KASPERSKY LAB

Kaspersky® Anti-Virus 5.5 for Samba Servers

MANUEL DE L'ADMINISTRATEUR

KASPERSKY® ANTI-VIRUS 5.5 FOR SAMBA SERVERS

Manuel de l'administrateur

http://www.kaspersky.com/fr

Date d'édition : Novembre 2006

Sommaire

CHAPITRE 1. INTRODUCTION

L'augmentation du nombre d'utilisateurs d'ordinateurs et le développement des moyens d'échange de données par courrier électronique ou via Internet accroient le risque d'infection des ordinateurs par des virus informatiques et exposent les données à un plus grand danger de dégradation ou de vol par des programmes malveillants.

Parmi les différents canaux utilisés par les programmes malveillants pour se propager, les plus dangereux sont :

Internet

Le réseau mondial d'information est le principal vecteur de diffusion de n'importe quel type de programme malveillant. En règle générale, les virus et autres programmes malveillants sont chargés sur des sites Internet populaires sous la forme d'applications utiles et gratuites. Il existe également de nombreux scripts exécutés automatiquement à l'ouverture de pages Web qui peuvent contenir des programmes malveillants.

Courrier électronique

Les messages électroniques envoyés dans les boîtes aux lettres des utilisateurs et enregistrés dans les bases de données de messagerie peuvent contenir des virus. Ces programmes malveillants peuvent se trouver en pièce jointe ou dans le corps du message. En règle générale, les messages électroniques peuvent contenir des virus et des vers de messagerie. Il est possible d'infecter les données de l'ordinateur en ouvrant le message ou en enregistrant la pièce jointe sur le disque dur.

Vulnérabilités des applications

Ces « failles » dans les applications profitent aux pirates informatiques. Elles leur permettent d'obtenir un accès frauduleux à votre ordinateur et, par conséquent, à vos données, aux ressources de réseau et à d'autres sources d'informations.

Les virus sont nettement moins répandus dans les systèmes Unix que dans les systèmes Windows par exemple, et ce en raison des particularités de ces plates-formes. Cela ne signifie pas pour autant que les utilisateurs du système d'exploitation Unix ne courent aucun danger. Examinons en détail les types de programmes malveillants.

1.1. Virus informatiques et programmes malveillants

Afin de pouvoir identifier les menaces qui planent sur vos données, il convient de définir les différents types de programmes malveillants et leur modus operandi. Il existe trois catégories de programmes malveillants :

- **Les vers** (*Worms*) : ils se propagent à l'aide des ressources du réseau. Les vers doivent leur nom à leur manière de passer d'un ordinateur à l'autre en exploitant le courrier électronique ainsi que d'autres canaux d'information. Cette technique leur permet de se diffuser à une très grande vitesse.

  Ils s'introduisent dans l'ordinateur, relèvent les adresses des autres machines connectées au réseau et y envoient leur copie. De plus, les vers exploitent également les données contenues dans le carnet d'adresses des clients de messagerie. Certains représentants de cette catégorie de programmes malveillants peuvent créer des fichiers de travail sur les disques du système, mais ils peuvent très bien ignorer les ressources de l'ordinateur, à l'exception de la mémoire vive.

- **Les virus** (*Viruses*) : il s'agit de programmes qui infectent d'autres programmes. Ils insèrent leur code dans celui de l'application ciblée afin de pouvoir prendre les commandes au moment de l'exécution des fichiers infectés. Cette définition simple permet d'identifier une des principales actions exécutées par les virus, à savoir *l'infection*. La vitesse de propagation des virus est légèrement inférieure à celle des vers.

- **Les chevaux de Troie** (*Trojans*) : il s'agit d'applications qui réalisent diverses opérations sur l'ordinateur infecté à l'insu de l'utilisateur. Cela va de la destruction de données sauvegardées sur le disque dur au vol d'informations confidentielles en passant par le « plantage» du système. Ces programmes malicieux ne sont pas des virus au sens traditionnel du terme (en effet, ils ne peuvent infecter les autres applications ou les données). Les chevaux de Troie sont incapables de s'introduire eux-mêmes dans un ordinateur. Au contraire, ils sont diffusés par des personnes mal intentionnées qui les présentent sous les traits d'applications « utiles ». Ceci étant dit, les dommages qu'ils occasionnent peuvent être bien plus sérieux que ceux produits par les attaques de virus traditionnelles.

Les *vers et les chevaux de Troie* sont les catégories les plus fréquentes dernièrement dans les systèmes Unix.

Dans ce manuel, le terme « virus » désignera aussi bien les virus que les chevaux de Troie et les vers. Le type de programme malveillant sera précisé au besoin.

1.2. Présentation et fonctions principales de Kaspersky Anti-Virus

Le logiciel **Kaspersky® Anti-Virus 5.5 forSamba Servers** (ci-après **Kaspersky Anti-Virus**) assure la protection antivirus des objets sur les serveurs Samba tournant sous Linux ou FreeBSD.

Le logiciel permet une analyse à deux niveaux du système de fichiers du serveur : analyse en temps réel et analyse à la demande. Lorsque des programmes malveillants sont découverts, Kaspersky Anti-Virus est capable de réparer ou de bloquer efficacement les objets infectés pour éviter la propagation de l'épidémie et il signale l'incident à l'administrateur du système.

L'application exploite également la technologie iChecker™, une technologie intelligente qui permet d'accélérer sensiblement l'analyse des fichiers.

Kaspersky Anti-Virus for Samba Servers contient plusieurs composants chargés des fonctions suivantes :

- *Protection en temps réel* du serveur de fichiers Samba contre les codes malveillants (**On-Access Scanner***)*.
- *Recherche et neutralisation* du code malveillant dans le système de fichiers du serveur *à la demande* (**On-Demand Scanner***)*.
- *Notification de l'administrateur* en cas de découverte d'objets suspects ou infectés.
- *Préservation de l'actualité des bases antivirus* (**keepup2date**).
- *Administration locale et à distance* grâce au module d'administration Web (**Webmin**).

De plus, Kaspersky Anti-Virus offre la fonction suivante :

- Utilisation de scripts définis par l'utilisateur en cas d'événement de type « fichier infecté découvert ».
- Transfert des objets infects (ou suspects) dans un répertoire spécial (quarantaine).

- Conservation de la copie originale de l'objet avant la réparation (Backup) et possibilité de le restaurer en cas de problème lors de la réparation.
- Conservation dans le cache des données relatives aux fichiers déjà analysés, ce qui permet de réduire sensiblement la durée de l'analyse du fichier lorsqu'une nouvelle requête lui est adressée (les données du cache sont conservées jusqu'au redémarrage de l'application).
- Restriction du nombre de fichiers analysés simultanément pendant la protection en temps réel et mise des fichiers restants envoyés pour analyse dans une file d'attente.
- Possibilité d'arrêter l'analyse antivirus des fichiers en arrière plan lorsque la charge du serveur dépasse un seuil prédéfini par l'utilisateur et de reprendre l'analyse lorsque la charge revient à un niveau acceptable.
- Possibilité de définir pour chaque répertoire partagé n'importe quelle combinaison de mode « d'analyse à l'ouverture » et « d'analyse lors de l'enregistrement ».
- Possibilité de procéder à des configurations individuelles de la protection antivirus pour chaque répertoire partagé.
- Lors de la mise à jour des bases antivirus, l'application détermine le serveur de mise à jour de Kaspersky Lab le moins sollicité. De plus, en cas de perte de la connexion, le téléchargement reprend à l'endroit où il avait été interrompu.
- Possibilité de revenir à l'état antérieur à la mise à jour des bases antivirus et des modules de l'application ;

1.3. Configuration requise

Pour que **Kaspersky Anti-Virus for Samba Servers** fonctionne au maximum de ses capacités, votre ordinateur doit avoir la configuration suivante :

- Processeur Intel Pentium® de 133 Mhz minimum ;
- 64 Mo de RAM ;
- 100 Mo sur le disque dur pour l'installation de l'application et la conservation des fichiers temporaires.

- Configuration logicielle :
  - Pour les plateformes 32 bits, un des systèmes d'exploitation suivants :
    - RedHat Linux 9.0.

- RedHat Enterprise Linux Advanced Server 4 UPD3.
- SUSE Linux Enterprise Server 9.0 SP3.
- SUSE Linux Professional 10.1.
- Debian GNU/Linux version 3.1 R2.
- Mandriva 2006.
- FreeBSD version 4.11.
- FreeBSD version 5.4.
- FreeBSD version 6.1.

- Pour les plateformes 64 bits, un des systèmes d'exploitation suivants :
  - RedHat Enterprise Linux Advanced Server 4 UPD3.
  - RedHat Fedora Core 5.
  - SUSE Linux Professional 10.1.
  - SUSE Linux Enterprise Server 9 SP3.
- Webmin (www.webmin.com) pour l'administration à distance de Kaspersky Anti-Virus.
- Interprète Perl 5.0 ou suivant (www.perl.org).
- Utilitaire which ;
- Serveur Samba version 2..2.7 ou suivante ou version 3.0.0 à 3.0.23c.

Kaspersky Anti-Virus n'est pas compatible avec SELinux. L'utilisation de SELinux peut entraîner l'affichage de différents avertissements dans le fichier système du rapport de l'application.

De plus, si votre serveur est doté d'une protection à l'aide de listes de contrôle d'accès au système de fichiers (File System Access Control Lists, ACL), il convient de configurer le serveur Samba pour la prise en charge de cette fonction.

1.4. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-Virus chez un distributeur ou détaillant, ou visiter un de nos magasins en ligne (par exemple www.kaspersky.com/fr, rubrique **Boutique en ligne**).

La boîte du logiciel contient :

- Une enveloppe cachetée contenant le CD d'installation où les fichiers du logiciel sont enregistrés ;
- Le manuel de l'utilisateur ;
- La clé de licence, enregistrée sur une disquette spéciale ;
- La carte d'enregistrement (mentionnant le numéro de série du logiciel) ;
- Le contrat de licence.

Avant de décacheter l'enveloppe contenant le CD (ou les disquettes), veuillez lire attentivement le contrat de licence.

Si vous achetez Kaspersky Anti-Virus en ligne, le fichier d'installation du produit est téléchargé du site Web de Kaspersky Lab. Ce fichier d'installation inclut ce guide de l'utilisateur. La clé de licence sera envoyée par courrier électronique dès la réception du paiement.

Contrat de licence

Le contrat de licence constitue l'accord juridique passé entre vous et Kaspersky Lab Ltd., stipulant les conditions d'utilisation du logiciel que vous avez acquis.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les termes du contrat de licence, vous pouvez retourner la boîte contenant le logiciel au distributeur agréé qui vous l'a vendu et être intégralement remboursé. Dans ce cas, l'enveloppe contenant le CD (ou les disquettes) ne doit en aucun cas avoir été décachetée.

L'ouverture de l'enveloppe cachetée contenant le CD d'installation (ou les disquettes) implique que vous acceptez les termes du contrat de licence.

1.5. Services réservés aux utilisateurs enregistrés

Kaspersky Lab Ltd. offre à ses utilisateurs légalement enregistrés une gamme élargie de prestations leur permettant d'augmenter l'efficacité d'utilisation du logiciel Kaspersky Anti-Virus.

L'acquisition de la licence vous confère le statut d'utilisateur enregistré du programme et durant toute la période de validité de cette licence, vous bénéficiez des prestations suivantes :

- Nouvelles versions de ce logiciel, fournies gratuitement ;
- Assistance téléphonique et par voie électronique sur l'installation, la configuration et l'utilisation de ce logiciel ;
- Avis de lancement des nouveaux logiciels de la société Kaspersky Lab et informations sur l'apparition de nouveaux virus dans le monde (ne bénéficient de ce dernier service que les utilisateurs ayant souscrit un abonnement au bulletin de Kaspersky Lab).

Le service d'assistance technique ne répond ni aux questions portant sur le fonctionnement et l'utilisation des systèmes d'exploitation, ni à celles sur le fonctionnement des différentes technologies.

1.6. Notations conventionnelles

Le texte de la documentation se distingue par divers éléments de mise en forme en fonction de son affectation sémantique. Le tableau ci-après illustre les conventions typographiques utilisées dans ce manuel.

Mise en forme	Fonction sémantique
Caractères gras	Nom de menu, des options du menu, des fenêtres, des éléments des boîtes de dialogue, etc.
 Remarque.	Informations complémentaires, remarques.
 Attention !	Informations auxquelles il est recommandé d'accorder une attention particulière.
 *Pour exécuter une action,* 1. Etape 1. 2. …	Description de la séquence d'étapes que l'utilisateur doit suivre ou des actions possibles.

Mise en forme	Fonction sémantique
 Tâche ou exemple	Formulation du problème ou exemple d'utilisation du logiciel
 Solution	Solution du problème exposé
[argument] – valeur de l'argument.	Argument de la ligne de commande.
`Texte des messages d'information et de la ligne de commandes`	Texte des fichiers de configuration, des messages d'information et de la ligne de commandes.

CHAPITRE 2. ARCHITECTURE INTERNE DE KASPERSKY ANTI-VIRUS

Avant d'étudier les différentes fonctions de Kaspersky Anti-Virus for Samba Servers, nous allons aborder en détail son architecture interne. Vous obtiendrez ainsi une représentation plus complète de l'algorithme de fonctionnement de l'antivirus.

2.1. Composants

Kaspersky Anti-Virus for Samba Servers contient les composants suivants :

- *kavsamba (On-Access Scanner)*;
- *kavscanner (On-Demand Scanner)*;
- *keepup2date.*

Le composant *kavsamba* est lui-même constitué de deux modules : *kavsamba.so* et *kavsamba.* Le module *kavsamba.so* est une bibliothèque dynamique intégrée au serveur Samba dont le rôle est d'intercepter les sollicitations de fichiers via le serveur Samba. Le module *kavsamba* est un démon qui analyse les fichiers transmis par *kavsamba.so* avant de les traiter selon les paramètres définis. L'échange de données entre le module et le démon s'opère via le socket local (Unix Domain sockets).

Le composant *kavscanner* intervient dans la protection antivirus des systèmes de fichiers. L'analyse des systèmes de fichiers du serveur ou des fichiers de répertoires distincts s'effectue soit à la demande de l'administrateur, soit selon un horaire établi (en fonction des paramètres définis).

Le composant *keepup2date* prend en charge la mise à jour des bases antivirus utilisées par le logiciel pour détecter les virus et réparer les fichiers infectés. Ce composant permet également de télécharger les mises à jour des modules de l'application.

2.2. Algorithme de fonctionnement

Cette section est consacrée à l'architecture interne de l'application du point de vue de la protection antivirus en temps réel. L'analyse à la demande est relativement simple et ne nécessite pas d'explications particulières.

Voici donc une description de l'algorithme de fonctionnement :

1. Lorsqu'un utilisateur tente d'accéder à un fichier quelconque via le serveur Samba, le serveur intercepte la requête et celle-ci est transmise au module *kavsamba.so*.
2. Le module *kavsamba.so* envoie les données relatives à la requête (nom du fichier, chemin d'accès complet, identifiant de l'utilisateur souhaitant accéder au fichier et le nom de domaine de l'ordinateur) au module *kavsamba* via le CIP en utilisant le protocole binaire.
3. Le module *kavsamba* recherche la présence éventuelle de virus dans le fichier et le traite en fonction des paramètres définis dans le fichier de configuration (y compris la réparation à l'aide des bases antivirus, pour autant que cette option ait été activée).
4. Une fois l'analyse et le traitement du fichier terminés, *kavsamba.so* reçoit de *kavsamba* le code d'accès (autorisé ou non) qui définit le statut du fichier.
5. Conformément au statut de l'objet, *kavsamba.so* enverra au serveur Samba l'autorisation d'accéder ou non à l'objet.

L'accès au fichier est bloqué si ce dernier est infecté ou potentiellement infecté par un virus (Infected, CureFailed, Warning, Suspicion). Dans tous les autres cas de figure, l'accès sera autorisé.

CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS

Avant de procéder à l'installation de Kaspersky Anti-Virus :

- Assurez-vous que la configuration matérielle et logicielle du système répond aux exigences minimales pour l'installation de Kaspersky Anti-Virus (cf. point 1.3, page 9).
- Ouvrez la session avec les privilèges d'utilisateur **root**.

3.1. Installation du logiciel sur un serveur Linux

Kaspersky Anti-Virus pour Linux est distribué sous deux formats :

- **.rpm** : pour les systèmes compatibles avec RPM Package Manager;
- **.deb** : pour la distribution Debian.

Afin de lancer l'installation de Kaspersky Anti-Virus depuis le paquetage RPM, saisissez la commande :

```
rpm –i <nom_du_paquetage>
```

Afin de lancer l'installation de Kaspersky Anti-Virus depuis le paquetage deb, saisissez la commande :

```
dpkg –i <nom_du_paquetage>
```

3.2. Installation du logiciel sur un serveur FreeBSD

Le fichier d'installation de Kaspersky Anti-Virus pour les serveurs tournant sous FreeBSD se présente sous la forme d'un paquetage pkg.

Afin de lancer l'installation de Kaspersky Anti-Virus depuis le paquetage pkg, saisissez la commande :

```
pkg_add <nom_du_paquetage>
```

3.3. Procédure d'installation

Il existe toute une série de raisons qui pourraient entraîner l'apparition d'un code d'erreur à la fin du processus d'installation. Dans ce cas, assurez-vous que la configuration de votre ordinateur correspond bien à la configuration minimale requise (cf. point 1.3, page 9) et que vous entrez dans le système avec les privilèges de l'utilisateur root.

L'installation de l'application sur le serveur se déroule en plusieurs étapes :

1. Copie des fichiers d'installation sur le serveur.
2. Configuration du composant *keepup2date* ;
3. Installation (mise à jour) des bases antivirus ;

   

   N'oubliez pas d'installer les bases antivirus avant la première utilisation de l'application. La recherche des virus et la réparation des objets infectés s'opèrent sur la base des définitions contenues dans les bases antivirus, à savoir la description de l'ensemble des virus connus à ce jour et les méthodes de réparation des objets infectés. L'analyse et le traitement des fichiers sans bases antivirus est impossible.

   N'oubliez pas que la configuration automatique du logiciel n'est pas possible si les bases antivirus n'ont pas été installées.

4. Installation de la clé de licence.

   Il est impossible d'utiliser et de configurer le logiciel si la clé de licence n'a pas été installée. Toutefois, si vous ne disposez pas encore de la clé de licence (par exemple, vous avez acheté le logiciel en ligne mais vous n'avez pas encore reçu le message contenant la clé de licence), sachez qu'il est possible de l'activer non pas au moment de l'installation, mais plus tard, avant de commencer à utiliser le logiciel.

5. Installation du module Webmin.

   Le module de gestion à distance de Webmin sera installé uniquement si Webmin a été installé dans le répertoire standard. Une fois le module installé, vous recevrez les recommandations de configuration correspondantes pour son interaction avec l'application.

3.4. Configuration du logiciel

La configuration du système s'opère dès que les fichiers d'installation ont été copiés sur le serveur. En fonction du gestionnaire de paquetage, la configuration sera lancée automatiquement ou nécessitera l'intervention de l'utilisateur (si le gestionnaire de paquetage ne prend pas en charge les scripts interactifs, comme RPM). Dans ce cas, les messages indispensables seront affichés à l'écran.

La procédure de configuration du logiciel comprend :

- La recherche du serveur Samba installé et la comparaison de sa version à la configuration logicielle requise.
- La recherche et la modification du fichier de configuration du serveur Samba.
- La recherche d'éventuels objets VFS dans le fichier de configuration du serveur Samba. Si le fichier de configuration du serveur Samba contient déjà des lignes avec les objets VFS utilisés, des commentaires seront ajoutés à ces lignes.

Si vous utilisez le système d'exploitation FreeBSD et un serveur Samba dont la version est comprise entre 3.0 et 3.0.9, il est possible que les modules VFS créent des difficultés en raison des particularités du système d'exploitation.
Pour garantir le fonctionnement adéquat de l'application avec les objets VFS, il est conseillé de mettre le serveur Samba à niveau ou d'installer le correctif pour serveur Samba (pour obtenir de plus amples informations sur le correctif, consultez le site https://bugzilla.samba.org/show_bug.cgi?id=2100).

Si, au cours de la configuration du système, vous deviez fournir des renseignements complémentaires (par exemple, le chemin d'accès au fichier de configuration du serveur Samba), la console du serveur affichera les messages correspondants. La configuration sera interrompue si des réponses inexactes sont fournies.

Une fois que toutes ces étapes ont été réalisées sans erreurs, l'application est prête à l'emploi et aucun message complémentaire n'est affiché. Le fichier de configuration livré avec l'application contient tous les paramètres indispensables pour commencer à utiliser l'application.

N'oubliez pas de redémarrer le serveur Samba avant de commencer à utiliser le logiciel.

3.5. Disposition des fichiers dans les répertoires

Après l'installation de Kaspersky Anti-Virus, pour autant que tous les chemins d'accès proposés par défaut lors de l'installation aient été acceptés, les fichiers seront répartis de la manière suivante :

Pour le système d'exploitation Linux :

/etc/opt/kaspersky/ : répertoire contenant le fichier de configuration de Kaspersky Anti-Virus et d'autres fichiers de paramétrage :

kav4samba.conf : fichier de configuration.

/var/opt/kaspersky/kav4samba/bases et */var/opt/kaspersky/kav4samba/licenses* : répertoire contenant les bases antivirus et les clés de licence.

/opt/kaspersky/kav4samba/ : le répertoire principal de Kaspersky Anti-Virus reprenant :

/bin/ : le répertoire contenant les exécutables de l'ensemble des composants de Kaspersky Anti-Virus for Samba-servers :

kav4samba-kavscanner : l'exécutable de kavscanner (On-Demand Scanner), le composant de protection antivirus des serveurs de fichiers ;

kav4samba-licensemanager : fichier exécutable du composant license-manager de gestion des clés de licence.

kav4samba-keepup2date : l'exécutable du composant keepup2date chargé de la mise à jour des bases antivirus.

/sbin/kav4samba-kavsamba : fichier exécutable du composant de protection en temps réel kavsamba (On-Access Scanner).
/lib/bin/setup/kavsamba_setup.pl : script responsable de l'intégration au serveur Samba.

/share/man : répertoire contenant les fichiers man.

Afin d'activer le système d'aide de Kaspersky Anti-Virus (les pages manual), attribuez la valeur **/opt/kaspersky/kav4samba/share/man** à la variable MANPATH.

/opt/kaspersky/kav4samba/lib/ : répertoire contenant le module Samba pour les systèmes d'exploitation 32 bits.

/opt/kaspersky/kav4samba/lib64/ : répertoire contenant le module Samba pour les systèmes d'exploitation 64 bits.

/opt/kaspersky/kav4samba/share/contrib/kavsamba.wbm : répertoire contenant le module Webmin.

/opt/kaspersky/kav4samba/share/contrib/vox.sh : script de réparation des archives.

/opt/kaspersky/kav4samba/share/doc/ : répertoire de la licence et de la documentation sur Samba.

/opt/kaspersky/kav4samba/src/ : répertoire contenant le code source du module pour serveur Samba.

/var/opt/kaspersky/kav4samba/bases/ : répertoire contenant les bases antivirus.

/var/opt/kaspersky/kav4samba/bases.backup/ : répertoire contenant les copies de sauvegarde des bases antivirus (au cas où il faudrait revenir à l'état antérieur à la mise à jour des bases).

/var/log/kaspersky / : répertoire contenant les rapports (fichiers log) de fonctionnement des composants de l'application.

Pour le système d'exploitation FreeBSD :

/usr/local/etc/kaspersky/ : répertoire contenant le fichier de configuration de Kaspersky Anti-Virus et d'autres fichiers de paramétrage :

kav4samba.conf : fichier de configuration.

kav4samba.conf.default : fichier de configuration reprenant les paramètres par défaut.

/var/db/kaspersky/kav4samba/bases/ et */var/db/kaspersky/kav4samba/licenses/* : répertoires contenant les bases antivirus et les clés de licence.

/usr/local/ : répertoire système prévu pour l'installation de l'application par l'administrateur. Kaspersky Anti-Virus ajoute à ce dossier les fichiers exécutables de tous les composants :

kav4samba-kavscanner : l'exécutable de kavscanner (On-Demand Scanner), le composant de protection antivirus des serveurs de fichiers ;

kav4samba-licensemanager : fichier exécutable du composant license-manager de gestion des clés de licence.

kav4samba-keepup2date : l'exécutable du composant keepup2date chargé de la mise à jour des bases antivirus.

/usr/local/sbin/kav4samba-kavsamba : fichier exécutable du composant de protection en temps réel kavsamba (On-Access Scanner).

/usr/local/libexec/kaspersky/kav4samba/setup/kavsamba_setup.pl : script responsable de l'intégration au serveur Samba.

/usr/local/man/ : répertoire contenant les fichiers man.

/usr/local/lib/kaspersky/kav4samba/ : répertoire contenant le module Samba pour les systèmes d'exploitation 32 bits.

/usr/local/share/kav4samba/contrib/kavsamba.wbm : répertoire contenant le module Webmin.

/usr/local/share/kav4samba/contrib/vox.sh : script de réparation des archives.

/usr/local/share/doc/kav4samba/ : répertoire de la licence et de la documentation sur Samba.

/usr/local/src/kav4samba/ : répertoire contenant le code source du module pour serveur Samba.

/var/db/kaspersky/kav4samba/bases.backup/ : répertoire contenant les copies de sauvegarde des bases antivirus (au cas où il faudrait revenir à l'état antérieur à la mise à jour des bases).

/var/log/kaspersky/ : répertoire contenant les rapports (fichiers log) de fonctionnement des composants de l'application.

Pour les exemples présentés dans la suite de ce manuel, nous supposerons que Kaspersky Anti-Virus est installé sur un serveur tournant sous Linux.

3.6. Mise à niveau de la version du serveur Samba

La distribution de Kaspersky Anti-Virus contient les modules vfs binaires pour les versions de Samba prises en charge.

Si une nouvelle version de Samba Servers, incompatible avec Kaspersky Anti-Virus, est installée, il est possible de sélectionner manuellement le module vfs de l'application.

Pour ce faire :

Si vous utilisez Linux, saisissez dans la ligne de commande :

```
cd /opt/kaspersky/kav4samba/src
./configure --with-sambasrc=<path_to_samba> && make
```

où <path_to_samba> représente le chemin d'accès au module d'origine du serveur Samba.

Si vous utilisez FreeBSD, saisissez dans la ligne de commande :

```
cd /usr/local/src/kav4samba
```

./configure --with-sambasrc=<path_to_samba> && make

où <path_to_samba> représente le chemin d'accès au module d'origine du serveur Samba.

Le sous-répertoire **/lib** contiendra la version actualisée du module vfs. La configuration et l'installation de ce module incombent à l'administrateur.

3.7. Suppression de Kaspersky Anti-Virus

La désinstallation pour le serveur Samba requiert :

- Un utilisateur disposant de tous les privilèges (**root** ou autre utilisateur dont l'UID=0). Si vous ne disposez pas de ces privilèges au moment de la désinstallation, vous devrez absolument vous connecter en tant que **root**.
- L'arrêt du serveur Samba.

La désinstallation n'arrête pas automatiquement le fonctionnement du serveur Samba !

La suppression de Kaspersky Anti-Virus se déroulera automatiquement. La procédure peut être lancée de différentes manières en fonction de la distribution utilisée.

Si vous avez utilisé le paquetage RPM de Kaspersky Anti-Virus for Samba Servers lors de l'installation, saisissez la commande suivante pour lancer le processus de désinstallation :

```
rpm -e <nom_du_paquetage>
```

Si vous avez utilisé le paquetage deb de Kaspersky Anti-Virus for Samba Servers lors de l'installation, saisissez la commande suivante pour lancer le processus de désinstallation :

```
dpkg -r <nom_du_paquetage>
```

Etant donné les particularités du système d'exploitation Debian GNU/Linux, il est impossible de supprimer automatiquement les scripts d'administration de Kaspersky Anti-Virus. A la fin de la désinstallation, l'administrateur devra supprimer manuellement le script **/opt/kaspersky/kav4samba/lib/bin/kav4samba**.

Si vous avez utilisé le paquetage pkg de Kaspersky Anti-Virus for Samba Servers lors de l'installation, saisissez la commande suivante pour lancer le processus de désinstallation :

```
pkg_delete <nom_du_paquetage>
```

Si la procédure de désinstallation se déroule sans erreurs, aucune notification complémentaire ne sera fournie.

Si le module d'administration à distance de **Webmin** a été installé lors de l'installation de l'application, il faudra le supprimer manuellement.

Pour ce faire, sélectionnez l'onglet **Webmin Modules** dans la fenêtre principale de Webmin et dans la liste **Delete Modules**, choisissez la ligne **KAV for Samba Servers** avant de cliquer sur le bouton **Delete Selected Modules**.

CHAPITRE 4. CONFIGURATION DU LOGICIEL APRES L'INSTALLATION

Le système qui accueille Kaspersky Anti-Virus est analysé au cours de l'installation et certains paramètres de configuration du logiciel sont définis automatiquement. Il existe toute une série de paramètres du fichier de configuration de l'application qui sont définis par défaut comme étant les plus commodes pour l'utilisation de Kaspersky Anti-Virus (cf. point 4.1, p. 24).

Avant de commencer à utiliser l'application, il est conseillé d'installer ou d'actualiser les bases antivirus au cas où cela n'aurait pas été fait lors de l'installation !

Configurez également la coopération entre Kaspersky Anti-Virus et le paquet Webmin.

Ce chapitre présente les paramètres définis par défaut. Nous nous pencherons également en détail sur la configuration indispensable pour utiliser le logiciel.

4.1. Configuration de l'application par défaut

Tous les paramètres de fonctionnement de Kaspersky Anti-Virus sont repris dans le fichier de configuration de l'application utilisé par défaut.

Vous pouvez créer vos propres fichiers de configuration à utiliser lors de l'exécution de tâches particulières ou en tant que fichier de configuration par défaut.

Examinons en détail les paramètres définis par défaut dans le fichier de configuration. Sur la base de ces informations, vous pourrez décider si Kaspersky Anti-Virus doit être configuré davantage (cf. Chapitre 6, p. 42) afin d'être utilisé au maximum de ses capacités dans le contexte de votre entreprise.

Par défaut, la configuration de Kaspersky Anti-Virus est telle que le composant de protection antivirus en temps réel (*kavsamba*) commence à travailler dès le démarrage du système d'exploitation. Lors du lancement du composant d'analyse à la demande (*kavscanner*) sans arguments via la ligne de commande,

les répertoires et le système de fichiers de l'ordinateur sont soumis à la *recherche de virus*, en commençant par le répertoire actuel.

En cas de découverte de fichiers infectés, suspects ou endommagés, les notifications adéquates seront affichées sur la console du serveur ou consignées dans le fichier du rapport.

Nous attirons votre attention sur le fait que *LA REPARATION* des objets infectés *N'EST PAS REALISEE PAR DEFAUT* !

4.2. Installation des bases antivirus

La recherche de virus et la réparation des objets infectés s'opèrent sur la base des définitions contenues dans les bases antivirus. Les bases antivirus contiennent la définition de tous les programmes malveillants connus à ce jour et les moyens de réparer les objets qu'ils ont infectés. Il est dès lors primordial d'utiliser des bases antivirus à jour.

De nouveaux virus voient le jour quotidiennement. Il est vivement conseillé d'actualiser les bases antivirus **directement** après l'installation de l'application car les bases livrées avec la distribution ne sont déjà plus d'actualité au moment de l'installation.

Kaspersky Anti-Virus actualise les bases à l'aide du composant *keepup2date.* Pour lancer la mise à jour, saisissez la commande :

```
/chemin d'accès/à/kav4samba-keepup2date
```

Les bases antivirus seront téléchargées depuis les serveurs de mises à jour de Kaspersky Lab et sauvegardées dans le répertoire indiqué dans le fichier de configuration.

4.3. Configuration de la collaboration avec Webmin

Si vous envisagez l'administration à distance de Kaspersky Anti-Virus, nous vous conseillons de configurer sa collaboration avec Webmin.

Grâce à Webmin, il est possible par exemple de limiter l'accès au programme en introduisant des mots de passe.

Par défaut, tous les paramètres définis à distance par Webmin sont conservés dans le fichier de configuration de Kaspersky Anti-Virus, utilisé par défaut.

Si vous désirez créer un fichier de configuration alternatif à l'aide de Webmin, vous devrez :

1. Copier les données du fichier de configuration actuel dans un nouveau fichier qu'il faudra enregistrer absolument sous un autre nom. Modifier ensuite le contenu du nouveau fichier (alternatif) de configuration en fonction de vos besoins ;
2. Indiquer le nom du fichier de configuration alternatif dans le champ **Full path to KAV config** sur l'onglet **Config edit**.

Pour obtenir de plus amples informations sur les différents paramètres du programme Webmin , consultez la documentation qui s'y rapporte. Si vous avez des questions sur le module d'administration à distance de l'application, vous pouvez également consulter l'aide en ligne de Webmin.

La suite du présent manuel **ne fournit pas d'explication sur le lancement ou la configuration de tâche à distance via Webmin !**

4.4. Modes de fonctionnement recommandés

Kaspersky Lab vous propose quelques exemples de configuration pour une utilisation optimale de Kaspersky Anti-Virus for Samba Servers en fonction de la charge de votre serveur. Nous allons les aborder en détail.

4.4.1. Mode de fonctionnement optimal

Ce mode de fonctionnement permet d'atteindre l'équilibre parfait entre vitesse du serveur et niveau de sécurité.

Afin de configurer le logiciel pour le mode de fonctionnement optimal, modifiez le fichier de configuration de la façon suivante :

- Définissez la taille du cache de fichiers de manière à ce qu'il soit égal au nombre de fichiers accessibles via le serveur Samba. Nous vous rappelons qu'un enregistrement relatif à un fichier sain occupe environ 50 octets dans le cache. (section **[samba.options]** paramètre **FileCacheSize**).
- Définissez les paramètres de la section **[path]** de cette façon :

```
IcheckerDbFile=
/var/opt/kaspersky/kav4samba/ichecker.db
```

- Définissez les paramètres de la section **[samba.options]** de cette façon :

```
Packed=yes
Archives=yes
SelfExtArchives=yes
MailBases=yes
MailPlain=yes
Heuristic=yes
Cure=yes
Ichecker=yes
CheckFilesLimit=20
BgCheckFilesLimit=5
BgSheduleTime=10
HashType=md5
```

- Définissez les paramètres de la section **[samba.path]** de cette façon :

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
SambaConfigFile=/etc/samba/smb.conf
```

- Définissez les paramètres de la section **[samba.actions]** de cette façon :

```
OnInfected= MovePath /tmp/infected
OnSuspicion=MovePath /tmp/suspicious
OnWarning=MovePath /tmp/warning
```

- Définissez les paramètres de la section **[samba.shares]** de cette façon **:**

```
CheckOnOpen=yes
CheckOnClose=yes
```

De plus, assurez-vous que *kavscanner* exploite la technologie **iChecker** (section **[scanner.options]** paramètre **IChecker=yes**). De même, les composants *kavsamba* et *kavscanner* doivent utiliser des valeurs identiques pour les paramètres **Packed Archives SelfExtArchives MailBases MailPlain Heuristic** (sections **[scanner.options]** et **[samba.options]**).

4.4.2. Mode de vitesse d'exécution maximale

Ce mode met l'accent sur la vitesse d'exécution de l'application. Toutefois, la fiabilité de la protection antivirus est quelque peu réduite.

Il est conseillé de désactiver l'analyse des archives et de ne pas analyser les fichiers lors de la fermeture. Autrement dit, l'application n'analyse pas les archives qui pourraient être infectées. De même, il se peut que des objets infectés soient enregistrés sur le serveur. Ces objets seront analysés uniquement à l'ouverture (lorsque l'utilisateur réalise une opération de lecture).

Afin de configurer le logiciel pour ce mode de fonctionnement, modifiez le fichier de configuration de la façon suivante :

- Définissez les paramètres de la section **[samba.options]** de cette façon :

```
Ichecker=no
FileCacheSize=15000
CheckFilesLimit=0
HashType=crc32
```

- Définissez les paramètres de la section **[samba.shares]** de cette façon :

```
CheckOnOpen=yes
CheckOnClose=no
```

4.4.3. Mode de fiabilité maximale

Cette variante de la configuration permet d'obtenir la fiabilité maximale au niveau de la protection du serveur car les fichiers sont analysés aussi bien à la lecture qu'à l'écriture. Le fonctionnement de l'application sera toutefois quelque peu ralenti.

Afin de configurer le logiciel pour ce mode de fonctionnement, modifiez le fichier de configuration de la façon suivante :

- Définissez les paramètres de la section **[samba.options]** de cette façon :

```
Packed=yes
Archives=yes
SelfExtArchives=yes
```

```
MailBases=yes
MailPlain=yes
Heuristic=yes
Cure=yes
FileCacheSize=0
CheckFilesLimit=0
BgCheckFilesLimit=0
BgSheduleTime=0
HashType=md5
```

- Définissez les paramètres de la section **[samba.path]** de cette façon :

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
```

- Définissez les paramètres de la section **[samba.actions]** de cette façon :

```
OnInfected=remove
OnSuspicion=remove
OnWarning=remove
```

De plus, assurez-vous que *kavscanner* exploite la technologie **iChecker** (section **[scanner.options]** paramètre **IChecker=yes**). De même, les composants *kavsamba* et *kavscanner* doivent utiliser des valeurs identiques pour les paramètres **Packed Archives SelfExtArchives MailBases MailPlain Heuristic** (sections **[scanner.options]** et **[samba.options]**).

4.4.4. Mode d'analyse des fichiers souvent mis à jour

Ce mode est prévu pour la protection antivirus des dossiers partagés qui renferment des fichiers qui sont régulièrement mis à jour.

Le mode d'analyse des fichiers souvent mis à jour se distingue **du mode de fonctionnement recommandé** (cf. point 4.4.1, p. 26) par le fait que afin d'augmenter la vitesse d'exécution, les fichiers de certains dossiers partagés ne sont pas vérifiés après l'écriture (dans l'exemple repris ci-après, il s'agira du dossier public).

Pour ce type de dossiers, il est conseillé de désactiver l'analyse des fichiers qu'ils contiennent au moment de l'écriture. Ainsi, le contenu du dossier est analysé soit au moment où l'utilisateur tente d'y accéder, soit en arrière-plan.

Les paramètres généraux des autres dossiers sont identiques aux paramètres du **mode recommandé**.

Afin de configurer le logiciel pour ce mode de fonctionnement, modifiez le fichier de configuration de la façon suivante :

- Définissez les paramètres de la section **[path]** de cette façon :

```
IcheckerDbFile=
/var/opt/kaspersky/kav4samba/ichecker.db
```

- Définissez les paramètres de la section **[samba.options]** de cette façon :

```
Packed=yes
Archives=yes
SelfExtArchives=yes
MailBases=yes
MailPlain=yes
Heuristic=yes
Cure=yes
Ichecker=yes
FileCacheSize=20000
CheckFilesLimit=20
BgCheckFilesLimit=5
BgSheduleTime=10
HashType=md5
```

- Définissez les paramètres de la section **[samba.path]** de cette façon :

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
SambaConfigFile=/etc/samba/smb.conf
```

- Définissez les paramètres de la section **[samba.actions]** de cette façon :

```
OnInfected=remove
OnSuspicion=remove
OnWarning=remove
```

- Définissez les paramètres de la section **[samba.shares]** de cette façon :

```
CheckOnOpen=yes
CheckOnClose=yes
```

- Définissez les paramètres de la section **[samba.shares:public]** de cette façon :

```
CheckOnOpen=yes
CheckOnClose=no
```

CHAPITRE 5. UTILISATION DE KASPERSKY ANTI-VIRUS FOR SAMBA SERVERS

La protection antivirus est offerte aussi bien en temps réel qu'à la demande. Voici une description détaillée de ces deux modes.

Le mode de *protection en temps* réel est assuré par le composant *kavsamba* qui intercepte les requêtes adressées aux fichiers via le serveur Samba à l'ouverture et qui vérifie les fichiers en arrière-plan lors de leur fermeture. Le système recherche la présence éventuelle de virus et traite les fichiers en fonction des paramètres établis. L'accès aux fichiers jugés dangereux est bloqué.

Lors de *l'analyse à la demande*, réalisée par le composant *kavscanner*, il est possible de soumettre n'importe quel fichier à l'analyse (y compris les bases de messagerie, les archives, etc.). Le traitement des fichiers infectés dépendra des paramètres définis dans le fichier de configuration.

De plus, il convient de citer parmi les composants importants de la protection antivirus *la mise à jour des bases antivirus* par l'intermédiaire du composant *keepup2date*. Ce composant est chargé de l'actualisation des bases antivirus et des modules du logiciel localement ou à distance.

Remarquez que dans tous exemples présentés ci-après pour le composant *kavsamba*, il faudra toujours réinitialiser Kaspersky Anti-Virus à chaque fois que des modifications auront été apportées au fichier de configuration. Pour obtenir de plus amples informations sur le redémarrage, consultez le point 6.4 à la page 53.

5.1. Mise à jour des bases antivirus

L'actualisation des bases antivirus, réalisée à l'aide du composant *keepup2date* de l'application, est un élément incontournable pour offrir une protection complète. Les serveurs de mise à jour de Kaspersky Lab sont les serveurs d'où pourront être téléchargées les mises à jour des bases antivirus utilisées pour la recherche antivirus et la réparation des objets infectés. En voici quelques-uns :

http://downloads1.kaspersky-labs.com/

http://downloads2.kaspersky-labs.com/

ftp://downloads1.kaspersky-labs.com/, etc.

Le fichier *updcfg.xml*, inclus dans la distribution de l'application, reprend la liste des serveurs depuis lesquels il est possible de copier les mises à jour.

Au moment de la mise à jour, le composant *keepup2date* consulte cette liste, choisit une adresse et tente de télécharger les bases antivirus depuis le serveur. Lorsque l'adresse sélectionnée ne répond pas, le composant choisit l'adresse suivante et tente à nouveau de télécharger les bases antivirus.

Les versions actualisées des bases antivirus sont publiées plusieurs fois par heure sur les serveurs de mise à jour de Kaspersky Lab.

Une fois que la mise à jour a réussi, le système exécute la commande définie dans le paramètre **PostUpdateCmd** de la section **[updater.options]** du fichier de configuration. Par défaut, cette commande lance le rechargement automatique des bases antivirus. Toute modification erronée de ce paramètre peut entraîner un dysfonctionnement de l'application ou la non-utilisation des bases actualisées.

Tous les paramètres du composant *keepup2date* sont repris dans les options **[updater.*]** du fichier de configuration.

Au cas où la structure du réseau local serait relativement complexe, il est recommandé de télécharger les mises à jour toutes les heures depuis les serveurs, de les placer dans un répertoire quelconque du réseau et de configurer la copie des mises à jour depuis ce répertoire pour les ordinateurs locaux du réseau. Pour en savoir plus sur la création d'un répertoire de réseau, consultez le point 5.1.3 à la page 35.

Les mises à jour peuvent être programmées par l'intermédiaire de **cron** (cf. point 5.1.1, page 33) ou lancées à la demande de l'administrateur depuis la ligne de commande (cf. point 5.1.2, page 34).

Il est vivement conseillé de programmer l'actualisation des bases antivirus au moins une fois par heure !

La version 5.5 de Kaspersky Anti-Virus permet également de sélectionner les bases antivirus utilisées, ce qui permet de garantir la fiabilité optimale de la protection antivirus.

Bases antivirus standard : bases antivirus qui contiennent les définitions détaillées de tous les virus connus à ce jour ainsi que des méthodes de découverte et de réparation. Ces bases antivirus sont utilisées par défaut.

Bases antivirus élargies : ces bases antivirus contiennent, en plus des définitions de virus, des renseignements relatifs aux riskwares et aux logiciels publicitaires.

Les programmes du groupe à risque contiennent des failles qui peuvent être exploitées par les pirates informatiques ou qui permettent d'introduire des programmes non-autorisés, etc.

Les logiciels de diffusion de publicités sont installés en même temps qu'une application quelconque et diffusent ensuite des publicités, soit dans de nouvelles fenêtres, soit sur le site Internet sujet de la promotion. En plus des publicités forcées, ces programmes entraînent également une surcharge sensible des lignes de communication et augmentent le trafic total.

Les bases antivirus standard suffisent au mode de fonctionnement normal. Les bases étendues sont utilisées pour garantir une meilleure sécurité des informations. L'utilisation de bases antivirus plus complètes entraînent une augmentation des ressources nécessaires à l'analyse des données.

5.1.1. Mise à jour automatique des bases antivirus

Vous pouvez planifier la mise à jour régulière automatique des bases antivirus à l'aide du programme cron.

Tâche : configurer la mise à jour automatique des bases antivirus toutes les 3 heures. Consigner dans le journal système uniquement les erreurs survenues lors du fonctionnement du programme. Tenir un journal général pour tous les lancements de tâches, n'afficher aucune information sur la console.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Dans le fichier de configuration de l'application, définissez les paramètres requis, par exemple :

   ```
   [updater.options]
   KeepSilent=yes
   [updater.report]
   Append=yes
   ReportLevel=4
   ```

2. Editez le fichier qui définit les règles de fonctionnement du processus cron (**crontab –e**) à l'aide de la ligne :

```
0 0-23/3 * * */opt/kaspersky/kav4samba/bin/kav4samba-keepup2date
```

Tâche : configurer le téléchargement des mises à jour des bases antivirus depuis les sources de Kaspersky Lab. L'adresse du site sera choisie dans la liste livrée avec le composant *keepup2date*.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

Attribuez la valeur **No** au paramètre **UseUpdateServerUrl** de la section **[updater.options]**.

Tâche : configurer le téléchargement des mises à jour des bases antivirus depuis l'adresse indiquée par l'administrateur. Si le téléchargement des mises à jour au départ de cette adresse est impossible, interrompre la mise à jour.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

Attribuez la valeur **Yes** aux paramètres **UseUpdateServerUrl** et **UseUpdateServerUrlOnly** de la section **[updater.options]**. De plus, le paramètre **UpdateServerUrl** doit contenir l'adresse du serveur de mise à jour.

Tâche : configurer le téléchargement des mises à jour des bases antivirus depuis l'adresse indiquée par l'administrateur. Si la mise à jour au départ de cette adresse est impossible, se rabattre sur une adresse de la liste proposée par Kaspersky Anti-Virus.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

Attribuez la valeur **Yes** au paramètre **UseUpdateServerUrl** de la section **[updater.options]** et la valeur **No** au paramètre **UseUpdateServerUrlOnly**. De plus, le paramètre **UpdateServerUrl** doit contenir l'adresse du serveur de mise à jour.

5.1.2. Mise à jour à la demande des bases antivirus

La ligne de commande vous permet de lancer à n'importe quel moment la mise à jour des bases antivirus.

Tâche : lancer la mise à jour des bases antivirus et consigner les résultats de l'opération dans le fichier */tmp/updatesreport.log*.

Solution : pour exécuter cette tâche, veuillez saisir dans la ligne de commande :

```
# kav4samba-keepup2date -l /tmp/updatesreport.log
```

Si vous devez mettre à jour les bases antivirus sur plusieurs ordinateurs, il est plus facile de télécharger les bases une seule fois, de les sauvegarder dans un répertoire de réseau quelconque et de procéder ensuite à la mise à jour depuis ce répertoire.

Tâche : organiser la mise à jour des bases antivirus au départ du répertoire de réseau **/home/bases** ou depuis les serveurs de Kaspersky Lab au cas où ce répertoire serait inaccessible ou vide. Consigner les résultats dans le fichier report.txt.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Dans le fichier de configuration de l'application, définissez les paramètres requis :

   ```
   [updater.options]
   UpdateServerUrl=/home/bases
   UseUpdateServerUrl=yes
   UseUpdateServerUrlOnly=no
   ```

2. Saisissez dans la ligne de commande :

   ```
   # kav4samba-keepup2date -l /tmp/report.txt
   ```

5.1.3. Création d'un répertoire de réseau pour la conservation et la copie des bases antivirus

Pour que l'actualisation des bases antivirus au départ d'un répertoire de réseau réussisse, la structure des fichiers dans ce répertoire doit être en tout point conforme à la structure dans les serveurs de mise à jour de Kaspersky Lab. Voici la marche à suivre :

Tâche : créer un répertoire de réseau pour la copie ultérieure des bases antivirus sur les postes du réseau.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Créez un répertoire local.
2. Lancez le composant *keepup2date* de la manière suivante :

   ```
   # kav4samba-keepup2date -u <dir>
   ```

   où `<dir>` représente le chemin d'accès complet au répertoire créé.

3. Donnez aux postes locaux les privilèges de lecture dans ce répertoire.

Tâche : configurer la mise à jour des bases antivirus via un serveur proxy.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Dans la section **[updater.options]** du fichier de configuration, attribuez au paramètre **UseProxy** la valeur **Yes**.
2. Assurez-vous que le paramètre **ProxyAddress** dans la section **[updater.options]** du fichier de configuration contient l'adresse du serveur proxy. L'adresse doit être conforme au format suivant : **http://username:password@ip_address:port**. Les valeurs **ip_address** et **port** sont obligatoires, tandis que **username** et **password** sont nécessaires uniquement si le serveur proxy requiert une autorisation.

ou:

1. Dans la section **[updater.options]** du fichier de configuration, attribuez au paramètre **UseProxy** la valeur **Yes**.
2. Définissez la variable **http_proxy** au format **http://username:password@ip_address:port**. N'oubliez pas que cette variable sera prise en compte uniquement si le paramètre **UseProxy** de la section **[updater.options]** manque ou s'il possède la valeur **Yes**.

5.2. Protection antivirus en temps réel des serveurs Samba

Le composant *kavsamba*, qui surveille les requêtes adressées aux fichiers via le serveur Samba, prend en charge la protection antivirus en temps réel. *Kavsamba* démarre lors du lancement des services du système d'exploitation. Dès que *kavsamba* a analysé le fichier sollicité à l'aide du moteur antivirus intégré, il décide de l'action à prendre (autoriser ou non l'accès).

Le mode de réparation des objets infectés est désactivé par défaut. En d'autres termes, l'accès aux fichiers infectés, suspects ou endommagés est uniquement bloqué et les informations pertinentes sont intégrées au rapport.

Tous les paramètres du composant *kavsamba* sont repris dans les sections **[samba.*]** du fichier de configuration de l'application.
Vous pouvez activer différents modes de réparation des fichiers infectés, par exemple les déplacer dans un répertoire distinct, etc. Pour ce faire, il faut modifier les paramètres correspondants dans le fichier de configuration. Pour obtenir de plus amples informations, consultez le point 6.1.3 à la page 44.

5.2.1. Configuration des messages d'alerte de l'utilisateur

Dans la mesure où *kavsamba* fonctionne en arrière-plan, la console affiche uniquement les informations de démarrage et d'aide. Il est possible de personnaliser le mode de réception de ces messages d'alerte et de les envoyer via courrier électronique ou via l'utilitaire standard **smbclient**. Voici une description détaillée de cette fonction.

5.2.1.1. Surveillance et notification via smbclient

L'utilitaire standard **smbclient** sert au transfert des messages **winpopup** à l'ordinateur local. Sous Windows, ce type de message (**winpopup**) apparaît à l'écran de l'utilisateur pour autant que le service de messagerie ait été activé. Dans plusieurs cas, cet utilitaire est installé automatiquement mais avant de commencer à utiliser l'application, il faut s'assurer que **smbclient** est installé.

Cette possibilité est très utile pour avertir les utilisateurs en cas de tentative d'accès à un fichier infecté via le serveur Samba.

Vous trouverez ci-après un exemple illustrant ce mode d'alerte :

Tâche : afficher sur l'écran de l'utilisateur un message d'alerte en cas de tentative d'accès à un fichier infecté via le serveur Samba.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Définissez l'action à réaliser sur le fichier infecté (dans ce cas, il s'agit de l'affichage d'une notification). Pour ce faire, saisissez la ligne suivante dans la section **[samba.notify]** du fichier de configuration en guise d'action :

```
OnInfected=exec echo "%USER%
%FULLPATH%/%FILENAME% is infected by %VIRUSNAME%"
| smbclient -M %USERHOST%
```

2. Redémarrez Kaspersky Anti-Virus.

5.2.1.2. Surveillance et notification via courrier électronique

Si vous optez pour la surveillance avec alerte via courrier électronique, les avertissements relatifs aux tentatives d'accès à des fichiers infectés ou suspects seront repris dans le corps du message envoyé à l'adresse indiquée.

Le système de messagerie doit être configuré si vous souhaitez recevoir les notifications par courrier électronique !

Tâche : avertir l'administrateur qu'un utilisateur a tenté d'accéder à un fichier infecté ou suspect via le serveur Samba.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Spécifiez l'action à exécuter sur l'objet infecté. Pour ce faire, saisissez la ligne suivante dans la section **[samba.notify]** du fichier de configuration en guise d'action :

```
OnInfected=exec echo "%USER%
%FULLPATH%/%FILENAME% from %USERHOST% is infected
by %VIRUSNAME%" | mail -s 'Virus notification'
spam-virus@localhost.ru
OnWarning=exec echo "%USER% %FULLPATH%/%FILENAME%
from %USERHOST% is probably infected by
%VIRUSNAME%" | mail -s 'Virus notification' spam-
virus@localhost.ru
OnSuspicion=exec echo "%USER%
%FULLPATH%/%FILENAME% from %USERHOST% is probably
infected by %VIRUSNAME%" | mail -s 'Virus notifi-
cation' spam-virus@localhost.ru
```

N'oubliez pas de redémarrer Kaspersky Anti-Virus (cf. point 6.4, p. 53).

5.3. Protection antivirus des systèmes de fichiers

L'analyse à la demande peut être lancée exclusivement par l'utilisateur **root** !

La protection antivirus des systèmes de fichiers du serveur est prise en charge par le composant *kavscanner*. Celui-ci recherche la présence éventuelle de virus dans les fichiers du serveur et traite les objets infectés et/ou suspects en fonction des paramètres établis. Le traitement des objets peut avoir un caractère exclusivement informatif (saisie des informations dans le rapport et envoi d'un message sur la console du serveur, alerte de l'administrateur) ou peut entraîner des modifications (réparation, déplacement dans un répertoire distinct, suppression).

Tous les paramètres du composant *kavscanner* sont repris dans les sections **[scanner.*]** du fichier de configuration de l'application.

Par défaut, *kavscanner* avertit uniquement l'utilisateur/administrateur de la découverte d'objets infectés. Pour obtenir de plus amples informations sur la configuration des actions à exécuter sur un fichier, consultez le point 6.2.3 à la page 49.

L'administrateur peut analyser les systèmes de fichiers du serveur de façon ponctuelle via la ligne de commande ou automatiquement selon un horaire établi à l'aide de l'utilitaire **cron**. Vous pouvez analyser aussi bien l'ensemble des systèmes de fichiers du serveur que des répertoires distincts. Il est possible également d'analyser les secteurs des disques.

Nous allons maintenant passer en revue quelques-unes des tâches les plus fréquentes dans le cadre de la protection antivirus des systèmes de fichiers d'un serveur.

La recherche de la présence éventuelle de virus est un processus qui peut monopoliser beaucoup de ressources si elle est porte sur tout l'ordinateur. Il convient de rappeler que cette opération ralentira l'activité du serveur. Pour cette raison, il est préférable de procéder à l'analyse quand la charge du serveur est à son niveau le plus bas.

5.3.1. Analyse des fichiers à la demande

La recherche de la présence éventuelle de virus dans un répertoire distinct du serveur et la réparation des fichiers infectés figurent parmi les tâches que peut exécuter Kaspersky Anti-Virus.

Tâche : lancer l'analyse du répertoire **/tmp** avec la réparation automatique de l'ensemble des objets infectés qui auront été identifiés. Supprimer tous les objets qui n'auront pas pu être réparés.

Les résultats de l'opération (date d'exécution, renseignements sur tous les fichiers, à l'exception des fichiers sains) seront repris uniquement dans le fichier-rapport *kavscanner-date_du_jour.log* sauvegardé dans le même répertoire.

Solution : pour exécutez cette tâche, saisissez dans la ligne de commande :

```
#./kav4samba-kavscanner -rlq
-o kavscanner-`date +%F`.log -i3 -ePASBME -j3 -mCn
/tmp
```

5.3.2. Analyse programmée d'un répertoire (cron)

L'utilitaire **cron** de lancement automatique de programmes vous permet de définir l'exécution automatique de n'importe quelle tâche de Kaspersky Anti-Virus for Samba Servers, y compris l'analyse d'un répertoire.

Tâche : lancer chaque jour à 0h00 l'analyse du répertoire /home. Utiliser les paramètres d'analyse spécifiés dans le fichier de configuration /etc/kav/kavscaner.cron.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Créez le fichier de configuration */etc/kav/kavscaner.cron* dans lequel vous définirez tous les paramètres d'analyse indispensables.
2. Editez le fichier qui définit les règles de fonctionnement du processus cron (**crontab –e**) : insérez la ligne suivante :

```
0 0 * * * /path/to/kav4samba-kavscanner -c
/etc/kav/kavscaner.cron /home
```

5.3.3. Autres possibilités : utilisation de fichiers de script

Kaspersky Anti-Virus vous permet d'utiliser diverses commandes Unix/Linux standard ainsi que des fichiers de script pour réaliser un traitement supplémentaire des objets analysés. Grâce à ces outils, les administrateurs expérimentés peuvent définir eux-mêmes les actions à exécuter sur les objets aux statuts divers, élargissant ainsi les fonctionnalités de Kaspersky Anti-Virus.

5.3.3.1. Envoi de messages d'alerte à l'administrateur

L'utilisation conjointe de Kaspersky Anti-Virus et des outils Unix/Linux traditionnels vous permet de configurer les messages d'alerte envoyés à l'administrateur du serveur en cas de découverte de fichiers infectés, suspects ou endommagés dans les systèmes de fichiers.

Tâche : configurer les messages d'alerte envoyés à l'administrateur en cas de découverte d'archives et de fichiers infectés dans les systèmes de fichiers à chaque analyse du serveur réalisée conformément aux paramètres du fichier de configuration de l'application.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

Dans le fichier de configuration de l'application, spécifiez les règles de traitement des objets simples et des conteneurs :

```
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is
infected by %VIRUSNAME% | mail -s kav4samba-
kavscanner admin@localhost.ru
[scanner.container]
```

OnInfected=exec echo archive %FULLPATH%/%FILENAME% is infected, viruses list is in the attached file %LIST% | mail -s kav4samba-kavscanner -a %LIST% admin@localhost.ru

CHAPITRE 6. CONFIGURATION COMPLEMENTAIRE

Ce chapitre aborde en détail les possibilités de configuration supplémentaires de Kaspersky Anti-Virus. Contrairement aux paramètres indispensables définis lors de l'installation (cf. point 3.3, p. 17) et sans lesquels il est impossible d'utiliser l'application, les paramètres complémentaires sont définis par l'administrateur en fonction de ses besoins. Les possibilités de l'application sont ainsi étendues et cette dernière peut être plus facilement intégrée au cadre opérationnel concret d'une entreprise.

6.1. Configuration de la protection antivirus en temps réel

Comme vous l'avez lu plus haut, c'est le composant *kavsamba* qui prend en charge la protection antivirus en temps réel des serveurs Samba.

La configuration du composant permet de personnaliser les paramètres suivants :

- Zone d'analyse : le chemin et les objets à protéger (cf. point 6.1.1, p. 42).
- Le mode d'analyse et de réparation des fichiers (cf. point 6.1.2, p. 43).
- Les actions exécutées sur les fichiers (cf. point 6.1.3, p. 44).
- Le mode de copie de sauvegarde (cf. point 6.1.5, p. 50).
- La composition des rapports et des notifications (cf. point 6.5, p. 55).

6.1.1. Zone de surveillance

La zone d'analyse du composant *kavsamba* comporte le *chemin d'accès* et les *objets à protéger*.

Le *chemin d'accès* fait référence à l'ensemble des systèmes de fichiers auxquels l'utilisateur peut accéder via le serveur Samba. Il est possible d'exclure certains répertoires et fichiers dans le fichier de configuration de l'application (section **[samba.options]**, paramètres **ExcludeMask** et **ExcludeDirs**).

Les *objets à protéger* (les types de fichiers qui seront soumis à l'analyse antivirus) sont définis uniquement par les paramètres du fichier de configuration de l'application dans la section **[samba.options]**.

Lors du lancement de *kavsamba*, vous ne pouvez pas utiliser la ligne de commande pour définir ou limiter la zone de surveillance. Cette option est disponible uniquement pour l'analyse antivirus des systèmes de fichiers du serveur (composant *kavscanner*).

6.1.2. Mode d'analyse et de réparation des fichiers

Kavsamba prend en charge les deux opérations d'accès au fichier suivantes : ouverture et fermeture. Par défaut, tous les fichiers qui ne sont pas vides sont analysés à l'ouverture tandis qu'à la fermeture, ils sont vérifiés uniquement s'ils ont été modifiés.

La réparation des fichiers infectés découverts est désactivée par défaut. Autrement dit, l'utilisateur et/ou l'administrateur est uniquement averti de la découverte de virus et d'objets suspects. La notification prend la forme d'une entrée dans le fichier du rapport (cf. point 6.6, p. 55). L'accès à ces objets est bloqué automatiquement.

L'activation du mode de réparation des objets infectés s'opère à l'aide du fichier de configuration (section **[samba.options]**, paramètre **Cure=yes**). Si *kavsamba* repère un fichier infecté (un fichier dont le statut est **Infected**) lors de l'analyse, il agira en fonction des paramètres définis dans le fichier de configuration (cf. point 6.1.3, p. 44).

Après l'analyse (et la réparation), le fichier reçoit un des statuts suivants :

- **Clear** : le fichier n'est pas infecté.
- **Infected** : le fichier est infecté.
- **Cured** : le fichier infecté a bien été réparé.
- **CureFailed** : le fichier infecté n'a pas pu être réparé.
- **Warning** : le code du fichier ressemble à celui d'un virus connu.
- **Suspicion** : le fichier pourrait être infecté par un virus inconnu.
- **Protected** : le fichier ne peut pas être analysé car il est crypté.
- **Corrupted** : le fichier est corrompu.

En fonction du statut attribué, l'accès au fichier sera interdit (**Infected**, **CureFailed, Warning, Suspicion**) ou autorisé (tous les autres états).

Les fichiers qui ont reçu le statut **CureFailed** sont traités comme des objets infectés !

N'oubliez pas que pour accélérer l'analyse des objets conteneurs (archives), *kavsamba* arrête l'analyse après le premier virus découvert dans l'archive et lui attribue le statut **Infected**. Autrement dit, même si l'objet est infecté par plusieurs virus, *kavsamba* en indiquera uniquement un seul dans le journal.

6.1.3. Actions exécutées sur les fichiers

Pour les fichiers correspondant à l'état **Infected**, **Suspicious**, **Warning**, **Cured**, **Protected**, **Corrupted** ou **Error**, il est possible de définir l'exécution d'actions telles que :

- *transfert dans un répertoire quelconque* : les fichiers dont le statut correspond à un statut défini sont déplacés dans un autre répertoire. Vous avez le choix entre transfert *simple* et transfert *récursif* ;
- *Suppression* du fichier du système de fichiers ;
- *Exécution d'une certaine commande* : traitement des fichiers à l'aide de commandes Linux standard, de fichiers de script, etc.

Remarquez que *kavsamba* n'opère pas de distinction entre les actions à exécuter sur des fichiers ou celles à exécuter sur des objets conteneurs. Ceci explique pourquoi il peut arriver que le rapport indique pour un objet infecté le nom de plusieurs virus.

Vous pouvez configurer les règles de traitement des objets de l'une des deux manières suivantes :

- Indication dans le fichier de configuration de l'application si vous souhaitez les appliquer par défaut (section **[samba.actions]**).
- Indication des règles de traitement dans un fichier de configuration alternatif que vous utiliserez au moment du lancement du composant.

N'oubliez pas que le répertoire de réseau /**homes** est un répertoire virtuel qui fait référence aux répertoires principaux de tous les utilisateurs. Il ne faut pas définir des paramètres particuliers de protection antivirus pour de tels répertoires.

C'est la raison pour laquelle la définition des paramètres de protection des répertoires principaux des utilisateurs s'opère dans la section **[samba.shares]**. Si la protection antivirus dans la section **[samba.shares]** est désactivée, les répertoires principaux des utilisateurs ne seront pas protégés.

6.1.4. Isolement des objets infectés

Le déplacement des fichiers infectés dans un répertoire distinct permet de les isoler (section **[samba.actions]** paramètre **MovePath**). Le transfert a lieu lorsque la réparation du fichier a échoué (par exemple, seuls 2 des 3 virus qui infectaient un fichier ont pu être éliminés).

L'administrateur peut décider de déplacer les objets dans des répertoires différents en fonction du statut du fichier.

Au cas où vous auriez l'intention de conserver un tel répertoire, il est conseillé de l'exclure de l'analyse à l'aide du paramètre **ExcludeDirs** (section **[samba.options]**) dans le fichier de configuration.

Tâche : rechercher la présence éventuelle de virus dans tous les fichiers appelés via le serveur Samba et réparer, le cas échéant, les objets infectés. En cas d'échec de la réparation, déplacer les objets infectés avec le chemin d'accès complet dans le répertoire **/tmp/infected**.

Solution : réalisez les opérations suivantes pour exécuter cette tâche :

1. Activez le mode de réparation des objets infectés dans le fichier de configuration (paramètre **Cure=yes** de la section **[samba. options]**).
2. Définissez la règle d'isolement des objets infectés. Pour ce faire, saisissez la ligne suivante dans la section **[samba.actions]** du fichier de configuration :

   ```
   OnInfected=MovePath /tmp/infected
   ```

3. Redémarrez Kaspersky Anti-Virus (cf. point 6.4, p. 53).

6.1.5. Mode de copie de sauvegarde des objets

Si l'objet analysé est infecté et que l'action sélectionnée est la suppression dans le système de fichiers, le risque existe de perdre des données importantes. Pour éviter cela, Kaspersky Anti-Virus offre la possibilité de copier les fichiers dans le répertoire backup.

Avant qu'un fichier ne soit réparé ou effacé, une copie est créée dans le répertoire de sauvegarde (section **[samba.path]**, paramètre **BackupPath**). Vous disposerez ainsi d'une copie de sauvegarde (et de la possibilité de restaurer le fichier d'origine) au cas où le fichier serait corrompu lors de la réparation. Le fichier est conservé dans le répertoire de sauvegarde avec le chemin complet. Lorsqu'un fichier est enregistré à nouveau au même endroit, la copie la plus récente remplace automatiquement la copie précédente.

Attention : le mode d'enregistrement dans le dossier de sauvegarde n'est pas activé par défaut et pour cette raison, le chemin d'accès au répertoire où seront conservées les copies de sauvegarde n'est pas défini. Vous devrez le définir vous-même si vous souhaitez exploiter cette possibilité.

Lorsqu'un objet est supprimé du système de fichiers, sa copie est conservée jusqu'au moment où l'administrateur décidera de la supprimer également.

6.2. Configuration de la protection antivirus des systèmes de fichiers

La protection antivirus des systèmes de fichiers du serveur est prise en charge par *kavscanner*. Le fichier de configuration de l'application renferme les paramètres de fonctionnement, adoptés par défaut, du composant *kavscanner* (section **[scanner]**). Ils ont été établis pour fournir un degré maximum d'analyse des systèmes de fichiers accessibles depuis le poste de travail sur lequel est installé le logiciel. La recherche de la présence éventuelle de virus porte sur tous les fichiers accessibles, y compris :

- Les fichiers compressés ;
- Les archives ;
- Les archives auto-extractibles ;

- Les bases de données de messagerie électronique ;
- Les messages électroniques.

Les paramètres de la protection antivirus des systèmes de fichiers du serveur peuvent être répartis en trois groupes qui définissent respectivement :

- La zone d'analyse (cf. point 6.2.1, p. 47) (ce paramètre est semblable à la zone de surveillance dans le cadre de la protection en temps réel).
- Le mode d'analyse et de réparation des fichiers (cf. point 6.2.2, p. 48).
- Les actions exécutées sur les fichiers (cf. point 6.2.3, p. 49).

Examinons en détail les paramètres de chacun de ces groupes.

6.2.1. Zone d'analyse

La zone d'analyse peut être divisée en deux parties :

- Le *chemin d'analyse* : la liste des répertoires et des fichiers soumis à l'analyse antivirus ;
- Les *objets à analyser* : les types de fichiers qui seront soumis à l'analyse antivirus (archives, messages électroniques, etc.).

Par défaut, l'analyse porte sur tous les objets des systèmes de fichiers accessibles, à commencer par le répertoire actuel.

Afin de pouvoir vérifier l'ensemble des systèmes de fichiers du serveur, il faut impérativement revenir au répertoire racine ou indiquer la zone d'analyse dans la ligne de commande.

Vous pouvez redéfinir le chemin d'analyse de l'une des manières suivantes :

- En reprenant les répertoires et les fichiers avec leur chemin absolu et relatif (par rapport au répertoire actuel) directement dans la ligne de commande lors du lancement du composant, séparés par un espace.
- En spécifiant le chemin d'analyse dans un fichier texte et en sélectionnant ce dernier via la ligne de commande grâce à l'argument **-@ <nom_fichier>**. Chaque objet dans un tel fichier figure sur une nouvelle ligne avec son chemin d'accès absolu.

Lorsque la ligne de commande reprend à la fois le chemin d'analyse et le fichier texte avec la liste des objets à analyser, les objets indiqués dans la ligne de commandes sont analysés avant ceux du fichier.

- En introduisant dans le fichier de configuration de l'application les masques des fichiers et des répertoires qui seront exclus de la zone d'analyse (section **[scanner.options]**, paramètres **ExcludeMask** et **ExcludeDirs**), ce qui a pour effet de limiter le nombre de chemins, qu'il s'agisse des chemins par défaut (tous, en commençant par le répertoire en cours) ou de ceux énumérés dans la ligne de commande.
- En désactivant la *vérification récursive des répertoires* (section **[scanner.options]**, paramètre **Recursion** ou argument **–r**).
- En ayant créé un fichier de configuration alternatif et en ayant précisé son utilisation à l'aide de l'argument **–c <nom_fichier>** au moment du lancement du composant.

Les objets à analyser sont eux aussi indiqués par défaut dans le fichier de configuration de l'application (section **[scanner.options]**) et peuvent être redéfinis via :

- Des arguments de la ligne de commande au moment du lancement du composant ;
- L'utilisation d'un fichier de configuration alternatif.

6.2.2. Mode d'analyse et de réparation des fichiers

Le mode d'analyse et de réparation des fichiers pour le composant *kavscanner* est en tout point identique à celui du composant *kavsamba*, si ce n'est que *kavscanner* exécute diverses actions sur les fichiers dont l'état est **Corrupted** (pour de plus amples informations sur les actions, consultez le point 6.1.3 à la page 44).

Nous vous rappelons que la réparation est désactivée par défaut. Les seules actions possibles sont l'analyse antivirus et la notification, sur la console ou dans le rapport, en cas de découverte d'objets infectés, suspects ou endommagés.

Suite à l'analyse antivirus, chaque fichier reçoit un statut quelconque (**Clear**, **Infected**, **Warning**, etc.) qui déclenche l'exécution de l'action définie dans le fichier de configuration.

Lorsque le mode de réparation est activé (section **[scanner.options]**, paramètre **Cure=yes**), les tentatives de réparation porteront sur le fichier dont le statut est **Infected**.

6.2.3. Actions exécutées sur les fichiers

Les actions exécutées sur les fichiers dépendent du statut qui leur a été attribué. Par défaut, la seule action possible est l'avertissement de la découverte de fichiers avec tel ou tel statut via des notifications affichées sur la console ou consignées dans le rapport.

Toutefois, pour les fichiers correspondant à l'état **Infected**, **Suspicious**, **Warning**, **Cured**, **Protected**, **Corrupted** ou **Error** (il est possible, tout comme pour *kavsamba*) de définir l'exécution d'actions telles que :

- *transfert dans un répertoire quelconque* : les fichiers dont le statut correspond à un statut défini sont déplacés dans un autre répertoire. Vous avez le choix entre transfert *simple* et transfert *récursif* (*avec chemin complet)* ;
- *Suppression du fichier* du système de fichiers ;
- *Exécution d'une certaine commande* : traitement des fichiers à l'aide de commandes Unix/Linux standard, de fichiers de script, etc.

Lors de l'analyse des systèmes de fichiers du serveur, le composant *kavscanner* de Kaspersky Anti-Virus opère une distinction entre les objets *simples* (un fichier) et les *objets conteneurs* (qui renferment plusieurs autres objets, exemple : les archives). Les actions exécutées sur de tels objets diffèrent également et sont définies dans deux sections distinctes du fichier de configuration. Pour les objets simples, il s'agit de la section **[scanner.object]**, tandis que pour les conteneurs, il s'agit de la section **[scanner.container]**.

Les actions réservées aux archives auto-extractibles peuvent varier également : s'il s'agit de l'archive elle-même qui est infectée, elle sera considérée comme un objet simple. Si l'infection touche un des objets inclus dans l'archive, alors elle sera considérée comme un objet conteneur. Par conséquent, les actions sur cette archive seront régies par des paramètres définis dans différentes sections du fichier de configuration.

Il est possible de préciser l'action à exécuter sur un fichier quelconque :

- Via le fichier de configuration de l'application si vous souhaitez les appliquer par défaut (sections **[scanner.object]** et **[scanner.container]**).
- Via un fichier de configuration alternatif que vous utiliserez au moment du lancement du composant.
- Via un argument de la ligne de commande au cours de la session en cours au moment du lancement du composant *kavscanner.*

6.2.4. Mode de copie de sauvegarde

La configuration du processus de création de copies de sauvegarde lors de l'analyse antivirus des systèmes de fichiers est identique à celle indiquée au point 6.1.5 de la page 46 dans le cadre de la protection antivirus en temps réel. Dès lors, nous ne nous attarderons pas ici sur la configuration de ce mode.

Tâche : procéder à l'analyse antivirus de tous les objets contenus dans les répertoires et des fichiers repris dans le fichier */tmp/download.lst* et procéder, le cas échéant, à leur réparation. En cas d'échec de la réparation, déplacer les objets infectés et suspects avec les chemins complets respectivement dans les répertoires **/tmp/infected** et **/tmp/suspicious** et les avertissements dans **/tmp/warning**.

Solution : suivez les étapes décrites ci-après pour exécuter cette tâche :

1. Créez le fichier de configuration alernatif *scan_sample.conf*
2. Vérifiez que le mode réparation des objets infectés est bel et bien activé (**Cure=yes** dans la section **[scanner.options]**).
3. Spécifiez les règles de traitement des objets infectés. Pour ce faire, définissez les paramètres suivants dans les sections **[scanner.object]** et **[scanner.container]** du fichier de configuration *scan_sample.conf* :

```
OnInfected=MovePath /tmp/infected
OnSuspicion=MovePath /tmp/suspicious
OnWarning=MovePath /tmp/warning
```

4. Saisissez dans la ligne de commande :

```
# kav4samba-kavscanner - -@/tmp/downloads.lst  -c
sample_scan.conf
```

6.3. Optimisation du fonctionnement de Kaspersky Anti-Virus for Samba Servers

Afin de réduire la charge à laquelle est soumis le serveur, le fonctionnement de Kaspersky Anti-Virus for Samba Servers peut être optimisé de plusieurs manières. Nous allons les aborder en détail.

Utilisation des bases de données iChecker et du cache de fichiers analysés.

Cette application exploite diverses technologies qui permettent de ne pas devoir procéder à une analyse antivirus chaque fois que le fichier est appelé et qui préfèrent les méthodes reposant sur la comparaison des données existantes relatives à ce fichier. L'algorithme d'analyse antivirus de l'objet (fichier) fonctionne de la manière suivante :

Lors de la première analyse de n'importe quel fichier, les informations qui s'y rapportent (nom, somme de contrôle) sont stockées dans une de ces bases de données :

- La base de données iChecker est une base générale qui contient les informations relatives aux fichiers analysés et sains de certains formats. Cette base contient des informations relatives à tous les objets, qu'ils aient été analysés par le composant *kavsamba* ou *kavscanner*.
- Le cache des fichiers analysés est une base de données qui contient les informations relatives aux fichiers analysés par *kavsamba*. Cette base existe dans la mémoire vive et elle est supprimée à la fin du travail du composant *kavsamba*.

Ainsi, lorsque l'information récoltée sur un fichier lors de l'analyse ne peut être sauvegardée dans la base iChecker (soit le fichier est infecté, soit son format n'est pas pris en charge), elle est sauvegardée dans le cache.

Par la suite, chaque fois que l'utilisateur appellera ce fichier, une recherche sera lancée tout d'abord dans la base iChecker, puis ensuite (lorsque l'objet n'a pas été trouvé dans la première base de données) dans le cache. Le nom du fichier constitue le critère de recherche. Si une des bases renferme des informations à propos de ce fichier, elles sont comparées aux informations actuelles du fichier. Si l'état actuel du fichier correspond parfaitement à sa description dans la base de données, le système considère que le fichier est inchangé et ne procède pas à l'analyse antivirus.

Par contre, une analyse antivirus complète du fichier sera lancée lorsque aucune des deux bases de données (la base iChecker et le cache) ne contient des informations relatives au fichier appelé.

Si vous avez modifié la sélection de bases antivirus utilisées, il faudra supprimer manuellement les informations de la base iChecker (le chemin d'accès complet à la base est défini par le paramètre **IcheckerDbFile** de la section **[path]** du fichier de configuration de l'application.

Cela s'explique par le fait que la base peut contenir des objets infectés qui n'ont pas été identifiés par les bases antivirus standard mais bien par les bases

antivirus étendues. Les fichiers dont les informations sont reprises dans la base iChecker ne sont pas analysés à nouveau, ce qui peut entraîner l'infection de l'ordinateur.

Analyse en arrière-plan.

Dans la mesure où la recherche d'informations sur les objets appelés dans les bases de données décrites ci-dessus est très rapide, la charge du serveur est considérablement réduite, ce qui permet d'utiliser encore plus efficacement les possibilités du serveur en introduisant : *l'analyse en arrière-plan des fichiers*.

Lorsqu'il tourne, Kaspersky Anti-Virus détermine la charge du serveur. Si celle-ci est inférieure à une valeur prédéfinie, l'application vérifie en arrière-plan les fichiers contenus dans les répertoires partagés, ainsi que les fichiers qui ont été modifiés au cours du travail.

La charge détermine le nombre maximum de fichiers qui peuvent être analysés simultanément (section **[samba.options]** paramètre **CheckFilesLimit**). Elle détermine également le nombre de fichiers analysés simultanément en arrière-plan (section **[samba.options]** paramètre **BgCheckFilesLimit**) et l'intervalle à l'issue duquel un nouveau fichier est soumis à l'analyse antivirus (section **[samba.options]** paramètre**BgSheduleTime**).

Lorsque le nombre de fichiers à analyser dépasse la valeur maximale autorisée, les fichiers analysés une nouvelle fois sont placés dans la file d'attente et ne seront pas analysés tant que la charge n'est pas repassée au-dessous de la valeur admise.

Dans ce cas, les utilisateurs à l'origine de la requête d'analyse attendront la réponse un peu plus longtemps que prévu. A la fin de l'analyse, le fichier est supprimé de la file d'attente. Aucun message complémentaire n'est affiché dans ce cas.

Si la fréquence des requêtes n'est pas définie (**BgSheduleTime=0**), l'analyse en arrière-plan n'aura pas lieu.

La charge maximale autorisée sur le serveur est ainsi déterminée.

6.4. Redémarrage de Kaspersky Anti-Virus

A chaque redémarrage de Kaspersky Anti-Virus, l'accès à **[samba.shares],** protégé par Kaspersky Anti-Virus sera bloqué.

Le redémarrage de Kaspersky Anti-Virus peut s'opérer de plusieurs manières :

- Le redémarrage "à chaud", recommandé après l'actualisation des bases antivirus.

  Dans ce cas, les bases antivirus sont rechargées et toutes les connexions sont maintenues. Le composant *kavsamba* n'est pas relancé, ce qui veut dire que le cache des fichiers est préservé, etc.

  Pour effectuer un redémarrage "à chaud" saisissez la commande suivante :

  Pour les distributions de Linux :

  ```
  /etc/init.d/kav4samba reload_avbase
  ```

  Pour les distributions de FreeBSD :

  ```
  /usr/local/etc/rc.d/kav4samba.sh reload_avbase
  ```

  Dans ce cas, le processus *kavsamba* reçoit le signal **SIGUSR1**.

- Le redémarrage "à froid", recommandé après la modification du fichier de configuration, des paramètres ou après l'installation d'une nouvelle clé de licence.

  Dans ce cas, le fichier de configuration et les bases sont relus et toutes les connexions avec l'utilisateur sont interrompues car l'application s'arrête avant de redémarrer.

  Pour effectuer un redémarrage "à froid" saisissez la commande suivante :

  Pour les distributions de Linux :

  ```
  /etc/init.d/kav4samba reload
  ```

  Pour les distributions de FreeBSD :

  ```
  /usr/local/etc/rc.d/kav4samba.sh reload
  ```

  Dans ce cas, le processus *kavsamba* reçoit le signal **SIGHUP**.

- L'arrêt forcé de Kaspersky Anti-Virus est obtenu en saisissant la commande suivante :

Pour les distributions de Linux :

```
/etc/init.d/kav4samba stop
```

Pour les distributions de FreeBSD :

```
/usr/local/etc/rc.d/kav4samba.sh stop
```

La commande envoie au processus *kavsamba* le signal **SIGTERM** qui entraîne l'arrêt de *kavsamba* avec la fermeture de toutes ses copies engendrées et Kaspersky Anti-Virus s'arrête correctement.

Il est fortement déconseillé de ne pas arrêter le processus *kavsamba* à l'aide de la commande **kill –9**. Cette commande entraînerait l'arrêt du processus sans toutefois éliminer toute une série de fichiers temporaires et de travail qu'il faudrait supprimer manuellement. Lorsque ces fichiers ne sont pas supprimés, certaines applications estiment que le processus est en cours.

6.5. Adaptation du format d'affichage de la date et de l'heure

Kaspersky Anti-Virus génère au cours de son activité des rapports pour chacun de ses composants ainsi que toute une série de notifications destinées aux utilisateurs et aux administrateurs. Cette information s'accompagne toujours de la date et de l'heure à laquelle elle a été enregistrée.

Kaspersky Anti-Virus utilise par défaut les formats de date et d'heure qui répondent à la norme strftime :

%H:%M:%S : format d'affichage de l'heure (hh.mm.ss).

%d/%m/%y : format d'affichage de la date (jj.mm.aa).

Vous pouvez, si vous le souhaitez, modifier le format d'affichage de la date et de l'heure. L'adaptation du format s'opère dans la section **[locale]** du fichier de configuration de l'application. Vous pouvez spécifier les formats suivants :

%I:%M:%S %P : pour représenter l'heure au format 12 heures (paramètre **TimeFormat**).

%y/%m/%d et**%m/%d/%y** : pour représenter la date (paramètre **DateFormat**) (aa.mm.jj et mm.jj.aa respectivement).

6.6. Paramètres de composition des rapports de Kaspersky Anti-Virus

Les résultats des activités de chacun des composants de Kaspersky Anti-Virus sont enregistrés dans un rapport publié dans un fichier.

Les résultats du traitement antivirus des systèmes de fichiers du serveur apparaissent également sur la console. Par défaut, les informations contenues dans le rapport ou affichées à l'écran sont identiques. Si vous souhaitez que les informations affichées sur la console diffèrent de celle reprises dans le journal, vous devrez procéder à quelques modifications de paramètres.

Vous pouvez modifier le volume de l'information présentée en choisissant différents *niveaux de détails*.

Le **niveau de détails** se présente sous la forme d'un chiffre qui définit le degré de concrétisation dans le rapport des informations relatives aux activités des composants. Le dernier niveau contient chaque fois les informations du niveau précédent en plus de quelques renseignements complémentaires.

Le tableau ci-après reprend tous les niveaux de détails possibles pour le rapport.

Niveaux	Nom du niveau	Signification
0	Erreurs critiques	Informations relatives uniquement aux erreurs critiques (les erreurs qui entraînent l'arrêt des applications lorsque ces dernières ne sont pas en mesure d'exécuter une action quelconque). Par exemple, lorsque le composant est infecté ou lorsqu'une erreur est survenue au moment de la vérification et du chargement des bases antivirus et des clés de licence.
1	Erreurs	Informations sur les autres types d'erreurs, notamment les erreurs qui n'entraînent pas l'arrêt des composants, par exemple les informations sur les erreurs survenues lors de l'analyse d'un objet.

Niveaux	Nom du niveau	Signification
2	Avertissement	Informations relatives aux erreurs qui peuvent entraîner l'arrêt de l'application (par exemple, informations sur le manque d'espace sur le disque dur).
3	Info, Notice	Communications importantes à caractère informatif. Par exemple : informations précisant si le composant est lancé ou pas, chemin d'accès du fichier de configuration, zone d'analyse, renseignements relatifs aux bases antivirus, aux clés de licence, statistiques qui en découlent.
4	Activité	Communications sur l'analyse d'objets conformément au niveau de détails du rapport d'analyse.
10	Debug	Toutes les notifications relatives au débogage, par exemple le contenu du fichier de configuration.

Les informations portant sur les erreurs critiques dans le cadre de l'activité d'un composant sont toujours reprises, quel que soit le niveau de détails choisi. Le niveau optimum est le niveau **4** qui est défini par défaut.

CHAPITRE 7. GESTION DES CLES DE LICENCE

La licence d'utilisation de Kaspersky Anti-Virus for Samba Servers est limitée dans le temps (en règle générale, il s'agit d'une durée de validité d'un an à partir de l'acquisition). Lorsque la licence est parvenue à échéance, Kaspersky Anti-Virus continue à fonctionner mais il n'est plus possible de procéder aux mises à jour des bases antivirus. Le programme continuera à réparer les objets infectés en utilisant les vieilles bases antivirus.

La clé de licence vous donne le droit d'utiliser le logiciel et contient toutes les informations pertinentes qui touchent à la licence que vous avez acquise, telles que : le type de licence, sa date d'expiration, les informations relatives aux distributeurs, etc.

En plus du droit d'utilisation du logiciel pendant la durée de validité de la licence, vous bénéficiez également des avantages suivants :

- Assistance technique 24h/7 ;
- Mise à jour des bases antivirus *toutes les heures* ;
- Mise à niveau de l'application (correctif) ;
- Accès aux nouvelles versions du logiciel (mise à niveau) ;
- Informations en temps utile sur l'émergence de nouveaux virus.

Dès que votre licence arrive à expiration, vous êtes automatiquement privé de l'accès aux services mentionnés ci-dessus. Kaspersky Anti-Virus continuera à assurer le traitement antivirus des systèmes de fichiers du serveur. Toutefois, il utilisera pour ce faire les bases antivirus du jour correspondant à la date d'expiration de la licence. La fonction de mise à jour automatique des bases antivirus ne sera plus disponible. En cas de tentative de mise à jour manuelle des bases antivirus, l'application ne fonctionnera plus.

Il est dès lors très important de consulter régulièrement les informations fournies avec la clé de licence et de prêter une attention toute particulière à sa date d'expiration.

7.1.1. Consultation des informations relatives à la clé de licence

Les informations relatives aux clés de licence activées sont consultables dans les rapports d'activité des composants *kavscanner* et *kavsamba* car ces informations sont chargées à chaque démarrage d'un de ces composants.

De plus, Kaspersky Anti-Virus dispose d'un composant particulier appelé *licensemanager* qui vous permet non seulement de consulter l'ensemble des informations relatives aux clés, mais également quelques renseignements complémentaires.

Ces renseignements peuvent être affichés sur la console du serveur ou être consultés à distance depuis n'importe quel ordinateur de votre réseau grâce à Webmin.

Afin de consulter les informations relatives à l'ensemble des clés de licence installées :

Saisissez dans la ligne de commande :

```
#./kav4samba-licensemanager –s
```

Des informations semblables à ceci seront affichées :

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2006.
Portions Copyright (C) Lan Crypto
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix", expires
04-07-2003 in 28 days
```

Pour consulter les informations relatives à la clé de licence :

Saisissez, par exemple, la commande suivante :

```
#./kav4samba-licensemanager -k 00053E3D.key
```

Des informations semblables à ceci seront affichées :

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2006.
Portions Copyright (C) Lan Crypto
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus
for Linux", expires 04-07-2003 in 28 days
```

7.1.2. Prolongation de la licence

Lorsque vous prolongez votre licence d'utilisation de Kaspersky Anti-Virus, l'application récupère toutes ses fonctions, dont la mise à jour des bases antivirus. De plus, l'accès aux services complémentaires cités au point **Error! Reference source not found.** de la page **Error! Bookmark not defined.** est également rétabli.

La durée de validité de la licence dépend du type de licence choisi lors de l'achat de l'application.

Pour renouveler la licence d'utilisation de Kaspersky Anti-Virus, vous devez :

vous mettre en rapport avec le distributeur chez lequel vous avez acheté l'application et demander une prolongation de la licence d'utilisation de Kaspersky Anti-Virus.

ou :

contacter directement le Service Ventes (sales@kaspersky.com) de Kaspersky Lab pour acheter une nouvelle clé ou remplissez le formulaire sur notre site (www.kaspersky.com/fr) dans la rubrique **Produits→Renouveler votre licence**. Dès réception du paiement, vous recevrez la clé de licence à l'adresse électronique saisie dans le formulaire.

Kaspersky Lab organise régulièrement des promotions qui permettent de profiter de remises importantes sur l'acquisition de nouvelles licences. Vous trouverez les informations sur ces offres dans la rubrique **Produits→Actions et offres spéciales**.

La clé de licence ainsi acquise doit être activée à l'aide de l'utilitaire *licensemanager* (paramètre **LicensePath** du fichier de configuration de l'application).

Pour installer la nouvelle clé de licence, vous devez :

saisir, par exemple, la commande suivante :

```
#./kav4samba-licensemanager -a 00053E3D.key
```

Les informations suivantes apparaîtront sur la console du serveur :

```
Kaspersky license manager. Version 5.5.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2006.
```

```
Key file 00053E3D.key is successfully registered
```

Une fois cette démarche accomplie, nous vous conseillons de mettre à jour les bases antivirus.

Si vous souhaitez installer une nouvelle clé de licence avant la date d'expiration de la licence en cours, vous pouvez attribuer à la nouvelle clé le statut de réserve. La clé de réserve commence à fonctionner dès la fin de la période de validité de la clé précédente. La durée de validité de la clé de réserve est calculée à partir de son activation.

L'installation de la clé de réserve se déroule de la même manière que l'installation de la clé principale. Par la suite, lors de la consultation des informations relatives aux clés de licence, la console du serveur affichera les renseignements non seulement sur la clé en cours mais aussi sur les clés de réserve.

7.1.3. Suppression de la clé de licence

Pour supprimer toutes les clés de licence installées :

Saisissez la commande suivante :

```
#./kav4samba-licensemanager –da
```

Les informations suivantes apparaîtront sur la console du serveur :

```
Kaspersky license manager. Version 5.5.0.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2006.
Active key was successfully removed
```

Afin de supprimer la clé de réserve :

Saisissez la commande suivante :

```
#./kav4samba-licensemanager –dr
```

Les informations suivantes apparaîtront sur la console du serveur :

```
Kaspersky license manager. Version 5.5.0.0/RELEASE
Copyright (C) Kaspersky Lab. 1998-2006.
Active key was successfully removed
```

CHAPITRE 8. VERIFICATION DU BON FONCTIONNEMENT DU LOGICIEL ANTIVIRUS

Une fois que vous aurez installé et configuré Kaspersky Anti-Virus, nous vous conseillons de vérifier l'exactitude de paramètres et le bon fonctionnement du logiciel à l'aide d'un « virus » d'essai et d'une de ses modifications.

Ce virus d'essai a été développé spécialement par l'organisation eicar (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Il NE S'AGIT PAS D'UN VIRUS et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considèrent comme un virus.

N'utilisez jamais d'authentiques virus pour vérifier le fonctionnement de votre antivirus.

Vous pouvez télécharger le « virus » d'essai depuis le site officiel de l'organisation **EICAR**: http://www.eicar.org/anti_virus_test_file.htm. Si vous n'avez pas accès à Internet, vous pouvez créer ce « virus » d'essai vous-même. Pour ce faire, saisissez la ligne suivante dans n'importe quel éditeur de fichier texte et enregistrez le fichier sous le nom **eicar.com** :

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Le fichier que vous aurez téléchargé depuis le site de **EICAR** ou que vous aurez créé vous-même contient le corps du « virus » d'essai standard. Lorsque l'antivirus le découvre, il lui attribue le statut **Infecté**, n'essaye pas de le réparer et exécute l'action définie par l'administrateur pour les objets de ce type.

Afin de vérifier le comportement de Kaspersky Anti-Virus lors de la découverte d'objets d'un autre type, vous pouvez modifier le contenu du « virus » d'essai standard en ajoutant un des préfixes repris au tableau 1.

Vous pourrez vérifier le bon fonctionnement de Kaspersky Anti-Virus à l'aide du « virus » EICAR modifié uniquement si vous disposez des bases antivirus ultérieures au 24 octobre 2003 (mise à jour cumulée : octobre 2003).

Tableau 1. Modifications du « virus » d'essai

Préfixe	Type d'objet
Pas de préfixe, « virus » d'essai standard	**INFECTED** L'objet ne sera pas réparé.
CORR–	**Corrupted**. L'objet est corrompu
SUSP-	**Suspicious** (code d'un virus inconnu).
WARN-	**Warning** (code modifié d'un virus connu).
ERRO-	**Error** Une erreur s'est produite suite à l'analyse.
CURE-	**Cured**. L'objet sera réparé et le texte du corps du « virus » sera remplacé par CURED.
DELE-	L'objet sera effacé automatiquement.

La première colonne reprend les préfixes qu'il faudra ajouter au début de la ligne de code du « virus »d'essai standard (par exemple : CORR–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*). La deuxième colonne reprend la description des types d'objet identifiés par l'antivirus suite à l'ajout des différents préfixes. Les actions exécutées sur chacun de ces objets dépendent des paramètres de l'antivirus définis par l'administrateur.

CHAPITRE 9. QUESTIONS SUR L'UTILISATION DE L'APPLICATION

Ce chapitre est consacré aux questions les plus fréquemment posées par les utilisateurs sur l'installation, la configuration et l'utilisation de Kaspersky Anti-Virus. Nous avons tenté d'y répondre de la manière la plus exhaustive qui soit.

Question : Kaspersky Anti-Virus peut-il être utilisé simultanément avec les logiciels d'autres éditeurs ?

Afin d'éviter tout risque de conflit, nous vous conseillons de supprimer les logiciels antivirus d'éditeurs tiers avant d'installer Kaspersky Anti-Virus.

Question : Kaspersky Anti-Virus n'analyse pas le fichier une deuxième fois. Pourquoi ?

En effet, Kaspersky Anti-Virus ne procèdera pas à une nouvelle analyse d'un fichier si ce dernier n'a pas été modifié depuis la dernière analyse.

Cela est possible grâce à la nouvelle technologie iChecker™. Cette technologie repose sur l'utilisation de bases de données contenant les sommes de contrôle des objets.

Question : Pourquoi Kaspersky Anti-Virus entraîne-t-il une baisse des performances du serveur et surcharge-t-il le processeur ?

La détection des virus est avant tout une tâche mathématique liée à l'analyse de la structure, de la somme de contrôle et des données mathématiques. Pour cette raison, la principale ressource utilisée par tout logiciel antivirus est le processeur. De plus, chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse. C'est le prix à payer pour garantir la fiabilité et la sécurité des données.

A la différence d'autres logiciels antivirus qui réduisent la durée de l'analyse en éliminant des bases antivirus les virus les plus complexes à

identifier ou les plus rares (à l'endroit où est basée la société productrice), ainsi que les fichiers les plus difficiles à analyser (comme les fichiers PDF), Kaspersky Lab estime que la tâche attendue de tout antivirus est de garantir une véritable protection de l'utilisateur contre les virus. Il ne peut être question de protection partielle. Qui plus est, la « protection partielle » est pire que l'absence de protection (dans ce cas au moins, l'utilisateur adopte lui-même des mesures de prévention).

Kaspersky Anti-Virus confère à l'utilisateur un sentiment de protection totale. Il va de soi que Kaspersky Anti-Virus permet à l'utilisateur expérimenté d'accélérer la vitesse de l'analyse au détriment du niveau global de sécurité grâce à l'exclusion de toute une série de différents fichiers. Toutefois, nous ne vous conseillons pas d'agir ainsi si vous souhaitez vous sentir vraiment en sécurité.

Signe de la protection maximale qu'il assure aux utilisateurs, Kaspersky Anti-Virus reconnaît plus de 40 archives et programmes d'installation et est capable de reconnaître plus de 350 types de fichiers différents. Ceci est très important au niveau de la sécurité antivirus car chacun des formats reconnus ci-dessus peut contenir un code malicieux exécutable. Néanmoins, il convient de remarquer que chaque nouvelle version du logiciel est plus rapide que la précédente, malgré l'augmentation quotidienne du nombre de virus identifiés par Kaspersky Anti-Virus (plus de 30 nouveaux virus chaque jour) et l'augmentation constante des formats pris en charge. Tout ceci est rendu possible grâce aux nouvelles technologies développées par Kaspersky Lab comme iChecker. Ces technologies permettent de rechercher d'éventuels virus dans les fichiers une seule fois, lors de la première analyse. Si ce fichier n'a pas été modifié depuis la dernière analyse, il ne sera pas repris dans l'analyse suivante. Autrement dit, les performances du logiciel antivirus sont nettement accrues après la première analyse du fichier.

Question : A quoi sert la clé de licence? Mon antivirus fonctionnera-t-il sans elle ?

Kaspersky Anti-Virus ne peut fonctionner sans la clé de licence.

Si vous n'avez pas encore décidé d'acheter ou non Kaspersky Anti-Virus, nous pouvons vous fournir une clé d'évaluation (trial-key) qui fonctionnera deux semaines ou un mois. Passé ce délai, la clé sera bloquée.

Question : Que se passe-t-il lorsque la licence d'utilisation du logiciel arrive à échéance ?

Lorsque la licence est parvenue à échéance, Kaspersky Anti-Virus continue à fonctionner mais il n'est plus possible de procéder aux mises à jour des bases antivirus. Le programme continuera à réparer les objets infectés en utilisant les vieilles bases antivirus.

Le téléchargement des bases antivirus depuis le site de Kaspersky Lab à l'aide de Kaspersky Anti-Virus ne sera plus possible. Kaspersky Anti-Virus n'utilisera pas les bases antivirus que vous auriez réussi à télécharger sans son aide.

Par conséquent, nous ne pourrons pas garantir votre protection contre les nouveaux virus.

Question : La clé de licence de Kaspersky Anti-Virus est enregistrée sur une disquette. Que faire si je ne dispose pas d'un lecteur de disquettes ?

Plusieurs solutions existent.

Vous pouvez envoyer un message décrivant ce problème au service vente de Kaspersky Lab (sales@kaspersky.com). Indiquez la date et le lieu où vous avez acheté Kaspersky Anti-Virus ainsi que le numéro d'enregistrement complet. Les responsables du service vente enverront le fichier de clé à l'adresse électronique que vous aurez indiquée.

Vous pouvez également lire la disquette sur un autre ordinateur doté d'un lecteur et l'enregistrer sur un support que vous pourrez lire sur votre ordinateur. Lors de l'installation de Kaspersky Anti-Virus, il suffira d'indiquer ce support en tant que source de la clé de licence.

Vous pouvez également envoyer le fichier de clé par courrier électronique à votre propre adresse au départ d'un ordinateur doté d'un lecteur de disquette. Une fois que vous aurez reçu le message, enregistrez la clé dans un répertoire sur votre disque dur et lors de l'installation de Kaspersky Anti-Virus indiquez ce répertoire en tant que source de la clé de licence.

Question : Mon antivirus ne fonctionne pas.

Que puis-je faire ?

Avant tout, vérifiez si la solution de votre problème n'est pas décrite dans les pages de ce manuel, et plus particulièrement dans cette rubrique. Consultez également la rubrique d'assistance technique (disponible en anglais) de notre site Internet (**Protection en temps réel**

→ **Banque de solutions** → **Kaspersky Anti-Virus 5.5 for Samba Servers**).

Nous vous conseillons également de vous adresser à la société qui vous a vendu Kaspersky Anti-Virus ou bien d'envoyer une requête au service d'assistance technique (http://www.kaspersky.ru/helpdesk.html) de Kaspersky Lab.

Question : Une personne mal intentionnée pourrait-elle remplacer les bases antivirus ?

Une personne mal intentionnée peut télécharger les bases antivirus depuis le site de Kaspersky Lab et les copier dans le répertoire où elles sont stockées. Toutefois, Kaspersky Anti-Virus ne les utilisera pas.

Chaque base antivirus dispose d'une signature unique que Kaspersky Anti-Virus vérifie lorsqu'il consulte ces bases. Si la signature ne correspond pas à celle octroyée par Kaspersky Lab et que la date de la base de données est postérieure à la date d'expiration de la licence, Kaspersky Anti-Virus n'utilisera pas cette base.

Question : Les microprocesseurs de l'architecture X (PowerPC, SPARC, Alpha, PA-RISC, etc.) sont-ils pris en charge ?

La version actuelle de l'application ne prend pas ces types de microprocesseurs en charge.

Question : Kaspersky Anti-Virus for Unix tournera-t-il sur ma distribution de Linux?

Les essais de Kaspersky Anti-Virus version 5.5 ont été réalisés sur les distributions Red Hat, Debian, SUSE et Mandriva et c'est pour ces distributions que Kaspersky Anti-Virus a été compilé.

Si la distribution n'est pas reprise dans la liste, il se peut que l'application ne fonctionne pas correctement. Cela est dû avant tout aux spécificités du système d'exploitation. Par exemple, il se peut que la distribution de votre système utilise une autre version de la bibliothèque ou que les scripts d'initialisation du système se trouvent dans un emplacement inhabituel. L'assistance technique de Kaspersky Lab ne pourra pas vous aider dans un tel cas de figure.

Question : Comment puis-je décompresser les fichiers .tgz ou tar.gz ?

Vous pouvez décompresser les fichiers *.tgz* ou *.tar.gz* à l'aide de la commande suivante :

```
tar zxvf <nom_du_l'archive>
```

Question : est-il possible de contrôler Kaspersky Anti-Virus par l'intermédiaire de Network Control Centre pour Windows ?

Il n'est pas possible d'utiliser Network Control Centre pour Windows conjointement à Kaspersky Anti-Virus for Unix. La version actuelle de l'application prévoit la configuration à distance par l'intermédiaire du module spécial de Webmin inclus dans le logiciel.

Question : Comment puis-je enregistrer dans un fichier ce que le logiciel affiche sur la console ?

Vous pouvez résoudre ce problème de la manière suivante : Saisissez la commande :

```
$ some_app > ./text_file 2>&1
```

Où :

`some_app` représente l'application dont les entrées normales et les entrées relatives aux erreurs survenues doivent être enregistrées dans un fichier;

`text_file` représente le chemin d'accès complet au fichier où seront enregistrées les informations.

Par exemple :

```
$keepup2date > ./updater.log 2>&1
```

Dans ce cas, les messages standard et les messages d'erreur du composant *keepup2date* seront enregistrés dans le fichier *updater.log* du répertoire courant.

ANNEXE A. RENSEIGNEMENTS COMPLEMENTAIRES SUR L'APPLICATION

Cette annexe décrit l'arborescence des répertoires de Kaspersky Anti-Virus après l'installation, le fichier de configuration ainsi que les arguments de la ligne de commande pour les différents composants et leurs codes de retour. Vous y trouverez également un exemple de fichier de script pour la réparation des objets.

A.1. Fichier de configuration de Kaspersky Anti-Virus

Kaspersky Anti-Virus est installé avec le fichier de configuration *kav4fsambaservers.conf* qui reprend les paramètres de fonctionnement de l'application. Cette section aborde en détail chaque groupe de paramètres du fichier de configuration. Dans ces descriptions, les paramètres sont présentés avec leur valeur par défaut, quand elle existe.

La section **[path]** regroupe les paramètres qui définissent les chemins d'accès aux fichiers indispensables au fonctionnement du logiciel :

BasesPath : chemin d'accès complet aux bases antivirus.

LicensePath : chemin d'accès complet au répertoire contenant les clés de licence.

IcheckerDbFile : chemin d'accès complet au répertoire de conservation des bases analysées à l'aide de la technologie iChecker.

La section **[locale]** contient les paramètres qui définissent le format de la date et de l'heure :

TimeFormat=%H:%M:%S : format d'affichage de l'heure conformément à strftime.

Vous pouvez opter pour le format 12 heures (am, pm) : **%I:%M:%S %P**

DateFormat=%d/%m/%y : format d'affichage de la date conformément à strftime.

Vous pouvez modifier le format d'affichage de la date et choisir : **%y/%m/%d** ou**%m/%d/%y**.

La section **[samba.options]** contient les paramètres d'analyse en temps réel :

ExcludeDir=masque1:masque2:...:masqueN : masques des répertoires qui seront exclus de l'analyse. Par défaut, tous les répertoires sont analysés.

ExcludeMask=masque1:masque2:...:masqueN : masques des fichiers qui seront exclus de l'analyse. Par défaut, tous les fichiers sont analysés.

Packed=yes : mode d'analyse des fichiers compactés. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Archives=yes : mode d'analyse des archives. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

SelfExtArchives=yes : mode d'analyse des archives auto-extractibles. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre. Si le mode d'analyse des archives est activé (**Archives=yes**), les archives auto-extractibles seront analysées même si le paramètre **SelfExtArchives** possède la valeur **no**.

MailBases=yes : mode d'analyse des bases de données de messagerie. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

MailPlain=yes : mode d'analyse des bases de données de messagerie électronique au format texte. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Heuristic=yes : mode d'utilisation de l'analyse heuristique pendant l'analyse. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Cure=no : mode de réparation des objets infectés. Afin d'activer ce mode, attribuez la valeur **yes** à ce paramètre.

Ichecker=yes : mode d'utilisation de la technologie iChecker pour l'analyse antivirus. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

FileCacheSize : nombre d'entrées relatives aux objets sains conservés dans le cache de fichiers.

BgCheckFilesLimit : nombre maximum d'objets analysés simultanément en arrière plan. Si la valeur du paramètre est égale à **0**, alors l'analyse en arrière plan n'est pas exécutée.

BgSheduleTime : période à l'issue de laquelle l'analyse antivirus d'un nouveau fichier du répertoire partage est lancée en arrière-plan (en secondes).

HashType=md5|crc32 : type de cache utilisé. Il s'agit par défaut du type **md5**.

UseAVbasesSet=standart|extended : sélection de bases antivirus utilisées par l'application. L'ensemble **extended** contient, en plus des définitions de l'ensemble **standard**, les signatures de programmes présentant un danger potentiel tels que : les logiciels publicitaires, les programmes d'administration à distance, etc.

La section **[samba.path]** regroupe les paramètres qui définissent le chemin d'accès aux fichiers importants sans lesquels le module kavsamba ne pourra fonctionner :

BackupPath= chemin : chemin d'accès complet au répertoire contenant les copies de sauvegarde des objets analysés.

SambaConfigFile=chemin : chemin d'accès complet au fichier de configuration du serveur Samba.

PidFile=chemin : chemin d'accès complet au fichier pid du composant kavsamba.

La section **[samba.shares]** regroupe les paramètres qui définissent les options d'analyse des fichiers dans les répertoires partagés :

CheckOnOpen :analyse antivirus du fichier à chaque requête d'ouverture.

CheckOnClose : analyse antivirus du fichier lors de la sauvegarde.

Un section du style **[samba.shares:SHARENAME]** *peut être créée* dans le fichier de configuration et elle doit contenir les paramètres qui définissent les options de la protection antivirus pour un répertoire partagé en particulier, (par exemple, le répertoire **SHARENAME**):

CheckOnOpen :analyse antivirus du fichier à chaque requête d'ouverture.

CheckOnClose : analyse antivirus du fichier lors de la sauvegarde.

Si des paramètres individuels de protection du répertoire partagé sont définis, alors ce répertoire ne sera pas accessible tant que Kaspersky Anti-Virus n'est pas lancé.

La section **[samba.actions]** contient les paramètres qui définissent les actions à réaliser sur les objets d'un type quelconque :

OnInfected=action : action exécutée en cas de découverte d'un fichier infecté. Lorsque le mode réparation a été activé, cette action sera exécutée sur les fichiers qui n'auront pas pu être réparés.

OnSuspicion=action : action exécutée en cas de découverte d'un fichier suspect dont le code évoque celui d'un virus qui n'aurait pas encore été identifié par Kaspersky Lab.

OnWarning=action : action exécutée en cas de découverte d'un fichier dont le code ressemble à celui d'un virus connu.

OnCured=action : action à réaliser après la découverte et la réparation réussie d'un objet infecté.

OnProtected=action : action exécutée en cas de découverte d'un objet infecté protégé par un mot de passe. Il est impossible d'analyser de tels objets.

OnCorrupted=action : action exécutée en cas de découverte d'un fichier corrompu.

OnError=action : action exécutée lorsqu'une erreur système survient lors de l'analyse de l'objet.

La syntaxe du paramètre **action** comprend deux parties : l'action elle-même et son paramètre complémentaire, séparés par un espace. La valeur attribuée au paramètre complémentaire est reprise entre guillemets. Par exemple : **OnInfected=move /tmp/infected**

Les actions suivantes sont possibles :

- *move* <*répertoire*> : déplace le fichier dans le <répertoire>.
- *movePath* <*répertoire*> : déplace le fichier dans le <répertoire> de manière récursive (avec le chemin absolu).
- *remove* : supprime le fichier.
- *exec* <*paramètre*> : exécute sur l'objet l'action définie par la valeur <paramètre>.

Voici une liste des macros de paramètre d'action complémentaire :

- %VIRUSNAME% : nom du virus découvert
- %FULLPATH% : chemin d'accès complet au répertoire.
- %FILENAME% : nom du fichier sans son chemin d'accès.

La section **[samba.notify]** contient les paramètres qui définissent l'envoi de notification suite à la découverte d'objets d'un type quelconque :

OnInfected=action : notification en cas de découverte d'un fichier infecté.

OnSuspicion=action : notification en cas de découverte d'un fichier suspect dont le code évoque celui d'un virus qui n'aurait pas encore été identifié par Kaspersky Lab.

OnWarning=action : notification en cas de découverte d'un fichier dont le code ressemble à celui d'un virus connu.

OnCured=action : notification après la découverte et la réparation réussie d'un objet infecté.

OnProtected=action :notification en cas de découverte d'un objet infecté protégé par un mot de passe. Il est impossible d'analyser de tels objets.

OnCorrupted=action : notification en cas de découverte d'un fichier corrompu.

OnError=action : notification lorsqu'une erreur système survient lors de l'analyse de l'objet.

Les actions suivantes sont possibles :

- *move <répertoire>* : déplace le fichier dans le <répertoire>.
- *movePath <répertoire>* : déplace le fichier dans le <répertoire> de manière récursive (avec le chemin absolu).
- *remove* : supprime le fichier.
- *exec <paramètre>* : exécute sur l'objet l'action définie par la valeur <paramètre>.

Voici une liste des macros de paramètre d'action complémentaire :

- %USER% : nom de l'utilisateur voulant accéder au fichier.
- %USERIP% : adresse IP de l'utilisateur souhaitant accéder au fichier.
- %USERHOST% : hôte de l'utilisateur d'où la requête a été envoyée vers le fichier.
- %VIRUSNAME% : nom du virus découvert
- %FULLPATH% : chemin d'accès complet au répertoire.
- %FILENAME% : nom du fichier sans son chemin d'accès.

La section **[samba.report]** regroupe les paramètres de composition du rapport d'activité de kavsamba :

ReportFileName : nom du fichier où sont consignés les résultats du fonctionnement du composant.

ReportMaxSize : taille du rapport (en octets).

ReportLevel : niveau de détails du rapport.

Append=yes : mode d'ajout de notifications complémentaires au fichier du rapport. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

ShowOK=yes : mode de consignation dans le rapport des notifications relatives aux fichiers sains. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

La section **[scanner.options]** regroupe les paramètres d'analyse des systèmes de fichiers du serveur :

ExcludeDir=masque1:masque2:...:masqueN : masques des répertoires qui seront exclus de l'analyse. Par défaut, tous les répertoires sont analysés.

ExcludeMask=masque1:masque2:...:masqueN : masques des fichiers qui seront exclus de l'analyse. Par défaut, tous les fichiers sont analysés.

Packed=yes : mode d'analyse des fichiers compactés. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Archives=yes : mode d'analyse des archives. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

SelfExtArchives=yes : mode d'analyse des archives auto-extractibles. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre. Si le mode d'analyse des archives est activé (**Archives=yes**)**,** les archives auto-extractibles seront analysées même si le paramètre **SelfExtArchives** possède la valeur **no**.

MailBases=yes : mode d'analyse des bases de données de messagerie. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

MailPlain=yes : mode d'analyse des bases de données de messagerie électronique au format texte. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Heuristic=yes : mode d'utilisation de l'analyse heuristique pendant l'analyse. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Recursion=yes : mode de passage récursif des répertoires lors de l'analyse antivirus. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Ichecker=yes : mode d'utilisation de la technologie iChecker pour l'analyse antivirus. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

Cure=no : mode de réparation des objets infectés. Afin d'activer ce mode, attribuez la valeur **yes** à ce paramètre.

UseAVbasesSet=standardt|extended : sélection de bases antivirus utilisées par l'application. L'ensemble **extended** contient, en plus des définitions de l'ensemble **standard**, les signatures de programmes présentant un danger potentiel tels que : les logiciels publicitaires, les programmes d'administration à distance, etc.

FollowSymlinks : mode de fonctionnement avec les liens symboliques. Si la valeur de ce paramètres est égale à **yes**, tous les liens symboliques sont suivis. Si la valeur du paramètre est égale à **no**, les liens symboliques vers les répertoires ne seront pas suivis.

MaxLoadAvg : paramètre numérique qui indique la charge du serveur. Lorsque la charge dépasse la valeur définie, l'analyse antivirus est temporairement suspendue. L'analyse reprendra dès que la charge du serveur repassera en dessous de la valeur définie.

La section **[scanner.path]** contient le paramètre qui définit le chemin d'accès aux fichiers importants sans lesquels le module kavscanner ne pourra fonctionner :

BackupPath= chemin : chemin d'accès complet au répertoire contenant les copies de sauvegarde des objets analysés.

La section **[scanner.object]** regroupe les paramètres qui définissent les actions à exécuter sur les objets simples de n'importe quel type dans le cadre de la protection antivirus des serveurs de fichiers.

OnInfected=action : action exécutée en cas de découverte d'un fichier infecté. Lorsque le mode réparation a été activé, cette action sera exécutée sur les fichiers qui n'auront pas pu être réparés.

OnSuspicion=action : action exécutée en cas de découverte d'un fichier suspect dont le code évoque celui d'un virus qui n'aurait pas encore été identifié par Kaspersky Lab.

OnWarning=action : action exécutée en cas de découverte d'un fichier dont le code ressemble à celui d'un virus connu.

OnCorrupted=action : action exécutée en cas de découverte d'un fichier corrompu.

OnCured=action : action à réaliser après la découverte et la réparation réussie d'un objet infecté.

OnProtected=action : action exécutée en cas de découverte d'un objet infecté protégé par un mot de passe. Il est impossible d'analyser de tels objets.

OnError=action : action exécutée lorsqu'une erreur survient lors de l'analyse de l'objet.

La syntaxe du paramètre **action** comprend deux parties : l'action elle-même et son paramètre complémentaire, séparés par un espace. La valeur attribuée au paramètre complémentaire est reprise entre guillemets. Par exemple : **OnInfected=move /tmp/infected**

Les actions suivantes sont possibles :

- *move <répertoire>* : déplace le fichier dans le <répertoire>.
- *movePath <répertoire>* : déplace le fichier dans le <répertoire> de manière récursive (avec le chemin absolu).
- *remove* : supprime le fichier.
- *exec <paramètre>* : exécute sur l'objet l'action définie par la valeur <paramètre>.

Les variables suivantes peuvent être utilisées en guise de paramètre complémentaire pour l'action **exec** :

- %LIST% : nom du fichier ou liste des noms de fichiers infectés, suspects et corrompus découverts dans l'archive. Le format du fichier ressemble à ceci : **<nom du virus>\t<nom du fichier>**.
- %FULLPATH% : chemin d'accès complet au conteneur.
- %FILENAME% : nom du fichier sans son chemin d'accès.
- %CONTAINERTYPE% : type de conteneur sous la forme d'une ligne.

La section **[scanner.container]** regroupe les paramètres qui définissent les actions à exécuter sur les archives dans le cadre de la protection antivirus des systèmes de fichiers du serveur :

OnCorrupted=action : action exécutée en cas de découverte d'un conteneur corrompu.

OnInfected=action : action exécutée en cas de découverte d'un objet infecté dans l'archive. Lorsque le mode de réparation des fichiers infectés a été activé, cette action est exécutée sur les conteneurs qui n'ont pas pu être réparés et uniquement après l'exécution des actions sur les objets de ce conteneur.

OnSuspicion=action : action exécutée en cas de découverte d'un objet suspect dans l'archive.

OnWarning=action : action exécutée en cas de découverte, à l'intérieur du conteneur, d'un objet dont le code ressemble à celui d'un virus connu.

OnCured=action : action exécutée en cas de découverte, à l'intérieur du conteneur, d'un objet infecté qui a pu être réparé.

OnProtected=action : action exécutée en cas de découverte, à l'intérieure du conteneur, d'un objet infecté protégé par un mot de passe. Il est impossible d'analyser de tels objets.

OnError=action : action exécutée lorsqu'une erreur survient lors de l'analyse du conteneur.

La syntaxe des actions à exécuter sur tous les types d'objets mentionnés ci-dessus est identique à celle décrite pour les objets dans la section **[scanner.object]**.

La section **[scanner.report]** regroupe les paramètres de composition du rapport d'activité de kavscanner :

ReportFileName : nom du fichier où sont consignés les résultats du fonctionnement du composant.

ReportLevel=4 : niveau de détails du rapport.

Append=yes : mode d'ajout de notifications complémentaires au fichier du rapport. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

ShowOK=yes : mode de consignation dans le rapport des notifications relatives aux fichiers sains. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

ShowContainerResultOnly=no : représentation dans le rapport des résultats de l'analyse de l'archive au format concis. Afin de représenter les informations dans un format concis, attribuez la valeur **yes** au paramètre.

ShowObjectResultOnly=no : représentation dans le rapport des résultats de l'analyse des objets simples au format concis. Afin de représenter les informations dans un format concis, attribuez la valeur **yes** au paramètre.

La section **[updater.path]** regroupe les paramètres qui définissent le chemin d'accès aux fichiers indispensables au fonctionnement du composant de mise à jour des bases antivirus :

AVBasesTestPath : chemin d'accès complet au répertoire où sont copiées les bases antivirus.

BackUpPath : chemin d'accès complet au répertoire où sont conservées les bases antivirus de sauvegarde.

La section **[updater.options]** regroupe les paramètres de fonctionnement de keepup2date :

UseUpdateServerUrl=no : mode de mise à jour depuis l'adresse définie au paramètre **UpdateServerUrl**.

UseUpdateServerUrlOnly=no : utilisation exclusive pour la mise à jour des bases antivirus de l'adresse indiquée au paramètre **UpdateServerUrl**. Si la valeur **no** est attribuée, alors en cas d'échec de la mise à jour depuis l'adresse **UpdateServerUrl** c'est une autre adresse de la liste de serveurs qui sera utilisée.

PostUpdateCmd : commande exécutée directement après la réussite de la mise à jour des bases antivirus. La valeur définie dans le fichier de configuration d'origine lance automatiquement la relecture des bases antivirus actualisées par l'application. Il est déconseillé de modifier ce paramètre.

RegionSettings=ru : code de la région (deux premières lettres du nom de la région) où se trouve l'utilisateur. Il détermine la sélection du serveur de mise à jour de Kaspersky Lab le plus proche pour le téléchargement des mises à jour des bases antivirus.

ConnectTimeout=30 délai de déconnexion pour la mise à jour des bases (en secondes). Si aucune donnée n'est reçue pendant la durée définie lors du téléchargement des mises à jour, un autre serveur de mise à jour sera sélectionné dans la liste des serveurs de Kaspersky Lab.

UseProxy : mode d'utilisation du serveur proxy pour la connexion au serveur de mise à jour de Kaspersky Lab. Si la valeur du paramètre est **no**, le serveur proxy ne sera pas utilisé. Si la valeur du paramètre est **yes**, l'adresse utilisée pour le serveur proxy est celle définie au paramètre **ProxyAddress**. Si le paramètre **ProxyAddress** n'a pas de valeur définie, c'est la valeur de la variable **http_proxy** qui sera utilisée. Si la variable n'est pas définie, le serveur proxy ne sera pas utilisé.

ProxyAddress : adresse pour la connexion au serveur proxy. Le paramètre est défini sous la forme **http://username:password@url:port**. Dans l'adresse du serveur proxy, les paramètres **username** et/ou **password** ne sont pas obligatoires. Si l'adresse n'est pas indiquée, sa valeur sera celle de la variable **http_proxy**.

La section **[updater.report]** regroupe les paramètres de composition du rapport d'activité de keepup2date :

Append=yes : mode d'ajout de notifications complémentaires au fichier du rapport. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

ReportFileName : nom du fichier où sont consignés les résultats du fonctionnement du composant.

ReportLevel=4 : niveau de détails du rapport.

A.2. Arguments de la ligne de commande pour le composant kavsamba

Il est possible de redéfinir les paramètres du fichier de configuration au moment du démarrage du programme à l'aide des arguments de la ligne de commande. Nous allons les aborder en détail.

Options d'aide :	
–h	Affiche sur la console l'aide du composant kavsamba.
–v	Affiche la version du programme.
Options de configuration :	
–c (–y) <chemin_du_fichier>	Utilise le fichier de configuration alternatif **<chemin_du_fichier>**.

A.3. Codes de retour du composant kavsamba

Le composant kavsamba peut renvoyer les codes suivants lors de son fonctionnement :

0	Le composant est lancé.
64	L'information relative à la licence est manquante ou bien aucune clé de licence n'a été trouvée dans les chemins spécifiés dans le fichier de configuration.
65	Impossible de charger le fichier de configuration.
70	Le composant kavsamba est corrompu.

A.4. Arguments de la ligne de commande pour le composant kavscanner

Il est possible de redéfinir les paramètres du fichier de configuration au moment du démarrage du programme à l'aide des arguments de la ligne de commande. Nous allons les aborder en détail.

Options d'aide :	
–h	Affiche sur la console l'aide du composant kavscanner.
–v	Affiche la version du programme.
Options de configuration :	
–c (–C) <chemin_du_fichier>	Utilise le fichier de configuration alternatif **<chemin_du_fichier>**.
–g<chemin_du_fichier>	Enregistre dans le fichier **<chemin_du_fichier>** la liste de tous les virus connus dont les définitions sont reprises dans les bases antivirus.
–f	Ignore la signature endommagée du composant kavscanner et tente de réparer le composant.
Options d'analyse :	
–e <options>	Modifie l'option d'analyse utilisée par défaut. Les modes suivants peuvent être utilisés en guise d'**<option>** :
P/p	Active/désactive l'analyse des fichiers compressés.
A/a	Active/désactive l'analyse des archives.
S/s	Active/désactive l'analyse des archives auto-extractibles (la désactivation de l'analyse des archives auto-extractibles requiert que l'analyse des archives soit également désactivée).

B/b	Active/désactive l'analyse des bases de données de messagerie électronique.
M/m	Active/désactive l'analyse des messages au format texte.
E/e	Active/désactive l'analyseur heuristique du code.
–R/r	Active/désactive l'analyse récursive.
-S/s	Active/désactive le mode de suivi des liens symboliques.
–l	Analyse uniquement les systèmes de fichiers locaux.
Options de composition du rapport :	
–q	N'affiche pas la notification sur la console.
–o <nom>	Spécifie le nom du fichier dans lequel le rapport d'activité du composant sera repris. Si le nom n'est pas précisé, le rapport ne sera pas composé.
–j<numéro>	Spécifie le niveau de détails du rapport en fonction du volume d'informations qu'il présente. Les niveaux suivants peuvent être attribués en guise d'**<options>** :
1	Affiche/n'affiche pas les messages sur les erreurs diverses.
2	Affiche/n'affiche pas les messages informatifs.
3	Affiche/n'affiche pas les messages relatifs à l'analyse.
10	Affiche/n'affiche pas les messages de débogage.
–x<options>	Spécifie le niveau de détails du rapport d'analyse affiché sur la console. Les niveaux suivants peuvent être attribués en guise d'**<options>** :
O/o	Format concis/étendu de la notification relative à l'analyse d'un objet simple.

C/c	Format concis/étendu de la notification relative à l'analyse d'une archive.
N/n	Active/désactive l'affichage à l'écran des notifications relatives aux fichiers sains.
P/p	Active/désactive l'affichage sur la console des notifications relatives à l'activité en cours du composant.
–m<options>	Spécifie le niveau de détails du rapport d'analyse consigné dans le fichier du rapport. Les modes suivants peuvent être utilisés en guise d'**<options>** :
O/o	Format concis/étendu de la notification relative à l'analyse d'un objet simple.
C/c	Format concis/étendu de la notification relative à l'analyse d'une archive.
N/n	Active/désactive l'affichage dans le rapport des notifications relatives aux fichiers sains.
Options des fichiers :	
–p<options> <nom_du_fichier>	Conserve la liste des objets dans le fichier spécifié ; chaque objet est conservé sur une nouvelle ligne avec son chemin d'accès complet. Les **<options>** suivantes sont envisageables :
i	Sauvegarde la liste des objets infectés dans le fichier **<nom_du_fichier>**.
s	Sauvegarde la liste des objets suspects dans le fichier **<nom_du_fichier>**.
c	Sauvegarde la liste des objets corrompus dans le fichier **<nom_du_fichier>**.
w	Sauvegarde la liste des objets dont le code est identique à celui d'un virus connu dans le fichier **<nom_du_fichier>**.

–@ <filelist.lst>	Analyse les objets dont le chemin est repris dans le fichier **<filelist.lst>**.
Options de traitement des fichiers (la définition de ces arguments dans la ligne de commande annule l'exécution de l'action définie dans le fichier de configuration) :	
–i0	Procède uniquement à l'analyse antivirus.
–i1	Répare les objets infectés. Les ignore quand la réparation n'est pas possible.
–i2	Répare les objets infectés. Si la réparation n'est pas possible, et que l'objet est simple, il est supprimé. Ne supprime pas les objets infectés du conteneur.
–i3	Répare les objets infectés. Si la réparation n'est pas possible, et que l'objet est simple, il est supprimé. Si l'objet infecté se trouve dans un conteneur, supprime tout le conteneur.
–i4	Supprime les objets infectés et les conteneurs.

A.5. Codes de retour du composant kavscanner

Le composant kavscanner peut renvoyer les codes suivants lors de son fonctionnement :

0	Aucun virus n'a été trouvé.
5	Tous les objets infectés ont été réparés.
10	Découverte d'archives protégées par un mot de passe.
15	Découverte de fichiers corrompus.
20	Découverte de fichiers suspects.
21	Découverte de fichiers dont le code est semblable à celui de virus connus.

25	Découverte de fichiers infectés.
30	Une erreur système est survenue lors de l'analyse des fichiers.
50	Impossible de charger les bases antivirus (le chemin indiqué dans le fichier de configuration n'a pas été trouvé).
55	Les bases anti-virus sont endommagées.
60	La date des bases antivirus est ultérieure à la date d'expiration de la clé de licence.
64	L'information relative à la licence est manquante ou bien aucune clé de licence n'a été trouvée dans les chemins spécifiés dans le fichier de configuration.
65	Impossible de charger le fichier de configuration.
66	Option incorrecte du fichier de configuration.
70	Le composant kavscanner est corrompu.
75	Le composant kavscanner est endommagé et ne peut pas être réparé.

A.6. Arguments de la ligne de commande pour le composant licensemanager

Options d'aide :	
–h	Affiche sur la console l'aide du composant *licensemanager*.
–v	Affiche la version du programme.
Options pour l'utilisation des clés de licence :	
–s	Affiche sur la console les informations sur l'ensemble des

	clés de licence activées.
–c (–C) <chemin_du_fichier>	Utilise le fichier de configuration alternatif **<chemin_du_fichier_de_clé>**.
–k <chemin_du_fichier>	Affiche sur la console les informations relatives à la clé **<chemin_du_fichier_de_clé>**.
–a <chemin_du_fichier>	Installe la clé de licence **<chemin_du_fichier_de_clé>**.
–d <a|r>	Supprime toutes les clés de licence/supprime la clé de licence de réserve.

A.7. Codes de retour du composant licensemanager

Le composant licensemanager peut renvoyer les codes suivants lors de son fonctionnement :

0	Le composant a bien chargé les informations relatives à la clé de licence et a terminé son travail.
30	Une erreur système est survenue lors du fonctionnement du composant.
64	L'information relative à la licence est manquante ou bien aucune clé de licence n'a été trouvée dans les chemins spécifiés dans le fichier de configuration.
65	Impossible de charger le fichier de configuration.
66	Option incorrecte du fichier de configuration.

A.8. Arguments de la ligne de commande du composant keepup2date

Options d'aide :	
–v	Affiche sur la console la version de l'application et arrête le composant.
–h	Affiche sur la console l'aide relative aux arguments de la ligne de commande pris en charge par le composant et arrête le composant.
–s	Affiche sur la console la liste des serveurs de mise à jour avec le code de région.
Options de fonctionnement :	
–r	Remise des bases antivirus à l'état antérieur à la mise à jour.
–k	N'exécute pas la commande **PostUpdateCmd** après la réussite de la mise à jour des bases antivirus.
–q	Mode de fonctionnement du composant dans lequel aucun message n'est affiché sur la console.
–e	Mode de fonctionnement du composant au cours duquel seuls les messages relatifs aux erreurs système critiques sont affichées.
–b <chemin>	Lors de la mise à jour, crée une copie de sauvegarde des bases antivirus existantes dans le répertoire **<chemin>**.
–x <chemin_du_fichier>	Copie toutes les mises à jour des bases antivirus dans le répertoire local **<chemin_du_fichier>**.
–t <chemin>	Utilise le répertoire **<chemin>** pour l'enregistrement des fichiers temporaires.

–u<chemin_du_fichier>	Copie les dernières mises à jour des bases antivirus dans le répertoire local **<chemin_du_fichier>**.
–c <chemin_du_fichier>	Utilise le fichier de configuration alternatif **<chemin_du_fichier>**. La clé fonctionne uniquement si une appplication de Kaspersky Lab est installée sur le serveur ou si l'application mise à jour est définie par l'argument **–p** (dans le cas contraire, un message relatif à l'existence de plusieurs applications sera affiché).
–g <URL>	Adresse pour la mise à jour des bases antivirus. Lorsque cette clé est redéfinie, la mise à jour sera réalisée depuis l'adresse indiquée.
–d <chemin_du_fichier>	Utilise le fichier pid du composant situé dans le répertoire local **<chemin_du_fichier>**.
Options de composition du rapport :	
–l <chemin_du_fichier>	Enregistre les résultats de l'activité du composant dans le fichier **<chemin_du_fichier>**.

A.9. Codes de retour du composant keepup2date

Le composant *keepup2date* peut renvoyer les codes suivants lors de son fonctionnement :

0	La mise à jour des bases antivirus n'est pas nécessaire.
1	La mise à jour des bases antivirus s'est déroulée sans erreurs.
10	Une erreur critique s'est produite; la mise à jour a été interrompue.
12	Une erreur s'est produite lors de la remise à l'état antérieur à la dernière mise à jour des bases antivirus.
30	Echec du lancement de la commande **PostUpdateCmd** après la mise à jour des bases.
60	L'information relative à la licence est manquante ou bien aucune clé de licence n'a été trouvée dans les chemins spécifiés dans le fichier de configuration.
75	Impossible de charger le fichier de configuration ou présence d'une erreur dans ses paramètres.

ANNEXE B. KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

B.1. Autres produits antivirus

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protège les ordinateurs personnels tournant sous Microsoft Windows 98/ME, 2000/NT/XP contre tous les types de virus connus, y compris les logiciels à risque (riskware). Le programme contrôle en permanence toute les sources d'infection potentielles : le courrier électronique, Internet, les disquettes, les CD-Rom, etc. Le système unique d'analyse heuristique des données neutralise efficacement les virus inconnus. Le logiciel peut fonctionner dans l'un des modes suivants (ces différents modes peuvent être utilisés séparément ou conjointement) :

- La **protection en temps réel** permet de rechercher la présence éventuelle de virus dans tous les objets exécutés, ouverts et enregistrés sur l'ordinateur.
- **L'analyse à la demande** permet de rechercher la présence éventuelle de virus et de réparer, le cas échéant, les objets infectés sur tout l'ordinateur ou sur des disques, dans des fichiers ou des dossiers particuliers. Cette analyse peut-être lancée manuellement ou automatiquement selon un horaire défini.

Kaspersky Anti-Virus® Personal ignore à chaque analyse les objets qui n'ont pas été modifiés depuis la dernière analyse, aussi bien dans le cadre de l'analyse en temps réel qu'à la demande. Ceci se traduit par une **nette augmentation de la rapidité d'exécution de l'application**.

Le logiciel représente donc un obstacle de taille pour les virus qui tenteraient d'infecter l'ordinateur via le courrier électronique. Kaspersky Anti-Virus® Personal analyse et répare automatiquement tous les messages entrants et sortants via les protocoles POP3 et SMTP. Il décèle également avec efficacité les virus dans les bases de données de messagerie.

Le logiciel est compatible avec plus de 700 formats de fichiers archivés ou compressés et assure l'analyse antivirale automatique de leur contenu. Il peut également supprimer tout code malveillant des fichiers archivés au format **ZIP, CAB, RAR, ARJ, LHA** et **ICE**.

La simplicité de la configuration du logiciel est assurée grâce à l'existance de trois niveaux prédéfinis : **Sécurité maximale**, **Recommandé** et **Vitesse maximale**.

Les bases de données antivirus sont actualisées toutes les trois heures. Leur distribution est garantie même en cas de coupure ou de modification de la connexion.

Kaspersky Anti-Virus® Personal Pro

Le paquet logiciel est conçu pour offrir une protection antivirale intégrale des ordinateurs personnels sous système d'exploitation Microsoft Windows 98/ME, Microsoft Windows 2000/NT, et Microsoft Windows XP, ainsi que des applications Microsoft Office. Kaspersky Anti-Virus® Personal Pro dispose d'un outil intégré de mise à jour pour le téléchargement des bases de données antivirus et des modules de programmes. Un système exclusif d'analyse heuristique détecte efficacement même les virus inconnus. Ce système d'analyse heuristique de seconde génération parvient à neutraliser les virus inconnus. L'utilisateur peut facilement configurer l'application à travers une interface simple et facile.

Kaspersky Anti-Virus® Personal Pro possède les caractéristiques suivantes :

- **Analyse à la demande** des unités locales ;
- **Protection automatique en temps réel** de tous les fichiers, contre les virus;
- **Filtre de courrier** qui analyse et désinfecte automatiquement tout le trafic de messagerie entrant et sortant de n'importe quel client de messagerie utilisant les protocoles POP3 et SMTP et détecte efficacement les virus dans les bases de données de messagerie ;
- **Bloqueur de comportements** qui assure une protection maximale des applications MS Office contre les virus ;
- **Analyseur de fichier compressés –** Kaspersky Anti-Virus prend en charge plus de 700 formats de fichiers d'archives ou compressés ; il assure l'analyse antivirale automatique de leur contenu, ainsi que la suppression de tout code dangereux dans les fichiers au format **ZIP**, **CAB**, **RAR**, **ARJ**, **LHA** ou **ICE**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Microsoft Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus provenant d'un réseau local adjacent et d'Internet.

Kaspersky® Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte n'importe quelle action d'une application suspecte et bloque son accès au réseau. Cette solution permet de protéger vos données confidentielles sur votre machine.

La technologie SmartStealth™ rend la détection de votre ordinateur depuis l'extérieur très difficile: en étant invisible, votre ordinateur est protégé contre les attaques des pirates informatiques et cela n'a absolument aucune influence négative sur votre utilisation d'Internet. Le logiciel garantit la transparence et l'accès normal aux données.

Kaspersky® Anti-Hacker bloque les attaques réseau malicieuses les plus fréquentes et est à l'affût des tentatives d'analyse des ports de votre ordinateur.

Le logiciel permet une administration simplifiée, avec un choix de cinq niveaux de sécurité. Par défaut, le logiciel démarre en mode apprentissage, qui configure automatiquement la sécurité de votre système en fonction de vos réponses à des événements variés. Ce mode permet de configurer le pare-feu pour un utilisateur et un ordinateur particulier.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite est une suite logicielle conçue pour organiser la protection intégrée des ordinateurs personnels tournant sous Microsoft Windows. Cette solution bloque l'intrusion des programmes malveillants et des riskwares via toutes les sources d'infection possible, vous protège contre l'accès non-autorisés à vos données et lutte contre le courrier indésirable.

Kaspersky® Personal Security Suite possède les fonctions suivantes :

- Protection des données de votre ordinateur contre les virus.
- Protection des utilisateurs des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express contre le courrier indésirable.
- Protection de l'ordinateur contre l'accès non-autorisé aux données ainsi que contre les attaques de pirates informatiques réalisées depuis le réseau local ou Internet.

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la "météo" des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d'informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S'abonner et se désabonner aux canaux d'information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d'informations non lues;

- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l'information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky OnLine Scanner

Il s'agit d'un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l'ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs inquiétudes sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s'agit d'un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l'ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs inquiétudes sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky Anti-Virus 6.0

Kaspersky Anti-Virus 6.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.

- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers**. Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive**. Kaspersky Anti-Virus 6.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus normaux.
- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.
- **Bloquer les macros Visual Basic for Applications dangereuses** dans les documents Microsoft Office.
- **Restaurer le système** après les actions malveillantes des logiciels espion : grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espion. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés (Microsoft Office Outlook, Microsoft Outlook Express et The Bat!)
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.

- **Protection du système de fichiers :** n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système arpès une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer.

Kaspersky® Internet Security 6.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif (**technologie SmartStealth™**) empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé,toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos téléphones intelligents. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;

- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

Kaspersky® Security for PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés grâce au chiffrement de l'accès à l'appareil et à l'ensemble des données sauvegardées des ordinateurs portables ou des cartes mémoire.

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile garantit la protection antivirus des appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le logiciel est capable de réaliser des analyses antivirus sophistiquées dont :

- **L'analyse à la demande** de la mémoire de l'appareil nomade, de la carte mémoire, d'un répertoire particulier ou d'un fichier distinct. En cas de découverte d'un objet infecté, il sera placé dans le répertoire de quarantaine ou il sera supprimé ;
- **L'analyse en temps réel :** tous les objets entrants ou modifiés sont automatiquement analysés, de même que les fichiers auxquels des requêtes sont adressées ;
- **L'analyse programmée** des informations conservées dans la mémoire de l'appareil nomade ;
- **Protection contre les sms et mms indésirables.**

Kaspersky Anti-Virus® Business Optimal

Ce paquet logiciel offre une protection intégrale des données sur des réseaux des petites et moyennes entreprises.

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale[1] intégrale de :

- Postes de travail sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD et Linux et les entrepôts de fichiers sous Samba ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail et qmail ;

[1] En fonction du type de livraison

- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition.

Kaspersky Anti-Virus® Business Optimal comprend également un système d'installation et d'administration centralisé : le Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

Ce paquet logiciel offre une protection intégrale des données sur des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Compatibles avec la majorité des systèmes d'exploitation et des applications utilisés actuellement, les composants sont unis par un système d'administration centralisé et disposent d'une interface utilisateur identique. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

- *Postes de travail* sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD et Linux et les entrepôts de fichiers sous Samba ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail et qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition, Microsoft ISA Server 2004 Enterprise Edition ;
- *Ordinateurs de poche* sous Symbian OS, Microsoft Windows CE et Palm OS et téléphones intelligents tournant sous Microsoft Windows Mobile 2003 for Smartphone et Microsoft Smartphone 2002.

Kaspersky® Corporate Suite dispose également d'un *système d'installation et d'administration centralisé* : Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques

révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix est une solution conçue pour le traitement antivirus des messages livrés via le protocole SMTP. L'application contient toute une série d'outils de filtrage du flux de messagerie : selon le nom et le type MIME des fichiers joints ainsi que plusieurs moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques. Citons, entre autres, les restrictions au niveau de la taille des messages, du nombre de destinataires, etc. La prise en charge de la technologie DNS Black List évite de recevoir des messages en provenance de serveurs repris dans la liste des serveurs de diffusion de courrier indésirable.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange recherche la présence éventuelle de virus dans le courrier entrant et sortant, ainsi que dans les messages enregistrés sur le serveur, y compris les messages dans les dossiers partagés. Il rejette également le courrier indésirable grâce à l'exploitation de technologies intelligentes d'identification des messages non sollicités conjointement aux technologies développées par Microsoft. L'application recherche la présence d'éventuels virus dans tous les messages qui arrivent sur le serveur Exchange via le protocole SMTP à l'aide de technologies mises au point par Kaspersky Lab et identifie le courrier indésirable grâce à des filtres formels (adresse électronique, adresse IP, taille du message, en-tête) et à l'analyse du contenu du message et des pièces jointes à l' aide de technologies intelligentes dont des signatures graphiques uniques qui permettent d'identifier le courrier indésirable sous forme graphique. Le corps du message et les pièces jointes sont soumis à l'analyse.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des systèmes de messagerie. L'application, qui est installée entre le pare-feu de l'entreprise et Internet, analyse tous les éléments du message électronique et recherche la présence éventuelle de virus et d'autres

programmes malveillants (spyware, adware, etc.). Il opère également un filtrage centralisé du courrier afin d'identifier le courrier indésirable. Le logiciel offre aussi plusieurs autres possibilités en matière de filtrage des flux de messagerie. L'application contient un ensemble d'outils de filtrage du courrier selon les noms et les types MIME des pièces jointes ainsi que divers moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques.

Kaspersky® Anti-Virus for Proxy Server

Kaspersky® Anti-Virus for Proxy Server est une solution antivirus développée pour la protection du trafic Internet transmis sur le protocole http via le serveur proxy. L'application analyse en temps réel le trafic Internet, empêche l'intrusion de programmes malveillants suite à la visite de sites Web et analyse les fichiers téléchargés via le réseau Internet.

Kaspersky® Anti-Virus for MIMESweeper for SMTP

Kaspersky® Anti-Virus for MIMESweeper for SMTP offre une analyse antivirus rapide du trafic SMTP sur les serveurs utilisant Clearswift MIMESweeper.

Le logigiciel se présente sous la forme d'un module externe pour MIMESweeper for SMTP de l'éditeur Clearswift. Il analyse en temps réel et traite le courrier entrant et sortant.

ANNEXE C. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul ; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. *Assistance technique.*

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus connus ou qu'il n'affichera pas de message de détection erroné.

(iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. *Limites de Responsabilité.*

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres) :

(a) Perte de revenus ;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);

(c) Perte de moyens de paiement ;

(d) Perte d'économies prévues ;

(e) Perte de marché ;

(f) Perte d'occasions commerciales ;

(g) Perte de clientèle ;

(h) Atteinte à l'image ;

(i) Perte, endommagement ou corruption des données ; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.