

KASPERSKY LAB

Kaspersky® Anti-Virus 5.5 for Linux and FreeBSD
Workstation and File Server

MANUEL DE
L'ADMINISTRATEUR

KASPERSKY® ANTI-VIRUS 5.5 FOR
LINUX AND FREEBSD WORKSTATION AND FILE SERVER

Manuel de l'administrateur

©Kaspersky Lab Ltd
Tél./Fax : +7 (495) 797-87-00
<http://www.kaspersky.com/fr>

Date d'édition : septembre 2006

Sommaire

CHAPITRE 1. INTRODUCTION	6
1.1. Virus informatiques et programmes malveillants	7
1.2. Présentation et fonctions principales de Kaspersky Anti-Virus.....	8
1.3. Nouveautés de la version 5.5	8
1.4. Licences	9
1.5. Configuration requise	10
1.6. Contenu du pack logiciel	11
1.7. Services réservés aux utilisateurs enregistrés	12
1.8. Notations conventionnelles	12
CHAPITRE 2. ALGORITHME DE FONCTIONNEMENT DE L'APPLICATION	14
CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS	16
3.1. Installation du logiciel sur un ordinateur Linux.....	16
3.2. Installation du logiciel sur un ordinateur FreeBSD	17
3.3. Procédure d'installation	17
3.4. Mise à niveau de l'application jusqu'à la version 5.5.....	18
3.5. Installation de la clé de licence.....	18
3.6. Répartition des fichiers de l'application dans les divers répertoires	19
3.7. Fin de l'installation	22
CHAPITRE 4. CONFIGURATION DE L'APPLICATION APRÈS L'INSTALLATION .	23
4.1. Configuration de l'application par défaut	23
4.2. Installation des bases antivirus	24
4.3. Configuration de l'administration avec Webmin	24
CHAPITRE 5. UTILISATION DE KASPERSKY ANTI-VIRUS.....	26
5.1. Mise à jour des bases antivirus.....	26
5.1.1. Nouvelles possibilités du composant de mise à jour.....	27
5.1.2. Mise à jour automatique des bases anti-virus	28
5.1.3. Mise à jour à la demande des bases antivirus	30
5.1.4. Création d'un répertoire réseau pour la conservation et la copie des bases antivirus	31

5.2. Protection antivirus des systèmes de fichiers.....	32
5.2.1. Zone d'analyse.....	33
5.2.2. Mode d'analyse et de réparation des objets.....	34
5.2.3. Actions à exécuter sur les objets.....	35
5.2.4. Analyse à la demande d'un répertoire particulier	36
5.2.5. Analyse programmée	36
5.2.6. Autres possibilités : utilisation de fichiers de script	37
5.2.6.1. Réparation des objets infectés dans une archive.....	37
5.2.6.2. Envoi de messages d'alerte à l'administrateur	38
5.3. Protection antivirus en temps réel.....	39
5.4. Gestion des clés de licence	40
5.4.1. Consultation des informations relatives à la clé de licence.....	40
5.4.2. Prolongation de la licence	42
CHAPITRE 6. CONFIGURATION COMPLÉMENTAIRE	44
6.1. Optimisation du fonctionnement de Kaspersky Anti-Virus.....	44
6.2. Transfert d'objets dans le répertoire de quarantaine.....	46
6.3. Mode de copie de sauvegarde des objets (backup).....	47
6.4. Adaptation du format d'affichage de la date et de l'heure.....	48
6.5. Paramètres de composition des rapports de Kaspersky Anti-Virus	49
CHAPITRE 7. SUPPRESSION DE KASPERSKY ANTI-VIRUS.....	51
CHAPITRE 8. VERIFICATION DU BON FONCTIONNEMENT DU LOGICIEL ANTIVIRUS.....	52
ANNEXE A. RENSEIGNEMENTS COMPLÉMENTAIRES SUR L'APPLICATION ...	54
A.1. Fichier de configuration de Kaspersky Anti-Virus	54
A.2. Arguments de la ligne de commande pour le composant kavscanner.....	62
A.3. Codes de retour du composant kavscanner	65
A.4. Arguments de la ligne de commande pour le composant kavmonitor.....	67
A.5. Arguments de la ligne de commande pour le composant licensemanager	67
A.6. Codes de retour du composant licensemanager.....	68
A.7. Arguments de la ligne de commande du composant keepup2date	68
A.8. Codes de retour du composant keepup2date	70
ANNEXE B. QUESTIONS FREQUEMMENT POSEES.....	71
ANNEXE C. KASPERSKY LAB	78

C.1. Autres produits antivirus	79
C.2. Coordonnées	88
ANNEXE D. CONTRAT DE LICENCE	89

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 accroissent le risque d'infection des ordinateurs par des virus informatiques et exposent les données à un plus grand danger de dégradation ou de vol de données 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 illicite à votre ordinateur et, par conséquent, à vos données, aux ressources de réseau et à d'autres sources d'information.

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 " crash " 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 rencontrés sur 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

Kaspersky® Anti-Virus for Linux and FreeBSD Workstation and File Server (par la suite *Kaspersky Anti-Virus* ou l'*application*) a été développé pour assurer la protection antivirus des serveurs de fichiers et des postes de travail tournant sous Linux ou FreeBSD.

Kaspersky Anti-Virus for Linux and FreeBSD permet de :

- *Assurer la protection en temps réel du système de fichiers contre les codes malveillants* : interception des requêtes adressées aux fichiers ; analyse ; réparation ou suppression des objets infectés.
- *Analyser les objets à la demande* : recherche des objets infectés et suspects (y compris dans les secteurs d'analyse définis) ; analyse des objets ; réparation et suppression des objets infectés.
- *Mettre en quarantaine les objets suspects et corrompus* : conservation des fichiers suspects dans le dossier de quarantaine.
- *Créer une copie de l'objet infecté dans le répertoire de sauvegarde avant la réparation ou la suppression* afin de pouvoir éventuellement le restaurer à la demande au cas où il contiendrait des données importantes ou d'étudier l'infection.
- *Mettre à jour les bases antivirus* ; elles sont téléchargées depuis les serveurs de mise à jour de Kaspersky Lab. Il est également possible de procéder à la mise à jour depuis un répertoire local.
- *Administrer et configurer Kaspersky Anti-Virus* par l'intermédiaire de l'interface Web du programme Webmin et du fichier de configuration du logiciel.

1.3. Nouveautés de la version 5.5

Les modifications suivantes ont été introduites dans **Kaspersky Anti-Virus 5.5 for Linux and FreeBSD Workstation and File Server** :

- Le composant *kavmonitor* a été ajouté. Il garantit la protection en temps réel des fichiers contre les virus.
- Intégration de nouvelles technologies d'obtention des mises à jour des bases antivirus et des modules de l'application, dont la vérification de l'intégrité et de la possibilité d'utiliser les bases téléchargées. Le trafic de réseau est ainsi fortement réduit.
- Sélection du type de bases antivirus téléchargées (standard ou étendues). Qui plus est, il est possible de définir le type de bases utilisées pour chaque composant de l'application pris séparément.
- Simplification de la procédure d'installation et de suppression de l'application.
- Importation de la configuration de la version antérieure d'Anti-Virus (version 5.0) lors de l'installation. Il est ainsi possible d'obtenir plus rapidement une configuration opérationnelle.
- Possibilité de créer un dossier de sauvegarde pour conserver les copies des objets suspects ou infectés avant de les réparer ou de les supprimer. Cela permet d'éviter la perte des données originales au cas où un problème surviendrait pendant la réparation de l'objet.
- Afin de réduire la charge sur le processeur lors de l'exécution de l'analyse antivirus, l'application exploite les technologies de consultation de la base de données iChecker™ et de la mise en cache à deux niveaux des objets analysés.
- Possibilité de limiter le nombre d'objets analysés simultanément en arrière plan, ce qui permet d'optimiser la charge de l'ordinateur.
- Possibilité de générer la liste des virus découverts.
- Plus grand choix d'actions à exécuter en cas de découverte d'objets de divers statuts.
- Prise en charge de la plate-forme 64 bits.
- Plus d'options pour l'analyse antivirus à la demande.

1.4. Licences

La politique de licence appliquée à Kaspersky Anti-Virus prévoit une restriction de l'utilisation de l'application sur la base de la **durée d'utilisation** (il s'agit en général d'une durée de validité d'un an à dater de l'acquisition de l'application).

1.5. Configuration requise

Kaspersky Anti-Virus donnera les meilleurs résultats dans les configurations suivantes :

- Configuration matérielle :
 - 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.
 - RedHat Fedora Core 5.
 - SUSE Linux Enterprise Server 9.0 SP3.
 - Novell Linux Desktop 9.
 - 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 LES 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 ;
- Paquets d'installation pour la compilation de programme (gcc, binutils, glibc-devel, make, ld) ainsi que le noyau de code source du système d'exploitation pour l'utilisation du composant *kavmonitor*.



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.

1.6. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-Virus chez un distributeur ou détaillant, ou visiter l'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 N° de série du produit) ;
- 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.

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 implique que vous acceptez les termes du contrat de licence.

1.7. 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 antivirus ;
- 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.

1.8. 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 du menu, des options du menu, des fenêtres, des éléments des boîtes de dialogue, etc.

Mise en forme	Fonction sémantique
 Remarque.	Informations complémentaires, remarques.
 Attention !	Informations auxquelles il est recommandé d'accorder une attention particulière.
 Pour exécuter une action, <ol style="list-style-type: none"> 1. Etape 1. 2. ... 	Description de la séquence d'étapes que l'utilisateur doit suivre ou des actions possibles.
 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. ALGORITHME DE FONCTIONNEMENT DE L'APPLICATION

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

Kaspersky Anti-Virus comprend :

- *Kavscanner*, le composant d'analyse antivirus à la demande ;
- *Kavmonitor*, le composant d'analyse antivirus en temps réel;
- *Keepup2date*, le module de mise à jour des bases antivirus;
- *Licensemanager*, l'utilitaire de gestion des clés de licence ;
- *Le module d'administration à distance* pour Webmin.

Voici une présentation détaillée de l'algorithme de fonctionnement de l'application dans le cadre de la protection en temps réel (c.-à-d. à l'aide de *kavmonitor*).

Les étapes sont les suivantes :

1. Lorsqu'un programme quelconque adresse une requête à un objet du système de fichiers (requête d'ouverture, d'exécution ou de fermeture de fichier), celle-ci est interceptée par le module du moteur de *kavmonitor* et le fichier est soumis à l'analyse antivirus.
2. Le traitement du fichier intercepté est réalisé à l'aide d'un démon faisant partie de *kavmonitor*. Le démon 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 restauration à l'aide des bases antivirus, pour autant que cette option ait été activée).
3. Après le traitement du fichier, le module envoie à *kavmonitor* le code de retour (autorisé/refusé) définissant l'état du fichier.
4. Conformément à l'état de l'objet, le composant *kavmonitor* autorise l'accès au fichier ou le bloque (dans ce cas, le fichier reçoit un code d'erreur (Access denied)).

Suite à l'analyse (et au traitement), le fichier peut avoir un des états suivants :

- **Clean** : l'objet est sain.
- **Infected** : l'objet est infecté.
- **Cured** : l'objet infecté a pu être réparé.
- **CureFailed** : l'objet infecté n'a pas pu être réparé.
- **Warning** : le code de l'objet ressemble à celui d'un virus connu.
- **Suspicious** : l'objet pourrait être infecté par un virus inconnu.
- **Protected** : l'objet ne peut pas être analysé car il est crypté.
- **Corrupted** : l'objet est corrompu.
- **Error** : l'analyse de l'objet a entraîné une erreur système.

Les actions exécutées sur l'objet correspondant à un état particulier sont définies par les paramètres du fichier de configuration (pour de plus amples informations, consulter l'Annexe A à la page 54).

CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS

Il est conseillé de procéder aux vérifications reprises ci-après avant d'entamer 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 1.5, page 9). Le cas échéant, nous vous conseillons d'installer les applications comme Perl par exemple afin que vous puissiez exploiter toutes les fonctions du logiciel.
- Configurez la connexion Internet.
- Ouvrez la session avec les privilèges d'administrateur (**root**).

3.1. Installation du logiciel sur un ordinateur 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 ordinateur FreeBSD

Le fichier d'installation de Kaspersky Anti-Virus pour les ordinateurs 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

L'installation de l'application s'opère en mode automatique et comprend les étapes suivantes :

1. Copie des fichiers d'installation sur l'ordinateur.
2. Installation de la clé de licence.

Kaspersky Anti-Virus ne fonctionnera pas sans la clé de licence.

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 (pour de plus amples informations sur l'installation de la clé, consultez le point 0 à la page 40).

3. Configuration de *keepup2date*, le composant de mise à jour des bases antivirus.
4. L'installation (mise à jour) des bases antivirus ;



N'oubliez pas d'installer les bases antivirus avant la première utilisation de l'application. L'analyse et le traitement des fichiers sans bases antivirus est impossible.

5. Installation du module Webmin.

Le module d'administration à distance sera installé uniquement si *les chemins d'installation par défaut ont été utilisés lors de l'installation du paquet Webmin*. Une fois le module installé, vous recevrez les recommandations de configuration correspondantes pour son interaction avec l'application.



Lors de l'utilisation du système d'exploitation Linux, il ne faut pas oublier que la mise à jour du module du noyau du système d'exploitation doit s'accompagner de la mise à jour du module du noyau du composant kavmonitor

3.4. Mise à niveau de l'application jusqu'à la version 5.5

Une fois que l'application a été installée, le système recherche la présence éventuelle d'une version de Kaspersky Anti-Virus antérieure à la version 5.5.

Si une telle version existe, *certains paramètres de la version antérieure* seront importés dans le fichier de configuration de la version 5.5.



La suppression de la distribution de la version antérieure de Kaspersky Anti-Virus n'est pas réalisée lors de l'installation. Cette tâche revient à l'administrateur.

Une partie des paramètres standard du fichier de configuration (par exemple, le chemin d'accès au répertoire des bases antivirus) *n'est pas exportée*. Ils devront être définis lors de l'installation.

De plus, la logique de fonctionnement des composants individuels dans la version 5.5 a été quelque peu modifiée et de nouvelles options ont été introduites. C'est la raison pour laquelle il est conseillé de vérifier la bonne composition du fichier de configuration avant de commencer à utiliser l'application.

3.5. Installation de la clé de licence

La recherche de la clé de licence, le fichier indispensable au fonctionnement de Kaspersky Anti-Virus (le fichier avec l'extension *key*), se déroule à cette étape de l'installation. Ce fichier débloque toutes les fonctions de l'application. Il sera impossible d'utiliser Kaspersky Anti-Virus sans avoir installé au préalable la clé de licence.

Lorsque la clé de licence a été trouvée, le message correspondant apparaît sur la console et l'installation passe à l'étape suivante, à savoir l'installation des bases antivirus.

Si la clé de licence est introuvable, l'administrateur a la possibilité de saisir le chemin d'accès complet vers celle-ci. Si la clé de licence n'existe pas, abstenez-vous de saisir le chemin d'accès et poursuivez l'installation.

Dès que vous aurez reçu la clé de licence, il faudra l'installer (pour de plus amples informations, consultez le point 0 à la page 40).

3.6. Répartition des fichiers de l'application dans les divers répertoires



Après l'installation de Kaspersky Anti-Virus sur un poste de travail tournant sous Linux, les fichiers de la distribution sont répartis de la manière suivante :

/etc/opt/kaspersky/ : répertoire contenant le fichier de configuration de Kaspersky Anti-Virus :

kav4ws.conf : le fichier de configuration.

/opt/kaspersky/kav4ws/ : le répertoire principal de Kaspersky Anti-Virus reprenant :

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

kav4ws-kavscanner : fichier exécutable du composant chargé de la protection antivirus ;

kav4ws-keepup2date : fichier exécutable chargé de la mise à jour des bases antivirus ;

kav4ws-licensemanager : fichier exécutable pour la gestion des clés de licence.

/lib/ : répertoire où se trouvent les fichiers de service de Kaspersky Anti-Virus.

/man/ : répertoire contenant les fichiers man.

/sbin/ : répertoire où se trouvent les services de Kaspersky Anti-Virus.

kav4ws-kavmonitor : fichier exécutable du composant chargé de la protection antivirus ;

/src/ : répertoire contenant le module du moteur antivirus de l'application.

/opt/kaspersky/kav4ws/share/contrib/kav4ws.wbm : module externe pour l'application Webmin.

/opt/kaspersky/kav4ws/share/contrib/vox.sh : script *vox.sh* utilisé pour la réparation des archives.

/opt/kaspersky/kav4ws/share/doc/LICENSE : le contrat de licence.

/var/opt/kaspersky/kav4ws/bases : le répertoire contenant les bases antivirus ;

/var/opt/kaspersky/kav4ws/bases.backup : le répertoire contenant les bases antivirus d'actualité avant la dernière mise jour ;



Afin d'activer le système d'aide de Kaspersky Anti-Virus (les pages man), donnez la valeur */opt/kaspersky/kav4ws/man* à la variable **MANPATH**.



Après l'installation de Kaspersky Anti-Virus sur un poste de travail tournant sous FreeBSD, les fichiers de la distribution sont répartis de la manière suivante :

/usr/local/etc/kaspersky/ : répertoire contenant le fichier de configuration de Kaspersky Anti-Virus :

kav4ws.conf : le fichier de configuration.

/usr/local/bin/ : le répertoire contenant les exécutables de l'ensemble des composants de Kaspersky Anti-Virus :

kav4ws-kavscanner : fichier exécutable du composant chargé de la protection antivirus ;

kav4ws-keepup2date : fichier exécutable chargé de la mise à jour des bases antivirus ;

kav4ws-licensemanager : fichier exécutable pour la gestion des clés de licence.

/usr/local/sbin/ : répertoire où se trouvent les services de Kaspersky Anti-Virus.

kav4ws-kavmonitor : fichier exécutable du composant chargé de la protection antivirus ;

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

/usr/local/src/kav4ws/ : répertoire contenant le module du moteur antivirus de l'application.

/usr/local/share/kav4ws/contrib/kav4ws.wbm : module externe pour l'application Webmin.

/usr/local/share/kav4ws/contrib/vox.sh : script vox.sh utilisé pour la réparation des archives.

/usr/local/share/doc/kav4ws/LICENSE : le contrat de licence.

/var/db/kaspersky/kav4ws/bases : le répertoire contenant les bases antivirus ;

/var/db/kaspersky/kav4ws/bases.backup : le répertoire contenant les bases antivirus d'actualité avant la dernière mise à jour ;



Après l'installation de Kaspersky Anti-Virus sur un serveur tournant sous Linux, les fichiers de la distribution sont répartis de la manière suivante :

/etc/opt/kaspersky/ : répertoire contenant le fichier de configuration de Kaspersky Anti-Virus :

kav4fs.conf : le fichier de configuration.

/opt/kaspersky/kav4fs/ : le répertoire principal de Kaspersky Anti-Virus reprenant :

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

kav4fs-kavscanner : fichier exécutable du composant chargé de la protection antivirus ;

kav4fs-keepup2date : fichier exécutable chargé de la mise à jour des bases antivirus ;

kav4fs-licensemanager : fichier exécutable pour la gestion des clés de licence.

/lib/ : répertoire où se trouvent les fichiers de service de Kaspersky Anti-Virus.

/man/ : répertoire contenant les fichiers man.

/sbin/ : répertoire où se trouvent les services de Kaspersky Anti-Virus.

kav4fs-kavmonitor : fichier exécutable du composant chargé de la protection antivirus ;

/src/ : répertoire contenant le module du moteur antivirus de l'application.

/opt/kaspersky/kav4ws/share/contrib/kav4fs.wbm : module externe pour l'application Webmin.

/opt/kaspersky/kav4fs/share/contrib/vox.sh : script *vox.sh* utilisé pour la réparation des archives.

/opt/kaspersky/kav4fs/share/doc/LICENSE : le contrat de licence.

/var/opt/kaspersky/kav4fs/bases : le répertoire contenant les bases antivirus ;

/var/opt/kaspersky/kav4fs/bases.backup : le répertoire contenant les bases antivirus d'actualité avant la dernière mise à jour ;



Afin d'activer le système d'aide de Kaspersky Anti-Virus (les pages man), donnez la valeur ***/opt/kaspersky/kav4fs/man*** à la variable ***MANPATH***.



Après l'installation de Kaspersky Anti-Virus sur un serveur tournant sous FreeBSD, les fichiers de la distribution sont répartis de la manière suivante :

/usr/local/etc/kaspersky/ : répertoire contenant le fichier de configuration de Kaspersky Anti-Virus :

kav4fs.conf : le fichier de configuration.

`/usr/local/bin/` : le répertoire contenant les exécutable de l'ensemble des composants de Kaspersky Anti-Virus :

`kav4fs-kavscanner` : fichier exécutable du composant chargé de la protection antivirus ;

`kav4fs-keepup2date` : fichier exécutable chargé de la mise à jour des bases antivirus ;

`kav4fs-licensemanager` : fichier exécutable pour la gestion des clés de licence.

`/usr/local/sbin/` : répertoire où se trouvent les services de Kaspersky Anti-Virus.

`kav4fs-kavmonitor` : fichier exécutable du composant chargé de la protection antivirus ;

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

`/usr/local/src/kav4fs/` : répertoire contenant le module du moteur antivirus de l'application.

`/usr/local/share/kav4fs/contrib/kav4fs.wbm` : module externe pour l'application Webmin.

`/usr/local/share/kav4fs/contrib/vox.sh` : script `vox.sh` utilisé pour la réparation des archives.

`/usr/local/share/doc/kav4fs/LICENSE` : le contrat de licence.

`/var/db/kaspersky/kav4fs/bases` : le répertoire contenant les bases antivirus ;

`/var/db/kaspersky/kav4fs/bases.backup` : le répertoire contenant les bases antivirus d'actualité avant la dernière mise à jour ;



Les exemples donnés ultérieurement concerneront les composants pour une installation sur un serveur tournant sous Linux.

3.7. Fin de l'installation

Si l'installation a réussi, le *message de circonstance* s'affichera. Le fichier de configuration livré avec l'application contient tous les paramètres indispensables pour commencer à utiliser l'application.

Il existe toutefois toute une série de paramètres qui ne sont pas définis lors de l'installation. Ces paramètres sont néanmoins importants car ils permettent d'utiliser Kaspersky Anti-Virus au maximum de ses possibilités. Autrement dit, après l'installation de l'application, il est conseillé de procéder à la configuration (cf. point Chapitre 4, p.23).

CHAPITRE 4. CONFIGURATION DE L'APPLICATION 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. De plus, 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, page 23).

Vous trouverez ci-après une description détaillée des paramètres de Kaspersky Anti-Virus acceptés par défaut ainsi qu'une liste des paramètres que l'administrateur *est invité à définir avant de commencer à utiliser l'application*.

4.1. Configuration de l'application par défaut

Tous les paramètres de fonctionnement de Kaspersky Anti-Virus sont repris dans le fichier de configuration **kav4fs.conf** utilisé par défaut.

La configuration de Kaspersky Anti-Virus est la suivante :

- Kaspersky Anti-Virus démarre automatiquement au lancement du système d'exploitation. L'application intercepte et analyse toutes les requêtes adressées au système de fichiers. En cas de découverte d'objets infectés, suspects ou corrompus, Kaspersky Anti-Virus consigne les messages correspondant dans le rapport **kavmonitor.log**.
- Lors du lancement de l'analyse à la demande sans arguments via la ligne de commande, les répertoires et le système de fichiers de l'ordinateur sont analysés, en commençant par le répertoire actuel. Les messages relatifs aux résultats de l'analyse de Kaspersky Anti-Virus sont affichés et consignés dans le rapport **kavscanner.log**.



Par défaut, les objets infectés ne sont ni réparés, ni isolés.

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 actualisées.



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/ kav4fs-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 l'administration avec Webmin

Si vous envisagez l'administration à distance de Kaspersky Anti-Virus, nous vous conseillons de configurer l'application 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 !**

CHAPITRE 5. UTILISATION DE KASPERSKY ANTI-VIRUS

Grâce à Kaspersky Anti-Virus, vous pouvez mettre sur pied la protection de votre ordinateur contre les virus : depuis un fichier particulier jusqu'au système de fichiers dans son ensemble.

La fonctionnalité de l'application repose sur les tâches que l'administrateur peut exécuter grâce à lui. Les tâches exécutées à l'aide de Kaspersky Anti-Virus peuvent être réparties en trois catégories :

- Actualisation des bases antivirus utilisées pour la recherche de virus et la réparation des objets infectés (pour de plus amples informations, consultez le point 5.1 à la page 26).
- Protection antivirus du système de fichiers de l'ordinateur (analyse programmée et/ou à la demande) (pour de plus amples informations, consultez le point 5.2 à la page 32).
- Protection antivirus en temps réel (pour de plus amples informations, consultez le point à la page 39).

Le présent chapitre est consacré aux tâches génériques liées à l'utilisation de Kaspersky Anti-Virus. Libre à vous, dans le cadre de votre entreprise, de les combiner ou de les rendre plus complexes.

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 de bases antivirus sont publiées toutes les heures 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 et 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 5.1.4 à la page 31.

Les mises à jour peuvent être programmées par l'intermédiaire de **cron** (cf. point 5.1.2, page 28) ou lancées à la demande par l'administrateur depuis la ligne de commande (cf. point 5.1.3, page 30).



Il est vivement conseillé de procéder à la mise à jour des bases antivirus toutes les heures !

5.1.1. Nouvelles possibilités du composant de mise à jour

Le composant d'actualisation des bases antivirus de la *version 5.5* de Kaspersky Anti-Virus *diffère de celui des versions précédentes*. Plusieurs des fonctions existantes ont été améliorées et de nouvelles possibilités ont été ajoutées :

- Sélection automatique du serveur de mise à jour le plus proche sur la base de la région indiquée dans le fichier de configuration ;
- Possibilité de télécharger et d'installer des mises à jour progressives en cas de publication d'une mise à jour cumulée, ce qui réduit le trafic sur le réseau.
- En cas de déconnexion pendant le téléchargement des mises à jour ou de changement de serveur après l'établissement de la connexion, le

composant téléchargera automatiquement les données manquantes des bases antivirus.

- Analyse de l'intégrité des bases téléchargées.
- Analyse des bases antivirus installées et téléchargement uniquement des éléments modifiés ou ajoutés. Cette mesure vise à réduire le trafic sur le réseau.
- Lancement de la commande spécifiée par l'utilisateur de rechargement des bases antivirus après une mise à jour réussie.
- Prise en charge du retour à la version antérieure à la mise à jour.
- Le nouveau composant peut fonctionner sans wget.
- Sélection du type de bases antivirus téléchargées (standard ou étendues).

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.

5.1.2. Mise à jour automatique des bases anti-virus

Vous pouvez programmer la mise à jour automatique des bases antivirus en modifiant le fichier de configuration.



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 commun pour tous les lancements de tâches, n'afficher aucune information sur la console.



Solution: réalisez les opérations 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=1
```

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/bin/kav4fs-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: réalisez les opérations 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: réalisez les opérations 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: réalisez les opérations 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 **UseUpdateServerUriOnly** . De plus, le paramètre **UpdateServerUrl** doit contenir l'adresse du serveur de mise à jour.

5.1.3. 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 :

```
# kav4fs-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: réalisez les opérations 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 :

```
# kav4fs-keepup2date -l /tmp/report.txt
```

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

Pour que l'actualisation des bases antivirus au départ d'un répertoire 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 réseau pour la copie ultérieure des bases antivirus sur les postes du réseau.



Solution: réalisez les opérations décrites ci-après pour exécuter cette tâche :

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

```
# kav4fs-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: réalisez les opérations 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 authentification.

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 des systèmes de fichiers

La protection antivirus des systèmes de fichiers de l'ordinateur est confiée au composant *kavscanner* qui analyse et traite les objets infectés et suspects conformément aux paramètres.



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



Par défaut, l'analyse à la demande peut être lancée exclusivement par l'utilisateur **root**.

Vous pouvez analyser aussi bien l'ensemble du système de fichiers que des répertoires ou des objets distincts. Les paramètres de la protection peuvent être rassemblés au sein de groupes définissant :

- La zone d'analyse (cf. point 5.2.1, page 33).
- Le mode d'analyse et de réparation des objets (cf. point 5.2.2, page 34).
- Les actions exécutées sur les objets (cf. point 5.2.3, page 35).
- Les paramètres de composition des rapports sur le résultat des activités (cf. point 6.5, page 49).

L'analyse des systèmes de fichiers de l'ordinateur peut être lancée :

- A la demande au départ de la ligne de commande (cf. point 5.2.4, p. 36).
- Selon un horaire défini à l'aide du programme **cron** (cf. point 5.2.5, page 36).



La recherche de la présence éventuelle de virus est un processus qui peut monopoliser énormément de ressources si elle porte sur l'ensemble de l'ordinateur. N'oubliez pas que ce processus ralentira l'ordinateur et que pour cette raison, il est conseillé de ne pas lancer d'autres processus en parallèle. Afin d'éviter ces inconvénients, nous vous conseillons d'analyser des répertoires distincts.

5.2.1. Zone d'analyse

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

- *le chemin de d'analyse* c.-à-d. la liste des répertoires et des fichiers soumis à la recherche de virus ;
- *Les objets à analyser* c.-à-d. les types de fichiers qui seront soumis à l'analyse (archives, etc.).

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



Afin de pouvoir analyser l'ensemble des systèmes de fichiers de l'ordinateur, il faut impérativement revenir au répertoire racine ou indiquer la zone d'analyse dans la ligne de commande à l'aide de `/`.

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.



Si le chemin d'analyse et le fichier texte reprenant les objets à analyser sont tous deux saisis dans la ligne de commande, la zone d'analyse sera celle reprise dans le fichier. Le chemin repris dans la ligne de commande sera ignoré.

- En introduisant dans le fichier de configuration **kav4fs.conf** 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 **kav4fs.conf** (section **[scanner.options]**) et peuvent être redéfinis via :

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

5.2.2. Mode d'analyse et de réparation des objets

La configuration de ce mode une option très importante de l'analyse car elle détermine si les fichiers infectés, découverts lors de l'analyse, seront réparés ou non.

L'option est désactivée par défaut. Autrement dit, seules l'analyse des objets et la notification sur l'écran de la console et dans le rapport (cf. point 6.5, page 49) en cas de découverte de virus ou de fichiers suspects ou corrompus sont prévues.

Au terme de l'analyse antivirus, chaque objet reçoit un des statuts suivants :

- **Clean** : aucun virus n'a été découvert (objet sain).
- **Infected** : l'objet est infecté.
- **Warning** : le code de l'objet ressemble à celui d'un virus connu.
- **Suspicious** : l'objet pourrait être infecté par un virus inconnu.
- **Corrupted** : l'objet est corrompu.
- **Protected** : l'objet ne peut pas être analysé car il est crypté (protégé par un mot de passe).

Lorsque le mode réparation est activé (section **[scanner.options]**, paramètre **Cure=yes**), seuls les objets dont le statut est **Infected** seront soumis au traitement antivirus. Après la réparation, l'objet reçoit un des statuts suivants :

- **Cured** : l'objet a été réparé.

- **CureFailed** : l'objet n'a pas pu être réparé. Le fichier qui reçoit ce statut est traité en fonction des règles définies pour les objets infectés.
- **Error** : une erreur s'est produite lors de l'analyse de l'objet.

5.2.3. Actions à exécuter sur les objets

Les actions exécutées sur les objets dépendent du statut (cf. Chapitre 2, page 14) qui leur a été attribué. Par défaut, le système ne fait que signaler la découverte d'objets d'un statut particulier. Il est toutefois possible de configurer toute une série d'actions pour les objets dont le statut est **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** et **Corrupted**. Par exemple :

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

Il convient de souligner que Kaspersky Anti-Virus opère une distinction entre les objets simples (un fichier) et les objets conteneur (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 déterminer l'action à exécuter sur un objet quelconque à l'aide d'une des méthodes suivantes :

- Les spécifier dans le fichier de configuration **kav4fs.conf** si vous souhaitez les appliquer par défaut (sections **[scanner.object]** et **[scanner.container]**).
- Indiquer l'action dans un fichier de configuration alternatif que vous utiliserez au moment du lancement du composant.



Si au moment du lancement du composant aucun fichier de configuration particulier n'est repris dans la ligne de commande, les paramètres appliqués seront ceux du fichier **kav4fs.conf**. Il n'est pas nécessaire de spécifier l'utilisation de ce fichier lors du lancement du composant.

- Les spécifier lors de la session de travail en cours à l'aide d'un argument de la ligne de commande au moment du lancement du composant **kavscanner**.

Qu'il s'agisse des objets simples ou des objets conteneur, la syntaxe des actions est la même (sections **[scanner.object]** et **[scanner.container]**).

5.2.4. Analyse à la demande d'un répertoire particulier

Une des tâches les plus fréquentes réalisées par Kaspersky Anti-Virus est la recherche de virus dans un répertoire particulier et la réparation des objets infectés.



Tâche: lancer la vérification 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. Créer dans ce même répertoire les fichiers *infected.lst*, *suspicion.lst*, *corrupted.lst* et *warning.lst* qui reprendront chacun respectivement la liste des objets infectés, suspects et endommagés découverts lors de l'analyse.

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 *kav4fs-kavscanner-date_du_jour-pid.log* sauvegardé dans le même répertoire.



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

```
# kav4fs-kavscanner -rlq -pi/tmp/infected.lst
-ps/tmp/suspicion.lst -pc/tmp/corrupted.lst
-pw/tmp/warning.lst -o /tmp/kav4fs-kavscanner-`date
"+%Y-%m-%d-$$"`.log -i3 -ePASBMe -j3 -mCn /tmp
```

5.2.5. Analyse programmée

C'est le programme **cron** qui permet le lancement programmé du programme et des tâches de Kaspersky Anti-Virus.



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



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

1. Créez le fichier de configuration `/etc/kav/scanhome.conf` 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**) à l'aide de la ligne :

```
0 0 * * * /path/to/kav4fs-kavscanner -c  
/etc/kav/scanhome.conf /home
```

5.2.6. Autres possibilités : utilisation de fichiers de script

Kaspersky Anti-Virus vous permet d'utiliser diverses commandes Unix 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.

5.2.6.1. Réparation des objets infectés dans une archive

Kaspersky Anti-Virus peut uniquement découvrir la présence d'objets suspects ou infectés au sein d'archives. Il ne peut pas procéder à leur réparation. Toutefois, la réparation est possible grâce à un fichier de script supplémentaire. Le présent document propose à titre d'exemple la réparation d'archives *tar*, *rar* et *zip* à l'aide du fichier de script *vox.sh*. Ce script est livré avec Kaspersky Anti-Virus.

Le script décompacte l'archive analysée, procède à l'analyse antivirus et au traitement de chaque objet puis recomprime les fichiers analysés. La présence de compacteur est donc indispensable dans le système.



Tâche: analyser à l'aide du script *vox.sh* une archive *tar* ou *zip*.



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

Saisissez dans la ligne de commande :

```
# /opt/kaspersky/kav4fs/share/contrib/vox.sh <chemin
d'accès au fichier archivé>
```

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

Grâce aux outils standards d'Unix, il est possible de configurer les différentes notifications de l'administrateur suite à la découverte, dans les systèmes de fichiers de l'ordinateur, d'objets infectés, suspects ou corrompus.



Tâche: configurer les messages d'alertes envoyés à l'administrateur en cas de découverte d'archives et de fichiers infectés dans les systèmes de fichiers à chaque analyse de l'ordinateur réalisée conformément aux paramètres du fichier de configuration **kav4fs.conf**. Lors de l'analyse, activer le mode de suivi des liens symboliques.



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

Dans le fichier de configuration **kav4fs.conf**, spécifiez les règles de traitement des objets et des conteneurs simples de la manière suivante :

```
[scanner.options]
FollowSymlinks=yes
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is
infected by %VIRUSNAME% |
mail -s kav4fs-kavscanner admin@localhost.ru
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
| mail -s kav4fs-kavscanner -a %LIST%
admin@localhost.ru
```



Avant d'exécuter l'exemple, l'utilisateur doit s'assurer que l'utilitaire **mail** est bien à son emplacement d'installation standard dans le système d'exploitation.

5.3. Protection antivirus en temps réel

La protection antivirus en temps réel du système de fichier de l'ordinateur est prise en charge par le composant *kavmonitor*.



Tous les paramètres du composant *kavmonitor* sont repris dans la section **[monitor.*]** du fichier de configuration.

Le composant *kavmonitor* est configuré de telle manière qu'à chaque tentative d'accès aux fichiers (ouverture, fermeture ou lancement), le composant *kavmonitor* réalise une analyse antivirus (en cas de fermeture de fichier, le composant vérifie seulement si le fichier a été modifié). Par défaut, tous les objets auxquels l'utilisateur adresse une requête sont soumis à la recherche de virus et de codes malveillants. Il s'agit notamment des :

- Fichiers compressés;
- Archives ;
- Archives auto-extractibles ;
- Bases de données de messagerie électronique ;
- Messages électroniques.

Sur la base des résultats de l'analyse, l'objet est soumis au traitement antivirus en fonction des paramètres du fichier de configuration de l'application.



Le mode de réparation des objets infectés découverts est désactivé par défaut ! Pour activer cette option, il faut attribuer la valeur **Yes** au paramètre **Cure** dans la section **[monitor.options]**.

Pour les objets dont le statut est **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** ou **CureFailed**, il est possible de configurer des actions complémentaires telles que :

- *transfert dans un répertoire quelconque* : les objets dont le statut correspond à un statut défini sont déplacés dans un autre répertoire. Vous avez le choix entre transfert *simple* et transfert *récuratif* (avec restauration du chemin complet) ;
- *Suppression* de l'objet du système de fichiers ;

Il est possible de configurer les règles de traitement des objets dans le fichier de configuration de l'application (section **[monitor. actions]**).

Une configuration complémentaire est également envisageable :

- A l'aide des paramètres **ExcludeDirs** et **ExcludeMask** , indiquez les répertoires qui seront exclus de l'analyse.
- Utilisation de la technologie de l'analyseur heuristique de code et iChecker.
- Réduction de la charge sur le serveur en précisant le nombre maximum d'objets pouvant être analysés simultanément.

5.4. Gestion des clés de licence

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/24 ;
- Mise à jour des bases antivirus toutes les heures ;
- Mise à jour du logiciel (patch) ;
- 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 fichiers. 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 des bases antivirus ne sera plus accessible.

Il est dès lors très important de consulter régulièrement le rapport qui contient les informations relatives à la clé de licence et de prêter une attention toute particulière à sa date d'expiration.

5.4.1. 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*, *kavmonitor* et *keepup2date*

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 de recevoir des renseignements d'ordre analytique.

Toutes les informations peuvent être affichées à l'écran.



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

Saisissez dans la ligne de commande :

```
kav4fs-licensemanager -s
```

Des informations semblables à ceci seront affichées :

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2007.
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
License file 0003E3E8.key, serial 011E-000413-
0003E3E8, "Kaspersky Anti-Virus for Linux File Srv
(licence per e-mail address)", expires 25-01-2004 in
234 days
```



Pour consulter les informations relatives à une clé en particulier :

Saisissez la commande suivante :

```
kav4fs-licensemanager -k 0003D3EA.key
```

Des informations de ce genre s'afficheront :

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2007.
Portions Copyright (C) Lan Crypto
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus
for Linux", expires 04-07-2003 in 28 days
```

5.4.2. 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 5.4 de la page 40 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**.

Il faudra ensuite activer la licence acquise de cette manière.



Pour installer la nouvelle clé de licence :

Saisissez dans la ligne de commande :

```
kav4fs-licensemanager -a <nom du fichier de clé>
```

Après cela, il est recommandé de mettre à jour les bases antivirus (cf. point 5.1, page 26).



Afin de supprimer la clé de licence :

Saisissez dans la ligne de commande :

```
kav4fs-licensemanager -d <nom du fichier de clé>
```

CHAPITRE 6. CONFIGURATION COMPLEMENTAIRE

Ce chapitre aborde les possibilités de configuration complémentaire de Kaspersky Anti-Virus. Les fonctionnalités de l'application sont ainsi élargies et ce dernier peut être plus facilement intégré au cadre opérationnel concret d'une entreprise.

6.1. Optimisation du fonctionnement de Kaspersky Anti-Virus

Afin de réduire la charge sur le processeur et d'accélérer le traitement antivirus, Kaspersky Anti-Virus propose des outils efficaces d'optimisation. Les voici présentés en détail.



Utilisation des bases de données iChecker et recours à technologie de mise en cache à deux niveaux des fichiers analysés.

Cette application exploite diverses technologies qui permettent de ne pas devoir procéder à une vérification 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 de vérification antivirus de l'objet (fichier) fonctionne de la manière suivante :

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

- La base de données iChecker est une base générale qui contient les informations relatives aux fichiers vérifiés et **sains** de certains formats. Cette base contient les informations relatives aux objets analysés par les composants *kavmonitor* et *kavscanner*.
- Le cache des fichiers vérifiés est une base de données qui contient les informations relatives aux fichiers analysés par *kavmonitor*. Le cache est constitué de deux niveaux : le premier niveau contient les informations relatives aux **fichiers sains** qui font l'objet des requêtes les plus fréquentes. Le cache de premier niveau se trouve dans le module du moteur, ce qui permet de réduire sensiblement la durée de la consultation. Si l'application découvre dans le cache de premier niveau

des données relatives au fichier faisant l'objet de la requête, elle lui attribue automatiquement le statut **clean** et ce fichier ne sera pas soumis à une analyse antivirus plus approfondie. Si ce premier niveau ne contient pas les informations requises, l'application va chercher dans le deuxième niveau qui contient les données relatives à **tous les fichiers analysés**. Les deux bases du cache sont dans la mémoire vive et elles ne sont pas conservées une fois que l'application est arrêtée.

Ainsi, lorsque l'information récoltée sur un fichier lors de la vérification 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.

Pour chaque requête ultérieure adressée par l'utilisateur au fichier, le système recherche dans le cache de premier niveau puis, si l'objet n'est pas présent dans la première base, dans la base iChecker et dans le cache de deuxième niveau. 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.



Restriction de la charge sur le processeur.

L'analyse des systèmes de fichiers peut prendre un certain temps, surtout si le volume de données est important. Dans ce genre de situation, la charge sur le processeur augmente considérablement. Le processeur doit continuer à réaliser les tâches en cours et il est souhaitable de disposer d'un mécanisme qui serait capable de suspendre l'analyse antivirus de l'ordinateur lorsque la charge dépasse un seuil défini.

Kaspersky Anti-Virus propose un tel mécanisme. Le fichier de configuration de la version 5.5 contient le paramètre **MaxLoadAvg** dans la section **[scanner.options]**. Lorsque ce paramètre est défini, *kavscanner* estime, au moment d'analyser chaque nouveau fichier, la charge du serveur **load average** et si la valeur indiquée dans le fichier de configuration est dépassée, *kavscanner* interrompt son fonctionnement jusqu'à ce que la valeur du paramètre **load average** repasse en-dessous du niveau indiqué.

De plus, il est possible de limiter également le nombre d'objets soumis simultanément à l'analyse en temps réel grâce au paramètre **CheckFileLimit** de la section **[monitor.options]** du fichier de configuration de l'application. Cela permet également de réduire la charge sur le processeur et d'accélérer l'analyse d'objets distincts.

6.2. Transfert d'objets dans le répertoire de quarantaine

Kaspersky Anti-Virus peut être configuré de telle sorte que tous les objets infectés soient transférés dans un répertoire particulier.

Un tel comportement peut être utilisé par exemple *si la réparation de l'objet a échoué* (par exemple, seuls 2 des trois virus détectés ont pu être supprimés) mais que le fichier renferme des informations cruciales.

Au cas où ce répertoire de quarantaine devrait figurer dans la structure du système de fichiers du serveur, il est préférable de ne pas l'inclure dans les analyses ultérieures. Pour ce faire, il faudra associer son chemin d'accès complet au paramètre **ExcludeDirs** de la section **[scanner.options]** du fichier de configuration.

Voici les tâches liées à l'isolement des objets infectés découverts lors de l'analyse à la demande du système de fichiers de l'ordinateur et dans le cadre de la protection en temps réel.



Tâche: rechercher la présence éventuelle de virus dans tous les objets repris dans le fichier */tmp/download.lst* et transférer les fichiers infectés, avec leur chemin d'accès complet, dans le répertoire */tmp/infected*. Consigner les informations relatives aux objets infectés, ainsi qu'aux objets suspects ou corrompus dans le fichier du rapport.



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

1. Ajoutez la ligne suivante en guise d'action à exécuter sur les objets infectés dans les sections **[scanner.object]** et **[scanner.container]** du fichier de configuration :

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

2. Le cas échéant, désactivez le mode de réparation (**Cure=no**).
3. Saisissez dans la ligne de commande :

```
# kav4fs-kavscanner -@/tmp/download.lst -ePASBME
-rq
-i0 -o /tmp/report.log -j3 -mCn
```

Compliquons légèrement la tâche en modifiant les droits d'accès aux fichiers du répertoire `/tmp/infected` et en autorisant uniquement la lecture et l'écriture. Pour ce faire, utilisez les outils Unix traditionnels (la commande **chmod**). Il faut donc apporter les modifications suivantes aux tâches à exécuter :

Dans les sections **[scanner.object]** et **[scanner.container]** du fichier de configuration de l'application, saisissez la ligne suivante en guise de règle de traitement des objets infectés :

```
OnInfected=exec mv %FULLPATH%/%FILENAME%
/tmp/infected/%FILENAME%; chmod -x
/tmp/infected/%FILENAME%
```



Tâche: rechercher la présence éventuelle de virus dans tous les fichiers faisant l'objet d'une requête et si le fichier est infecté, le réparer. 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 (**Cure=yes** de la section **[monitor.options]**).
2. Définissez la règle d'isolement des objets infectés. Pour ce faire, saisissez la ligne suivante dans la section **[monitor.actions]** du fichier de configuration :

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

6.3. Mode de copie de sauvegarde des objets (backup)

Si l'objet analysé est infecté et que l'action sélectionnée est la suppression dans 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 un répertoire de sauvegarde (backup).

Avant la réparation ou la suppression d'un objet, une copie de celui-ci est créée automatiquement dans le dossier de sauvegarde (section **[monitor.path]**, paramètre **BackupPath**). Vous disposerez ainsi d'une copie de sauvegarde (et la possibilité de restaurer le fichier d'origine) au cas où l'objet serait corrompu lors de la réparation. L'objet est enregistré dans le dossier de sauvegarde avec son chemin d'accès complet. Lorsqu'un objet 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 dossier où seront conservées les copies de sauvegarde n'est pas défini.

Pour activer le mode, définissez le chemin d'accès au répertoire de conservation des copies de sauvegarde des objets.



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



Les actions définies dans le fichier de configuration pour les objets infectés ne sont pas appliquées aux fichiers du dossier de sauvegarde !

6.4. 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.

%d/%m/%y – format d'affichage de la date.

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. Vous pouvez spécifier par exemple les formats suivants :

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

`%y!%m!%d` et `%m!%d!%y` : pour représenter la date (paramètre **DateFormat**) au format année/mois/jour et mois/jour/année respectivement.

6.5. 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 de l'ordinateur apparaissent également sur la console. Par défaut, les informations contenues dans le rapport ou affichées à l'écran sont identiques.

Pour consigner les informations relatives au fonctionnement de l'application dans le journal système, attribuez au paramètre **ReportFileName** des sections **[monitor.report]**, **[scanner.report]**, et **[updater.report]** la valeur **syslog**.

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
	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.

Niveaux	Nom du niveau	Signification
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.
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.

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. SUPPRESSION DE KASPERSKY ANTI-VIRUS

La procédure de suppression de Kaspersky Anti-Virus requiert :

- Les privilèges d'utilisateur **root**. Si vous ne disposez pas de ces privilèges au moment de la désinstallation, vous devrez absolument ouvrir une session tant que **root**.
- Le fichier du rapport d'installation.
- L'équivalence parfaite entre les noms et la taille des fichiers installés par Kaspersky Anti-Virus et ceux repris dans le fichier du rapport d'installation.

Avant d'entamer la procédure de désinstallation, il faudra également arrêter le composant **kavmonitor**.



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

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



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

```
pkg_delete <nom_du_paquetage>
```

La procédure de désinstallation sera exécutée automatiquement. Le message de circonstance apparaîtra sur la console une fois que la désinstallation sera terminée.

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 le bon fonctionnement de l'application 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  (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 dans le tableau ci-dessous.

Tableau. Modifications du « virus » d'essai

Préfixe	Type d'objet
Pas de préfixe, « virus » d'essai standard	Infecté. L'objet ne sera pas réparé.
CORR-	Corrompu.
SUSP-	Suspect (code d'un virus inconnu).
WARN-	Suspect (code modifié d'un virus connu).
ERRO-	Non- analysé suite à un échec.
CURE-	Réparé. L'objet sera réparé et le texte du corps du « virus » sera remplacé par CURE.
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-X50!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.

ANNEXE A. RENSEIGNEMENTS COMPLEMENTAIRES SUR L'APPLICATION

Cet appendice 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 **kav4fs.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 **[monitor.options]** contient les paramètres d'analyse en temps réel :

ExcludeDirs=masque1:masque2:...:masqueN : masques des répertoires qui seront exclus de l'analyse. Par défaut, tous les répertoires sont analysés. Les masques sont définis comme des masques shell standard.

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

IncludeDirs=masque1:masque2:...:masqueN : masque des répertoires qui seront analysés. Les masques sont définis comme des masques shell standard.

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 : taille du cache de fichiers (en Mo).

KereneICacheSize : taille du cache où se trouve le moteur antivirus (en Mo).

CheckFileLimit=20 : maximum d'objets analysés simultanément.

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

UseAVbasesSet=standard|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 **[monitor.path]** regroupe les paramètres qui définissent le chemin d'accès aux fichiers importants sans lesquels le module kavmonitor ne pourra fonctionner :

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

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

La section **[monitor.actions]** regroupe les paramètres qui définissent les actions à exécuter sur les objets d'un certain type en mode de protection en temps réel :

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 section **[monitor.report]** regroupe les paramètres de composition du rapport d'activité de kavmonitor :

ReportLevel=4 : niveau de détails du rapport.

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

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 :

Archives=yes : mode d'analyse des archives. 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.

ExcludeDirs=masque1:masque2:...:masqueN : masques des répertoires qui seront exclus de l'analyse. Par défaut, tous les répertoires sont analysés. Les masques sont définis comme des masques shell standard.

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

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

LocalFS=no : mode d'analyse du système de fichiers local uniquement. Afin d'activer ce mode, attribuez la valeur **yes** à ce paramètre.

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.

Packed=yes : mode d'analyse des fichiers compactés. 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.

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**.

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.

UseAVbasesSet=standard|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 ce paramètre a la valeur **yes**, les liens indiquant des répertoires seront suivis.

MaxLoadAvg : charge maximale du processeur.

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

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.

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 **[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 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 du paramètre **action** comprend deux parties : l'action elle-même et son paramètre complémentaire, séparé 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.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.

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

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.

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

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

La section **[scanner.display]** regroupe les paramètres d'affichage du rapport sur la console :

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

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

ShowOK=yes : mode d'affichage sur la console des notifications relatives aux fichiers sains. Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

ShowProgress=yes : mode de représentation sur la console de l'exécution des tâches en cours (chargement des bases antivirus, informations relatives à l'analyse en cours d'un fichier). Afin de désactiver ce mode, attribuez la valeur **no** à ce paramètre.

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

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

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.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.

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

KeepSilent=no : mode d'affichage sur la console des informations relatives aux activités du composant *keepup2date*. Afin de désactiver ce mode, attribuez la valeur **yes** à ce paramètre.

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**.

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.

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.

UpdateServerUrl=no http://url/ | ftp://url/ | /local_path/ : adresse pour la mise à jour des bases antivirus.

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 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.

PassiveFtp=no : mode d'utilisation de la connexion FTP en mode passif.

A.2. 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;
- 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 réursive;
- 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;

-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> Conserve la liste des objets dans le fichier spécifié ;chaque
<nom_du_fichi objet est conservé sur une nouvelle ligne avec son chemin

- er>** 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.3. 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.4. Arguments de la ligne de commande pour le composant **kavmonitor**

Options d'aide :

- h** Affiche sur la console l'aide relative au composant;
- v** Affiche la version du programme.

Options de configuration :

- c** Utilise le fichier de configuration alternatif `<chemin_du_fichier>`.

A.5. 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)** Utilise le fichier de configuration alternatif `<chemin_du_fichier>` `<chemin_du_fichier_de_clé>`;
- k** Affiche sur la console les informations relatives à la clé

<chemin_du_fichier> <chemin_du_fichier_de_clé>;

-a Installe la clé de licence <chemin_du_fichier_de_clé>;
<chemin_du_fichier>

-d Supprime la clé de licence.
<chemin_du_fichier>

A.6. 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.7. 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;
Options de fonctionnement :	
-r	Remise des bases antivirus à l'état antérieur à la mise à jour;
-s	Affiche sur la console la liste des serveurs de 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 application 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.8. 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. QUESTIONS FREQUEMMENT POSEES

Ce chapitre est consacré aux questions les plus fréquentes des 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 procédera 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 avec les sommes de contrôle des objets.



Question : Pourquoi Kaspersky Anti-Virus entraîne-t-il une baisse des performances de mon ordinateur et surcharge-t-il le processeur ?

La détection des virus est 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 Kaspersky Anti-Virus est le processeur. De plus, chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse.

A la différence des autres logiciels antivirus qui réduisent la durée de l'analyse en ignorant les virus les plus difficiles à déceler ou les plus rare (dans la zone géographique où l'éditeur est présent) ou en ignorant les formats plus complexe (par exemple, les pdf), Kaspersky Lab estime

que la tâche d'un antivirus est de garantir la véritable protection antivirus des utilisateurs.

Kaspersky Anti-Virus permet à l'utilisateur expérimenté d'accélérer l'analyse antivirus en excluant divers type de fichiers de l'analyse. Il convient de remarquer toutefois que cela s'accompagne d'une diminution du niveau de protection.

Kaspersky Anti-Virus est capable d'analyser plus de 700 formats de fichiers archivés ou compressés. 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™.



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.

Lorsque cette situation se présente, vous devez contacter votre administrateur de système et contactez la société où vous avez acheté Kaspersky® Anti-Virus ou Kaspersky Lab directement.



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 à votre problème n'est pas décrite dans les pages de ce manuel, et plus particulièrement dans cette rubrique. Consultez également notre site Internet.

Nous vous conseillons également de contacter le magasin où vous avez acheté Kaspersky Anti-Virus ou de consulter la banque de solutions sur le site de Kaspersky Lab (<http://kb.kaspersky.fr>).



Question : à quoi servent les mises à jour quotidiennes ?

Il y a encore quelques années, les virus étaient transmis via disquette et afin de protéger l'ordinateur, il suffisait d'installer un logiciel antivirus et de procéder de temps à autre à la mise à jour des bases antivirus. Les épidémies les plus récentes se sont répandues à travers le monde

entier en quelques heures uniquement et dans ces conditions, un logiciel antivirus équipé d'anciennes bases antivirus est impuissant face aux nouvelles menaces. Afin de ne pas devenir victime de la prochaine épidémie de virus, il est indispensable de mettre à jour les bases antivirus quotidiennement.

Chaque année, Kaspersky Lab augmente la fréquence de mise à jour des bases antivirus. Actuellement, les mises à jour sont diffusées toutes les trois heures.

La mise à jour des modules de l'application est une fonction supplémentaire. Ces mises à jour corrigent les défauts et apportent de nouvelles possibilités.



Question : *qu'est-ce qui a changé dans le service de mise à jour depuis la version 5.0 ?*

La gamme de produits, depuis la version 5.0, offerts par Kaspersky Lab présente un nouveau service de mise à jour. Le développement de cette nouvelle fonction s'est fondé sur les remarques des utilisateurs et sur les impératifs du marketing. De plus, il fallait renforcer le degré technologique de l'ensemble de la procédure de mise à jour, depuis la préparation chez Kaspersky Lab jusque l'actualisation des fichiers chez l'utilisateur.

Voici les avantages du nouveau système de mise à jour :

- Reprise du téléchargement des fichiers en cas de déconnexion : *désormais, il n'est plus nécessaire de télécharger à nouveau les données obtenues avant la déconnexion.*
- Réduction de moitié de la taille de la mise à jour cumulée. La mise à jour cumulée contient toute la base antivirus, ce qui explique pourquoi la taille de la mise à jour cumulée est de loin supérieure à la taille de la mise à jour traditionnelle. Le nouveau service introduit une nouvelle technologie qui permet d'utiliser les bases antivirus qui existent déjà pour la mise à jour cumulée.
- Accélération du téléchargement depuis Internet. Kaspersky Anti-Virus sélectionne le serveur de mise à jour situé dans votre région. De plus, la charge du serveur est répartie en fonction de

ses performances. Autrement dit, vous ne serez pas connecté à un serveur surchargé pendant qu'un autre n'est pas sollicité.

- Application des « listes noires » des clés. Ceci permet d'exclure des mises à jour les utilisateurs qui ne disposent pas de la licence d'utilisation de Kaspersky Anti-Virus. Ainsi, les utilisateurs qui possèdent une licence ne sont pas pénalisés à cause de serveurs surchargés.
- Les logiciels destinés aux entreprises autorisent la création d'un répertoire local pour la mise à jour des bases antivirus. Cette fonction est prévue pour les entreprises où les ordinateurs, protégés par les applications de Kaspersky Lab, sont regroupés au sein d'un réseau. N'importe quel ordinateur peut jouer le rôle de serveur de mise à jour. C'est lui qui recevra les mises à jour depuis Internet. Elles seront enregistrées dans un répertoire local accessible aux autres ordinateurs du réseau.



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

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 : Kaspersky Anti-Virus 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.

Pour connaître la liste des systèmes d'exploitation pris en charge, consultez le point 1.5 à la page 10.

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 : pourquoi le composant *kavmonitor* lance-t-il simultanément plusieurs processus ?

Le nombre de processus de *kavmonitor* lancés est défini par le paramètre **CheckFileLimit** du fichier de configuration de l'application et il détermine le nombre de fichiers qui peuvent être traités simultanément. Pour cette raison, le nombre de processus de *kavmonitor* est toujours égal au nombre de fichiers + 1 (par défaut, 20 processus sont lancés). S'il n'y a pas de fichiers à analyser, les processus ne gaspillent pas les ressources du système.



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 Linux and FreeBSD Workstation and File Server. 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 ?

Pour enregistrer les informations affichées sur la console lors du fonctionnement de Kaspersky Anti-Virus, il faut saisir la ligne appropriée dans le fichier de configuration ou saisir la commande suivante :

```
$ 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 :

```
$kav4fs-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 C. 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 automatisation 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.

C.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'existence 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 après 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 antivirale¹ 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 gmail ;

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 logiciel 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.

C.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE D. 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.