

Anti-virus serveur-client

L'usage et les techniques notées dans la présente documentation ne peuvent en aucun cas engendrer une responsabilité quelle que soit de RyXéo. L'usagé est seul responsable de la mise en œuvre ainsi que des contenus installés sur le serveur.

Bien qu'il n'existe que très peu de virus connus pour les systèmes Linux, le serveur AbulEdu traite beaucoup d'informations et de services accessibles à Windows. Ce dernier n'étant pas lui exempt de logiciels malveillants, RyXéo à mis en place dans votre serveur une solution pour débusquer les fichiers infectés.

Basé sur le logiciel libre Clamav, RyXéo propose aussi le déploiement automatique de sa version cliente Windows ClamWin. Contrairement aux versions dites freeware d'autres anti-virus gratuits, son utilisation est autorisée dans un cadre professionnel et scolaire.



Gestion de l'anti-virus coté serveur via WebAdmin :

Le service anti-virus coté serveur AbulEdu scan les dossiers des utilisateurs et des groupes (classes). il ne scan pas les fichiers système, ni les emails.

Bienvenue dans l'administration de votre serveur.

Utilisateurs et Groupes

- Utilisateurs
- Groupes
- Import automatique

Internet et Réseau

- Connexion internet
- Courrier électronique
- Filtrage Web
- Proxy parent
- Configuration réseau

Administrateurs

- Mot de passe

Gestion du serveur

- Abonnement Zen
- Informations
- Tour de CDs/DVDs
- Arrêter / Reboot
- Imprimantes
- Ajout de logiciels
- MySQL
- Antivirus**

Postes clients

Vous trouverez un nouveau menu dans WebAdmin : « Antivirus »

Rapport de scan antivirus du serveur

Vous trouverez ci-dessous le rapport de scan de l'antivirus. Les fichiers infectés sont déplacés dans un endroit où seul l'administrateur peut aller. Cliquez ici pour consulter le rapport de scan archivés.

Nom du virus	Fichier infecté
Trojan.Onlinegames-1541	/home/utilisateurs/bureau/Trojan-GameThief.Win32.Staem.b.zip déplacé vers /home/administrateurs/adminvirus/quarantaine/20110121/Trojan-GameThief.Win32.Staem.b.zip'
W32.Highway.A	/home/utilisateurs/prof/windows/Bureau/Virus.Win32.Highway.a.zip déplacé vers /home/administrateurs/adminvirus/quarantaine/20110121/Virus.Win32.Highway.a.zip'
W32.Highway.A	/home/administrateurs/adminvirus/quarantaine/20110121/Virus.Win32.Highway.b.zip'
W32.Randlle	/home/utilisateurs/prof/windows/Bureau/Virus.Win32.Randlle/Virus.Win32.Randlle'
W32.Randlle	/home/utilisateurs/prof/windows/Bureau/Virus.Win32.Randlle.zip déplacé vers /home/administrateurs/adminvirus/quarantaine/20110121/Virus.Win32.Randlle.zip'
W32.Warmup-1	/home/administrateurs/adminvirus/quarantaine/20110121/Virus.Win32.Warmup.a.zip'
Win-IOX	/home/utilisateurs/prof/windows/Bureau/Virus.Win32.IOX.zip déplacé vers /home/administrateurs/adminvirus/quarantaine/20110121/Virus.Win32.IOX.zip'

La page de ce menu rapporte la liste des derniers fichiers infectés, le nom ainsi que le chemin du virus (Linux).

Archives des rapports de scan antivirus du serveur

Vous trouverez ci-dessous la liste des archives de scan de l'antivirus. Vous pouvez consulter le détail d'un rapport en cliquant dessus.

- Rapport du : 21/01/2011

AbulEdu GNU/Linux est distribué sous licence GNU GPL version 2 sans aucune garantie d'aucune sorte. Copyright et droits d'auteurs © 1999-2008 Eric Seigne et Olivier Cortès pour le projet AbulEdu, ainsi qu'à tous les auteurs respectifs des logiciels libres utilisés (Notamment Ubuntu, Debian, Gentoo, Apache, PHP, MySQL, SFTP,...).

Le scan étant lancé régulièrement, une page liste les rapports archivés.

Nom du virus	Fichier infecté
Trojan.Onlinegames-1541	/home/utilisateurs/prof/windows/Bureau/Trojan-GameThief.Win32.Staem.b.zip déplacé vers /home/administrateurs/adminvirus/quarantaine/20110121/Trojan-GameThief.Win32.Staem.b.zip'

ClamAV ne sait pas encore désinfecter un fichier.

L'option la plus sûre est donc de le déplacer en « quarantaine » dans un répertoire daté de l'administrateur « adminvirus ».

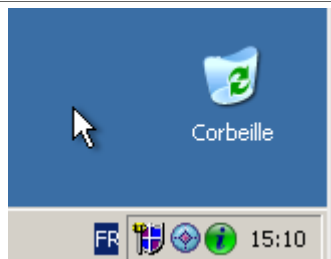
Il est possible de retrouver ce fichier si besoin.

Gestion de l'anti-virus coté client Windows :

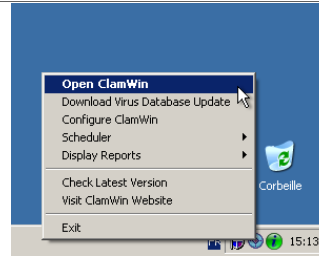
Le déploiement automatique de ClamWin sur les postes Windows n'est pas automatisé afin d'éviter les télécopages avec d'autres éventuels anti-virus.

Vous pouvez déclencher cette installation dans la rubrique « Ajout de logiciels » de l'interface d'administration du serveur WebAdmin.

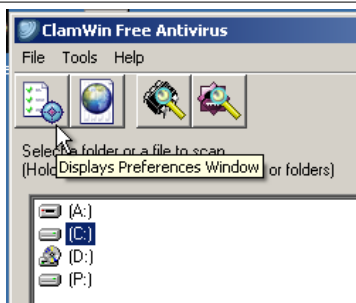
L'interface de ClamWin est pour l'instant en anglais.



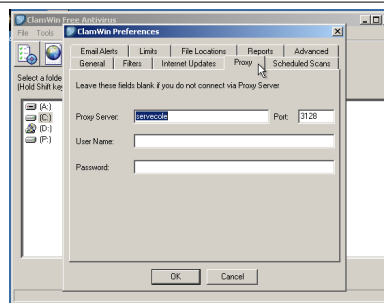
Les icônes de ClamSentinel et ClamWin dans la barre des tâches renseignent sur leur fonctionnement.



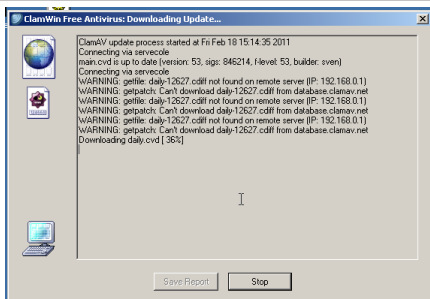
Vous pouvez ouvrir l'interface de ClamWin à l'aide du menu contextuel qui apparaît avec le clic droit de la souris sur le logo ClamWin.



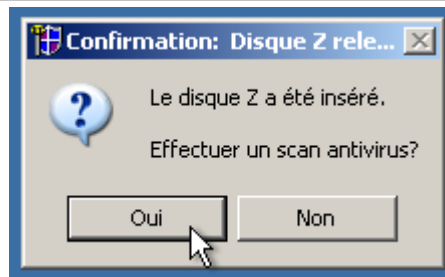
L'interface relativement simple de ClamWin.



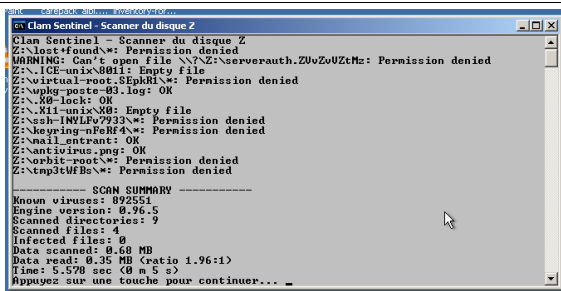
Pré-configuré lors du déploiement, les mises à jour doivent passer par le proxy du serveur.



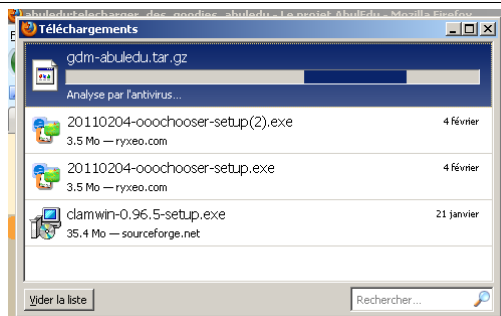
La fenêtre des mises à jour. Vérifiez leur bon déroulement.



Lors de l'insertion d'une clef mémoire USB, ClamSentinel vous propose d'en vérifier le contenu.



Vous visualisez le résultat du scan de la clef USB. La quarantaine des fichiers infectés se situe dans « mes documents/antivirus ». Ce répertoire sera purgé par le serveur régulièrement.



De même, lors d'un téléchargement, une analyse est lancée automatiquement sur le fichier.

RyXéo SARL - AbulEdu - NouvaLinux
 21 avenue E. et M. Dulout
 33600 Pessac - contact@ryxeo.com
 Tel: 05 35 54 01 18 - fax: 09 56 606 607
 centre de formation enregistré auprès de la Préfecture d'Aquitaine