files: 1068673
Infected files: 10
Data scanned: 53698.97 MB
Data read: 121399.67 MB (ratio 0.44:1)
Time: 166218.858 sec (2770 m 18 s)
```

#9 - 20/12/2010 09:10 - Eric Seigne

i-kbane beaucoup plus rapide ... alors qu'il y a plus de données, es-ce que ça serait le nombre de répertoires qui influerait sur les performances ?

```
----------- SCAN SUMMARY -----------
Known viruses: 856350
Engine version: 0.96.3
Scanned directories: 183456
Scanned files: 1023586
Infected files: 4996
Data scanned: 75174.98 MB
Data read: 114032.05 MB (ratio 0.66:1)
Time: 24489.867 sec (408 m 9 s)
```

#10 - 21/12/2010 14:54 - Stéphane Hays

Après avoir vérolé un compte utilisateur, tests manuel avec la commande horizon :
Mise à jour de la base ok, ainsi que la création des répertoires de quarantaine.

```
----------- SCAN SUMMARY -----------
Known viruses: 856481
Engine version: 0.96.3
Scanned directories: 2339
Scanned files: 1782
Infected files: 16
Data scanned: 931.97 MB
Data read: 2164.39 MB (ratio 0.43:1)
Time: 239.610 sec (3 m 59 s)
```

Tous les virus ont étés détectés et déplacés.

ATTENTION FAUX POSITIF :
/home/appli/utilitaires/abuledu-xp-home.exe: Trojan.Downloader-99407 FOUND
/home/appli/utilitaires/abuledu-xp-home.exe: moved to '/home/administrateurs/adminvirus/quarantaine/20101221/abuledu-xp-home.exe'

Tests de remplissage des logs à faire sur un serveur utilisé ou virtualbox :(ceux de tests sont éteins la nuit.

#11 - 21/12/2010 20:15 - Eric Seigne

J'ai supprimé appli de la liste des répertoires scannés ... mais c'est un peu "bof" dans la mesure où abuladmin a le droit d'y écrire et s'il choppe un virus ...

#12 - 22/12/2010 10:16 - Stéphane Hays

- Assigné à changé de Stéphane Hays à Eric Seigne

#13 - 10/01/2011 11:27 - Gilles Seban

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

#14 - 15/01/2011 15:07 - Eric Seigne

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

- Assigné à Eric Seigne supprimé

Bon, a mon avis on ne peut pas l'envoyer tel-quel, stéphane ça donne quoi au lycée st antoine et autres sites de tests ? si tu te connecte dans la journée es-ce que clamav tourne toujours comme je l'ai sur aristide briand ? dans cette école le processus clamav tourne en double et toute la journée, il y a trop de fichiers à scanner ...

Je pense qu'il ne vaut pas pousser ce paquet sur le dépôt officiel en l'état.

Éric

#15 - 21/01/2011 14:20 - Stéphane Hays

Pas de soucis particuliers au Lycée St Antoine, surement moins de fichiers.
Le cas de A Brian est spécial car pas de Windows dans l'école.
Je pense que Clamav devrait être un "option" non installée par défaut. ############
Pas de mise à jour avant un /etc/init.d/firewall restart

#16 - 10/02/2011 14:04 - Stéphane Hays

Fonctionnement satisfaisant au Lycée Saint Antoine.
Je pense qu'il serait bien de proposer dans Webadmin :
- un lien "scanner maintenant", et,
- ordonner les rapports par date chronologique.

#17 - 12/04/2011 17:07 - Eric Seigne

- Version cible mis à version-9.08

#18 - 14/04/2011 15:56 - Eric Seigne

- Statut changé de Pending - En attente à Fixed - Corrigé - Implémenté

- Assigné à mis à Eric Seigne

- % réalisé changé de 80 à 100

Validé à saint antoine, aristide briand et ...