Anti-virus serveur-client

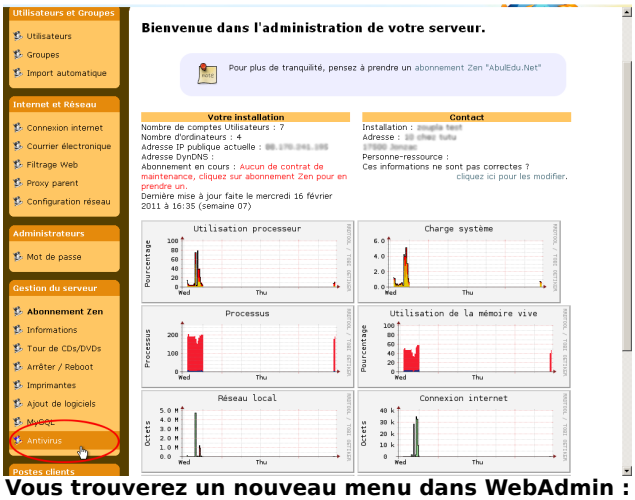
L'usage et les techniques notées dans la présente documentation ne peuvent en aucun cas engendrer une responsabilité quelle quelle soit de RyXéo. L'usagé est seul responsable de la mise en œuvre ainsi que des contenus installés sur le serveur.

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.

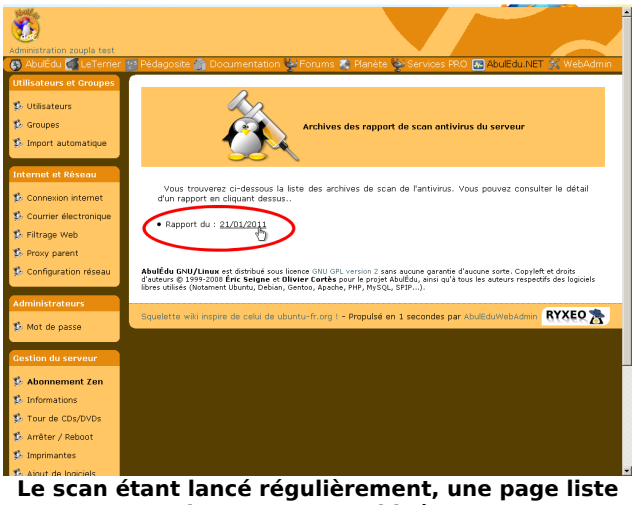
Gestion de l'anti-virus coté serveur via WebAdmin :

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.



Vous trouverez un nouveau menu dans WebAdmin : « Antivirus »

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



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'
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/utilisateurs/prof/windows/Bureau/Virus.Win32.Highway.b.zip déplacé vers '/home/administrateurs/adminvirus/quarantaine/20110121/Virus.Win32.Highway.b.zip'
W32.Ramdile	/home/utilisateurs/prof/windows/Bureau/Virus.Win32.Ramdile/Virus.Win32.Ramdile déplacé vers '/home/administrateurs/adminvirus/quarantaine/20110121 /Virus.Win32.Ramdile'

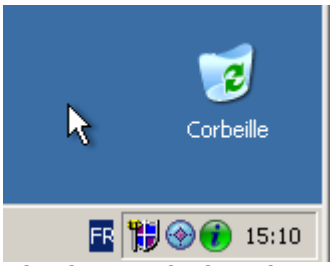
ClamAV ne sait pas encore désinfecter un fichier.

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

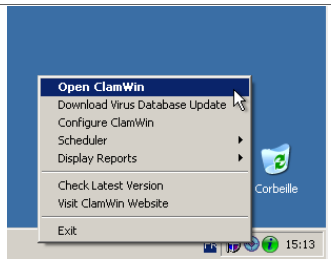
Il est possible de retrouver ce fichier si besoin.

Gestion de l'anti-virus coté client Windows :

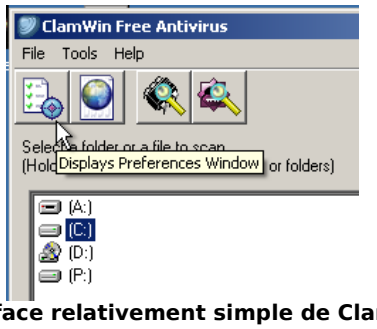
Le déploiement automatique de ClamWin sur les postes Windows n'est pas automatisé afin d'éviter les téléscopages avec d'autres éventuels anti-virus.
Vous pouvez déclencher cette installation dans la rubrique « Ajout de logiciels » de l'interface d'administration du serveur WebAdmin.
L'interface de ClamWin est pour l'instant en anglais.



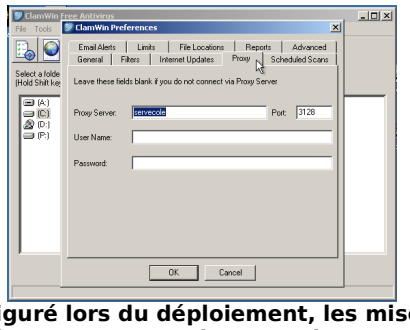
Les icônes de ClamSentinel et ClamWin dans la barre des tâches renseignent sur leur fonctionnement.



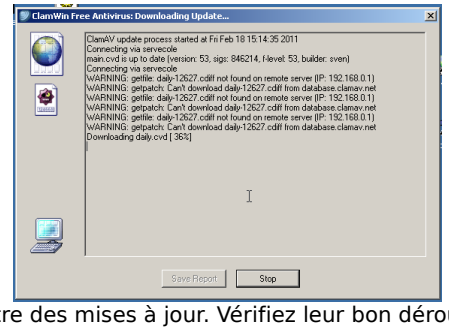
Vous pouvez ouvrir l'interface de ClamWin à l'aide du menu contextuel qui apparaît avec le clic droit de la souris sur le logo ClamWin.



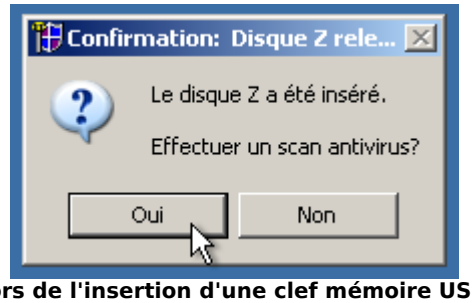
L'interface relativement simple de ClamWin.



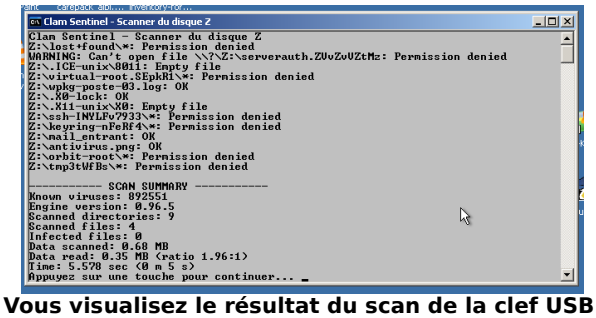
Pré-configuré lors du déploiement, les mises à jour doivent passer par le proxy du serveur.



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

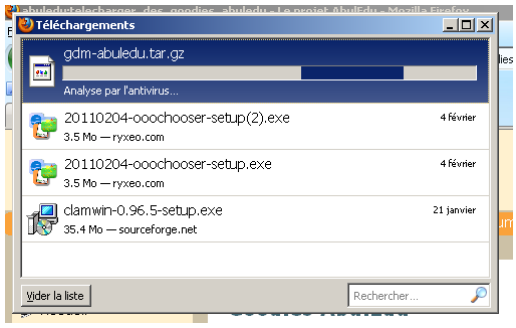


Lors de l'insertion d'une clef mémoire USB, ClamSentinel vous propose d'en vérifier le contenu.



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